Gestão de segurança do Xanadu

Última atualização: 18/11/2024

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

servicenow

A tradução automática pode proporcionar uma ideia básica do conteúdo em um idioma que você entende. Ela é totalmente automatizada e não envolve intervenção humana. A qualidade e a precisão da tradução automática podem variar significativamente de um texto para outro e entre diferentes pares de idiomas. A ServiceNow não garante a precisão e não se responsabiliza por possíveis erros. Alguns conteúdos (como imagens, vídeos, arquivos etc.) podem não ser traduzidos devido a limitações técnicas do sistema.

Alguns exemplos e gráficos aqui representados são fornecidos somente para fins de ilustração.
Nenhuma associação ou conexão real com produtos ou serviços ServiceNow é intencional ou deve ser inferida.

ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas e de produtos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Leia os Termos de Uso do Site do ServiceNow em www.servicenow.com/terms-of-use.html

Tradução automática

Sede da empresa
2225 Lawson Lane
Santa Clara, CA 95054
Estados Unidos
(408) 501-8550

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Índice

Operações de segurança 5
Exploração do Operações de segurança 7
Now Assist para Operações de segurança 13
Exploração do Now Assist para Operações de segurança 15
Configuração da Now Assist para Operações de segurança 17
Usando Now Assist para Operações de segurança para resolver incidentes de segurança 23
Aplicações da superfície de ataque 28
Resposta a vulnerabilidades 30
Resposta a vulnerabilidades de aplicações 796
Contêiner de Resposta a vulnerabilidades 1001
Conformidade de configurações 1072
Base para resposta a vulnerabilidades 1340
Resposta a vulnerabilidades Espaços 1347
Lista de materiais de software 1509
Aplicações de gestão de casos de segurança empresarial 1538
Security Incident Response 1540
Inteligência contra ameaças 3038
Controle de posturas de segurança 3295
Exploração do Controle de posturas de segurança 3297
Usando o espaço Controle de posturas de segurança 3307
Casos de uso, exemplos de política e conectores do Service Graph compatíveis no Controle de posturas de segurança 3324
Painel executivo de cibersegurança 3338
Aceitar pontuações de parâmetro de comparação 3358
Definir metas 3358
Simulação de segurança e integração de treinamento para Operações de segurança 3359
Painel de risco e conformidade para GRC: Metrics 3361
Central de segurança de inteligência contra ameaças 3372
Explorar Central de segurança de inteligência contra ameaças 3373
Separação de domínios e Central de segurança de inteligência contra ameaças 3376
Configurar Central de segurança de inteligência contra ameaças 3377
Exibir página inicial da Central de segurança de inteligência contra ameaças 3379
Integração da Central de segurança de inteligência contra ameaças 3382
Administração 3440
Como trabalhar com importações de dados 3482
Importar inteligência contra ameaças 3484
Workbench do analista de ameaça 3493

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Central de segurança de inteligência contra ameaças Biblioteca....3507
MITRE-ATT&CK™ Repositório....3641
Gestão e retenção de dados....3649
Fluxo funcional de processamento de dados de TISC....3658
Data Loss Prevention Incident Response....3660
Exploração do Data Loss Prevention Incident Response....3661
Instalando e configurando DLP IR Incident Response....3664
Administração de resposta a incidentes da DLP....3665
Data Loss Prevention Incident Response Gestão de incidentes....3719
Integração de entrada para Data Loss Prevention Incident Response....3737
Integrações da DLP....3740
Operações de segurança funcionalidade comum....3791
Criar e definir grupos de filtros nas Operações de segurança....3793
Transformação de dados compartilhados....3795
Operações de segurança processamento de e-mail....3799
Operações de segurança mapeamento de campo....3810
Operações de segurança transformações de valor de campo....3814
Operações de segurança mapeamento de dados de aprimoramento....3816
Operações de segurança escalação definida pelo usuário....3819
Criar substituições de propriedade separadas por domínio....3820
Criar um grupo de sistemas operacionais....3821
Configurar grupos de marcadores de segurança e marcadores....3823
Anotações de segurança....3827
Componentes instalados com Security Support Common....3829
Pesquisar Operações de segurança....3830
Referência do Security Operations Integrations....3830
Operações de segurança gatilhos de fluxo de trabalho....3944
Orquestração do Security Operations....3946

Tradução automática

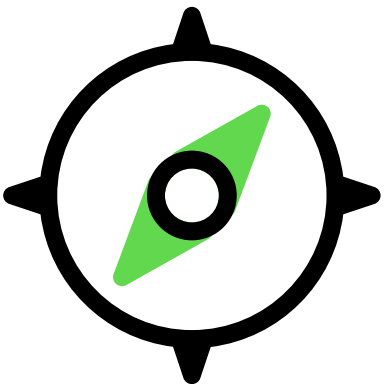
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança

ServiceNow® Operações de segurança As aplicações importam dados de incidentes de suas ferramentas de segurança para um mecanismo de resposta estruturado que usa fluxos de trabalho inteligentes, automação, visualizações de dados e uma conexão profunda com a TI para priorizar e resolver ameaças com base no impacto que elas representam para sua organização.

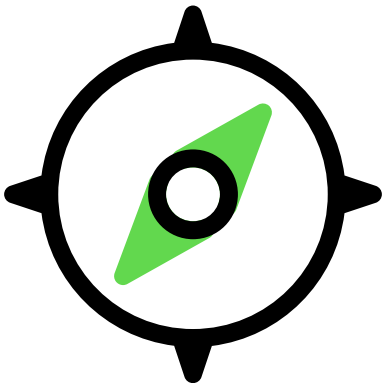
Escolha um desses blocos para começar.

Explorar as aplicações Operações de segurança e seus espaços



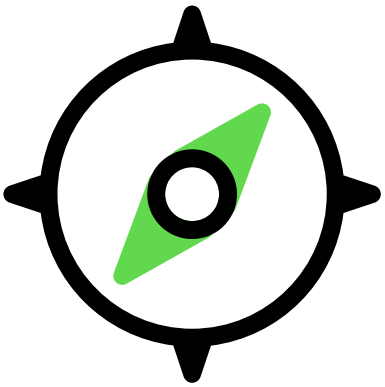
Saiba como as aplicações Operações de segurança podem ajudá-lo a melhorar sua postura de segurança.

Explorar o Now Assist para Operações de segurança



Saiba como o Now Assist para Operações de segurança é compatível com ServiceNow® habilidades de IA generativa (IA generativa) no Espaço de resposta a incidentes de segurança e na IU principal (UI16).

Explore as aplicações da superfície de ataque

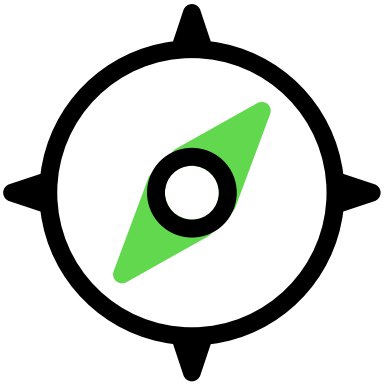


Saiba mais sobre as aplicações na Resposta a vulnerabilidades que ajudam a identificar e corrigir vulnerabilidades em sua superfície de ataque cibernético.

Tradução automática

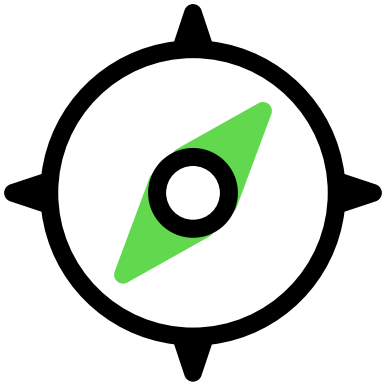
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar aplicações de gestão de casos de segurança empresarial



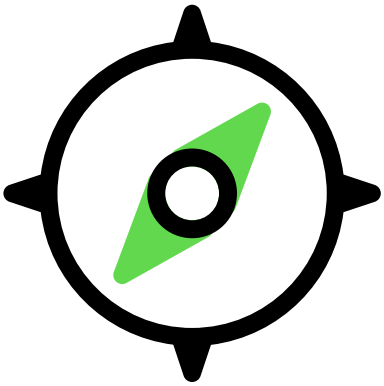
Saiba mais sobre as aplicações no Security Incident Response que ajudam a analisar, isolar e corrigir incidentes de segurança críticos à medida que eles evoluem.

Explore as aplicações de controle de posturas de segurança



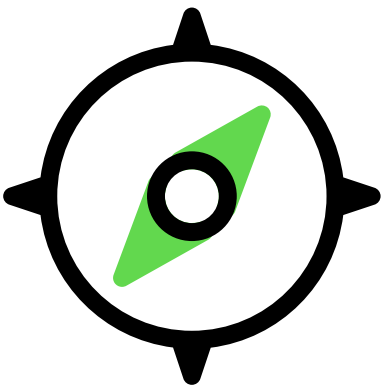
Saiba mais sobre as aplicações que ajudam você a obter informações sobre sua postura geral de segurança.

Explore o Painel executivo de segurança cibernética



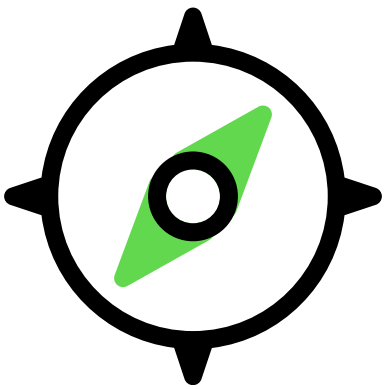
Saiba como o Painel executivo de segurança cibernética consolida dados de vários produtos SecOps em um painel unificado.

Explore a Central de segurança de inteligência contra ameaças



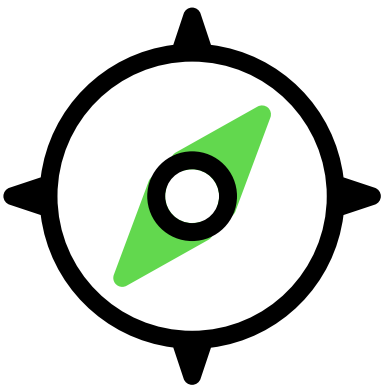
Saiba como a plataforma Central de segurança de inteligência contra ameaças (TISC) fornece soluções de tecnologia para agregação e gestão de inteligência contra ameaças.

Explorar Data Loss Prevention Incident Response



Saiba como você pode gerenciar informações confidenciais para seus clientes e identificar e proteger seus canais de perda de dados.

Explorar aplicações compartilhadas das Operações de segurança

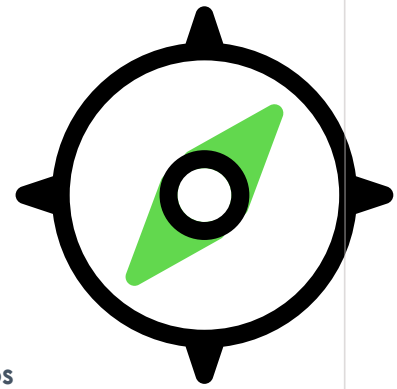


Saiba mais sobre os recursos e módulos que fornecem funcionalidade comum em Operações de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar cenários e exemplos



Saiba mais sobre como obter Operações de segurança aplicações do ServiceNow® Store e cenários para aplicações que você pode empregar ao usar os produtos.

Solucionar problemas e obter ajuda

- Comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Exploração do Operações de segurança

Proteja seus ativos e o ambiente empresarial com as aplicações da ServiceNow Operações de segurança e o poder do Now Platform®. Conecte suas equipes de segurança e TI para ajudá-lo a priorizar e resolver ameaças com base no impacto que elas representam para sua organização.

Visão geral Operações de segurança

O pacote Operações de segurança de aplicações ajuda a proteger seus ativos, melhorando sua postura geral de segurança. Por exemplo, ao integrar aplicações como Security Incident Response, Resposta a vulnerabilidadese Controle de posturas de segurança com as ferramentas de segurança existentes, os analistas, gerentes e equipes de TI do Centro de Operações de Segurança (SOC) podem:

- Responda às ameaças cibernéticas e de segurança em rápida evolução
- Identificar, priorizar e corrigir vulnerabilidades
- Exibir seu inventário de ativos completo
- Determinar a cobertura geral da ferramenta de segurança
- Resolva incidentes de segurança mais rapidamente com fluxos de trabalho inteligentes e ServiceNow habilidades de IA generativa (IA generativa). Para obter mais informações, consulte Now Assist para Operações de segurança.

Tradução automática

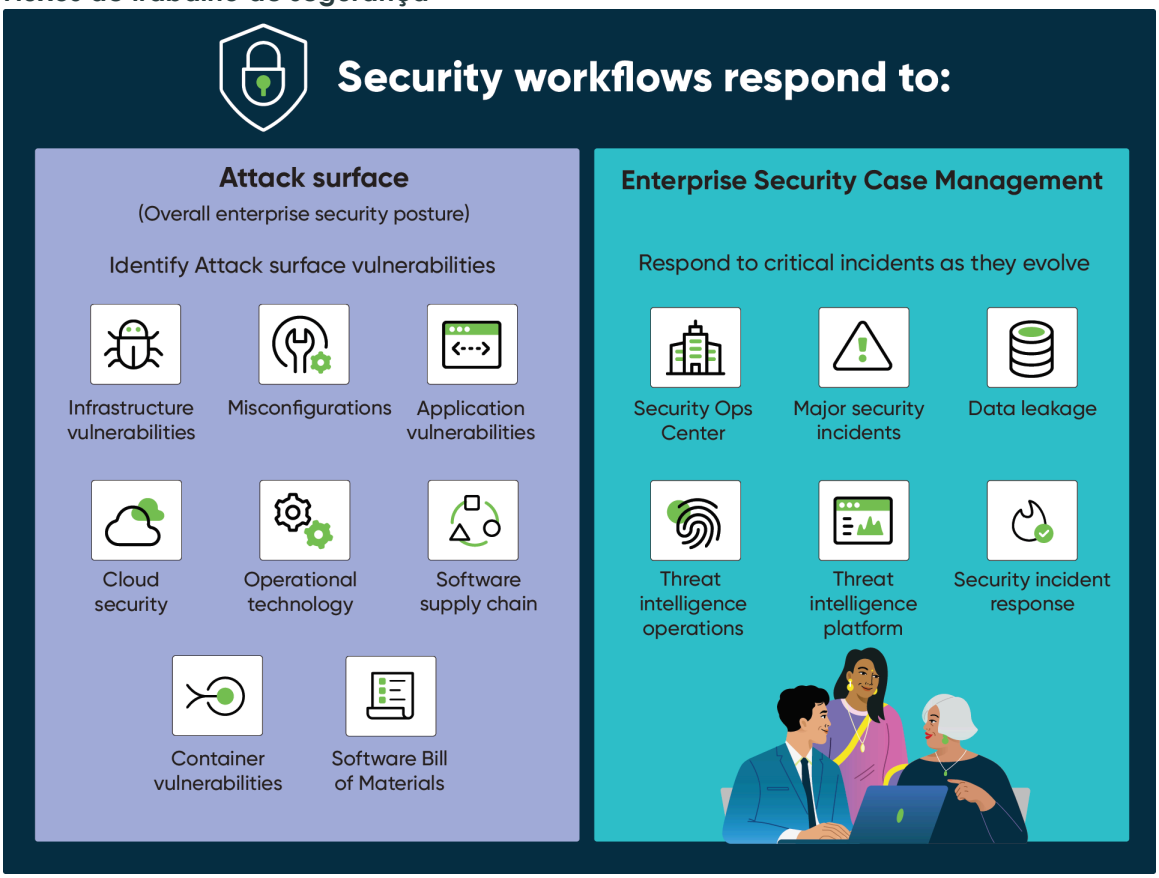
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança aplicações para fluxos de trabalho

As aplicações Operações de segurança se enquadram em duas categorias amplas para fluxos de trabalho Operações de segurança :

- Superfície de ataque — Aplicações e ferramentas que ajudam a antecipar, entender e fechar suas vulnerabilidades.
- Gestão de casos de segurança empresarial - Aplicações e ferramentas que ajudam você a agir rapidamente para responder a incidentes críticos.

Fluxos de trabalho de segurança



As duas categorias de aplicações Operações de segurança e os casos de uso que elas ajudam a resolver em seu ambiente empresarial.

Benefícios das aplicações Operações de segurança

Exiba Operações de segurança aplicações e dados com interfaces de usuário de última geração (espaços). Com os espaços, os analistas de segurança, gerentes do Centro de operações de segurança (SOC) e especialistas em correção da sua organização podem monitorar e gerenciar os seguintes tipos de fluxos de trabalho em um único local:

- O ciclo de vida dos incidentes de segurança, desde uma análise inicial até a contenção, erradicação e recuperação.
- As vulnerabilidades mais importantes para eles, para que possam decidir estrategicamente quais vulnerabilidades enviar para as equipes de TI corrigirem.
- Informações importantes e casos de uso importantes para cobertura da ferramenta de segurança e higiene de ativos que relatam e monitoram informações importadas sobre seus ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações da superfície de ataque

Aplicações que ajudam a antecipar ameaças e identificar vulnerabilidades

Aplicação	Descrição	Usuários
Controle de posturas de segurança	Obtenha informações sobre como as ferramentas de segurança estão implantadas e cobrem seus ativos com base em um inventário de ativos e dados importados. Os conectores do Service Graph e os produtos da ServiceNow, como HAM (Hardware Asset Management, Gestão de ativos de hardware - HAM) e Descoberta do ITOM, são compatíveis com importações de dados. As auditorias baseadas em políticas ajudam a priorizar a correção de combinações de alto risco, como exposição na Internet e vulnerabilidades conhecidas. Crie políticas e informações personalizadas para monitorar a conformidade dos ativos com os padrões de configuração da ferramenta de segurança interna.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Engenheiro de operações de TI • Proprietário do serviço (persona do responsável pela correção)
Resposta a vulnerabilidades	Verificadores de vulnerabilidade e ferramentas de avaliação de terceiros ajudam a identificar os riscos que as vulnerabilidades representam para os seguintes tipos de ativos: • Infraestrutura (host) • Contêiner • Aplicações • Lista de materiais de software As vulnerabilidades identificadas por essas ferramentas são convertidas	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Engenheiro de operações de TI • Proprietário do serviço (persona do responsável pela correção)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações que ajudam a antecipar ameaças e identificar vulnerabilidades

Aplicação	Descrição	Usuários
	em riscos para as equipes de segurança e de TI responsáveis por manter e proteger os ativos de uma organização.	
Conformidade de configurações	Verifique sua conformidade com as políticas corporativas ou de segurança. Identifique, priorize e corrija itens de configuração fora de conformidade com resultados de testes obtidos de integrações de avaliação de configuração segura (SCA) de terceiros.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Engenheiro de operações de TI • Proprietário do serviço (persona do responsável pela correção)

Aplicações de gestão de casos de segurança empresarial

Aplicações que ajudam você a responder a violações e incidentes críticos de segurança

Aplicação	Descrição	Usuários
Security Incident Response	Simplifique o processo de identificação de incidentes críticos aplicando poderosas ferramentas de fluxo de trabalho e automação que aceleram a correção. Integre suas ferramentas existentes do Gerenciador de informações e eventos de segurança (SIEM) com as aplicações Security Incident Response e Operações de segurança para importar dados de ameaças de várias origens e criar automaticamente incidentes de segurança priorizados.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Analista de inteligência contra ameaças
Gestão de incidentes graves de segurança	As capacidades de gestão de incidentes de segurança graves funcionam com as capacidades de produto de resposta a incidentes de segurança existentes.	• CISO • Analista de segurança da informação • Gerente de operações de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações que ajudam você a responder a violações e incidentes críticos de segurança

Aplicação	Descrição	Usuários
	Isso inclui a capacidade de um analista de segurança escalar um incidente de segurança padrão para um incidente de segurança grave, para que os novos recursos do produto estejam disponíveis para oferecer suporte ao processo de correção. Acompanhe o andamento do incidente de segurança grave (MSI) desde a descoberta até a análise. Propor soluções, promover e vincular incidentes de segurança e fechamento.	• Engenheiro de operações de TI • Proprietário do serviço (persona do responsável pela correção) • Conselho geral
Data Loss Prevention Incident Response	O Data Loss Prevention Incident Response (DLP IR) permite que você revise e gerencie o fluxo de trabalho de correção de incidentes do DLP de várias origens, como endpoint, rede, e-mail e nuvem.	• CISO • Analista de segurança da informação • Gerente de operações de segurança
Inteligência contra ameaças	Permite que as equipes de resposta a incidentes automatizem pesquisas, pesquisas e correlações de ameaças. A integração com o MITRE ATT&CK permite que você meça e entenda a cobertura de detecção e mitigação e auxilia na detecção de ameaças.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Analista de inteligência contra ameaças
Central de segurança de inteligência contra ameaças (TISC)	Agregue, selecione e gerencie inteligência contra ameaças de várias origens e conduza a gestão de casos de inteligência contra ameaças. Rastreie campanhas, operacionalize a inteligência contra ameaças e responda à inteligência acionável.	• CISO • Analista de segurança da informação • Gerente de operações de segurança • Analista de inteligência contra ameaças

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que explorar a seguir

Selecione um bloco para começar a usar os espaços Operações de segurança.

Espaço de resposta a incidentes de segurança	**Espaço para gerentes de vulnerabilidades**	**Espaço de controle de posturas de segurança**
Saiba mais sobre o Espaço de resposta a incidentes de segurança	Saiba mais sobre o Espaço do gerenciador de vulnerabilidades	Saiba mais sobre o espaço de controle de posturas de segurança
Espaço de avaliação de vulnerabilidade	**Espaço de correção de TI**	**Espaço da lista de materiais de software**
Saiba mais sobre o Espaço de avaliação de vulnerabilidade	Saiba mais sobre o Espaço de correção de TI	Saiba mais sobre o espaço da lista de materiais de software

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Espaço da Central de segurança de inteligência contra ameaças (TISC)	Espaço de resposta a incidentes de prevenção de perda de dados (DLP)	Espaço de gestão de incidentes graves de segurança (MSIM)
Saiba mais sobre o espaço de TISC	Saiba mais sobre o espaço da DLP	Saiba mais sobre o Espaço do MSIM

Solucionar problemas e obter ajuda

- Comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

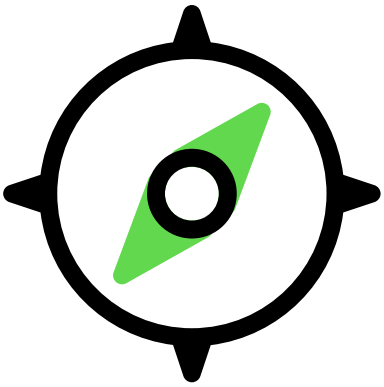
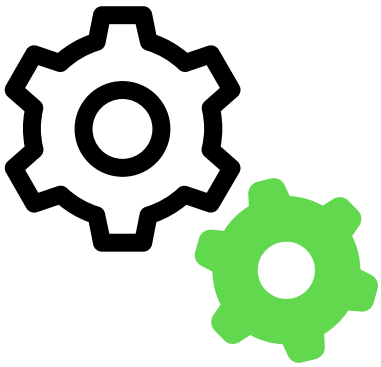
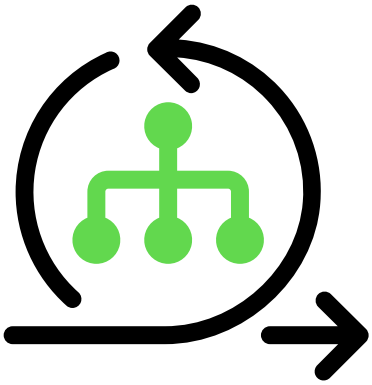
Now Assist para Operações de segurança

Os analistas de segurança podem usar fluxos de trabalho inteligentes e ServiceNow habilidades de IA generativa para ajudá-los a resolver incidentes de segurança. Os gerentes de segurança podem revisar o contexto de incidentes de segurança e anotações de fechamento rapidamente em um formato conciso e de fácil leitura com a aplicação Now Assist para Operações de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

Explorar	Configurar	Uso
		
Saiba mais sobre Now Assist para Operações de segurança	Saiba como configurar e ativar as habilidades para Now Assist para Operações de segurança	Aprenda a resumir detalhes e gerar anotações de fechamento para incidentes de segurança com IA generativa e Now Assist para Operações de segurança

Importante: Alguns produtos/recursos do Now Assist não estão disponíveis atualmente para clientes nos datacenters protegidos pelo FedRAMP, pela IL5 do DOD do NSC ou pelo IRAP da Austrália, clientes auto-hospedados ou em outros ambientes restritos. Para obter mais informações, consulte o artigo KB0743854 na Now Support Base de conhecimento. Verifique a existência de atualizações de disponibilidade em versões futuras.

Solucionar problemas e obter ajuda

- Comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Limitações de IA

Esta aplicação usa inteligência artificial (IA) e aprendizado de máquina, que são campos de estudo em rápida evolução que geram previsões com base em padrões de dados. Como resultado, esta aplicação nem sempre produz informações precisas, completas ou apropriadas. Além disso, não há garantia de que esta aplicação tenha sido totalmente treinada ou testada para o seu caso de uso. Para ajudar a atenuar esses problemas, recomendamos que você teste e avalie o uso desta aplicação quanto à precisão conforme apropriado para o seu caso de uso, empregue a revisão humana conforme apropriado e evite depender apenas de resultados gerados por IA para fins de tomada de decisão. Isso é especialmente importante se você optar por implantar esta aplicação em áreas com impactos importantes, como saúde, finanças, jurídico, emprego, segurança ou infraestrutura.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Processamento de dados

Esta aplicação requer que os dados sejam transferidos de ServiceNow instâncias individuais dos clientes para um ambiente centralizado ServiceNow, que pode estar localizado em uma região de datacenter diferente daquela em que sua instância se encontra e, potencialmente, para um provedor de nuvem de terceiros, como o Microsoft Azure. Esses dados são tratados pelas políticas e procedimentos internos da ServiceNow, incluindo as políticas disponíveis por meio do nosso Portal de conformidade CORE .

Coleta de dados

ServiceNow coleta e usa as entradas, saídas e edições nas saídas desta aplicação para desenvolver e melhorar tecnologias ServiceNow, incluindo modelos e produtos de IA ServiceNow. Além disso, esta aplicação coletará dados de incidentes de segurança. Os clientes podem recusar a coleta futura de dados a qualquer momento, conforme descrito na página Now Assist Recusar .

Exploração do Now Assist para Operações de segurança

Seus analistas de segurança podem usar fluxos de trabalho inteligentes e habilidades de IA generativa ServiceNow para ajudá-los a resolver incidentes de segurança dentro do fluxo de trabalho com a aplicação Now Assist para Operações de segurança. Com habilidades de IA generativa, eles podem revisar o contexto e as anotações de fechamento para incidentes de segurança rapidamente em um formato conciso e fácil de ler.

Visão geral Now Assist para Operações de segurança

Seus analistas de segurança têm a opção de resumir os detalhes do incidente de segurança e gerar notas de fechamento com IA generativa. Eles podem compartilhar resumos e anotações de fechamento com outros analistas, gerentes e principais partes interessadas.

Now Assist para Operações de segurança usuários

Usuários

Usuário	Descrição
Analistas e gerentes de segurança	Visualize detalhes do incidente de segurança, veja o possível impacto e exiba as principais ações de correção já realizadas com resumos de incidentes de segurança usando IA generativa. Os resumos oferecem aos analistas e gerentes uma vantagem nas investigações. Gere automaticamente um rascunho de anotações de fechamento usando IA generativa. As anotações de fechamento para incidentes de segurança são criadas rapidamente com base nas atividades de correção e contenção, além de outros detalhes relevantes que estão relacionados ao fechamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Benefícios do Now Assist para Operações de segurança

Recursos do Now Assist para Operações de segurança

Benefício	Recurso	Usuários
Acelere a triagem de incidentes de segurança com longos fluxos de atividades revisando anotações de trabalho e informações contextuais rapidamente em um formato conciso e de fácil leitura.	Gere resumos para incidentes de segurança que incluem as seguintes informações: • Problema • Detalhes • Observações • Principais ações realizadas • Detalhes do fechamento	• Analistas de segurança • Gerentes de segurança
Gere automaticamente um rascunho de anotações de fechamento para um incidente de segurança quando ele estiver pronto para fechamento. Os analistas podem modificar qualquer conteúdo gerado pela habilidade de IA editando-o, removendo-o ou adicionando suas próprias anotações antes de fecharem o incidente de segurança.	Gerar anotações de fechamento de incidente de segurança	• Analistas de segurança • Gerentes de segurança
Saiba mais sobre os detalhes de um incidente de segurança rapidamente acessando resumos e anotações de fechamento no painel Now Assist.	Acesse o resumo de IA generativa e as anotações de fechamento no painel Now Assist. Digite solicitações para obter informações mais básicas sobre incidentes de segurança no painel.	• Analistas de segurança • Gerentes de segurança
Personalize as habilidades de IA generativa para resumos e notas de fechamento para atender às suas necessidades.	Copie uma habilidade e modifique os campos da tabela relacionada de seleção, defina a disponibilidade da habilidade e escolha onde a habilidade será exibida.	administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que explorar a seguir

Para saber mais sobre como configurar e usar o Now Assist para Operações de segurança, consulte:

- Configuração da Now Assist para Operações de segurança
- Resumir um incidente de segurança com Now Assist para Operações de segurança
- Gerar notas de fechamento para um incidente de segurança com Now Assist para Operações de segurança
- Referência: entradas e gatilhos do Now Assist para Operações de segurança

Informações de suporte para Now Assist para Operações de segurança

Obtenha uma visão geral rápida das informações importantes relacionadas à aplicação Now Assist para Operações de segurança.

Versões compatíveis

- Para legado IU (UI16): Security Incident Response aplicação principal, v13.5.1
- Para Espaço de resposta a incidentes de segurança (Espaço SIR), v1.6.0

Interfaces do usuário compatíveis

O Now Assist para Operações de segurança inclui as habilidades de IA generativa listadas na tabela a seguir.

Now Assist para Operações de segurança interfaces e habilidades compatíveis

Interface	Recursos
Security Incident Response	• Resumo do incidente de segurança • Geração de anotações de fechamento • Painel do Now Assist
Legado IU16	• Resumo do incidente de segurança • Geração de anotações de fechamento • Painel do Now Assist

Configuração da Now Assist para Operações de segurança

A aplicação Now Assist para Operações de segurança é compatível com Espaço de resposta a incidentes de segurança e na IU principal legado (UI16). Você pode usar a configuração assistida no console Administrador do Now Assist para configurar Now Assist para Operações de segurança.

Visão geral da configuração

Ao compartilhar dados com o programa de desenvolvimento de IA ServiceNow®, você fornece dados relevantes para ajudar a melhorar a precisão da previsão, a experiência do usuário, personalizar produtos de acordo com as necessidades de negócio e reduzir as alucinações relacionadas às suas habilidades Now Assist ativadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode optar por recusar o compartilhamento de dados de uma instância ServiceNowAdministrador do Now Assist do console [] se não quiser participar. Consulte Recusar compartilhamento de dados para Now Assist . Repita o processo de recusa para todas as instâncias que usam a funcionalidade Now Assist.

Use o console do Administrador do Now Assist para configurar Now Assist para Operações de segurança. Este console contém tudo o que você precisa para instalar as aplicações e configurar as habilidades de IA generativa. Para obter informações adicionais, confira Definição de Now Assist configurações e recursos .

A tabela a seguir lista os recursos e as habilidades que você pode acessar no console do Administrador do Now Assist.

Now Assist para Operações de segurança recursos e habilidades no console Administrador do Now Assist

Produto da Now Assist Technology	Habilidades do incidente de segurança
Operações de segurança	Resumo do incidente de segurança **Nota:** O resumo de incidentes oferece suporte a incidentes de segurança em qualquer estado diferente de **Rascunho**.
	Geração de anotações de resolução.

1. Instalar plug-ins de Now Assist .

   Instale a aplicação Now Assist para Operações de segurança (sn_sec_gen_ai).

2. Configurar e ativar uma habilidade para Now Assist para Operações de segurança

   Configure e revise os detalhes de uma habilidade. Você ativa uma habilidade do Configuração assistida.

Usando Configuração assistida para implementar Now Assist para Operações de segurança

Configuração assistida fornece uma sequência de tarefas que ajudam a configurar Now Assist para Operações de segurança em sua instância ServiceNow. Para abrir o Configuração assistida para Now Assist para Operações de segurança, navegue até **Todos** > **Administrador do Now Assist** > **Recursos**.

Para mais informações, consulte Configurar e ativar uma habilidade para Now Assist para Operações de segurança.

Configurar e ativar uma habilidade para Now Assist para Operações de segurança

Configure e revise os detalhes de uma habilidade no Configuração assistida. Você pode ativar uma habilidade do Configuração assistida.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administrador do Now Assist** > **Recursos**.
2. Com a **tecnologia** selecionada no painel de navegação, selecione **Operações de segurança** na lista.
   Essas habilidades de incidente de segurança são exibidas no cartão de incidente de segurança:
   - Resumo do incidente de segurança
   - Geração de anotações de resolução
3. Selecione **Exibir detalhes**.
4. Selecione **Ativar habilidade** para a habilidade desejada.
5. Siga as etapas para configurar e ativar uma habilidade usando o Configuração assistida.

   a. No painel de navegação, selecione **Escolher entrada** para configurar as entradas ou os gatilhos da habilidade selecionada.

   Estes modelos de entrada para a habilidade são listados: **Trabalho em andamento**, **Revisão**e **Encerrado**. O modelo **Trabalho em andamento** está selecionado.

   Você pode preferir deixar esses modelos de entrada em suas configurações padrão até se familiarizar com o funcionamento das habilidades para Now Assist para Operações de segurança.

   No entanto, você pode modificar alguns dos campos da tabela relacionada, testar o prompt em um incidente de segurança, definir a disponibilidade da habilidade e escolher onde a habilidade será exibida.

   Se você optar por modificar os campos, selecione somente as opções compatíveis nas listas fornecidas como parte dos dados de entrada.

   Se você modificar as entradas ou os gatilhos de uma habilidade, determinará como e quando uma habilidade será usada. Você não pode modificar a fonte de dados de entrada de uma habilidade. A fonte de dados contém as tabelas e os campos dos quais a habilidade depende. No entanto, você pode copiar uma habilidade e personalizá-la. Para obter mais informações, consulte Personalizar uma habilidade do Now Assist para Operações de segurança.

6. Selecione **Salvar e continuar** para ir para a próxima etapa no Configuração assistida.
7. Opcional: Teste o prompt em um registro de incidente de segurança.
8. Selecione **Salvar e continuar** para ir para a próxima etapa no Configuração assistida.
9. Opcional: Escolha uma das seguintes opções para definir a disponibilidade.

Opção	Descrição
A habilidade está sempre disponível	A habilidade está sempre disponível para os usuários.
Personalizar disponibilidade da habilidade	A habilidade está disponível somente quando determinadas condições são atendidas (padrão). (Optional) Use o Construtor de condições para definir suas condições.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Selecione **Salvar e continuar** para ir para a próxima etapa no Configuração assistida.
11. Escolha **Selecionar exibição** para determinar onde você deseja exibir a habilidade.

Opção	Descrição
No produto	Now Assist habilidades são exibidas em formulários e espaços.
Painel do Now Assist	Now Assist habilidades estão disponíveis no painel Now Assist. **Nota:** Se você não vir esta opção, deverá ativar o painel do Now Assist. Para obter mais informações, consulte Ativar o painel Now Assist .

12. Selecione **Salvar e continuar** para prosseguir para a próxima etapa.
13. Revise suas escolhas e selecione **Ativar** para concluir a configuração da habilidade.
14. Selecione **Retornar ao incidente de segurança**.
    A habilidade é exibida na seção Habilidades ativas.

Personalizar uma habilidade do Now Assist para Operações de segurança

Personalize alguns dos campos de entrada de uma habilidade de IA generativa para atender aos requisitos do seu ambiente.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até o **Todos** > **Administrador do Now Assist** > **Recursos** guia do console Administrador do Now Assist.
2. Com a **tecnologia** selecionada no painel de navegação, selecione **Operações de segurança** na lista.
   Estas habilidades de incidente de segurança são exibidas:
   - Resumo do incidente de segurança
   - Geração de anotações de resolução
3. Crie uma cópia de uma habilidade e personalize os campos de entrada.

   a. No cartão do recurso Incidente de segurança, selecione **Exibir detalhes**.

   b. Na seção Habilidades ativas, localize a habilidade que você deseja copiar e selecione o ícone de mais ações (ícone de ⋮).

   c. Selecione **Fazer uma cópia**.

   d. Confirme sua escolha no modal.
   A configuração assistida é exibida.

   e. Em **Detalhes gerais**, insira um nome e uma descrição exclusivos para a habilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Prossiga para a próxima etapa selecionando **Salvar e continuar**.

g. Selecione **Escolher entrada**.

Se **Escolher entrada** for selecionado, estes modelos de entrada para a habilidade serão listados: Trabalho em andamento, Revisão e Encerrado. O modelo Trabalho em andamento está selecionado.

Você pode configurar alguns dos campos da tabela de entrada base, as condições e as listas relacionadas aos modelos. Selecione somente nas tabelas relacionadas compatíveis com as listas para os dados de entrada.

Você não pode modificar a tabela de entrada base [sn_si_incident] ou adicionar uma nova fonte de dados para sua cópia da habilidade de resumo de incidente de segurança.

h. Continue a modificar os campos editáveis no modelo Trabalho em andamento com o construtor de condições e as condições de filtragem.

i. Prossiga para a próxima etapa em Configuração assistida para o modelo Trabalho em andamento selecionando **Salvar e continuar**.

- **Personalizar prompt**: edite o prompt reordenando ou removendo as seções predefinidas. Você pode revisar e testar o prompt em um registro de incidente de segurança para cada configuração de modelo de entrada.
- **Definir disponibilidade**:

Opção	Descrição
A habilidade está sempre disponível	A habilidade está sempre disponível para os usuários.
Personalizar disponibilidade da habilidade	A habilidade está disponível somente quando as condições são atendidas (padrão). Use o Construtor de condições para definir suas condições.

- **Selecionar exibição**:

Opção	Descrição
No produto	Mostre o resumo do incidente de segurança em todos os produtos de segurança. Now Assist habilidades são exibidas em formulários e espaços.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Painel do Now Assist	Now Assist habilidades estão disponíveis no painel Now Assist. **Nota:** Se você não vir esta opção, deverá ativar o painel do Now Assist. Para obter mais informações, consulte Ativar o painel Now Assist .

j. Selecione **Salvar modelo** para salvar suas mudanças no modelo Trabalho em andamento.

k. Selecione o modelo Revisão.

l. Continue a modificar os campos editáveis nos modelos Revisão e Encerrado com as condições de filtragem conforme descrito nas etapas anteriores.

m. Selecione **Salvar e continuar** para prosseguir para a próxima etapa no Configuração assistida.

n. Selecione **Salvar modelo** para salvar suas mudanças em um modelo.

o. Selecione **Revisar e ativar** para revisar sua habilidade e fazer modificações adicionais.

4. Selecione **Ativar**.
   Sua habilidade é exibida na página Incidente de segurança nas habilidades Todos os incidentes de segurança disponíveis.
5. Selecione **Ativar habilidade**.

Entradas e gatilhos para Now Assist para Operações de segurança

Você pode configurar algumas das entradas ou gatilhos para uma habilidade de IA generativa. As entradas ou gatilhos permitem que você determine como e quando uma habilidade é usada.

Visão geral

As entradas identificam os dados usados para uma habilidade. As entradas incluem a tabela e os campos usados para gerar um resumo do incidente de segurança. Um gatilho inicia uma ação. Por exemplo, os gatilhos determinam quando o sistema gera um resumo.

Você pode modificar entradas e gatilhos, mas não pode modificar a fonte de dados de uma habilidade. A fonte de dados contém as tabelas e os campos dos quais a habilidade depende.

Habilidade de resumo do Incidente de segurança

As entradas para a habilidade de resumo de incidente de segurança identificam a tabela e os campos usados quando um resumo de incidente de segurança é gerado. A tabela a seguir lista as entradas para a habilidade de resumo do Incidente de segurança na página Escolher entrada no console do Administrador do Now Assist.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Entrada	Descrição
Fonte de dados	Tabela Incidente de segurança [sn_si_incident].
Campos de entrada	• Descrição resumida • Descrição • Estado • Prioridade • Anotações de trabalho • Comentários adicionais
Tabelas de entrada relacionada	• ICs afetados - item de configuração • Usuários afetados - Usuários • Security Incident Response Tarefa - Descrição resumida • Estado - Qualquer estado diferente de **Cancelado**. • Observáveis associados — A descoberta do observável é mal-intencionada ou suspeita.

Habilidade de geração de anotações de resolução

As entradas para a habilidade de geração de anotações de resolução identificam a tabela e os campos que são usados quando as anotações de resolução são geradas para um incidente de segurança. A tabela a seguir lista as entradas para a habilidade de geração de anotações de resolução na página Escolher entrada no console Administrador do Now Assist.

Entrada	Descrição
Fonte de dados	Tabela Incidente de segurança [sn_si_incident].
Campos de entrada	• Descrição resumida • Descrição • Anotações de trabalho • Comentários adicionais

Usando Now Assist para Operações de segurança para resolver incidentes de segurança

Os analistas de segurança podem resolver incidentes de segurança rapidamente em seu fluxo de trabalho com as habilidades de IA generativa compatíveis com Now Assist para Operações de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral de Now Assist para Operações de segurança

Seus analistas de segurança têm a opção de resumir os detalhes do incidente de segurança e gerar notas de fechamento com habilidades de IA generativa com Now Assist para Operações de segurança. Eles podem compartilhar esses resumos e anotações de fechamento com outros analistas, gerentes e principais partes interessadas.

Os gerentes e analistas de segurança podem solicitar resumos de incidentes de segurança e notas de fechamento fáceis de ler nos seguintes locais:

- Registros de incidentes de segurança
- Security Incident Response espaço
- O painel Now Assist

1. Resumir um incidente de segurança com Now Assist para Operações de segurança

   Gere um resumo para um incidente de segurança que inclui o problema subjacente, detalhes do incidente, dados de listas relacionadas (observáveis) e as principais ações já realizadas.

2. Gerar notas de fechamento para um incidente de segurança com Now Assist para Operações de segurança

   Gere automaticamente as anotações de fechamento para um incidente de segurança.

3. Solicitar habilidades de IA generativa no painel [Now Assist para Now Assist para Operações de segurança

   Gere resumos e notas de fechamento no painel Now Assist.

4. Personalizar uma habilidade do Now Assist para Operações de segurança

   Personalize os campos de entrada de uma habilidade para atender aos requisitos do seu ambiente.

Resumir um incidente de segurança com Now Assist para Operações de segurança

Entenda o contexto de um incidente de segurança com a habilidade de IA generativa de resumo de incidente de segurança.

Antes de Iniciar

Você pode resumir um incidente de segurança na legado IU principal (UI16) e na Espaço de resposta a incidentes de segurança. Deve haver um mínimo de 200 palavras nos campos usados para os dados de entrada para resumir um incidente usando IA generativa. Para obter mais informações sobre os campos de entrada, consulte Entradas e gatilhos para Now Assist para Operações de segurança.

Funções necessárias: si_analystsn, si.manager ou sn_si.basic

Procedimento

1. Na IU principal legado, navegue até **Todos** > **Incidente de segurança** > **Incidentes** e abra um incidente de segurança atribuído a você.
2. Como alternativa, navegue até **Todos** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na guia **Visão geral**, selecione **Resumir**.
   - O resumo gerado é exibido em uma faixa na parte superior do registro de incidente de segurança no legado Core UI16.
   - O resumo gerado é exibido na guia **Visão geral** no Espaço de resposta a incidentes de segurança.
4. Opcional: Selecione uma das seguintes opções depois que o resumo for gerado.

   (Optional) Os resumos gerados pela IA podem não ter detalhes importantes. Você pode preferir revisar o resumo para verificar a precisão e a integridade antes de prosseguir.

Opção	Descrição
Exibir detalhes sobre o resumo	Selecione o ícone de informações (ícone ⓘ) ao lado do incidente de segurança resumido por Now Assist.
Salve as informações de resumo adicionando-as às anotações de trabalho do incidente	**a.** Selecione **Compartilhar nas anotações de trabalho**. **b.** Verifique a precisão do conteúdo gerado por IA no modal e faça edições. **c.** Selecione **Salvar nas anotações de trabalho**.
Expandir ou recolher o resumo	Selecione o ícone de expansão (ícone de ⌄) ou o ícone de ⌃) ao lado de **Compartilhar nas anotações de trabalho** para expandir ou recolher o resumo.
Fornecer feedback	Selecione o ícone útil (Ícone 👍) para obter um feedback positivo. Selecione o ícone não útil (ícone 👎) se o resumo não foi útil. **Nota:** O feedback melhora o modelo de IA generativa e pode ajudar a melhorar as versões futuras dessa habilidade.
Copiar o resumo	Selecione o ícone de cópia (⧉) para copiar o resumo para a área de transferência.

Gerar notas de fechamento para um incidente de segurança com Now Assist para Operações de segurança

Gere automaticamente um rascunho das anotações de fechamento para um incidente de segurança ao fechá-lo. O rascunho é editável e será revisado antes do encerramento do incidente de segurança e pode ser usado ou modificado conforme necessário. As anotações de fechamento fornecem informações sobre a resolução de um incidente de segurança para outros analistas, gerentes e principais partes interessadas.

Antes de Iniciar

Funções necessárias: si_analystsn, si.manager ou sn_si.basic

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na IU principal legado, navegue até **Todos** > **Incidente de segurança** > **Incidentes** e abra um incidente de segurança atribuído a você.
2. Como alternativa, navegue até **Todos** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
3. Encerre o incidente de segurança.

Opção	Descrição
Fechar o incidente de segurança no legado do Core UI16	**a.** Altere o campo **Estado** para **Encerrado**. O modal de passador é exibido. **b.** Revise cada etapa e selecione **Avançar**. **c.** Selecione **Fornecer detalhes da resolução**. **Nota:** Você pode revisar o texto gerado e verificar se ele está correto antes de fechar o incidente de segurança. Edite as anotações ou exclua-as para fornecer as suas próprias anotações. **d.** Atualize o Código de fechamento e selecione **Fechar incidente**. O resumo da resolução é exibido na seção Informações de resolução no registro do incidente de segurança.
Fechar o incidente de segurança do Espaço de resposta a incidentes de segurança	**a.** Na guia **Detalhes** do espaço, altere o campo **Estado** para **Encerrado**. O modal de passador é exibido. **b.** Revise cada etapa e selecione **Avançar**. **c.** Selecione **Fornecer detalhes da resolução**. **Nota:** Você pode revisar o texto gerado e verificar se ele está correto antes de fechar o incidente de segurança. Edite as anotações ou exclua-as para fornecer as suas próprias anotações. **d.** Atualize o Código de fechamento e selecione **Fechar incidente**. O resumo da resolução é exibido na guia **Detalhes** no registro do incidente de segurança no espaço.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar habilidades de IA generativa no painel [Now Assist para Now Assist para Operações de segurança

Solicite um resumo do incidente de segurança ou anotações de fechamento no painel Now Assist.

Antes de Iniciar

Consulte Painel do Now Assist para saber como ativar o painel Now Assist.

Funções necessárias: si_analystsn, si.manager ou sn_si.basic

Procedimento

1. Faça login em uma instância em que Now Assist para Operações de segurança esteja instalado.
2. Na IU principal legado, navegue até **Todos** > **Incidente de segurança** > **Incidentes** e abra um incidente de segurança atribuído a você.
3. Como alternativa, navegue até **Todos** > **Incidente de segurança** > **Espaço de resposta a incidentes de segurança** e abra um incidente de segurança atribuído a você.
4. Selecione o ícone do Now Assist (ícone do ✦).

Opção	Descrição
Gerar anotações de resolução	No painel Now Assist, selecione **Gerar anotações de resolução**. As anotações de fechamento geradas no painel são idênticas às geradas quando você fecha um incidente de segurança de um registro. As anotações de fechamento para incidentes de segurança são criadas com base em todas as ações realizadas para correção e contenção, além de outros detalhes relevantes relacionados ao fechamento. **Nota:** Você pode revisar o texto gerado e verificar se ele está correto antes de fechar o incidente de segurança. Edite as anotações ou exclua-as para fornecer as suas próprias anotações.
Resumir um incidente de segurança	No painel Now Assist, selecione **Resumir um registro**. O resumo gerado no painel é idêntico ao que você gera a partir de um registro de incidente de segurança.

Tradução automática

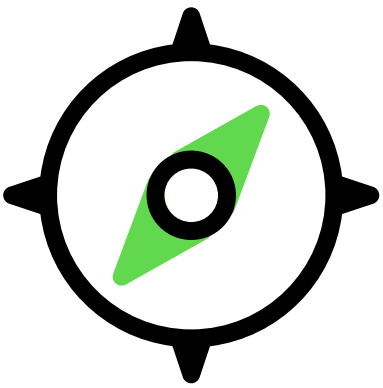
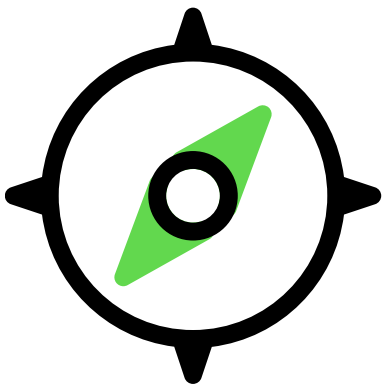
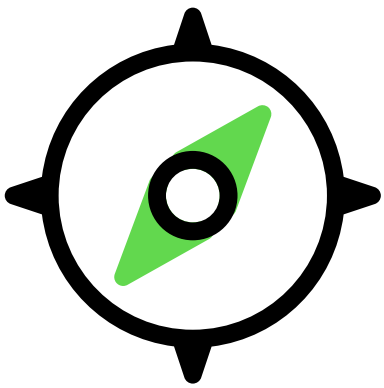
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Os resumos gerados pela IA podem não ter detalhes importantes. Você pode preferir revisar o resumo para verificar a precisão e a integridade antes de prosseguir.

Aplicações da superfície de ataque

As aplicações Resposta a vulnerabilidades que compõem as aplicações de superfície de ataque ajudam você a priorizar seus ativos vulneráveis e adicionam contexto para ajudá-lo a determinar quando os sistemas críticos para os negócios estão comprometidos. Usando o CMDB, suas equipes de segurança também podem identificar facilmente dependências entre sistemas e avaliar rapidamente o impacto nos negócios de mudanças ou tempos de inatividade.

Resposta a vulnerabilidades aplicações

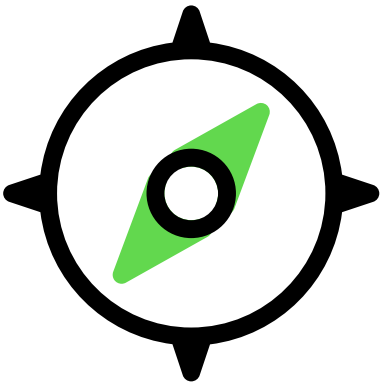
Resposta a vulnerabilidades	Resposta a vulnerabilidades de aplicações	Resposta a vulnerabilidades do contêiner
		
Saiba mais sobre a aplicação Resposta a vulnerabilidades	Saiba mais sobre a aplicação Resposta a vulnerabilidades da aplicação	Saiba mais sobre a aplicação Resposta a vulnerabilidades do contêiner

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

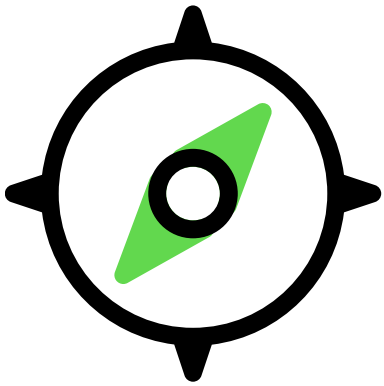
Resposta a vulnerabilidades aplicações

Conformidade de configurações



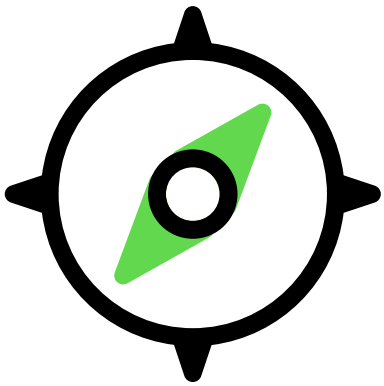
Saiba mais sobre a aplicação Conformidade de configuração

Lista de materiais de software



Saiba mais sobre as aplicações da lista de materiais de software

Recursos compartilhados de aplicações da Resposta a vulnerabilidades



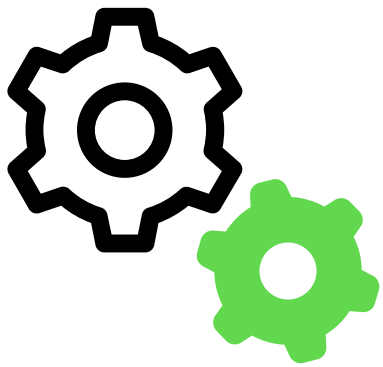
Saiba mais sobre os recursos compartilhados entre as aplicações da Resposta a vulnerabilidades

Resposta a vulnerabilidades Espaços

Espaço para gerentes de vulnerabilidades

Saiba mais sobre o Espaço do gerenciador de vulnerabilidades

Espaço de correção de TI



Saiba mais sobre o Espaço de correção de TI

Espaço de avaliação de vulnerabilidade

Saiba mais sobre o Espaço de avaliação de vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

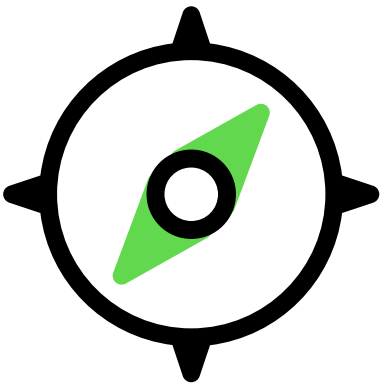
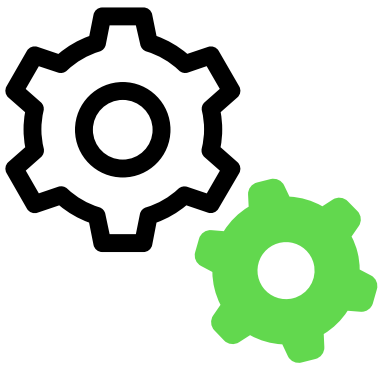
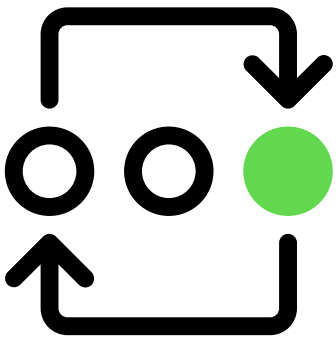
Solucionar problemas e obter ajuda

- Comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Resposta a vulnerabilidades

O Banco de dados nacional de vulnerabilidades (NVD) e outras origens coletam informações sobre vulnerabilidades conhecidas. Essas vulnerabilidades podem incluir fraquezas no software, sistemas operacionais que o malware pode explorar e outros ataques. A aplicação ServiceNow® Resposta a vulnerabilidades ajuda a rastrear, priorizar e resolver essas vulnerabilidades.

Resposta a vulnerabilidades

Explorar	Instalar e configurar	Integrar
		
Saiba mais sobre os recursos da Resposta a vulnerabilidades	Instalar e configurar a aplicação Resposta a vulnerabilidades	Estenda a Resposta a vulnerabilidades integrando-a a outras aplicações

Tradução automática

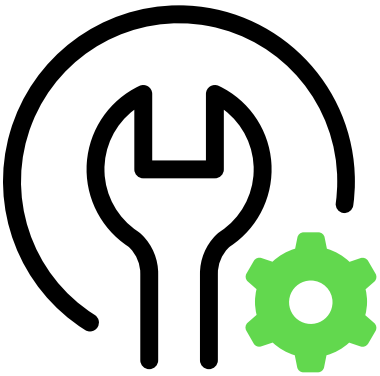
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades

Explorar e usar os Espaços de resposta a vulnerabilidades

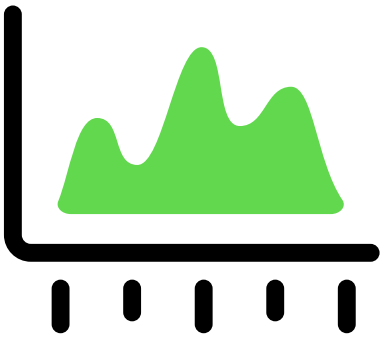
Aprenda a usar o Gerenciador de vulnerabilidades e os Espaços de correção de TI

Corrigir



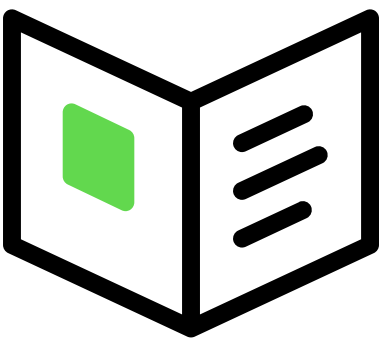
Use os recursos da Resposta a vulnerabilidades para corrigir suas vulnerabilidades e proteger seus ativos

Análise e Emissão de relatórios



Monitorar o andamento da correção

Referência



Obtenha mais detalhes sobre notas de versão, componentes e informações de referência da Resposta a vulnerabilidades sobre campos, tabelas e propriedades

Tradução automática

Explorar a aplicação Resposta a vulnerabilidades

A aplicação ServiceNow® Resposta a vulnerabilidades importa e agrupa automaticamente itens vulneráveis de acordo com regras que permitem corrigir vulnerabilidades rapidamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os dados de vulnerabilidade são extraídos de fontes externas, como o National Vulnerability Database (NVD) e integrações de terceiros, e processados com aplicações desenvolvidas por ServiceNow®.

Assista a uma visão geral sobre a resposta a vulnerabilidades que define itens vulneráveis, tarefas de correção e seus ciclos de vida.

Visão geral da resposta de vulnerabilidade típica em uma empresa versus a resposta de vulnerabilidade com a ServiceNow e define itens vulneráveis, grupos de vulnerabilidades e seus ciclos de vida.

Resposta a vulnerabilidades e seu ambiente empresarial

Normalmente, em um ambiente empresarial, as organizações usam scanners de vulnerabilidade e ferramentas de avaliação para identificar e gerenciar os riscos que as vulnerabilidades representam para seus ativos. As vulnerabilidades identificadas por essas ferramentas são convertidas em riscos para as equipes de segurança e de TI responsáveis por manter e proteger os ativos de uma organização. Alguns riscos podem incluir, entre outros, os seguintes tipos de vulnerabilidades identificadas:

- Dependência em software desatualizado ou sistemas configurados incorretamente
- Protocolos de rede não seguros
- Dependência em bibliotecas de software de terceiros com falhas
- Higienização de administração do sistema ruim ou inconsistente
- Imagens do sistema de linha de base que não são protegidas

Conforme esses riscos potenciais são expostos, as equipes de segurança e TI geralmente enfrentam desafios para processar e lidar com o volume de informações de vulnerabilidade geradas por suas ferramentas de verificação e avaliação. Especificamente, essas equipes se veem sobrecarregadas ao gerenciar um alto volume de vulnerabilidades identificadas e elaborar esforços de resposta acionáveis para mitigar os possíveis riscos que suas organizações enfrentam.

Você pode identificar esses desafios à sua própria postura de segurança, fazendo as seguintes perguntas:

- Quais vulnerabilidades identificadas devem ser revisadas primeiro?
- O que essas vulnerabilidades identificadas significam para nossa organização?
- Quem deve ser responsável e possuir os riscos identificados?
- Quem deve estar ativo, trabalhando para resolver/mitigar esses riscos?
- Como reduzimos efetivamente as vulnerabilidades identificadas com os recursos que temos?
- Quais são os possíveis resultados não intencionais da redução das vulnerabilidades identificadas?
- Que processo devemos seguir para corrigir vulnerabilidades, rastrear as etapas que executamos e acompanhar para garantir que nossas ações funcionaram?
- Como sabemos se estamos progredindo na redução de nossa postura de risco geral?

Resposta a vulnerabilidades e o Now Platform®

Resposta a vulnerabilidades é um membro do pacote de aplicações Operações de segurança. Juntas, essas aplicações conectam a segurança ao seu departamento de TI,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aumentam a velocidade e a eficiência de sua resposta e fornecem uma exibição definitiva de sua postura de segurança.

Visão geral do Security Operations

A aplicação ServiceNow Resposta a vulnerabilidades tem dois objetivos principais:

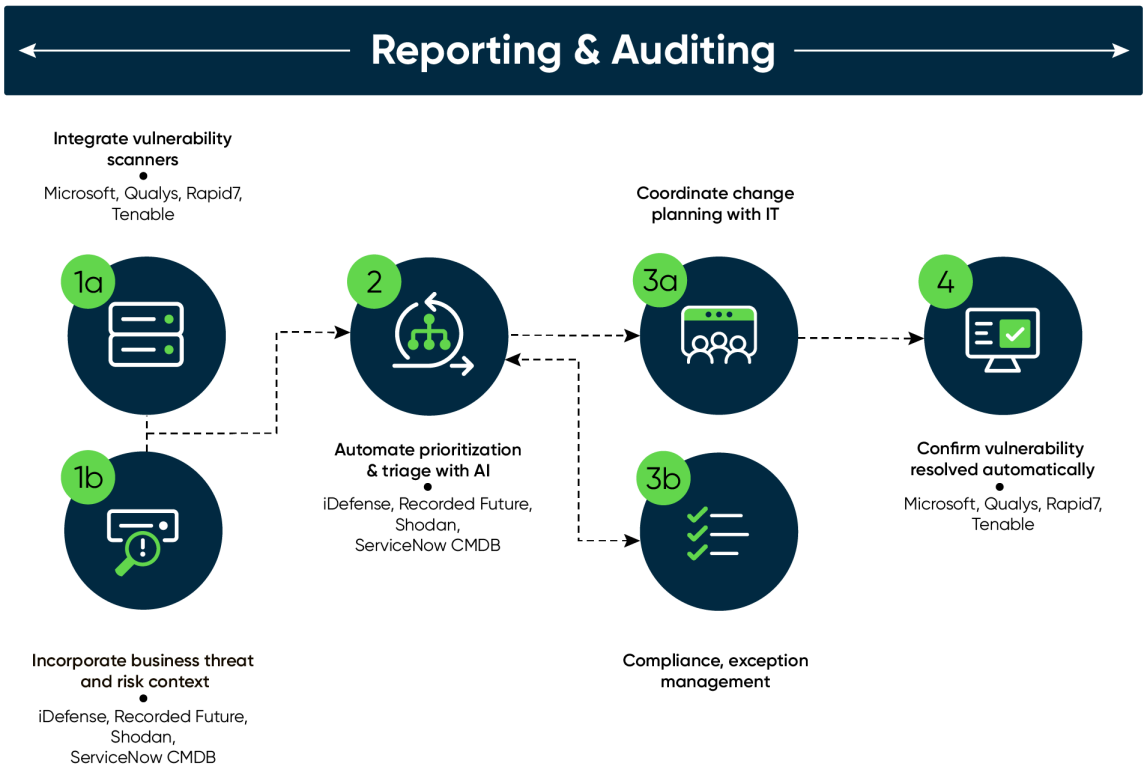
- Ajude as equipes de segurança com problemas para lidar com grandes quantidades de dados de vulnerabilidade.
- Ajude as equipes de operações encarregadas de resolver vulnerabilidades.

Dessa forma, você pode usar a aplicação Resposta a vulnerabilidades para automatizar o fluxo de informações, desde a integração até a investigação e, em seguida, até a resolução.

O processo de gestão de vulnerabilidades no Now Platform® pode envolver processos, dados, relatórios e automação com o CMDB.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Integre scanners de terceiros e aplicações ServiceNow® com a aplicação Resposta a vulnerabilidades para ingerir dados de vulnerabilidade conhecidos.
- Aprimore seus dados de vulnerabilidade ingeridos com exploração, inteligência contra ameaças, risco e contexto de negócios. Use esses dados para ajudá-lo nas estratégias de patch e correção.
- As vulnerabilidades importadas do NVD e os dados de detecção de produtos de terceiros são reconciliados com os ativos no seu CMDB. A triagem pode incluir: criar tarefas de correção compostas por vários itens vulneráveis, ou seja, seus ativos que estão determinados a ter vulnerabilidades, agrupar essas tarefas por categoria, priorizá-las e atribuí-las a equipes.
- Empregue a gestão coordenada de mudanças e exceções para ajudá-lo a resolver vulnerabilidades que podem exigir intervenção manual adicional, mais tempo para resolver ou pesquisa extensa.
- Confirme se as vulnerabilidades são resolvidas e atualizadas automaticamente pelas detecções de seus produtos de scanner.

Quem pode usar Resposta a vulnerabilidades na sua organização

Resposta a vulnerabilidades Os usuários geralmente se enquadram em duas personas.

Analista de vulnerabilidade

A persona do analista de vulnerabilidades geralmente é Segurança, Risco e conformidade ou Gestão. Esses usuários monitoram vulnerabilidades e determinam quando iniciar os processos de correção.

Importante: O analista de vulnerabilidades usa principalmente o Vulnerability Manager Workspace para monitorar e criar tarefas de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Responsável pela correção

A persona do Proprietário de correção geralmente faz parte das Operações de TI, DevOps/Engenharia ou de um Responsável pelo serviço. Esses usuários concluem as tarefas de correção necessárias para corrigir vulnerabilidades. Eles podem enviar solicitações de exceção ou mudança se processos controlados forem necessários para manutenção ou remoção de ativos.

Importante: O proprietário de correção trabalha principalmente em tarefas de correção de dentro do Espaço de correção de problemas de TI.

Resposta a vulnerabilidades de aplicações

O recurso Resposta a vulnerabilidades de aplicações (AVR) da aplicação ServiceNow® Resposta a vulnerabilidades importa itens vulneráveis da aplicação (AVITs) e, de acordo com as regras, permite corrigir vulnerabilidades da aplicação. Ele está disponível com assinatura separada. Para obter a documentação de Resposta a vulnerabilidades de aplicações, consulte Explorando Resposta a vulnerabilidades de aplicações.

Versões disponíveis

Para obter um dicionário de termos e mais referências que incluem links, solução de problemas, artigos de conhecimento, além de dados de campo nos formulários e registros encontrados em Resposta a vulnerabilidades, consulte Resposta a vulnerabilidades informações de referência.

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades v23.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Instalação de Resposta a vulnerabilidades e aplicações compatíveis

A aplicação Resposta a vulnerabilidades está disponível no ServiceNow Store. A aplicação é compatível com outras ServiceNow aplicações e integrações de terceiros que você também baixa do ServiceNow Store. Mais opções também estão disponíveis para estender a configuração básica.

Tarefas de configuração básica

A aplicação Resposta a vulnerabilidades é necessária como uma primeira etapa. Para obter mais informações sobre como instalá-lo, consulte Check-list de implementação da aplicação Resposta a vulnerabilidades e Instalar a aplicação Resposta a vulnerabilidades.

- Depois que a instalação for concluída, você poderá Configurar a Resposta a vulnerabilidades usando o Assistente de configuração.

  Com o Assistente de configuração, atribua usuários e grupos para acesso à aplicação, crie ou edite regras de atribuição, regras de tarefa de correção e datas de destino, configure calculadoras de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você também pode selecionar, instalar e configurar uma ou mais integrações de terceiros compatíveis no Assistente de configuração. Essas integrações recuperam dados de vulnerabilidade de sistemas e fornecedores externos. Para obter mais informações sobre como as integrações funcionam e as integrações compatíveis com Resposta a vulnerabilidades, consulte Integrações do Resposta a vulnerabilidades.
- Antes de implementar integrações de terceiros, execute a integração do NVD e o trabalho agendado do CWE como parte da configuração inicial do Resposta a vulnerabilidades.

  Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros e Configure e execute o trabalho agendado para atualizar registros de CWE para obter mais informações sobre como instalar, configurar e exibir as bibliotecas do NVD e do CWE.

- Selecione uma aplicação de análise, quando aplicável. A aplicação Performance Analytics Content Pack for Vulnerability Response contém relatórios que cobrem todas as fases do ciclo de vida de gestão de vulnerabilidades.

  [Opcional] Instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades [PA] aplicação.

- Selecione uma aplicação de soluções, quando aplicável. A gestão de soluções ajuda a correlacionar as vulnerabilidades em seu ambiente com as soluções que podem corrigi-las. [Opcional] Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades.

  Nota:

  - Quando a aplicação Solução de gestão de vulnerabilidade está habilitada, o Integração com a solução Microsoft Security Response Center e o Red Hat Solution Integration ficam disponíveis para edição no Assistente de configuração.

  - Solução de gestão de vulnerabilidade requer uma assinatura separada. Para obter mais informações, consulte Solução de gestão de vulnerabilidade.

- [Opcional] Instale o aplicativo ServiceNow Agent e o Resposta a vulnerabilidades aplicativo para celular para Experiência de dispositivos móveis Resposta a vulnerabilidades.

Outras tarefas de configuração que você pode executar

Essas tarefas de configuração adicionais são adicionadas à configuração básica e à correção de suporte com opções para emissão de relatórios, notificações por e-mail, configuração de integração nativa e trabalho com itens vulneráveis. A maioria dessas tarefas é realizada fora do Assistente de configuração. Consulte Tarefas adicionais Resposta a vulnerabilidades de instalação e configuração.

Tarefas avançadas fora da configuração básica

Essas tarefas de configuração opcionais são realizadas fora do Assistente de configuração e exigem codificação ou conhecimento avançado ServiceNow e não são consideradas parte da configuração básica. Consulte Tarefas de configuração avançadas Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades personas e funções granulares

Antes de corrigir vulnerabilidades com sucesso com a aplicação Resposta a vulnerabilidades, você deve atribuir personas e funções aos usuários e grupos no Assistente de configuração.

Uma das primeiras etapas de configuração necessárias para a aplicação Resposta a vulnerabilidades é atribuir funções a usuários e grupos. As funções definem o que usuários e grupos podem ver e fazer em Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidadese em todas as integrações de terceiros com Resposta a vulnerabilidades.

Você atribui funções de persona a usuários e grupos existentes no Assistente de configuração. Consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Nota:

Se você for um cliente de upgrade, poderá continuar usando suas funções existentes para a aplicação Resposta a vulnerabilidades. O acesso de usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e o proprietário de correção anteriores à v10.3 não foram alterados.

No entanto, para obter mais controle sobre o que usuários e grupos podem fazer e ver na aplicação Resposta a vulnerabilidades no nível da tarefa, talvez você prefira usar funções granulares. Para obter mais informações, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Se você já atribuiu funções usando o Assistente de configuração e deseja gerenciar atribuições de função granulares para todos os usuários e grupos do módulo Administração de usuários, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades para obter mais informações.

Funções de persona e funções granulares iniciando

Termos-chave.

Função

As funções definem o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades.

Grupo

Um conjunto de usuários que compartilham determinadas funções e uma finalidade comum.

Função de persona

Uma função pré-configurada na aplicação que é composta por várias funções granulares. As funções de persona em Assistente de configuração, Administrador de vulnerabilidade, Analista de vulnerabilidade, Proprietário de correção, Gerenciador de itens de configuração e Gerenciador de exceções foram projetadas para corresponder a cargos comuns para gerentes, analistas e proprietários de serviço em uma organização de TI ou grupo de correção de vulnerabilidades.

Funções herdadas

Um termo que descreve as funções que os usuários adquirem automaticamente quando outras funções são atribuídas a eles. Por exemplo, todos os usuários ou grupos atribuídos com a função de persona sn_vul.remediation_owner também herdam as funções granulares sn_vul.read_assigned,sn_vul.write_assigned.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de controle de acesso (ACL)

As listas de controle de acesso restringem o acesso aos dados exigindo que os usuários passem por um conjunto de requisitos antes que possam interagir com eles.

A partir da Resposta a vulnerabilidades v16.5, para proteger os relatórios contra exposição, defina as **ACLs All report_view** como `active=true`. Esta ACL garante que os dados protegidos estejam disponíveis somente para usuários autorizados.

Você atribui grupos e usuários a funções de persona no Assistente de configuração.

Nota: No Assistente de configuração, a função de administrador do sistema (admin) é necessária para as tarefas na primeira seção, atribuindo funções e instalando integrações. Depois de atribuir funções de persona no Assistente de configuração e instalar integrações, você pode preferir atribuir um usuário ou grupo com a função sn_vul.vulnerability_admin para concluir todas as tarefas restantes no Assistente de configuração e gerenciar a aplicação Resposta a vulnerabilidades.

A tabela a seguir lista as funções de persona Resposta a vulnerabilidades instaladas com a aplicação.

Funções de persona para Resposta a vulnerabilidades	**Descrição**
Atribua sn_vul.vulnerability_admin - Administrador de vulnerabilidade a usuários ou grupos.	Usuários com esta função têm acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Usuários com esta função configuram todas as aplicações e regras de VR e instalam integrações de terceiros.
Atribua sn_vul.vulnerability_analyst - Analista de vulnerabilidade a usuários e grupos.	Usuários e grupos com esta função exibem e atualizam todos os registros para correção de VI.
Atribua sn_vul.remediation_owner - Proprietário da correção a usuários e grupos.	Usuários e grupos com esta função corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem. Grupos ou usuários com esta função exibem e atualizam os registros atribuídos a eles ou a um grupo ao qual pertencem.
Atribua sn_vul.ci_manager a usuários e grupos.	Usuários e grupos com esta função gerenciam a reclassificação de itens de configuração (ICs) incompatíveis que não são encontrados no Configuration Management Database (CMDB).
Atribua acesso de leitura a áreas específicas na aplicação por tarefa.	Por exemplo, atribua sn_vul.read_all para que um usuário possa exibir todos os registros de VR. Para acesso de leitura para exibir regras de tarefa de correção, atribua sn_vul.read_group_rules. Usuários e grupos com esta função não atualizam registros.

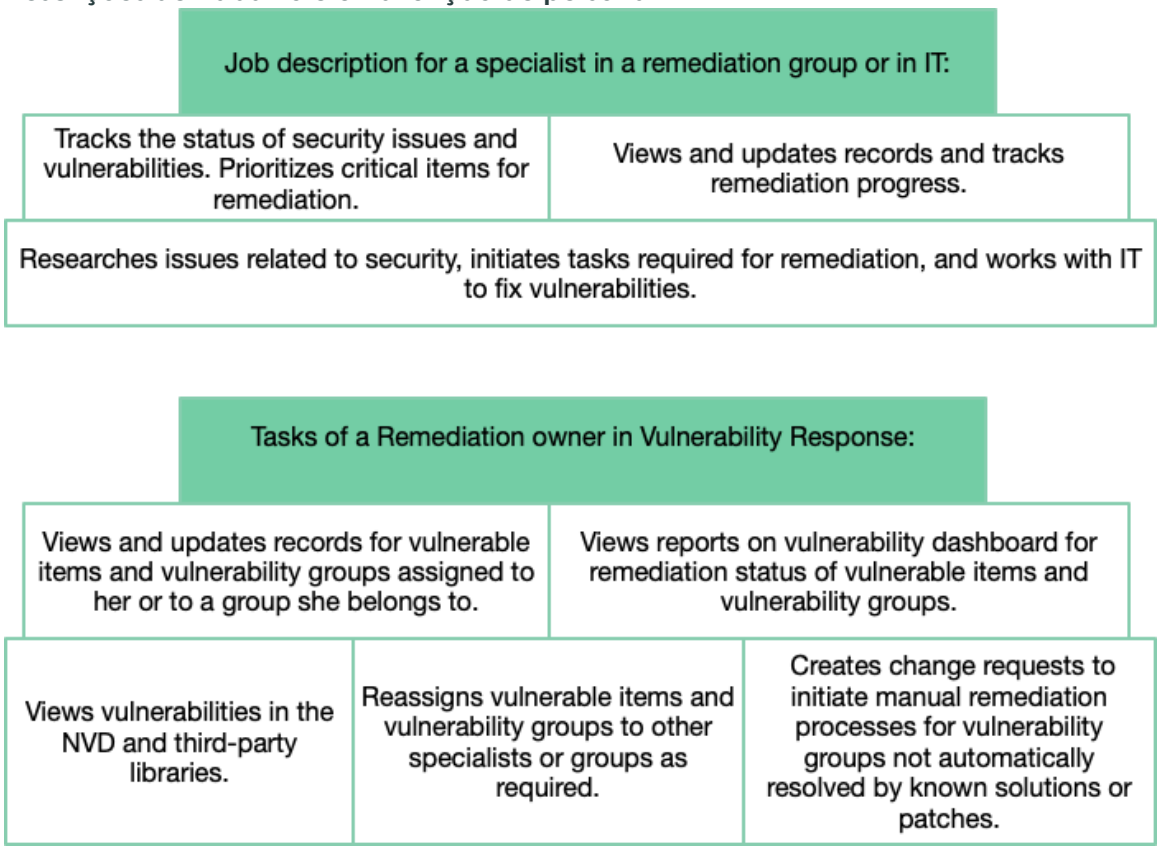
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções granulares e funções de persona

Uma maneira de pensar nas funções de persona é considerar como suas descrições podem estar relacionadas a descrições de trabalho para vários cargos de TI ou de correção de vulnerabilidades em sua organização. A figura a seguir ilustra uma possível descrição de trabalho para um especialista em correção de TI e como as tarefas associadas a esse trabalho se relacionam com as tarefas de uma função de persona de proprietário de correção na aplicação Resposta a vulnerabilidades.

Descrições de trabalho e uma função de persona



A descrição do trabalho e a função de persona do responsável pela correção podem ser definidas como uma série de tarefas de correção. Na imagem anterior, uma descrição de trabalho e uma função de persona em blocos verdes estão sobre as tarefas que os descrevem. Neste exemplo, alguns dos requisitos de trabalho típicos de um especialista em um grupo de correção correspondem diretamente às tarefas que compõem a persona do responsável pela correção em Resposta a vulnerabilidades: revisar e atualizar registros, rastrear o status de correção de vulnerabilidades, priorizar itens para correção, e aplique correções e patches com a TI.

Às vezes, no entanto, os trabalhos em sua organização podem não corresponder diretamente às tarefas que compõem uma das cinco funções de persona na aplicação Resposta a vulnerabilidades. Por vários motivos, como proteger dados confidenciais ou cumprir regulamentações, você deve limitar o acesso amplo que algumas das funções de persona fornecem aos usuários e grupos. Ou, inversamente, você deve fornecer aos usuários e grupos mais acesso para que eles possam realizar seus trabalhos. Usando funções granulares, você pode personalizar facilmente funções e controlar o acesso de usuários e grupos a Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidadese integrações de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As funções granulares definem as tarefas

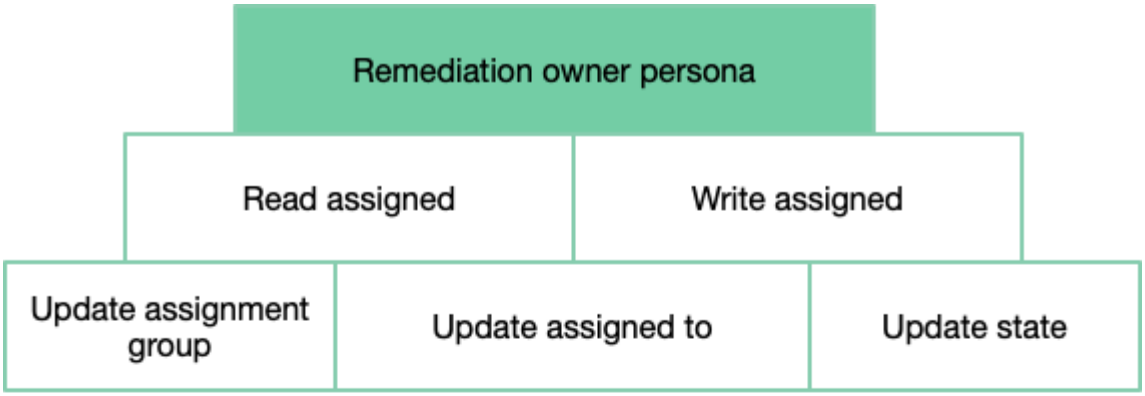
Os nomes das funções granulares em Resposta a vulnerabilidades geralmente descrevem o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Por exemplo, na imagem anterior, os usuários e grupos com a persona do responsável pela correção atribuída têm as funções granulares sn_vul.read_assigned e sn_vul.write_assigned. Essas funções granulares permitem que usuários ou grupos exibam e atualizem itens vulneráveis e registros de tarefas de correção atribuídos a eles. Para exibir descrições de funções granulares específicas, como um usuário com a função de administrador do sistema, navegue até **Administração de usuários** > **Funções** e localize a função desejada. As funções que são herdadas automaticamente quando uma função é atribuída são listadas. Além disso, quando uma função depende de outras atribuições de função, todas as funções necessárias também são listadas.

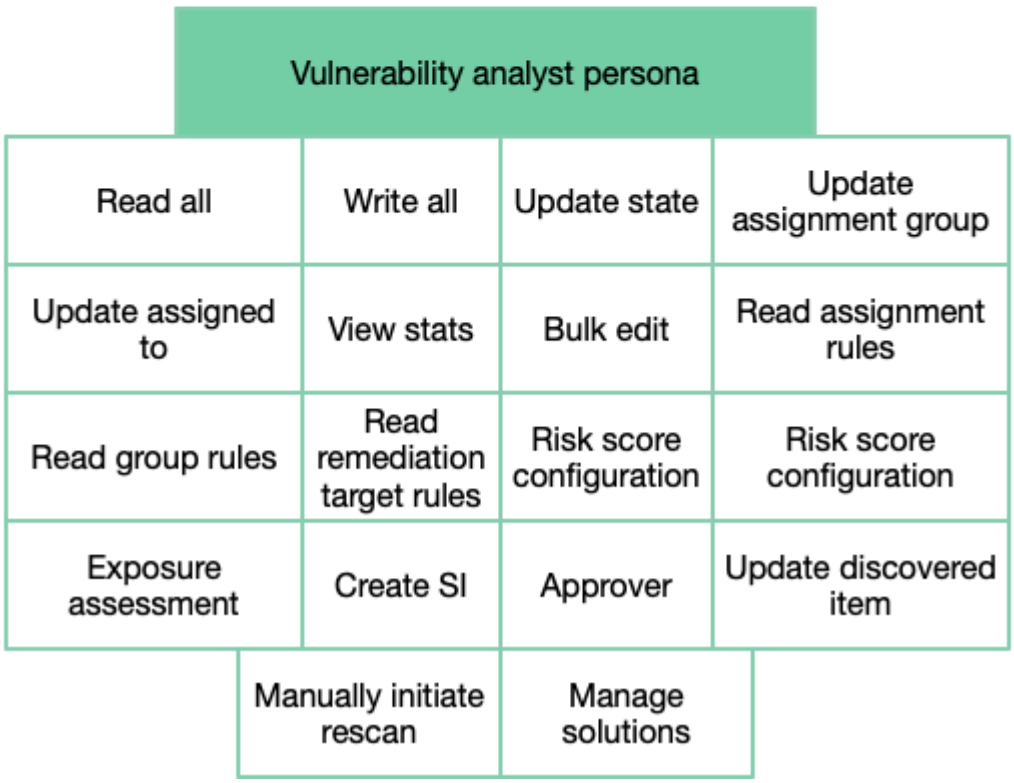
Na imagem a seguir, as funções granulares da persona do responsável pela correção e da persona do analista de vulnerabilidade são ilustradas. Observe que a persona do responsável pela correção não inclui as permissões read_all e write_all da persona do analista de vulnerabilidades. As funções granulares, read_all e write_all, são necessárias para que usuários e grupos possam ler e editar todos os registros de item vulnerável e tarefa de correção. Para personalizar essas funções, basta adicionar ou remover funções granulares para expandir ou limitar o acesso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções granulares e as personas do responsável pela correção e do analista de vulnerabilidades





Se você quiser que seus usuários e grupos tenham mais acesso do que as funções de persona permitem, você poderá adicionar funções mais granulares a usuários e grupos. Por outro lado, se você quiser limitar o acesso de usuários e grupos específicos no nível da tarefa, poderá remover funções granulares.

Nota: Para atribuir e editar funções granulares no módulo Administração de usuários, a função de administrador do sistema é necessária.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções granulares no módulo Administração de usuários

Para obter um exemplo de como gerenciar funções granulares para um usuário ou grupo, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Para atribuir funções de persona, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Resposta a vulnerabilidades visão geral das regras de atribuição

Defina os critérios pelos quais os itens vulneráveis (VITs) são atribuídos automaticamente a um grupo de atribuição para correção.

Uma regra de atribuição padrão, **Atribuir ao grupo de suporte de IC**, está incluída no sistema de base que atribui itens vulneráveis ao **grupo de suporte de IC**. A regra Atribuir ao grupo de suporte de IC atribui um VIT a qualquer grupo de suporte definido para o item de configuração (IC) associado ao VIT.

Nota: As regras de atribuição não reavaliam atribuições criadas manualmente.

O tipo de atribuição, seja **Manual** ou **Regra**, está disponível no formulário VIT e na exibição de lista. Qualquer VIT que foi atribuído originalmente por uma regra, mas posteriormente reatribuído manualmente, contém uma referência à regra original.

Use as informações de Regra de atribuição e Tipo de atribuição para identificar casos em que as regras de atribuição não encontraram uma correspondência correta para o destinatário pretendido. Você também pode usar as informações para identificar quais regras tiveram mais reatribuições.

Os grupos de atribuição definidos por Regras de atribuição são usados por **Regras de tarefa** de correção para atribuir proprietários a Tarefas de correção (VULs).

Nota: Para disponibilizar Rapid7 InsightVM etiquetas do ativo para uso no filtro de condição para Regras de atribuição, você deve executar a integração da lista de ativos Rapid7 InsightVM antes das outras integrações Rapid7 InsightVM.

A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.

Atribuindo itens vulneráveis automaticamente

Existem três maneiras diferentes de atribuir itens vulneráveis usando **Atribuir usando**:

- Grupode usuários : esta opção permite selecionar qualquer um dos grupos de usuários Now Platform® existentes.
- Campo de grupo deusuários : esta opção permite que você escolha qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir:
  - Nenhum: indica que não há valor padrão para este campo obrigatório
  - Item de configuração: grupo de aprovação
  - Item de configuração: grupo de atribuição
  - Item de configuração: grupo de suporte
- Script: esta opção permite definir as condições usando um script. Esta opção requer codificação ou conhecimento avançado ServiceNow. Para obter mais informações sobre como usar o editor de script para definir condições complexas, consulte o artigo KB0965240 da base de conhecimento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Execute regras de alta prioridade (itens que precisam de tratamento especial, onde o risco é crítico ou um VIT deve ser tratado pela conformidade regulatória) primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir VITs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.

Processo de avaliação da regra de atribuição

Regras de atribuição são usadas para avaliar e atribuir um VIT quando um novo VIT é aberto, ou seja, importado, criado manualmente ou reaberto. A menos que você reaplique manualmente as regras de atribuição após o VIT ou seu estado mudar, um IV será avaliado uma vez.

O processo a seguir é usado para cada VIT novo, atualizado ou reaberto:

- Para cada regra de atribuição de vulnerabilidade, o VIT é comparado ao filtro de atribuição, com a regra de ordem mais baixa primeiro.
- Quando a condição corresponde, o VIT é atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Onde as condições não encontrarem uma correspondência entre todas as outras regras, o VIT será atribuído ao grupo de atribuição padrão, se houver uma regra padrão.

  Depois que o item vulnerável é atribuído, a regra de tarefa de correção apropriada usa a atribuição como um de seus critérios para colocar os itens vulneráveis em uma tarefa de correção. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral e Filtrando em Resposta a vulnerabilidades.

  Nota: A regra padrão é a regra com o maior valor de ordem de execução. Uma regra final a ser usada que é um bom contato é `active=true`. Se não houver regra padrão, o VIT permanecerá não atribuído quando a regra da tarefa de correção fizer a atribuição.

Reaplicando regras de atribuição

Ao alterar uma regra de atribuição, use o botão **Aplicar mudanças** na página da lista Regras de atribuição para executar novamente todas as regras alteradas em todos os VITs abertos ativos, exceto aqueles que foram atribuídos manualmente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se o *Reapply all vulnerability assignment rules* trabalho agendado não tiver sido executado antes da primeira vez que você usar **Aplicar mudanças**, ele executará todas as regras de atribuição em todos os VITs abertos, exceto os IVs que foram atribuídos manualmente. Depois disso, todos os usos subsequentes de **Aplicar mudanças** executam novamente somente as regras alteradas e quaisquer regras dependentes. As mudanças em uma regra podem resultar em um VIT correspondendo a uma regra não modificada diferente. A reaplicação de regras de atribuição não reagrupa os itens vulneráveis.

O trabalho agendado [*Reapply all vulnerability assignment rules*] está inativo por padrão. Quando ativado, ele aplica todas as regras a todos os VITs abertos, exceto aqueles atribuídos manualmente. Ele pode ser executado **Diariamente**, **Semanalmente**, **Mensalmente**, **Periodicamente**, **Uma vez**ou **Sob demanda**. Dependendo de quantos IVs ativos você tiver em seu ambiente, lembre-se de definir o campo **Executar** corretamente após a execução inicial para evitar impactos no desempenho.

Os clientes de upgrade devem consultar as Resposta a vulnerabilidades Notas de versão para obter informações sobre o impacto deste recurso nos VITs existentes.

Importante: Como administrador e analista de vulnerabilidades, você pode obter as atribuições mais recentes dos itens vulneráveis selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que executar as Regras de atribuição para todos os itens vulneráveis na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Quando um grupo de atribuição em uma regra de atribuição muda, os itens vulneráveis podem ser reavaliados e reagrupados automaticamente, habilitando a propriedade do sistema sn_vul.rerun_task_rules e a regra de negócio Link para Tarefas de correção.

Para habilitar a propriedade do sistema:

1. Navegar até **Todos** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Abra a propriedade do sistema sn_vul.rerun_task_rules.
3. No campo **Valor**, defina o valor como verdadeiro.

Quando a propriedade do sistema é definida como verdadeira e as regras de atribuição são reaplicadas, os itens vulneráveis são desvinculados das tarefas de correção, onde a condição não corresponde mais.

Nota: Por padrão, a propriedade do sistema sn_vul.rerun_task_rules é definida como falsa.

Para automatizar o reagrupamento de itens vulneráveis, você deve ativar a regra de negócio Vincular tarefas de correção.

Para habilitar a regra de negócio:

1. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócio**.
2. Abra a regra de negócio Link para Tarefas de correção.
3. Marque a caixa de seleção **Ativo** para ativar a regra de negócio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A regra de negócio ao ser habilitada reagrupa os itens vulneráveis movendo-os para o grupo relevante ou criando um grupo se eles não puderem ser agrupados em nenhum grupo existente.

Nota:

- Os itens vulneráveis são removidos dos grupos sem excluir os grupos.
- Somente os itens criados usando regras de tarefa de correção ou esforço de correção são removidos.
- O reagrupamento é feito automaticamente somente quando o grupo de atribuição muda como parte de uma regra de atribuição e não quando é alterado manualmente.

O reagrupamento em espaços é realizado para tarefas de correção, que são criadas a partir de um esforço de correção.

Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral

Configure tarefas de correção (VULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis (VI) e analisá-los em massa. Os critérios pelos quais as tarefas de correção são formadas são configurados para que você não precise atribuir manualmente itens vulneráveis em tarefas de correção. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Acompanhar contagens de adiamento para itens vulneráveis e tarefas de correção

Rastreie o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou uma tarefa de correção foi adiado. Um trabalho agendado, **definir contagens de adiamento**, é executado diariamente para publicar contagens dos registros que foram adiados mais de uma vez na coluna Contagem de adiamento. Os registros são exibidos nos módulos de vários adiamentos para VR, AVR e CVR.

Atualizando itens vulneráveis automaticamente

Nota: A automação de atualização de item vulnerável se aplica somente a tarefas de correção criadas usando o filtro de condição ou o grupo de filtros. A automação não se aplica a IVs que foram adicionados manualmente ou agrupados usando Regras de tarefa de correção.

Quando a caixa de seleção **Atualizar automaticamente itens vulneráveis relacionados** estiver marcada, novos IVs correspondentes aos critérios de filtro da tarefa de correção serão adicionados automaticamente à tarefa. Itens vulneráveis na tarefa de correção que não correspondem mais aos critérios de filtro são removidos automaticamente da tarefa.

Por padrão, quando a tarefa de correção deixa o estado **Aberto**, a caixa de seleção é desmarcada. Se você quiser que os itens vulneráveis continuem sendo adicionados à tarefa de correção, independentemente do estado, desabilite a regra de negócio *`Set auto refresh vulnerable items`*.

Você pode marcar a caixa de seleção novamente manualmente no estado Sob investigação. **A atualização automática de itens vulneráveis relacionados** não é desabilitada quando a tarefa de correção passa para o estado **Aguardando implementação**. Uma vez no estado Aguardando implementação, nenhum novo item vulnerável poderá ser adicionado à tarefa existente, nem itens vulneráveis existentes poderão ser removidos dela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando uma tarefa de correção é criada manualmente e os IVs são adicionados usando o filtro **Condição** ou o **Grupo**de filtros , a caixa de seleção é desmarcada. Você tem a opção de marcar a caixa ou não.

Atualizando itens vulneráveis manualmente

Para tarefas de correção criadas manualmente com um **filtro de grupo** ou **condição**, quando você clica no link relacionado **Atualizar** itens vulneráveis associados na página **Tarefa** de correção, todos os itens vulneráveis que correspondem aos critérios de filtro são adicionados. Os itens que não correspondem mais aos critérios são removidos. Esta ação permite uma atualização imediata da lista de itens vulneráveis e é usada independentemente de a caixa de seleção **Atualizar automaticamente os itens vulneráveis relacionados** estar marcada ou não.

As tarefas de correção criadas manualmente usando os tipos de filtro **Condição** ou **Grupo** de filtros são atualizadas uma vez por hora.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem definir como os itens vulneráveis são agrupados e atribuídos automaticamente. Uma regra padrão, **Vulnerabilidade**, está incluída no sistema de base que reúne itens vulneráveis com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis a partir do VI. Esses valores podem incluir grupo de suporte de item de configuração (IC), gravidade da vulnerabilidade e assim por diante.

Você pode criar qualquer número de condições. Depois de definir uma seleção de Agrupar por, outra linha será exibida. Você pode ter até seis seleções **de Agrupar por**. Você também pode automatizar a atribuição de grupo. Para obter mais informações, consulte Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção e Filtrando em Resposta a vulnerabilidades.

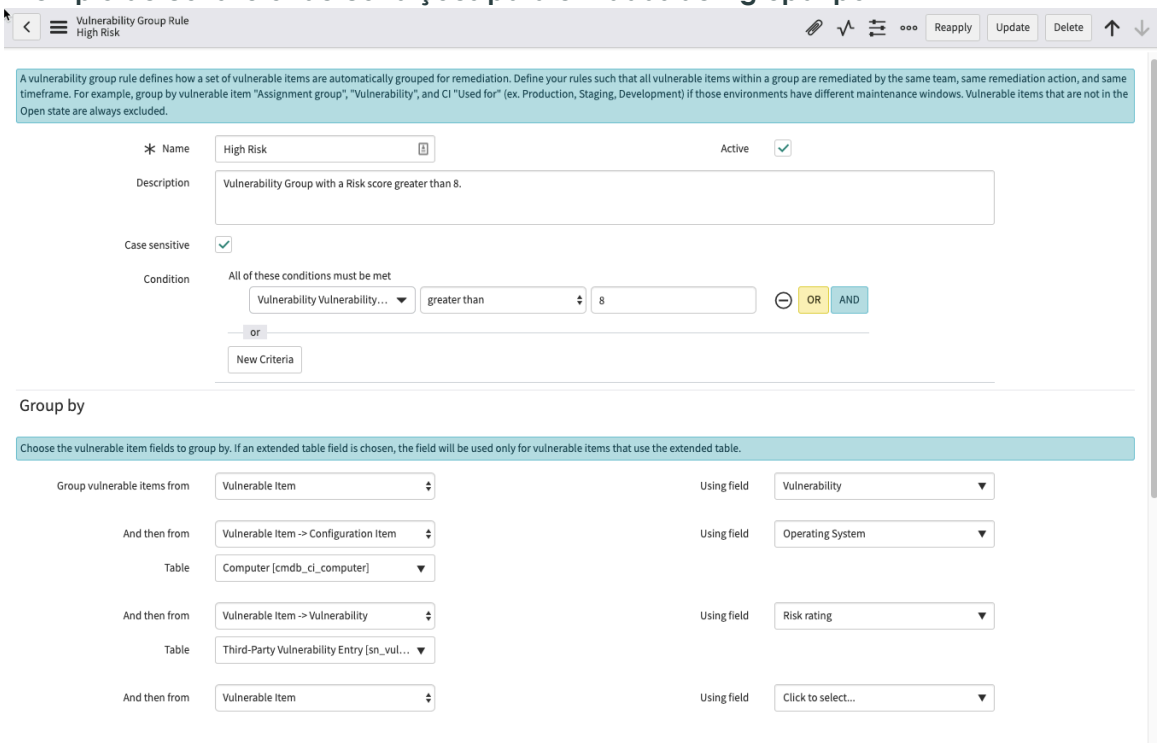
Nota: Para disponibilizar Rapid7 InsightVM etiquetas do ativo para uso no filtro de condição das Regras da tarefa de correção, você deve executar a integração da lista de ativos Rapid7 InsightVM antes das outras integrações Rapid7 InsightVM.

Por exemplo, você pode agrupar seus itens vulneráveis pelo centro de custos do IC vulnerável ou pelo vetor de ataque da vulnerabilidade. Você pode ter uma regra de tarefa para vulnerabilidades de baixa gravidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades com explorações - itens vulneráveis que expõem a empresa a mais riscos.

Um conjunto diferente de regras pode ser usado para itens vulneráveis que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado aos valores **Agrupar por** da regra da tarefa de correção para fazer a descrição resumida do novo registro. Consulte Criar manualmente uma tarefa de correção no Resposta a vulnerabilidades para obter mais informações sobre os campos disponíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de construtor de condições para entradas de Agrupar por



Quando um novo item vulnerável é criado, importado ou reaberto após ser fechado, as regras de vulnerabilidade são avaliadas em relação a ele. Um VI é avaliado apenas uma vez, automaticamente, a menos que seja reaberto após ser fechado ou as regras sejam reaplicadas manualmente.

O processo a seguir é usado para cada VI novo ou reaberto:

- Para cada regra de tarefa de correção, o VI é comparado ao filtro de regra de tarefa de correção.

- Para cada regra em que a condição da regra da tarefa de correção corresponde, a regra extrai os dados das seleções **Agrupar por** no VI. Ele cria um nome de grupo e um campo. Nesse caso, **Alto risco: QID-32342:** *resumo de QID-3242* (Nome: ID da vulnerabilidade: resumo da vulnerabilidade).

  Nota: O campo de descrição resumida está limitado a 160 caracteres. Resumos de vulnerabilidade mais longos são truncados.

  A regra verifica se há uma tarefa de correção **aberta** correspondente que esteja atribuída ao mesmo grupo de atribuição que o VI.

  - Se a tarefa for encontrada, o VI será adicionado à tarefa existente no estado **Aberto**.
  - Se nenhuma tarefa no estado **Aberto** for encontrada, a regra criará uma tarefa **de alto risco: QID-32342**, a atribuirá ao mesmo grupo de atribuição do VI e colocará o VI na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições da regra da tarefa de correção antes de ser colocada em uma tarefa de correção, muitas regras podem afetar o desempenho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelas **Regras de atribuição** no item vulnerável ao agrupar os itens e atribui a tarefa de correção para corresponder aos itens vulneráveis.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras no módulo **Regras de atribuição**. Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Quando uma regra de tarefa é excluída, no formulário ou na exibição de lista, você tem a opção de excluir todas as tarefas **Abertas** criadas por essa regra. As tarefas que não estão em **Aberto** são excluídas.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use o botão **Reaplicar** na página de regra de tarefa de correção para executar novamente a regra alterada em todas as tarefas de correção em **aberto** ativas criadas por essa regra. Ele exclui e recria automaticamente as tarefas de correção com base na regra alterada.

Importante: Como administrador e analista de vulnerabilidades, você pode avaliar as regras de tarefa de correção para itens vulneráveis selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que reaplicar as Regras de tarefa de correção na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Resposta a vulnerabilidades regras de destino de correção

As regras de destino de correção definem o intervalo de tempo esperado para corrigir itens vulneráveis (VI), assim como os SLAs fornecem um intervalo de tempo para corrigir a própria vulnerabilidade. Por exemplo, se um ativo contiver dados PCI (dados de cartão de crédito), a vulnerabilidade nesse item precisará ser corrigida em 30 dias de acordo com o PCI DSS.

Os gerentes de vulnerabilidade podem criar regras de meta de correção definindo:

- A meta de correção
- O destino do lembrete
- Os destinatários do lembrete e da notificação - que devem ser notificados quando os itens vulneráveis (IVs) passarem da data de meta de lembrete ou correção e não tiverem sido corrigidos.

Os analistas e gerentes de vulnerabilidade podem ver a data da meta de correção no formulário do item de vulnerabilidade e nas exibições de lista, desde que os itens vulneráveis não estejam no estado **Adiado**, **Resolvido**ou **Encerrado**. As regras de destino de correção são executadas na importação e executadas novamente se um IV for reaberto.

A **data da meta** de correção é codificada por cores na exibição de lista VI como pontos, da seguinte forma:

- Itens vulneráveis que não atingiram a data de notificação são mostrados em verde.
- Itens vulneráveis que se aproximam da data de meta de correção são mostrados em laranja.
- Itens vulneráveis após a data de meta de correção são mostrados em vermelho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um e-mail de resumo, por regra de meta de correção, é enviado quando um ou mais IVs estão se aproximando da data de meta de correção ou quando a data de meta de correção já passou.

As regras de destino de correção podem ser desativadas ou excluídas

Quando uma regra é desativada, as datas de meta de correção atuais dos IVs aos quais ela foi aplicada são apagadas. Se um VI atender a qualquer regra ativa, essa regra será aplicada, caso contrário, o VI não terá uma regra ou data de destino e seu status será **No Target**.

Quando as regras são excluídas, a data de **meta** de correção e os campos relacionados em IVs encerrados, adiados ou resolvidos são preservados. A data de **meta** de correção e os campos relacionados em IVs não encerrados são limpos e todas as regras dependentes são reaplicadas.

Cenário da regra de meta de correção

Quando várias regras de destino de correção são aplicadas ao mesmo item vulnerável, a regra mais restritiva é aplicada.

Nota: As metas de correção são calculadas a partir da data da **última abertura** mais o número de dias (medidos como incrementos de 24 horas).

A partir da V17.1, as metas de correção são calculadas a partir da **meta de (data)**. O valor padrão permanece **Data da última abertura**.

Por exemplo, se um item vulnerável atender à condição de duas regras de meta de correção:

Cenário: item vulnerável aberto pela última vez em 01/03/2018 às 10:00:00.

- Regra de meta de correção 1: Aberto pela última vez em 03/07/2018; a meta de correção é de 15 dias desde que foi aberta pela última vez; A data da meta de correção calculada é 16/03/2018 10:00:00.
- Regra de meta de correção 2: Aberto pela última vez em 10/03/2018; a meta de correção é de 10 dias desde que foi aberta pela última vez; A data da meta de correção calculada é 11/03/2018 10:00:00.

Neste cenário, a Regra de meta de correção 2 se aplica ao item vulnerável, já que ele tem a data mais restritiva. 10 dias desde que o item vulnerável foi identificado pela primeira vez versus 15 dias.

Nota: Depois que a regra de meta de correção é definida, as datas de meta de correção são calculadas pelo trabalho agendado *`Evaluate remediation targets`* .

Sobre o trabalho agendado Avaliar metas de correção

`Evaluate remediation targets` é executado uma vez às 4:00:00 diariamente.

Ele itera por meio de todas as regras de vulnerabilidade ativas, começando com as regras com a data de meta de correção mais antiga. Ele verifica todos os itens vulneráveis que:

- Não estão em um estado **Encerrado**, **Adiado**ou **Resolvido**.
- Não têm data de meta de correção.
- Ter uma data de meta de correção posterior à data na regra de meta de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Evaluate remediation targets adiciona uma data de meta de correção, se não existir uma, ou se uma regra resultar em uma data anterior à do registro, ele atualizará a data de meta existente. Por fim, ele atualiza os campos **Meta** de **correção e Status** da correção no formulário de item vulnerável.

Depois que o *Evaluate remediation targets* é executado, as notificações disponíveis são enviadas.

Evaluate remediation targets limpa os campos de correção no IV e interrompe o envio de notificações.

A partir da versão Resposta a vulnerabilidades v19.0, a propriedade *sn_sec_cmn.evaluate_targetmissed_records*, quando habilitada, evita que o trabalho agendado *Remediation Target Rules*] avalie IVs ausentes. Esta propriedade está habilitada por padrão.

Reaplicar regras de destino de correção

Ao alterar uma regra de destino de correção, use o botão **Aplicar mudanças** na página da lista Regras de destino de correção para executar novamente todas as regras alteradas em todos os VIs abertos ativos, exceto aqueles no estado **Encerrado**, **Adiado** ou **Resolvido**. Dependendo de quantos IVs você tiver, isso pode levar algum tempo.

Nota:

Se o trabalho agendado, *Evaluate remediation targets* estiver em execução, você não poderá iniciar um processo de reaplicação. No entanto, se um processo de reaplicação já estiver em execução e o trabalho agendado que ele acionou, eles serão executados em paralelo.

Os processos de reaplicação em Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações são independentes e podem ser executados em paralelo.

Importante: Como administrador e analista de vulnerabilidades, você pode obter a data da meta de correção mais recente para itens vulneráveis selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que executar as Regras de destino de correção para todos os itens vulneráveis na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Informações relacionadas

Criar ou editar Resposta a vulnerabilidades regras de destino de correção

Exibir o status da meta de correção de um Resposta a vulnerabilidades item vulnerável

Criar ou editar notificações de meta de correção

Grupos e regras de classificação de vulnerabilidade

Os grupos de classificação automatizam a classificação de valores de uma tabela com base nas regras de classificação definidas no grupo. A condição de cada regra é avaliada na ordem e a primeira regra correspondente é usada.

O sistema de base da Resposta a vulnerabilidades inclui os dois grupos de classificação a seguir, que classificam itens descobertos e vulnerabilidades, respectivamente:

- Classificação de itens descobertos
- Classificação de entrada de vulnerabilidade

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sempre que vulnerabilidades e itens descobertos são importados, as regras de classificação de vulnerabilidade nos respectivos grupos são executadas. Com base nas condições definidas na regra, os registros são classificados para o grupo de classificação relevante. Você pode criar, editar, excluir ou reaplicar essas regras a uma vulnerabilidade existente.

Nota:

- Para uma tabela selecionada, só pode haver um grupo de classificação ativo.
- Depois de criar um grupo, você não poderá excluí-lo.

Para obter mais informações, consulte Criar e editar uma regra de classificação, Aplicar uma regra a uma vulnerabilidade existente e Desativar ou excluir uma regra de classificação.

Soluções de aprendizado de máquina para Resposta a vulnerabilidades

Recomendações de atribuição de vulnerabilidade usa ServiceNow® Inteligência preditiva e aprendizado de máquina para recomendar grupos de atribuição para itens vulneráveis (IVs) e tarefas de correção (VULs ou RTs). Você pode reduzir o tempo gasto na identificação dos proprietários de descobertas de vulnerabilidades não atribuídas ou atribuídas incorretamente. Além disso, você pode ver uma pontuação de confiança gerada pelo sistema que avalia se o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade.

As capacidades Inteligência preditiva são usadas em Resposta a vulnerabilidades para fornecer melhores experiências de trabalho, criando e treinando um modelo de definição de solução que pode prever o grupo de atribuição com base nos dados existentes.

Para obter mais informações, consulte Inteligência preditiva .

Recomendações de atribuição de vulnerabilidade

Com a aplicação Recomendações de atribuição de vulnerabilidade (com.snc.vulnerability.recom), o sistema pode atribuir recomendações em Resposta a vulnerabilidades usando ServiceNow Inteligência preditiva. Este plug-in requer:

- Resposta a vulnerabilidades (`com.snc.vulnerability`)
- Inteligência preditiva (`com.glide.platform_ml`)

Para obter mais informações, consulte Inteligência preditiva .

Pontuações de confiança

Use a aplicação Recomendações de atribuição de vulnerabilidade para gerar a pontuação de confiança que relata o nível de confiança dos grupos de atribuição recomendados para os RTs ou VIs selecionados. A pontuação de confiança avalia se o sistema está confiante de que o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade. São exibidas até 10 recomendações. Essas recomendações são baseadas na maior probabilidade de atribuições bem-sucedidas. A primeira recomendação na lista significa que o sistema tem a maior confiança de que é o grupo de atribuição correto.

Por exemplo, em uma escala de 0 a 100, para cada grupo de atribuição, a pontuação de confiança sugere a probabilidade de um VI ou RT pertencer a esse grupo específico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

- Inteligência preditiva
- Criar e treinar uma solução de classificação
- Criação e treinamento de uma solução de semelhança
- Criação e treinamento de uma solução de clustering
- Definição de configurações avançadas para suas soluções de ML

Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros

Quando os dados são importados de uma integração de terceiros, o Resposta a vulnerabilidades usa automaticamente os dados do host para pesquisar correspondências no Configuration Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras são usadas para identificar itens de configuração (ICs) e adicioná-los ao registro de item vulnerável para ajudar na correção.

A partir da versão 19.0, navegue até **Operações de segurança** > **CMDB** > **Regras de pesquisa** para localizar a lista em sua instância.

Conforme os ativos são importados, uma pesquisa é realizada primeiro na lista de **itens descobertos** usando IDs de terceiros para encontrar correspondências com os itens de configuração (ICs) de importações anteriores. Quando uma correspondência de ID de host é encontrada, ela é usada como o campo **Item de configuração** no registro do item vulnerável.

Você pode ver como os ativos importados são mapeados para ICs usando a lista de **Itens descobertos**. Se uma correspondência não for encontrada ou o campo ID do host estiver vazio, as regras usarão as outras informações do host para tentar identificar corretamente o IC. Se uma correspondência ainda não for encontrada, um IC de espaço reservado será criado e designado como **IC incompatível**. Consulte ICS incompatíveis para obter mais informações sobre como esses ICs são tratados.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Cada origem pode ter várias implantações.

Nota: As regras de pesquisa de IC são compartilhadas por todas as implantações da integração de origem da vulnerabilidade. Se uma regra for excluída ou modificada, a exclusão ou as mudanças afetarão todas as implantações da integração de vulnerabilidade.

Ao tentar uma correspondência, a primeira etapa é uma pesquisa de ID de fornecedor para uma correspondência exata entre origem, source_instance e ID de fornecedor. Em seguida, as regras de pesquisa são executadas em ordem, da menor para a maior, e param quando uma regra retorna apenas um único IC como uma correspondência. Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Nota: Para evitar a correspondência em elementos de network de baixo nível, se um IC correspondente for `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic` ou `cmdb_ci_ip_address`, o IC primário será retornado.

Uma propriedade do sistema para excluir classes de IC está disponível. Esta propriedade não está disponível com atualização. Consulte Ignorar classes de IC para obter informações de atualização e instruções sobre como definir a propriedade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para facilitar a localização de problemas de correspondência, quando uma correspondência for encontrada, a regra de pesquisa de IC usada para localizá-la será adicionada ao registro de item descoberto no campo **Regra de correspondência de IC**. As regras de pesquisa são avaliadas primeiro pelo menor valor de **Pedido**.

Essas regras Qualys de pesquisa de IC são enviadas com o sistema de base.

- ID DE HOST DA QUALYS
- FQDN
- NetBIOS
- DNS
- IP

Essas regras Rapid7 de pesquisa de IC são enviadas com o sistema de base.

- MACAddress
- FQDN
- HostName
- IP

Essas regras de pesquisa de IC da Tenable.io são enviadas com o sistema de base.

- FQDN
- NETBIOS
- HOSTNAME
- MACAddress
- DNS

Essas regras de pesquisa de IC da Tenable.sc são enviadas com o sistema de base.

- MACAddress
- FQDN
- NETBIOS

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência dentro do CMDB pode resultar em longos tempos de processamento. Para evitar qualquer degradação potencial de recursos ou complicações de desempenho, teste todas as regras de pesquisa de IC personalizadas ou modificações nas **regras de pesquisa de IC** predefinidas. Consulte Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Resposta a vulnerabilidades regras de pesquisa de IC para obter mais informações sobre como evitar registros órfãos duplicados, excluir dados e limpar dados.

Nota: Para obter informações sobre a correspondência de IC, consulte KB0998706 .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicar novamente as regras de pesquisa de IC atualizadas

Ao alterar uma regra de pesquisa de IC, clique em **Aplicar mudanças** na página da lista Regras de pesquisa de IC para executar novamente todas as regras nos itens descobertos que:

- Foram correspondidos pelas regras atualizadas
- Não são correspondidos por nenhuma regra

Se o item de configuração (IC) mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. As detecções afetadas e os itens vulneráveis também são atualizados. Para obter mais informações, consulte Reaplicar regras de pesquisa de IC em itens descobertos selecionados.

Hardware não classificado

Se um ativo não encontrar uma correspondência em Configuration Management Database (CMDB) pelas regras de pesquisa de IC, o ativo será denominado como um hardware sem classe.

Quando os dados são importados de ServiceNow integrações criadas, Resposta a vulnerabilidades usa automaticamente os dados do host para pesquisar correspondências no CMDB. As regras de pesquisa de IC são usadas para identificar itens de configuração (ICs) e adicioná-los ao registro de item vulnerável para ajudar na correção. Se os ativos não forem encontrados no CMDB, o Mecanismo de identificação e reconciliação (IRE) executará suas próprias regras de identificação definidas na classe de hardware e em todos os seus secundários e criará um IC em uma classe de hardware não classificada. Quando Descoberta encontra este ativo, em vez de reclassificar o hardware não classificado existente, ele cria um IC. Isso ocorre porque a regra de identificação depende do nome do IC de hardware.

Se o Mecanismo de identificação e reconciliação (IRE) estiver ativado, a opção de reclassificação de itens descobertos não será compatível.

As extrações a seguir mostram a carga do IRE para criar IC em hardware não classificado por meio de Resposta a vulnerabilidades e Descoberta, respectivamente.

```
"className": "cmdb_ci_unclassed_hardware",

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

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

```
"className": "cmdb_ci_cmdb_ci_win_server"

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

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

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

Nesse caso, o IC de hardware não classificado existente não é reclassificado para o servidor Windows e, em vez disso, um novo IC no servidor Windows é criado. O motivo é que a regra de identificação depende do nome do IC de hardware. Se você observar as cargas úteis, o nome na carga útil de Resposta a vulnerabilidades é o mesmo que FQDN/NETBIOS, mas é apenas o nome do host da carga útil de Descoberta.

Informações relacionadas

Reclassificar hardware não classificado

ICS incompatíveis

Os itens de configuração (ICs) são correspondidos automaticamente com os ICs no Configuration Management Database (CMDB) quando são importados. Por padrão, o **Operações de segurança** > **CMDB** > **Itens Descobertos** O módulo lista os itens de configuração sem uma correspondência.

Se você achar que um IC incompatível pertence a uma classe existente no CMDB, revise suas regras de pesquisa de IC. Caso contrário, considere reclassificar o item de configuração.

Nota: O filtro padrão para esta lista está definido como **Incompatível**. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Se o Mecanismo de identificação e reconciliação (IRE) estiver ativado, a opção de reclassificação de itens descobertos não será compatível.

Informações relacionadas

Exibir e reclassificar itens de configuração incompatíveis

Reconciliar itens descobertos sem correspondência

Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Resposta a vulnerabilidades regras de pesquisa de IC

Desduplicação de itens de configuração existentes

Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação

Você pode criar itens de configuração (ICs) no Configuration Management Database (CMDB) usando a API do Mecanismo de identificação e reconciliação (IRE). Ao usar a API do IRE para criar ICs, você pode impedir a criação de ICs duplicados e reconciliar atributos de IC permitindo que somente fontes de dados autorizadas gravem em CMDB.

Uma classe de IC (tabela) é o nome da tabela original no banco de dados da instância. CMDB contém classes do sistema de base que armazenam dados sobre ICs.

Como usar o IRE para criação de IC

Antes de Resposta a vulnerabilidades v12.2, se um IC correspondente não for encontrado na lista Itens descobertos ou CMDB, um IC será criado na classe de IC incompatível (`sn_sec_cmn_unmatched_ci`). Para obter mais informações, consulte ICs incompatíveis.

A partir de Resposta a vulnerabilidades v12.2 a v18.0, se nenhuma correspondência for encontrada quando as regras de pesquisa de IC forem aplicadas, as informações do ativo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

serão enviadas para o IRE e um IC será criado em uma das *classes de hardware não classificado* e *dispositivo identificado por IP incompleto*. A partir da Resposta a vulnerabilidades v18.0, uma nova classe, *Cloud Resource*, também está incluída. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos em nuvem incompatíveis.

Classes de IC do CMDB

Nota: Para usar as novas classes, ative o plug-in CMDB CI Class Models. Caso contrário, os ICs serão criados na classe de IC incompatível.

Se o host que você importou de um scanner de terceiros não puder ser encontrado na lista de itens descobertos ou CMDB, ele será criado em uma das seguintes novas CMDB classes de IC.

Classes de IC do CMDB

CMDB **Classe de IC**	**Descrição**
Dispositivo identificado com IP incompleto (*cmdb_ci_incomplete_ip*)	O IC será criado nesta tabela se somente o endereço IP estiver disponível nas informações de host que são recebidas do scanner.
Hardware não classificado (*cmdb_ci_unclassed_hardware*)	O IC será criado nesta tabela se qualquer uma das seguintes informações estiver disponível nas informações de host que são recebidas do scanner: • Nome do host • Endereço IP • DNS • NETBIOS • Endereço MAC **Nota:** Se o endereço MAC estiver disponível, a entrada do adaptador de rede será criada e relacionada ao IC de hardware não classificado. Se os endereços IP e MAC estiverem disponíveis, o IC do endereço IP também será criado e relacionado ao IC de hardware não classificado.
Recurso de nuvem (*cmdb_ci_cmp_resource*)	O IC será criado nesta tabela se *Cloud Resource ID* estiver disponível nas informações de host que são recebidas do scanner.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Classes de IC do CMDB

CMDB **Classe de IC**	**Descrição**
	Nota: Se o Tipo de ativo de uma integração de scanner for *Híbrido* e a propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled* for falsa, os ICs serão criados na classe *Hardware* sem classe, mas não na classe *Recurso de nuvem*.

Se o Mecanismo de identificação e reconciliação (IRE) estiver ativado, a opção de reclassificação de itens descobertos não será compatível.

O sistema usará automaticamente uma classe de IC incompatível se ocorrer uma das seguintes situações:

- O plug-in CMDB de classe de IC não está ativado.
- O IRE gera uma exceção ao criar um IC.

  Para obter mais informações, consulte ICs incompatíveis.

Informações relacionadas

Aplicação da Store dos Modelos de classe de IC do CMDB

Mecanismo de Identificação e Reconciliação (IRE)

Atualizando classe de IC para ativos em nuvem incompatíveis

A partir da Resposta a vulnerabilidades v20.0, você pode categorizar os ativos de nuvem incompatíveis dos scanners Qualys, Rapid7 e Tenable em *hardware não classificado* usando a propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled*.

Esta propriedade do sistema com `falso` como valor padrão é enviada com o sistema de base. Ele classifica os ativos de nuvem incompatíveis em uma *classe de hardware não classificado* (*cmdb_ci_unclassed_hardware*) ou *recurso de nuvem* (*cmdb_ci_cmp_resource*) para as integrações que agregam ativos de infraestrutura e nuvem.

A partir de Resposta a vulnerabilidades v20.0, a coluna Tipo de ativo é adicionada à tabela Integrações de terceiros (`sn_sec_int_integration`) para identificar as integrações que oferecem suporte a ativos de infraestrutura e nuvem. A coluna Tipo de ativo tem o valor *Híbrido* para os scanners que recuperam ativos de infraestrutura e de nuvem. Por exemplo, as integrações Qualys, Rapid7 e Tenable têm o valor como *Híbrido* na coluna Tipo de ativo.

- Para a nova instalação de Resposta a vulnerabilidades v20.0 e superior, todos os ativos de nuvem incompatíveis são categorizados em:
  - *Classe de hardware não* classificada por padrão.
  - Classe *Recursos de nuvem*, se você alterar a propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled* para `verdadeira`.
- Para upgrades para Resposta a vulnerabilidades v20.0:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se houver ativos na classe *Recurso de nuvem*, a propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled* será definida como verdadeira para que os ativos de nuvem incompatíveis continuem a ser adicionados à classe *Recurso de nuvem* (*cmdb_ci_cmp_resource*).
- Caso contrário, a propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled* será definida como falsa para que os ativos de nuvem incompatíveis sejam categorizados na classe de *hardware sem* classe.

Nota: Se você modificar o valor da propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled*, certifique-se de excluir itens de configuração incompatíveis na classe de IC de destino anteriormente e reaplicar as regras de pesquisa. Para saber mais sobre como excluir os ICs existentes e reaplicar as regras de pesquisa de IC para que os novos ICs sejam criados na classe correta, consulte KB1533376 .

Itens Descobertos

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) no Configuration Management Database (CMDB) quando são importados usando **Regras de pesquisa de IC**. Os itens descobertos fornecem visibilidade sobre como a identificação de ativos é mapeada para ICs no CMDB.

Os Itens Descobertos são considerados **Correspondidos**, **Não Correspondidos**ou **Reclassificados**. Os ICs identificados estão no estado **Correspondido**.

Para facilitar a localização de possíveis problemas de correspondência, a regra de pesquisa de IC que correspondeu ao IC aparece no campo **de regra de correspondência de IC**.

Por padrão, o **Operações de segurança** > **CMDB** > **Itens Descobertos** O módulo lista itens de configuração incompatíveis. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter uma descrição dos campos em Itens descobertos, consulte Campos de formulário de Itens Descobertos. Para obter mais informações sobre como reconciliar itens descobertos incompatíveis e reaplicar regras de pesquisa de IC em itens descobertos selecionados, consulte Reconciliar itens descobertos sem correspondência e Reaplicar regras de pesquisa de IC em itens descobertos selecionados, respectivamente.

Mudanças de IC para itens descobertos

Quando um item de configuração (IC) em um item descoberto (DI) muda, as detecções afetadas e os itens vulneráveis (IVs) são atualizados. A pontuação de risco, as regras de atribuição, as regras de grupo e a regra de meta de correção são reavaliadas.

Se existir um VI com a mesma vulnerabilidade e IC, as detecções serão atualizadas com o VI existente e o VI atual será encerrado com o subestado como `invalidCI`. Anotações de trabalho são adicionadas pelos seguintes motivos:

- Quando as detecções são movidas de um VI para outro.
- Quando um VI duplicado é fechado.

Se você não quiser atualizar o IC do VI existente, defina a propriedade `sn_sec_cmn.update_on_ci_change` como `false`. Em seguida, quando um IC muda, um novo VI é criado e o existente é encerrado como um `IC inválido`.

O valor padrão da propriedade `sn_sec_cmn.update_on_ci_change` é `verdadeiro`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reavaliando itens descobertos

Quando novos dados são recebidos em um item descoberto, o item descoberto não é reavaliado imediatamente. Ao receber novos dados, a opção *reevaluate_ci* é definida como *true* por padrão.

O trabalho agendado *Re-apply CI Lookup Rules on the Changed Discovered items* avalia todos os itens descobertos cujos dados de origem estão sendo alterados pelo scanner. Ele reprocessa os itens descobertos e atualiza os itens vulneráveis relacionados ao item descoberto cujos dados de origem foram alterados. O valor deste trabalho agendado é *On Demand* por padrão.

Nota: Você também pode optar por executar este trabalho agendado diariamente.

Resposta a vulnerabilidades tarefa de correção e estados de itens vulneráveis

Com a aplicação Resposta a vulnerabilidades, você pode usar o modelo de estado para ver o status de uma tarefa de correção a qualquer momento. Saber como cada estado se relaciona e afeta um ao outro ajuda a determinar quando e como corrigir seus itens vulneráveis (IVs).

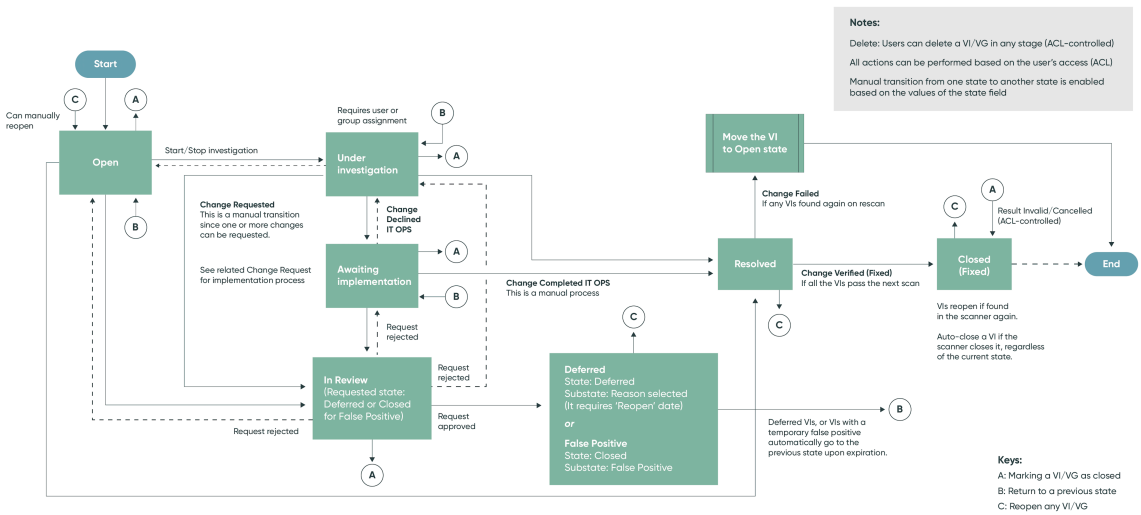
Estados da tarefa de correção

Casos de uso complexos às vezes podem fazer com que um item vulnerável esteja em um estado diferente da sua tarefa de correção. Entender como os estados funcionam ajuda a explicar esse comportamento e pode ajudar na criação de tarefas de correção e na criação ou edição de regras de tarefa de correção.

Nota: A partir da v23.0 de Resposta a vulnerabilidades, o fluxo de trabalho **de Aprovação de Estado de Item Vulnerável** foi descontinuado e substituído pelo fluxo Mudança de Aprovação de Estado de Vulnerabilidade no Flow Designer.

As tarefas de correção têm muitos estados possíveis, conforme mostrado no diagrama a seguir.

Fluxo de estado da Resposta a vulnerabilidades



Nota: Cada formulário de tarefa contém os botões **Seguir** e **Atualizar** que são padrão para tarefas ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os estados da tarefa de correção e as ações que você pode executar nela em um estado respectivo, consulte Resposta a vulnerabilidades estados da tarefa de correção.

Para obter mais informações sobre detecções, tarefa de correção e estados de itens vulneráveis, consulte Detecções, tarefas de correção e estados de itens vulneráveis.

Para obter mais informações sobre a tarefa de correção e os estados de VI, consulteTarefas de correção e estados de itens vulneráveis.

Para obter mais informações sobre o estado da tarefa de correção para IVs em vários grupos, consulte Estado da tarefa de correção para itens vulneráveis (IVs) em vários grupos.

Cálculo e exibição da idade do item vulnerável

A idade dos itens vulneráveis (VIs) é exibida na aplicação Resposta a vulnerabilidades com mais detalhes.

Visão geral

A idade do item vulnerável (VI) é exibida no formato Dias/Horas/Minutos na coluna Idade na exibição de lista de Itens vulneráveis e nos campos Idade e Idade encerrada nos registros de VI (VIT). A idade exibida em dígitos mais significativos pode ajudá-lo a executar com mais precisão as seguintes atividades:

- Configure regras no módulo Regras de exclusão automática para direcionar e excluir registros de VI específicos por Dias/Horas/Minutos. A remoção de registros com mais precisão pode aumentar seu desempenho, especialmente se você tiver um grande número de registros de VI em sua instância.
- Exiba relatórios com detalhes mais específicos no Performance Analytics para a aplicação Resposta a vulnerabilidades.
- Crie filtros que identifiquem somente os IVs desejados.
- Limpe as exibições de lista para exibir somente os IVs desejados.
- Referência com pontos com mais facilidade.

Um trabalho agendado calculou a idade e atualizou todos os IVs ativos. Em instâncias com um grande número de registros de VI, esse processo pode ser lento e afetar negativamente o desempenho. A idade do VI é calculada com mais eficiência sob demanda e exibida com dígitos mais significativos com uma coluna Idade aprimorada. A coluna Idade aprimorada é adicionada automaticamente quando você instala ou faz upgrade da aplicação Resposta a vulnerabilidades.

Nota: Se você executar um upgrade e a idade do VI não for exibida na exibição de lista de Itens vulneráveis e nos campos Idade e Idade encerrada nos registros de VI ativo (VIT) no formato Dias/Horas/Minutos (9 dias, 18 horas, 29 minutos) , a coluna de idade não será atual em sua instância. Para obter mais informações sobre como resolver esse problema após um upgrade, consulte KB0749231 .

A coluna de idade e os campos não são editáveis. Um gerenciador de vulnerabilidades com a permissão sn_vul.vulnerability_read ou a persona de administrador de vulnerabilidade pode exibir esse valor, e os proprietários de correção de TI com a função sn_vul.remediation_owner podem exibi-lo em registros atribuídos a eles.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

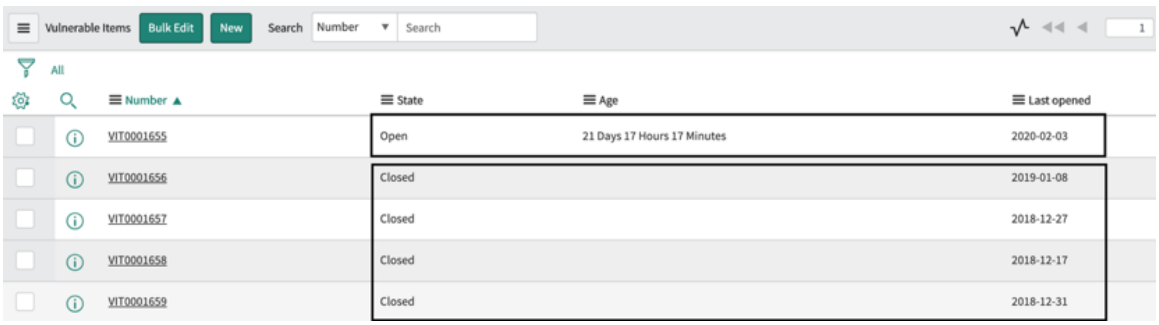
Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

A idade do VI é exibida conforme mostrado nas imagens a seguir.

Lista de itens vulneráveis

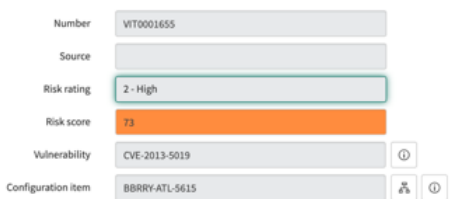
Conforme mostrado na figura a seguir, na exibição de lista de Itens vulneráveis, a Idade é exibida na coluna Idade em Dias/Horas/Minutos (21 Dias 17 Horas 17 minutos) somente para IVs ativos. IVs ativos são VIs em qualquer estado diferente de "Encerrado". Este valor de idade representa o número de dias em que o VI está ativo.

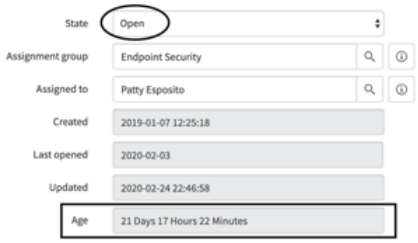
A idade não é exibida para IVs no estado "Encerrado". Para IVs anteriormente em um estado “Encerrado” e depois reabertos, o valor representa o número de dias em que o VI está ativo desde a data em que foi aberto pela última vez.



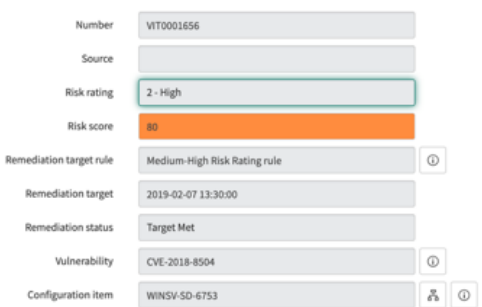
Idade nos registros de VI

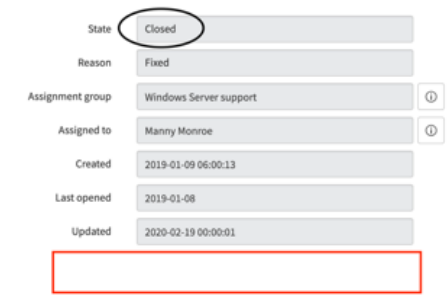
Nos registros de VI, o valor da coluna Idade na exibição de lista fica visível para IVs ativos no campo Idade.





O valor da coluna Idade não é exibido para registros de VI no estado "Encerrado".





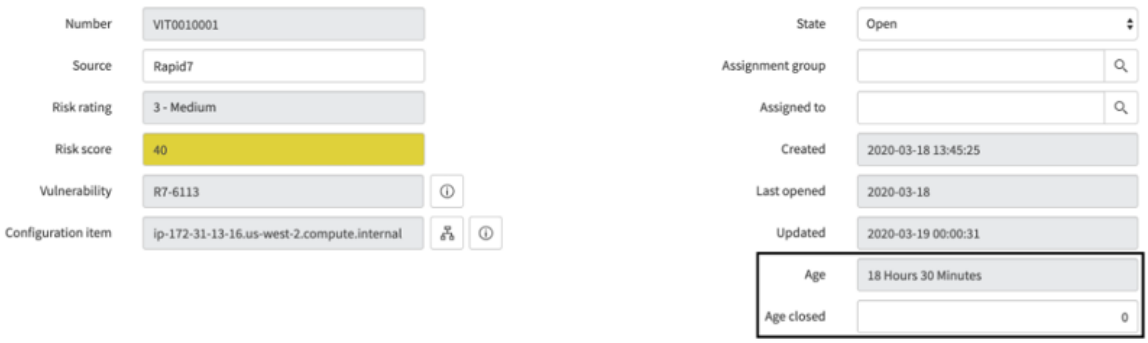
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Idade na lista de itens vulneráveis e nos registros de VI quando um VI é atualizado

Quando um VI está no estado "Encerrado", o campo Idade não é exibido. Quando o VI faz a transição para "Fechado", o valor em número de dias da coluna Idade é exibido no campo Encerrado com idade (9), conforme mostrado na figura a seguir. Este valor representa o número de dias em que o VI ficou ativo antes de fazer a transição para "Encerrado". Por exemplo, na imagem a seguir, este IV ficou ativo por 9 dias, 18 horas e 29 minutos, mas somente o número de dias (9) é exibido no registro encerrado.

Se este VI for reaberto, quando o estado do VI voltar para "Aberto", o campo Idade encerrada será redefinido para 0. Como o VI está ativo novamente, a idade em Dias/Horas/Minutos é exibida na exibição de lista na Idade coluna e no campo Idade no VIT.



Removendo atribuições de itens vulneráveis e tarefas de correção

Você pode limpar os campos **Atribuído a** e **Grupo de atribuição** em itens vulneráveis diretamente do item vulnerável (VIT) e dos registros de tarefa de correção que você determina que podem estar atribuídos incorretamente a você ou a seus grupos.

Visão geral

A partir da **v16.5**, os responsáveis pela correção podem atualizar os registros para reatribuição com o botão Cancelar atribuição nas aplicações Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações.

Caso de uso

Se você determinar que os IVs não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, convém remover a si mesmo ou seus grupos dos campos **Atribuído a** e **Grupo de atribuição** em vulneráveis registros de item e tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cancelar atribuição do módulo

O botão **Cancelar atribuição** é exibido nos seguintes registros em qualquer estado que não seja Encerrado ou Resolvido:

- Tarefas de correção (VULs) no ambiente clássico e nos espaços Resposta a vulnerabilidades. Se uma tarefa de correção for atualizada com este recurso, os campos **Atribuído a** e **Grupo de atribuição** em todos os IVs associados também serão limpos.
- Itens vulneráveis (VITs) no ambiente clássico e nos espaços Resposta a vulnerabilidades.
- Itens vulneráveis da aplicação (AVITs).

Todos os registros atualizados com o botão de IU ou manualmente são exibidos no módulo Não atribuído em seus respectivos módulos.

Para saber como reatribuir registros usando a ação de IU *Unassigned*, consulte Remover atribuições de itens vulneráveis.

Edição em massa

Você pode limpar os campos de atribuição de vários IVs em uma lista. Depois de selecionar os IVs e selecionar **Edição em massa**, na caixa de diálogo exibida, marque a caixa de seleção **Cancelar atribuição**.

Propriedades e notificações do sistema

Se você for um administrador com a função **sn_vulc.vulnerability_admin**, ao clicar em Cancelar atribuição em um registro, por padrão, a propriedade do sistema *sn_vul.unassign_vr.approval_required* aciona o fluxo de aprovação e cria um registro de aprovação de mudança de estado no estado de revisão e a solicitação de aprovação é gerada para o aprovador, o que é exibido na lista **Minhas aprovações**.

Nota: Como administrador de vulnerabilidades, você pode definir a propriedade do sistema *sn_vul.unassign_vr.approval_required* como **falsa** para desabilitar o processo de aprovação.

- Se o aprovador aprovar a solicitação, *sn_vul.default_assignment_group* limpará os campos **Atribuído a** e **Grupo de atribuição** e preencherá o campo **Tipo de atribuição** com **Não atribuído**. Como administrador de vulnerabilidades, você pode alterar o valor na propriedade do sistema *sn_vul.default_assignment_group* para que os campos de atribuição sejam limpos e um grupo específico seja atribuído. Por exemplo, se um usuário clicar em **Cancelar atribuição** em um registro e você quiser redirecioná-lo para um grupo específico para revisão, poderá adicionar um ID de sistema para o grupo de sua escolha no campo de valor da propriedade do sistema.

  Nota: Se você alterar este valor, as notificações de todos os IVs, AVITs e CVITs que não estão atribuídos serão enviadas para o grupo especificado.

- Se o aprovador rejeitar sua solicitação, o motivo da rejeição será exibido na guia **Anotações**.

Como alternativa, se *sn_vul.default_assignment_group* não estiver configurado para um grupo específico, por padrão, os usuários que você adicionar ao grupo de usuários de notificação de cancelamento de atribuição serão alertados quando os registros forem não atribuídos. A propriedade do sistema *sn_vul.default_assignment_group* determina as notificações para este grupo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O tipo de atribuição, seja **Manual**, **Regra**ou **Não atribuído**, está disponível nos registros VI e na exibição de lista. O tipo de atribuição **Não atribuído** é exibido nos registros depois que os campos **Atribuído a** e **Grupo de atribuição** são limpos pela propriedade do sistema do recurso.

Monitorando suas regras de atribuição com o trabalho agendado para este recurso

Um trabalho agendado diário conta os registros quando eles fazem a transição para o tipo de atribuição **Não atribuído**. Com essa contagem, os analistas de vulnerabilidade podem monitorar e ajustar regras de atribuição que possam não estar funcionando bem com base em regras de atribuição que tenham contagens mais altas de IVs não atribuídos.

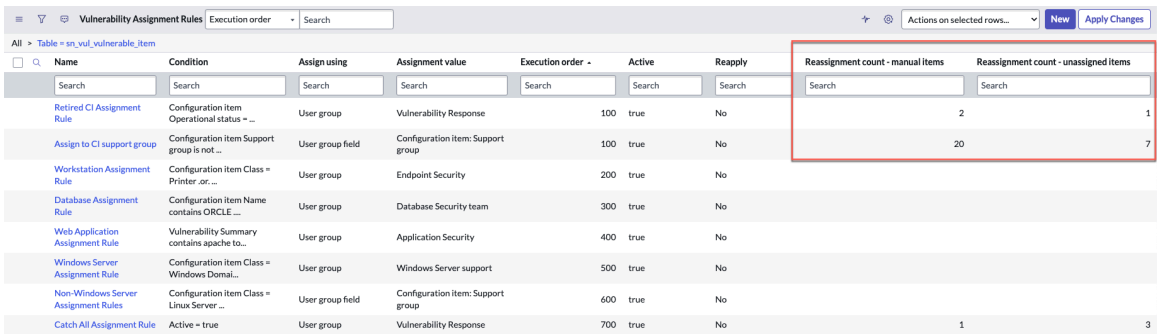
O trabalho agendado *Reassignment count for assignment rules* é executado diariamente e publica o número total de IVs não atribuídos por este recurso para uma regra de atribuição específica.

As contagens coletadas por este trabalho se aplicam aos itens vulneráveis e às regras de atribuição exclusivas para Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações. As contagens são exibidas por regra de atribuição em cada lista de regras de atribuição para cada módulo.

O trabalho também conta todos os registros que não foram atribuídos manualmente. As contagens manuais e as contagens coletadas por este recurso são publicadas na lista Regras de atribuição de vulnerabilidade em duas colunas: *Reassignment count - manual items* e *Reassignment count - unassigned items*.

1. Como administrador de vulnerabilidades, para exibir essas contagens, navegue até **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Clique no ícone de engrenagem no canto superior direito da lista e selecione *Reassignment count - manual items*e *Reassignment count - unassigned items* para exibição.
3. Qualquer VI que foi atribuído originalmente por uma regra, mas posteriormente reatribuído de forma automática ou manual, contém uma referência à regra original na exibição de lista.

O exemplo a seguir mostra contagens de reatribuições para duas regras de atribuição.



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

Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade

As calculadoras de vulnerabilidade automatizam o cálculo dos valores iniciais dos campos em itens vulneráveis. A condição de cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de vulnerabilidade

O sistema de base Resposta a vulnerabilidades inclui duas calculadoras de vulnerabilidade que definem a **pontuação de risco** básica no item vulnerável.

- **Calculadora de Risco Padrão**
- **Severidade da Vulnerabilidade**

Calculadoras de vulnerabilidade podem ser criadas para priorizar e classificar o impacto de itens vulneráveis com base em qualquer critério usando filtros de condição. Seja o impacto nos negócios da vulnerabilidade, a classe do item de configuração (IC) ou a idade do item vulnerável, você pode criar calculadoras de vulnerabilidade adicionais para definir outros campos em itens vulneráveis. Ou você pode personalizar as calculadoras de vulnerabilidade existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades. Para obter mais informações, consulte Criar uma calculadora Resposta a vulnerabilidades e Filtrando em Resposta a vulnerabilidades.

Além disso, você pode usar atributos no configuration_item [cmdb_ci] no Configuration Management Database (CMDB) para ajudá-lo a criar lógica para suas calculadoras de risco da Resposta a vulnerabilidades. Se, por exemplo, você determinar que os ICs externos em sua organização são mais vulneráveis e podem precisar de correção imediata, você pode atribuir atributos como *Internet Facing* para esses ICs. Este atributo e outros estão listados nas notas de versão do Common Service Data Model para a versão da família Orlando. Para obter informações e orientações atuais sobre o CMDB, consulte os seguintes tópicos:

- Modelo conceitual do Common Service Data Model
- Modelo de esquema do CMDB

Cada calculadora contém uma lista de regras de calculadora, com uma condição que determina quando aplicá-la. Quando a calculadora é executada, a condição de cada regra de calculadora é avaliada na ordem e a primeira regra de calculadora correspondente é usada.

A calculadora de **gravidade de vulnerabilidade** calcula a **pontuação de risco** dos itens vulneráveis usando a gravidade da vulnerabilidade normalizada.

Nota:

- Somente uma calculadora por campo de destino (**Pontuação de risco**) pode estar ativa por vez. **A gravidade da vulnerabilidade** está desabilitada por padrão.
- A partir da v23.0 de Resposta a vulnerabilidades, sempre que a pontuação de risco é atualizada em um VIT, a seção **Anotações** é atualizada com os seguintes detalhes:
  - Nome do grupo de calculadoras
  - Nome da calculadora: dependendo se a regra da calculadora é baseada em um modelo ou em um script, o nome é acrescentado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, clique em qualquer regra e marque a caixa de seleção **Exibição avançada**. Na caixa suspensa **Tipo de valor**, selecione a opção necessária. Se o modelo for selecionado, a pontuação de risco será atualizada de acordo com a condição especificada na regra. Se Script estiver selecionado, você poderá adicionar ou atualizar o script existente.

Todas as calculadoras de vulnerabilidade habilitadas definem os campos selecionados sempre que um item vulnerável é criado, quando um IC ou vulnerabilidade associada muda ou quando o link relacionado **Calcular pontuação de risco** em um item vulnerável

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

é usado. Por exemplo, a Pontuação de risco é atualizada automaticamente em registros de item vulnerável quando o valor de gravidade é atualizado em uma vulnerabilidade importada. Depois que uma importação de vulnerabilidade atualiza uma pontuação de vulnerabilidade, o sinalizador de recálculo é habilitado para essa vulnerabilidade. As pontuações de risco dos itens vulneráveis que têm o sinalizador de recálculo habilitado (verdadeiro) com essa vulnerabilidade são recalculadas.

Em um item vulnerável existente, se você clicar no link relacionado **Calcular pontuação de risco** e uma das calculadoras estiver habilitada, o campo **Pontuação de risco** no item vulnerável será atualizado.

Nota:

- O link relacionado **Calcular pontuação de risco** só fica visível quando pelo menos uma calculadora de vulnerabilidade está habilitada.
- A partir da v22.0 de Resposta a vulnerabilidades, você pode atualizar a pontuação de risco de um item vulnerável em Vulnerability Manager Workspace e Espaço de correção de problemas de TI selecionando o botão **Calcular pontuação de risco** na exibição de registro.
- A partir da versão 23.0 do Resposta a vulnerabilidades, sempre que a pontuação de risco em um VIT muda, os seguintes detalhes são documentados na seção Anotações do VIT:
  - Nome do grupo de calculadoras
  - Nome da calculadora
  - Valores de campo com sua ponderação e contribuição de pontuação de risco
  - Pontuação de risco final

Regras da Calculadora de Vulnerabilidade

A Calculadora de **risco padrão** da calculadora do sistema base contém a regra**Regra de risco padrão**, uma regra de calculadora de vulnerabilidade especializada chamada **Regra de risco**. Ele calcula a **pontuação de risco** com base em vários valores:

- Gravidade da vulnerabilidade
- Explorar informações
- Criticidade
- Exposição externa do IC com a vulnerabilidade
- Pontuações de EPSS

Você pode ajustar os valores a serem usados na **Regra de risco padrão** e quanto peso atribuir a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a **pontuação de risco**base.

Você pode personalizar os critérios para a regra de risco padrão. Para obter mais informações, consulte Definir campos e pesos para a regra de risco das Calculadoras de risco da Resposta a vulnerabilidades.

Para obter um exemplo de como as pontuações de risco das calculadoras de regra de risco são determinadas, consulte Exemplo de cálculo de pontuação de risco para Resposta a vulnerabilidades.

Atribuindo uma porcentagem de ponderação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode atribuir percentual de ponderação (0-100) no nível de valor do campo, por exemplo, você pode atribuir um percentual de ponderação a cada nível de gravidade (de nenhum a crítico).

Se o peso de gravidade for 50 para a regra de risco, e os seguintes valores de peso forem atribuídos para o nível de gravidade:

Gravidade da vulnerabilidade	Pontuação de risco
Crítico	100
Alto(a)	50
Médio	20
Nenhum(a)	0

Se a gravidade for crítica, o peso equivalente será 50. Se a gravidade for alta, o peso equivalente será 25 e, se a gravidade for média, o peso equivalente será 10. Se a gravidade for Nenhum, o peso equivalente será 0. Para obter mais informações, consulte Exemplo de cálculo de pontuação de risco para Resposta a vulnerabilidades.

Configurações de regra da calculadora de vulnerabilidade

Cada regra tem uma configuração de **Ordem**. No entanto, o primeiro a corresponder às condições atualiza o campo **Pontuação de risco** no item vulnerável. Para obter mais informações sobre configurações de regra da calculadora de vulnerabilidade, consulte Criar uma calculadora Resposta a vulnerabilidades. Regras de calculadora sem script normalmente criam menos impacto no desempenho do que as regras de calculadora com script.

A calculadora de **gravidade de vulnerabilidade** do sistema base contém regras de calculadora que atribuem a cada nível de gravidade (de nenhum a crítico) um valor (0-100) para **pontuação de risco** com base na gravidade. A**Severidade Desconhecida** é atribuída automaticamente a uma pontuação de risco de 100. Esses valores podem ser ajustados e, como a **Calculadora de risco padrão**, novas regras de calculadora ou novas regras de risco podem ser criadas.

Ponderações de pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação e classificação de risco com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio *`Update Risk Rating from Risk Score`* na tabela de itens vulneráveis é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Antes da versão 17.1 da aplicação Resposta a vulnerabilidades (VR), as seguintes classificações de risco eram fornecidas como parte da inclusão de script `VulnerabilityUtils`, que era codificada.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 18.0 de Resposta a vulnerabilidades,

- Os tipos de classificação de risco são enviados na tabela base como vr_risk_rating. Esses tipos são passados como parte da regra de negócio em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e regras de negócio relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as vulnerabilidades e exposições comuns associadas (CVEs) ou entradas de terceiros (TPEs) nos itens de vulnerabilidade (VIs) estão vinculadas a uma vulnerabilidade de exploração conhecida (KEV) de CVE.

Integração de vulnerabilidade da Tenable e regra de risco da Tenable

A regra de risco da Tenable está disponível com o Integrações de vulnerabilidade da Tenable. A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com uma nova calculadora de risco padrão em Resposta a vulnerabilidades. A Regra de risco da Tenable é instalada com a aplicação Integração de Resposta a vulnerabilidades com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade de Resposta a vulnerabilidades.

Esta regra de risco está desabilitada por padrão. Consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração.

Resposta a vulnerabilidades detecções de itens vulneráveis de integrações de terceiros

Exiba todas as informações coletadas por verificações de terceiros em sua instância Now Platform®. Exiba os resultados retornados das verificações na detecção e nos registros de item vulnerável (VI) em sua instância conforme esses resultados são exibidos nos scanners.

Visão geral

A aplicação Resposta a vulnerabilidades oferece suporte a integrações de terceiros que recuperam dados de itens vulneráveis do ambiente empresarial. Dados detalhados sobre detecções, ou seja, ocorrências únicas e distintas de vulnerabilidades conforme relatadas pelos scanners de suas integrações de terceiros, são importados e exibidos nos registros de detecção e de item vulnerável em sua instância da Now Platform.

As integrações de terceiros recuperam dados de detecção de itens vulneráveis. As detecções são ocorrências distintas de vulnerabilidades conforme relatadas pelos scanners. Os dados de detecção são emparelhados com itens vulneráveis e o estado de VI é atualizado com base no estado das detecções. Se um IV não for encontrado, um novo será criado. As detecções são abertas ou fechadas somente por dados encontrados diretamente por um scanner.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nas versões anteriores do Resposta a vulnerabilidades, as detecções de itens vulneráveis, o relacionamento entre um IC (ativo) em seu ambiente e uma vulnerabilidade importada de um scanner de terceiros, criavam um item vulnerável exclusivo em sua instância da Now Platform.

A granularidade dos dados originais fornecidos pelo scanner é preservada. Com as detecções, os dados de detecção são emparelhados com itens vulneráveis. Durante uma ingestão, se um item vulnerável não for encontrado, um novo VI será criado.

A partir da versão 21.1.2 de Resposta a vulnerabilidades, uma propriedade do sistema *sn_vul.show_last_open_detection* é fornecida no sistema de base. Por padrão, o valor desta propriedade é definido como falso e o comportamento atual de agregação dos valores da detecção inicial ao VI permanece inalterado. No entanto, se estiver definido como verdadeiro, um VI será atualizado automaticamente com a última detecção em aberto após uma ingestão. Os campos como endereço IP, SSL, Porta, Protocolo, NetBIOS e Prova são atualizados para as detecções de VI. Se necessário, você pode personalizar os campos de detecção que devem ser atualizados modificando o script `DetectionBase`.

Para exibir os valores da última detecção em aberto, navegue até a guia **Última detecção em aberto** na exibição do formulário VI. Para atualizar todos os IVs abertos no último ano com os últimos valores de detecção abertos, você pode executar o trabalho agendado *Update Last Open Detection Value To VITs* sob demanda. Este trabalho agendado também é fornecido no sistema de base.

Nota: Quando um item de configuração (IC) muda em um item descoberto, as atualizações correspondentes também são refletidas nas detecções. Como resultado, as detecções podem ser movidas de um VI para outro. Com base nessa mudança e no valor da propriedade *sn_vul.show_last_open_detection*, os valores das detecções são acumulados para os IVs de origem e de destino.

Versões compatíveis do Resposta a vulnerabilidades

Para obter mais informações sobre como instalar ou atualizar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades.

Integrações de terceiros compatíveis

Uma integração de terceiros compatível com sua aplicação Resposta a vulnerabilidades é necessária para detecções de itens vulneráveis. As seguintes integrações de terceiros são compatíveis com a aplicação Resposta a vulnerabilidades para detecções de itens vulneráveis:

- Qualys Host Detection Integration
- Depósito de dados da Rapid7:
  - Integração de item vulnerável
  - Integração de resolução de item vulnerável
- Integração de resolução de item vulnerável da Rapid7 (InsightVM)
  - Integração de VM de informação
  - Integração de item vulnerável - API
- Integrações de vulnerabilidade da Tenable
- Gestão de ameaças e vulnerabilidades do Microsoft Defender

Essas integrações de terceiros estão disponíveis com uma assinatura separada do ServiceNow Store. Para obter mais informações sobre essas integrações, consulte

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Resposta a vulnerabilidades e para obter mais informações sobre como obter direito.

Para verificar se o scanner de terceiros está configurado para importação, consulte Instalação e configuração da aplicação Integração Rapid7 para Operações de segurança e Instalar o Qualys Vulnerability Integration.

Termos-chave para detecções de itens vulneráveis

Vulnerabilidade

Dados sobre pontos fracos em software, sistemas operacionais e ativos importados de fontes internas e externas. Esses dados são importados e comparados aos ativos existentes (itens de configuração, ICs) listados no CMDB.

Item vulnerável

Um item vulnerável é criado ou atualizado quando uma vulnerabilidade importada corresponde a um IC no CMDB.

Detecção

Uma ocorrência única e distinta de uma vulnerabilidade conforme relatada por um scanner chamada de Detecção de item vulnerável no ambiente Now Platform. Uma detecção inclui dados aprimorados sobre uma vulnerabilidade e todos os itens vulneráveis correspondentes. Esses dados são exibidos no registro de detecção (VID#) e na exibição de lista de itens vulneráveis que inclui os seguintes detalhes:

- Primeiro encontrado (dados)
- Último encontrado (data)
- Nome DNS
- Net BIOSname
- Endereço IP
- Porta
- Protocolo
- Prova
- SSL
- Horas encontradas

Nota: Adicionar uma regra de negócio na tabela de detecção afetará o desempenho da ingestão.

Chave de detecção

Uma combinação com hash de campos que fornecia uma maneira de identificar e vincular uma detecção a um item vulnerável. As chaves de detecção são específicas de integração.

Configurações de chave de detecção

Scanner	Vulnerabilid	Porta	Protocolo	ID do ativo	Prova	NIC
Qualys	Sim	Sim	Sim	Sim	Não	N/D
Tenable	Sim	Sim	Sim	Sim	Não	N/D

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de chave de detecção

Scanner	Vulnerabilid	Porta	Protocolo	ID do ativo	Prova	NIC
Rapid7	Sim	Sim	Sim	Sim	Sim (não faz distinção entre maiúsculas e minúsculas)	Sim

Nota:

- Se a chave de detecção não for especificada, ou para versões anteriores a Resposta a vulnerabilidades 14.0, a chave de detecção será uma combinação de entrada de vulnerabilidade, porta, protocolo, ID de ativo e prova.
- A partir da v19.0 de Resposta a vulnerabilidades, uma nova NIC de chave de detecção é adicionada para Rapid7 InsightVM, que é ativado por padrão. As detecções existentes sem NIC são atualizadas com a primeira NIC de entrada na carga de Rapid7. A chave de detecção é recalculada e preenchida novamente na detecção, incluindo a NIC. Novas detecções serão criadas se detecções semelhantes forem vistas com valores de NIC diferentes. Esses dados não são acumulados para a tabela de itens vulneráveis. O valor da NIC é armazenado em uma nova coluna nas tabelas sn_vul_detection_key_config e sn_vul_detection.

Deduplicar

O processo usado pela aplicação Resposta a vulnerabilidades de recolhimento de detecções individuais em um único VI quando os dados atendem a determinados critérios codificados.

ID externo de VI

O valor armazenado no campo ID externo da tabela VI. Este valor é um hash composto pela combinação de chaves em um VI que representa o que o torna exclusivo na aplicação. Ele é composto por um IC e uma entrada vulnerável.

Reabrir itens vulneráveis resolvidos

Itens vulneráveis definidos como **Resolvidos** em sua instância Now Platform, mas não transicionados para **Encerrado/Corrigido** pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

IVs encerrados com um subestado **fixo** ou **obsoleto** serão reabertos se uma nova detecção for criada e os VIs puderem ser correspondidos com a nova vulnerabilidade.

De acordo com a inclusão de script, *`DetectionBase`*, método *`_shouldReOpenVI()`*, se o VIT foi **encerrado** anteriormente com subestado **fixo**, **obsoleto**ou **IC desativado**, ele será reaberto e a detecção será mapeada para o VIT existente.

Por exemplo, digamos que a data de encerramento de um VIT seja posterior à data last_found de uma detecção. Você espera que esses registros de VIT permaneçam fechados. No entanto, se você vir um VIT encerrado anteriormente reaberto, isso significa que o VIT foi encerrado por uma detecção anterior e a vulnerabilidade foi encontrada novamente em uma verificação posterior. Quando é encontrada uma nova detecção que

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

corresponde ao VIT encerrado que tem a mesma vulnerabilidade no item de configuração do VIT, o VIT é reaberto.

Para Rapid7 detecções, uma opção agora está disponível na página de configuração do Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como **Resolvidos**, mas não transicionados para **Encerrado/Corrigido** por verificações subsequentes, retornam para **Aberto** após o número de dias inserido.

Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como **Resolvidos**, mas que não foram transicionados para **Encerrado/Corrigido** por verificações subsequentes, esses IVs voltarão para **Aberto** quando a última data encontrada for posterior à data de Resolvido.

Exibir dados de detecção

Você exibe os dados importados das detecções de itens vulneráveis no registro VI. Para obter mais informações, consulte Exibir Resposta a vulnerabilidades dados de detecção de itens vulneráveis e Verificar Resposta a vulnerabilidades dados de detecção de item vulnerável em registros de execução de integração (VINTRUN).

Solução de gestão de vulnerabilidade

Correlacione automaticamente as vulnerabilidades em seu ambiente com as soluções que podem corrigi-las. Identifique as ações de correção que se aplicam às suas vulnerabilidades e priorize-as pela maior redução no risco de vulnerabilidade.

Solução de gestão de vulnerabilidade

As equipes de segurança e TI geralmente passam um tempo significativo pesquisando descobertas de vulnerabilidade para identificar os tratamentos mais eficazes para o ambiente. Dado o volume e a complexidade das vulnerabilidades em grandes organizações, traduzir descobertas de vulnerabilidade em tarefas de correção é um processo manual, tedioso e sujeito a erros.

Com Solução de gestão de vulnerabilidade, você pode correlacionar automaticamente suas descobertas de vulnerabilidade com as soluções que as corrigem. Identifique os patches de software, atualizações de configuração e outros controles que têm o maior impacto para sua organização sem a sobrecarga manual.

Requisitos do Solução de gestão de vulnerabilidade

Solução de gestão de vulnerabilidade é um recurso disponível na aplicação Resposta a vulnerabilidades. Solução de gestão de vulnerabilidade requer uma assinatura separada.

Para obter mais informações sobre como obter direitos para aplicações do ServiceNow Store, consulte . Consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades para obter mais informações sobre como instalar a aplicação depois de baixá-la na instância.

Depois de instalado, o Solução de gestão de vulnerabilidade fornece acesso aos dados da solução Microsoft Security Response Center e Red Hat de dentro de Resposta a vulnerabilidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Você pode configurar ambas as aplicações de solução de dentro do Assistente de configuração. Consulte Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade usando o Assistente de configuração.

Consulte Noções básicas sobre Integração com a solução Microsoft Security Response Center e Noções básicas sobre Red Hat Solution Integration para obter mais informações sobre as soluções importadas.

Versões disponíveis

Para a versão mais atual de Solução de gestão de vulnerabilidade, verifique se você tem a versão mais atual de Resposta a vulnerabilidades instalada.

Versão de lançamento de Solução de gestão de vulnerabilidade	**Versões compatíveis de** Resposta a vulnerabilidades	**Notas de versão**
Solução de gestão de vulnerabilidade v10.3	Resposta a vulnerabilidades v18.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Sobre soluções e substituição

Uma atualização substituída é uma substituição completa de uma versão ou versões anteriores. Por exemplo, uma atualização de hotfix pode ser substituída por um Service Pack. As soluções estão relacionadas a vulnerabilidades. As soluções também podem estar relacionadas a outras soluções em uma cadeia de substituição. As soluções abordam vulnerabilidades em soluções anteriores e são cumulativas. Solução de gestão de vulnerabilidade associa automaticamente vulnerabilidades de soluções anteriores a soluções substitutas. Se uma vulnerabilidade mais antiga for encontrada, qualquer solução de substituição superior poderá resolvê-la, mas a solução de substituição mais elevada será a preferencial, pois é a mais cumulativa.

Soluções potenciais versus preferenciais

Uma possível solução é aquela que pode resolver uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis. Uma solução preferencial é a solução única destinada a corrigir uma vulnerabilidade ou item vulnerável (VI). Ele comunica a intenção e permite métricas de implantação mais detalhadas.

Soluções Preferenciais

Solução de gestão de vulnerabilidade define automaticamente a solução mais eficaz (**Solução preferencial**) para a vulnerabilidade detectada com base na substituição mais alta quando existe apenas uma solução de substituição mais alta. Se houver mais de uma substituição mais alta para a vulnerabilidade, nenhum valor será definido. Em Resposta a vulnerabilidades, uma **Solução Preferencial** é a solução Microsoft Security Response Center ou Red Hat com a maior substituição derivada das soluções associadas à vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os valores de Solução preferencial podem ser definidos no item vulnerável ou na vulnerabilidade. Quando definido diretamente na vulnerabilidade, todos os itens vulneráveis associados à vulnerabilidade herdam essa solução. Altere os valores de **Solução Preferencial** para vários itens vulneráveis usando o recurso de edição em massa. Quando editado em massa, somente a **Solução preferencial** no item vulnerável é atualizada, pois a configuração da **solução preferencial** no nível de entrada de vulnerabilidade definiria a **solução preferencial** para todos os novos IVs daqui para frente. A edição em massa se aplica somente aos itens vulneráveis atuais.

Nota: Se houver várias soluções de substituição mais altas para uma vulnerabilidade, os valores de **Solução Preferencial** no nível da vulnerabilidade serão apagados, pois essa solução depende do ativo afetado. Quando houver várias soluções de substituição mais altas para uma vulnerabilidade, defina uma **Solução preferencial** no item vulnerável. Você pode definir uma solução diferente usando a lista de **pesquisa** no formulário de **item vulnerável**.

Todas as soluções preferenciais para os itens vulneráveis em tarefas de correção estão em uma lista relacionada no registro da **Tarefa** de correção.

Nem todas as importações de solução resultam em atualizações de dados completas. O processo de substituição é atualizado quando:

- Um item vulnerável foi criado.
- Os dados foram alterados em um VI ativo.

Nota: A partir da v22.0 de Resposta a vulnerabilidades, as soluções não são enfileiradas nos dois casos acima.

- Um novo mapeamento é criado para uma entrada de terceiros com o CVE.
- Novos dados de solução foram liberados desde a última importação, uma solução existente foi atualizada.

Aprimoramento da gestão de soluções e otimização de desempenho

As soluções são recebidas de várias integrações, incluindo Microsoft e Redhat. O primeiro fornece atualizações mensais e estabelece uma cadeia de dependências para rastrear a solução preferencial para vulnerabilidades. No entanto, outras integrações não seguem este formato de atualização e não precisam estabelecer uma cadeia de dependências para elas. Anteriormente, era usada uma lógica de processamento que envolvia a criação de um gráfico para manter a precedência e identificar as soluções de substituição mais altas. Essas soluções foram sugeridas como a solução preferencial para as vulnerabilidades. No entanto, como a construção do gráfico é demorada, as outras integrações são excluídas deste processo. Para melhorar o desempenho, a partir da v22.0 de Resposta a vulnerabilidades, o *`métodoutility.processNonGraphSolutions()`* é chamado no trabalho agendado *`Process Vulnerability Solutions Metrics Queue`*. Este método lida com soluções de integrações diferentes da Microsoft.

Em segundo lugar, as soluções são enfileiradas de várias origens usando o trabalho agendado *`Process Vulnerability Solutions Metrics Queue`*. Este trabalho programado envolve o acúmulo de soluções de entradas do NVD para entradas de terceiros, preenchendo soluções preferenciais em vulnerabilidades e atualizando as métricas de status de correção nas soluções. Nos seguintes cenários, somente as métricas de status de correção devem ser atualizadas:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando a solução preferencial muda nas vulnerabilidades
- Quando os VITs são criados ou excluídos
- Quando uma importação de VIT é concluída

Embora as soluções estejam enfileiradas para atualizar somente as métricas de status de correção, elas ainda tentam acumular soluções de entradas do NVD para entradas de terceiros e preencher as soluções preferenciais. Para otimizar esse processo, na tabela Solução de vulnerabilidade, a coluna **Status da atualização** foi introduzida. Quando as métricas de status de correção nas soluções precisam ser atualizadas sem exigir o acúmulo ou o preenchimento de soluções preferenciais, as soluções não são mais enfileiradas. Em vez disso, a coluna **Atualizar status** é atualizada diretamente como verdadeira. Essa abordagem permite lidar com casos em que somente as métricas de status de correção devem ser atualizadas, resultando em economia de tempo e recursos. No trabalho agendado, depois que o processamento das soluções enfileiradas é concluído, as soluções marcadas com um status de atualização como verdadeiro são identificadas. Em seguida, eles são iterados por meio dessas soluções, calculando as contagens e atualizando as métricas de status de correção de acordo. Esta etapa desempenha um papel significativo na melhoria do desempenho do trabalho agendado, pois o número de soluções que devem ser enfileiradas é reduzido. Para exibir as métricas de status de correção, navegue até a tabela Solução de vulnerabilidade [sn_vul_solution] e selecione uma solução de vulnerabilidade. Em seguida, selecione a guia **Status** da correção. A guia fornece os seguintes campos:

Métricas de status de correção

Campo	Descrição
Metas de solução preferencial - Status de correção de IVs para os quais esta é a solução preferencial	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de ICs	Número de ICs associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se a IVs para os quais esta solução é a preferencial. Esta contagem exclui itens vulneráveis adiados.
Percentual de ICs corrigidos	Percentual concluído para correção de IC. Aplica-se a IVs para os quais esta solução é

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas de status de correção

Campo	Descrição
	a preferencial. Esta contagem exclui itens vulneráveis adiados.
Metas de solução preferencial (inclui adiadas) - Status de correção de IVs, incluindo adiadas, para as quais esta é a solução preferencial	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Total de ICs	Número de ICs associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se a IVs para os quais esta solução é a preferencial.
Percentual de ICs corrigidos	Percentual concluído para correção de IC. Aplica-se a IVs para os quais esta solução é a preferencial.
Possíveis metas de solução - Status de correção de todos os IVs com uma vulnerabilidade relacionada a esta solução	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
Possíveis metas de solução (inclui adiados) – Status de correção de todos os IVs, incluindo adiados, com uma vulnerabilidade relacionada a esta solução	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção.
ICs Restantes	Número de ICs associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Em terceiro lugar, a disponibilidade de uma solução preferencial para vulnerabilidades e VITs deve ser garantida para corrigir as vulnerabilidades. No entanto, em situações em que existem várias soluções de substituição superiores para uma vulnerabilidade, uma solução preferencial não é preenchida devido à ambiguidade. Para lidar com esse cenário, é implementada uma abordagem que envolve a execução da lógica de processamento e o preenchimento da solução preferencial quando ela estiver disponível. Nos casos em que há apenas uma solução de substituição superior, ela é preenchida como a solução preferencial. Quando várias soluções de substituição superiores estão presentes, o campo de solução preferencial permanece vazio. No entanto, o objetivo é preencher a solução de substituição mais elevada, que é publicada como a mais recente, como a solução preferencial. Para isso, uma propriedade do sistema *sn_vul.latest_solutions* é introduzida. Por padrão, essa propriedade é definida como false. Se você quiser habilitar a capacidade de preencher as soluções mais recentes como a solução preferencial quando nenhuma solução preferencial estiver disponível, você poderá habilitar esta propriedade. Depois de habilitada, a coluna **Tipo de solução** é atualizada na tabela de vulnerabilidade com as seguintes opções:

- Preferencial: quando a solução preferencial é preenchida
- Mais recente: quando nenhuma solução preferencial está disponível, a solução mais recente do conjunto de soluções de substituição mais altas é selecionada com base no valor de data de publicação. O campo a ser selecionado como a solução mais recente pode ser personalizado usando a propriedade do sistema *sn_vul.latest_solutions*. Por padrão, o valor é definido como "data de publicação", mas pode ser alterado para "última modificação" para selecionar a solução com base na última coluna modificada nas soluções.
- Manual: quando o tipo de solução preferencial é atualizado manualmente. A precedência para este tipo de solução é a mais alta.

Em determinados cenários, a solução preferencial em um item vulnerável (VIT) pode ser diferente da solução preferencial na vulnerabilidade correspondente. Isso ocorre quando a solução preferencial é atualizada manualmente em um VIT e não na vulnerabilidade. Nesses casos, o campo **Tipo de solução** fica oculto no VIT.

O que Solução de gestão de vulnerabilidade faz

- Associa automaticamente novos itens vulneráveis (VITs) e tarefas de correção a soluções durante a Integração com a solução Microsoft Security Response Center importação do e Red Hat Solution Integration.

  MSRC As soluções estão associadas ao boletim mais recente em que a solução aparece.

- Associa automaticamente itens vulneráveis e tarefas de correção a soluções quando os registros de vulnerabilidade são associados manualmente a soluções.

  Nota: Itens vulneráveis reatribuídos manualmente a outra solução não são atualizados automaticamente com as mudanças de solução no nível da vulnerabilidade.

- MSRC: cria cadeias de substituição durante a importação que você pode exibir na lista relacionada da solução.
- Indica se uma solução é uma solução de substituição mais alta ou não.
- Lista a **pontuação de risco** da solução associada a cada solução para fornecer a você as maiores oportunidades de redução de risco.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Mantém o **status** de correção de soluções em **entradas de vulnerabilidade de terceiros**, **tarefas**de correção e registros de **solução de vulnerabilidade** para que você possa acompanhar o andamento da correção.

  Ele contém:

  - Contagens de itens vulneráveis por porcentagem corrigida, para os IVs com Soluções Preferenciais, com e sem esses VIs no estado Adiado.
  - Contagens de itens de configuração (IC) por porcentagem corrigida, para esses IVs com Soluções preferenciais, com e sem esses IVs no estado adiado.
  - Contagens de itens vulneráveis por porcentagem corrigida, para esses IVs com soluções potenciais, com e sem esses IVs no estado adiado.
  - Contagens de itens de configuração por porcentagem corrigida, para esses IVs com Soluções Preferenciais, com e sem esses VIs no estado Adiado.

O que você pode fazer com Solução de gestão de vulnerabilidade

- Crie, atualize, exiba ou exclua soluções associadas a vulnerabilidades, para que você possa rastrear soluções de vulnerabilidade que não são cobertas pelo conteúdo da solução de terceiros. A integração da solução com o Rapid7 Data warehouse não é compatível.
- Associe vulnerabilidades de terceiros e entradas do NVD a um registro de solução.
- Remova e associe novamente itens vulneráveis e tarefas de correção a uma solução.
- Exiba a **Solução preferencial** aplicável a uma determinada vulnerabilidade nos formulários de vulnerabilidade e item vulnerável.
- Exiba uma lista relacionada de **Soluções preferenciais** em formulários de tarefa de correção que listam todas as soluções que foram preferenciais por pelo menos um VI ativo nesse grupo.
- Exiba os detalhes do **status** de correção em uma solução que mostra a redução de risco associada à implantação da **solução preferencial** em vulnerabilidade, item vulnerável, tarefas de correção e formulários de solução.
- Exiba as vulnerabilidades aplicáveis a uma determinada solução no formulário de solução.
- MSRC: exiba as soluções substitutas para uma determinada solução em uma vulnerabilidade, para encontrar a atualização mais recente a ser implantada ou uma atualização anterior, mais focada e eficiente.
- Exibir listas de soluções classificadas para diferentes características.
  - Todos: soluções classificadas por data de publicação e número.
  - MSRC: maior substituição: soluções com itens vulneráveis ativos e não adiados. Classificado por **Substituição mais elevada**, **Data de publicação**e **Número**.
  - Com itens vulneráveis: soluções com itens vulneráveis ativos e não adiados. Classificado por **Substituição mais alta** ou **Preferencial**, **Pontuação de risco**e **Número**. Se implantadas, as entradas principais na lista fornecerão a maior redução de risco para os ativos em seu ambiente.

Pontuação de risco e classificação de risco do registro da solução

Nota: A **pontuação de risco** do registro da solução e a **classificação** de risco são distintas dos campos usados para vulnerabilidades, itens vulneráveis e tarefas de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A **pontuação de risco** do registro de solução é um cálculo ponderado com base na **pontuação de risco** do item vulnerável e em uma contagem de itens vulneráveis ativos com esta solução como sua **solução potencial**. A **pontuação de risco** da solução fornece uma estimativa da redução no risco que a solução deve realizar.

A **pontuação de risco** do registro da solução é calculada da seguinte forma:

- Ele começa com 85% da **pontuação de risco** mais alta ou máxima de um item vulnerável ativo com essa possível solução.
- A **pontuação de risco** do registro da solução tabula o número total de itens vulneráveis com essa solução em potencial. Para cada intervalo do número de itens vulneráveis, ele adiciona alguns pontos e chega a um total.
  - Os itens vulneráveis de 0 a 09 não adicionam pontos
  - De 10 a 99 itens vulneráveis adicionam 5 pontos
  - De 100 a 999 itens vulneráveis adicionam 10 pontos
  - 1.000 itens vulneráveis e além adicionam 15 pontos

  Por exemplo, para uma **pontuação de risco** de item vulnerável de 80, a **pontuação de risco** do registro de solução começará em 68. Se houvesse um total de 200 itens vulneráveis ativos com essa possível solução, a **pontuação final de risco** da solução seria 78.

A **classificação de risco** do registro de solução separa a **pontuação de risco** do registro de solução em intervalos de Crítico a Nenhum. A classificação de **risco da solução classifica** a redução de risco dos itens vulneráveis que esta solução corrige.

Até o VR v16.1, as classificações de risco separavam a **pontuação de risco** da solução resultante nos seguintes intervalos:

- 1 - Crítico (**pontuação de risco**da solução de 90+)
- 2 - Alto (**pontuação de risco**do registro de solução de 70-89)
- 3 - Médio (30-69 **Pontuação de risco**do registro de solução)
- 4 - Baixo (**pontuação de risco**do registro de solução de 1 a 29)
- 5 - Nenhum (0 **pontuação de risco do**registro da solução)

A partir do VR v16.1, as classificações de risco separam a **pontuação de risco** da solução resultante nos seguintes intervalos para a Gestão de soluções:

- 1 - Crítico (**pontuação de risco**da solução de 90+)
- 2 - Alto (**pontuação de risco**do registro de solução de 70-89)
- 3 - Médio (40-69 **Pontuação de risco**do registro de solução)
- 4 - Baixo (**pontuação de risco**do registro de solução de 1 a 39)
- 5 - Nenhum (0 **pontuação de risco do**registro da solução)

Casos de Uso

Exiba o andamento da implantação de status de um ciclo de patch atual usando o módulo de substituição mais alta, classificado por data.

Exiba as soluções de maior valor usando o módulo Com itens vulneráveis, classificadas por pontuação de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas de soluções comunicam os principais detalhes da solução, pontuações de risco e métricas de implantação. Use a **pontuação de risco** e as contagens de VI ativo para priorização. Veja quais soluções no ciclo de patch atual não estão progredindo, possivelmente uma indicação de um pré-requisito de implantação ausente.

Nota: Adicione **%VIs corrigidos (percent_nd_pref_vis_remediated)** no menu **Personalizar colunas da lista** para acompanhar o andamento da correção no formulário Soluções de vulnerabilidade.

Noções básicas sobre Integração com a solução Microsoft Security Response Center

Revise e implemente as soluções de correção propostas fornecidas pelo Integração com a solução Microsoft Security Response Center.

Integração com a solução Microsoft Security Response Center está incluído no recurso [Solução de gestão de vulnerabilidade do Resposta a vulnerabilidades, disponível por assinatura separada. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre como Resposta a vulnerabilidades incorpora soluções.

Microsoft Security Response Center investiga relatórios de vulnerabilidades de segurança que afetam os produtos e serviços da Microsoft e fornece informações da solução para ajudar a gerenciar os riscos à segurança. As soluções são correções conhecidas importadas para o seu Integração com a solução Microsoft Security Response Center do produto Microsoft Security Response Center.

O Integração com a solução Microsoft Security Response Center contém pontos de entrada para o produto Microsoft Security Response Center, invocado como trabalhos agendados. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Os trabalhos agendados são executados automaticamente e na ordem especificada. Você também pode executar trabalhos agendados individuais manualmente.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Para a versão mais atual das soluções Solução de gestão de vulnerabilidade e Microsoft Security Response Center, verifique se você tem a versão mais atual do Resposta a vulnerabilidades instalada.

Para obter mais informações sobre como instalar e configurar Solução de gestão de vulnerabilidade e integrações de solução, consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades e Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade usando o Assistente de configuração.

Versão de lançamento de Resposta a vulnerabilidades	**Versão de** Solução de gestão de vulnerabilidade	**Notas de versão**
Resposta a vulnerabilidades v15.0	v10.3	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções

Integração com a solução Microsoft Security Response Center tarefas envolvem as funções a seguir.

- sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto): pode ler, gravar e excluir registros.
- sn_vul.vulnerability_write: pode ler e gravar registros.
- sn_vul.vulnerability.read: pode ler registros.
- sn_vul.remediation_owner: pode ler e gravar anotações internas em registros atribuídos ao grupo de especialistas em correção ou ao indivíduo. (Contido na função itil.)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Integração com a solução Microsoft Security Response Center

Para exibir o Integração com a solução Microsoft Security Response Center, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.

A integração a seguir está incluída no sistema de base.

Integração com a solução Microsoft Security Response Center

Integração	Descrição
Integração da Solução do Centro de Resposta de Segurança da Microsoft	Recupera soluções e o mapeamento do banco de dados nacional de vulnerabilidades (NVD) para associar soluções a vulnerabilidades, itens vulneráveis e tarefas de correção. **Nota:** O Integração com a solução Microsoft Security Response Center não fornece soluções anteriores a 2016.

Soluções

Para exibir soluções importadas em uma lista, consulte Exibir uma solução.

Noções básicas sobre Red Hat Solution Integration

Você pode revisar e implementar as soluções de correção propostas fornecidas pelo Red Hat Solution Integration na aplicação Resposta a vulnerabilidades.

Red Hat Solution Integration está incluído no recurso [Solução de gestão de vulnerabilidade do Resposta a vulnerabilidades, disponível por assinatura separada. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre como Resposta a vulnerabilidades incorpora soluções.

Red Hat Solution Integration investiga relatórios de vulnerabilidades de segurança que afetam Red Hat produtos e serviços e fornece informações de solução para ajudar a gerenciar riscos de segurança. Soluções conhecidas como correções são importadas para seu Red Hat Solution Integration de Red Hat.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 21.0 do Resposta a vulnerabilidades, o Red Hat transmite cargas no formato CSAF (Common Security Advisory Framework), em vez do formato CVRF (Common Vulnerability Reporting Framework). CSAF, um padrão baseado em XML, difere em estrutura e formato de CVRF. Para acomodar essa mudança, um novo analisador de CSAF foi desenvolvido. Este analisador interpreta o formato CSAF, extraindo os campos necessários para preencher as tabelas adequadamente.

Nota: Por padrão, você receberá a carga no formato CSAF.

As extrações a seguir mostram o script de integração para analisar a carga recebida de Red Hat nos formatos CSAF e CVRF, respectivamente.

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

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

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

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

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

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

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

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

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

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

Red Hat Solution Integration contém pontos de entrada para o produto Red Hat, invocado como um trabalho agendado. O trabalho agendado simplifica o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Ele é executado automaticamente. Você também pode executar o trabalho agendado manualmente.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Para a versão mais atual das soluções Solução de gestão de vulnerabilidade e Red Hat, verifique se você tem a versão mais atual do Resposta a vulnerabilidades instalada.

Para obter mais informações sobre como instalar e configurar Solução de gestão de vulnerabilidade e integrações de solução, consulte Instalar a aplicação Solução de gestão

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de Resposta a vulnerabilidades e Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade usando o Assistente de configuração.

Versão de lançamento de Resposta a vulnerabilidades	**Versão de** Solução de gestão de vulnerabilidade	**Notas de versão**
Resposta a vulnerabilidades v15.0	v10.3	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Red Hat Solution Integration tarefas envolvem a seguinte função: sn_vul.configure_rhsa_integration

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Red Hat Solution Integration

Para exibir o Red Hat Solution Integration, navegue até **Resposta a vulnerabilidades** > **Administração** > **Integrações**.

A integração a seguir está incluída no sistema de base.

Integração do Red Hat

Integração	Descrição
Red Hat Solution Integration	Recupera soluções e o mapeamento do banco de dados nacional de vulnerabilidades (NVD) para associar soluções a vulnerabilidades, itens vulneráveis e tarefas de correção.

Soluções

Para exibir soluções importadas em uma lista, consulte Exibir uma solução.

Rapid7 gestão de soluções

As soluções são correções conhecidas que são importadas para o seu Integração com Rapid7 VulnerabilityRapid7 do data warehouse [] ou Rapid7 InsightVM. Rapid7 O data warehouse importa soluções e soluções substitutas. Com Rapid7 InsightVMo, você obtém soluções como parte da Integração de item vulnerável do Rapid7 - API.

A partir da versão 21.0 de Resposta a vulnerabilidades, há uma mudança na forma como as soluções são criadas por Rapid7 InsightVM. Em vez de depender dos campos **solution_summary**, **solution_fix**ou **solution_type**, Rapid7 InsightVM agora cria soluções usando

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

o solution_id fornecido pelo scanner. Isso significa que, mesmo que esses campos estejam vazios, uma solução será criada, desde que um ID de solução esteja disponível.

Para exibir as soluções importadas como uma lista, navegue até **Rapid7** > **Soluções**.

Se o plug-in Solução de gestão de vulnerabilidade estiver ativado, a versão mais recente do Integração com Rapid7 Vulnerability fornecerá os seguintes recursos principais em relação às soluções:

- A gestão de soluções Rapid7 foi movida para a gestão de soluções de vulnerabilidade.
- Foi introduzida uma nova integração de Gestão de soluções de pré-requisito do Rapid7 para o data warehouse. A integração busca a solução de pré-requisito do data warehouse Rapid7.
- A lista relacionada de Rapid7 (solução) em entradas de terceiros (TPE) está oculta.
- Os dados importados anteriormente podem ser exibidos no novo modelo de dados. As soluções Rapid7, a substituição de solução e o mapa de solução de vulnerabilidade são reimportados e o campo **Importar desde** é definido como vazio. O campo é preenchido no Gestão de soluções.
- As detecções são atualizadas para preencher o campo de solução. As detecções mostram as soluções, pois elas fazem parte da Gestão de soluções de vulnerabilidade.
- Rapid7 obtém maior preferência sobre outras soluções ao definir a solução preferencial no TPE para Rapid7 data warehouse.
- As soluções são acumuladas para itens vulneráveis (VI) de detecções para Rapid7 InsightVM.

Nota: Se você não ativou o plug-in Solução de gestão de vulnerabilidade, a aplicação funcionará como está.

Gerenciamento de soluções de vulnerabilidade

Se você ativou o plug-in Solução de gestão de vulnerabilidade, as soluções Rapid7Rapid7 para o data warehouse [] e Rapid7 InsightVM] serão preenchidas na tabela Soluções de vulnerabilidade [sn_vul_solution]. No entanto, se você não ativou o plug-in Solução de gestão de vulnerabilidade, o Integração com Rapid7 Vulnerability funcionará como está e importará as soluções na tabela [sn_vul_r7_solution] personalizada.

Para exibir a tabela de soluções de vulnerabilidade, navegue até **Todos** > **Resposta a vulnerabilidades** > **Soluções de vulnerabilidade** onde você pode exibir e comparar as soluções de diferentes fornecedores. Para exibir soluções importadas na tabela personalizada, navegue até **Todos** > **Integração com Rapid7 Vulnerability** > **Soluções**.

Nota: Agrupe por origem para exibir soluções com base em fornecedores.

Integração da Gestão de soluções de pré-requisito da Rapid7

Se você ativou o plug-in Solução de gestão de vulnerabilidade, um script de correção será executado e mudará a ordem das integrações. A nova integração de solução de pré-requisito do Rapid7 para data warehouse Rapid7 mapeia as soluções com as soluções de pré-requisito. As integrações são executadas na seguinte sequência:

1. Rapid7 Integração de solução
2. Rapid7 Solução de pré-requisito
3. Rapid7 Integração da solução substituta

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Rapid7 Integração do mapa de solução de vulnerabilidade
5. Rapid7 VI Solution Integration (de v19.0 de Resposta a vulnerabilidades)

Nota: Se você executar as integrações manualmente, comece com a Rapid7 Integração de Solução . Não altere a cadeia de Próxima integração na Integração Rapid7. A sequência é definida na coluna Próxima integração.

Lista relacionada de Rapid7 (Soluções) no TPE

Se você ativou o plug-in Solução de gestão de vulnerabilidade, poderá fazer o seguinte:

- Você pode exibir os TPEs navegando até **Todos** > **Resposta a vulnerabilidades** > **Terceiros**.
- Você não pode ver a lista relacionada Soluções (Rapid7), que estava disponível nas versões mais antigas.
- Você pode ver as soluções relacionadas ao Rapid7 na lista relacionada Soluções junto com as soluções de outras origens, como RedHat, Microsoft (MSRC) e assim por diante.

Se você não ativou o plug-in Solução de gestão de vulnerabilidade, ocorre o seguinte:

- A funcionalidade de listas relacionadas permanece a mesma.
- Você pode ver a lista relacionada de Soluções (Rapid7).
- A lista relacionada Soluções está oculta.

Solução preferencial em TPE e VIs

Rapid7 obtém a solução do data warehouse no nível de entrada de terceiros (TPE) e para Rapid7 InsightVM no nível de detecção.

Para um Rapid7 data warehouse, a solução é gerenciada da seguinte maneira:

- A solução preferencial é definida no TPE com base no mapeamento de vulnerabilidade e solução.
- Se a vulnerabilidade de Rapid7 tiver uma única solução de substituição mais alta de Rapid7, ela será definida como a solução preferencial, independentemente de outras soluções de fornecedores anexados a essa vulnerabilidade.
- Em todos os outros casos, o fluxo da solução preferencial permanece o mesmo. Para obter mais informações sobre o comportamento padrão das soluções preferenciais, consulte Solução de gestão de vulnerabilidade.

Para Rapid7 InsightVM, a solução é gerenciada da seguinte maneira:

- A solução preferencial é acumulada de detecções para IVs.
- Se houver uma única detecção e solução de Rapid7, a solução será acumulada para VI.
- Se houver várias detecções e todas tiverem a mesma solução de Rapid7, a solução será acumulada para VI.
- Se várias detecções tiverem várias soluções de Rapid7, a solução mais recente será acumulada para o VI.

A partir da v19.0 de Resposta a vulnerabilidades, a solução preferencial, gerada pelo Rapid7 Data Warehouse, é preenchida diretamente em itens vulneráveis Rapid7 ignorando a necessidade de Solução de gestão de vulnerabilidade. Essa mudança garante que qualquer dúvida sobre possíveis soluções para esses itens vulneráveis seja eliminada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para atingir esse preenchimento direto por meio de Rapid7, as seguintes etapas são executadas:

- Uma nova integração, Rapid7 VI Solution Integration, é estabelecida e integrada ao fluxo de trabalho de integração de vulnerabilidade Rapid7 existente.
- Uma nova tabela [sn_vul_r7_rapid7_vi_solution_import] foi criada.
- Um novo mapa de transformação de solução de VI do Rapid7 é criado.
- A inclusão de script Rapid7AssetsImportProcessor foi modificada para excluir o processamento de soluções geradas pelo Rapid7 em Solução de gestão de vulnerabilidade.

Após a execução da integração da solução Rapid7 VI, os dados não processados obtidos de Rapid7 são armazenados na tabela recém-criada. Posteriormente, a Transformação da solução de VI do Rapid7 é acionada, processando esses dados e preenchendo a solução preferencial diretamente na tabela de itens vulneráveis.

Nota: A integração da solução Rapid7 VI preenche a solução preferencial exclusivamente quando o plug-in Solução de gestão de vulnerabilidade é instalado.

A partir da v22.0 de Resposta a vulnerabilidades, as soluções de Rapid7 não estão mais enfileiradas ao executar o trabalho agendado *Process Vulnerability Solutions Metrics Queue*. Este trabalho programado envolve o acúmulo de soluções de entradas do NVD para entradas de terceiros, o preenchimento de soluções preferenciais em vulnerabilidades e a atualização das métricas de status de correção nas soluções. Nos seguintes cenários, somente as métricas de status de correção devem ser atualizadas:

- Quando a solução preferencial muda nas vulnerabilidades
- Quando os VITs são criados ou excluídos
- Quando uma importação de VIT é concluída

Embora as soluções estejam enfileiradas para atualizar somente as métricas de status de correção, elas ainda tentam acumular soluções de entradas do NVD para entradas de terceiros e preencher as soluções preferenciais. Para otimizar esse processo, na tabela Solução de vulnerabilidade, a coluna **Status da atualização** foi introduzida. Quando as métricas de status de correção nas soluções precisam ser atualizadas sem exigir o acúmulo de soluções de entradas do NVD para entradas de terceiros ou o preenchimento de soluções preferenciais, elas não são mais enfileiradas. Em vez disso, a coluna **Atualizar status** é atualizada diretamente como verdadeira. Essa abordagem permite lidar com casos em que somente as métricas de status de correção devem ser atualizadas, resultando em economia de tempo e recursos. No trabalho agendado, depois que o processamento das soluções enfileiradas é concluído, as soluções marcadas com um status de atualização como verdadeiro são identificadas. Em seguida, eles são iterados por meio dessas soluções, calculando as contagens e atualizando as métricas de status de correção de acordo. Esta etapa desempenha um papel significativo na melhoria do desempenho do trabalho agendado, pois o número de soluções que devem ser enfileiradas é reduzido.

Cadeia de substituição de solução importada do data warehouse Rapid7 para uma vulnerabilidade

Você pode exibir as soluções substitutas para uma solução selecionando uma solução de vulnerabilidade e selecionando a lista relacionada Soluções substitutas. Você pode exibir as soluções anteriores selecionando a lista relacionada Soluções anteriores. Quando você anexa qualquer solução ao TPE, a solução substituta dessa solução é anexada a esse TPE.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alterar a profundidade máxima da cadeia de substituição de solução em um gráfico por propriedade do sistema

A cadeia de substituição de solução recebida no modelo de dados Rapid7 é muito longa para criar o gráfico durante o preenchimento da solução preferencial. Portanto, para restringir a profundidade da cadeia, uma propriedade do sistema chamada *sn_vul.max_recursion_depth* com um valor 500 é criada. Se a profundidade da cadeia for maior que 500, o restante da cadeia será ignorado. Para alterar a profundidade máxima da cadeia, navegue até a tabela [sys_properties] e altere o valor da propriedade.

Atualizando a aplicação Rapid7

Se você fizer upgrade do plug-in Integração com Rapid7 Vulnerability e ainda não tiver ativado o plug-in Solução de gestão de vulnerabilidade, a aplicação funcionará como está.

Independentemente de você ativar o plug-in Solução de gestão de vulnerabilidade antes ou depois de atualizar a aplicação Rapid7, o campo **Importar desde** permanecerá vazio para as seguintes integrações:

- Integração da solução substituta da Rapid7
- Integração do mapa de solução de vulnerabilidade da Rapid7
- Integração da Solução Rapid7

> **Nota:** A partir da próxima execução de integração, os dados são preenchidos na tabela de soluções de vulnerabilidade.

Para Rapid7 InsightVM, os dados são recebidos no nível de detecção. Quando a integração Rapid7 InsightVM é executada, as soluções são importadas na tabela de soluções de vulnerabilidade.

Estrutura genérica para ingerir dados de qualquer fornecedor de solução

Uma estrutura genérica para integração de inteligência de solução está disponível para oferecer suporte à ingestão de dados em diferentes formatos de arquivo de fornecedores de soluções. Esses formatos aceleram a troca e o processamento de informações e facilitam o compartilhamento de informações críticas relacionadas à segurança em um formato de relatório padronizado.

Os formatos de arquivo compatíveis são:

Common Vulnerability Reporting Framework (CVRF)

O Common Vulnerability Reporting Framework (CVRF) é uma linguagem baseada em XML. Os principais fornecedores, como Oracle, Red Hat, Ciscoe Microsoft, oferecem suporte ao formato CVRF.

CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum)

O CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum) é um padrão de código aberto que fornece avisos de segurança estruturados e legíveis por máquina baseados em JSON. Os principais fornecedores, como Siemens, Red Hat, Hitachi e Schneider, oferecem suporte ao formato CSAF.

A gestão de soluções compatíveis com CVRF ou CSAF inclui os seguintes recursos principais:

- Configuração por meio do Assistente de configuração
- Suporte à importação de dados CVRF ou CSAF por meio da importação de arquivo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Suporte à importação de dados de CVRF ou CSAF por meio da URL de CVRF ou CSAF
- Suporte à importação de dados CVRF ou CSAF por meio de consultorias
- Mapeamento de soluções com vulnerabilidades relacionadas

O plug-in Resposta a vulnerabilidades se encarrega de atualizar os status das métricas da solução criada.

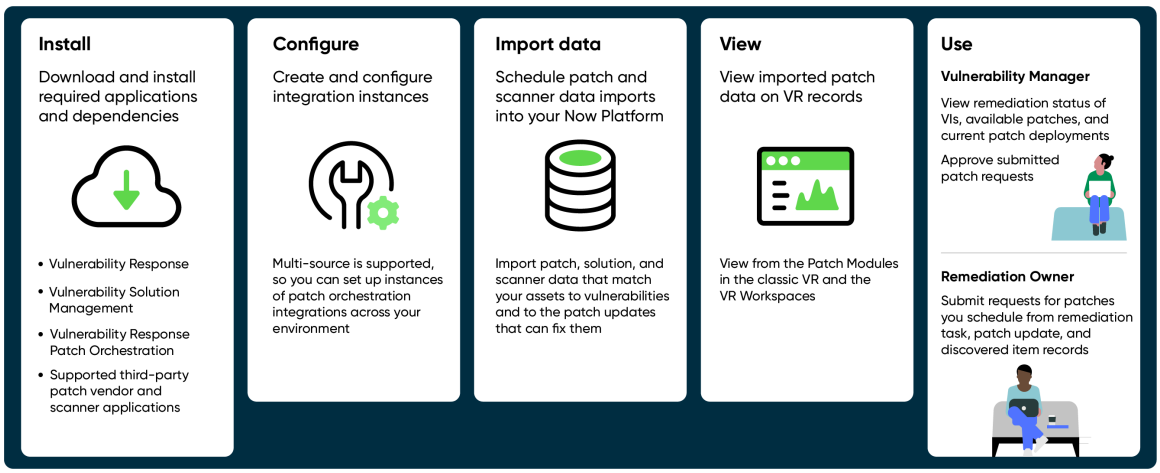
Para obter mais informações sobre como configurar os provedores de soluções, consulte Configurar provedores de soluções de vulnerabilidade.

Orquestração de patches com Resposta a vulnerabilidades

Você pode gerenciar patches e implantações de patches para vulnerabilidades críticas de grandes grupos de ativos com a Orquestração de patches com Resposta a vulnerabilidades. Resposta a vulnerabilidades A Orquestração de patches e as integrações de orquestração de patches estão disponíveis no ServiceNow® Store.

Noções básicas sobre a orquestração de patches com Resposta a vulnerabilidades

A orquestração de patches com Resposta a vulnerabilidades usa dados de importações agendadas de integrações de soluções de terceiros, fornecedores de patch e scanners de vulnerabilidade. Esses dados estão correlacionados na aplicação Resposta a vulnerabilidades. Essa organização de dados permite que você conclua as etapas do ciclo de correção de vulnerabilidades. Comece identificando vulnerabilidades, depois aplique patches e atualizações e, por fim, feche itens vulneráveis usando dados de scanner de terceiros, tudo de dentro da sua instância Now Platform®.



A orquestração de patches com Resposta a vulnerabilidades é compatível com o ambiente clássico e os espaços Resposta a vulnerabilidades.

Para obter informações sobre a orquestração de patches nos espaços de trabalho, consulte Orquestração de patches com os espaços Resposta a vulnerabilidades.

Com a orquestração de patches em Resposta a vulnerabilidades, os gerentes e analistas de vulnerabilidade e os especialistas em correção de TI podem executar as seguintes tarefas de correção:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Veja mais contexto e informações sobre os tipos de patches e fornecedores que compõem suas soluções (patches).
- Exiba e monitore dados de vulnerabilidade e solução, bem como o andamento da correção de vulnerabilidades de registros nos espaços Resposta a vulnerabilidades ou no ambiente clássico.
- Implante patches compatíveis com fornecedores de soluções de terceiros para seus Windows, CentOS, macOS, Oraclee outros ativos em intervalos regulares e programados. Você pode programar patches fora do horário comercial para evitar conflitos com aqueles que estão no trabalho.
- Usando dados de detecção importados fornecidos por scanners de terceiros, identifique os ativos que têm vulnerabilidades e não foram corrigidos ou não foram atualizados com sucesso por patches programados.
- Inicie e programe patches disponíveis para ativos que exigem atualizações de Atualização de patch, tarefa de correção e registros de itens descobertos na aplicação Resposta a vulnerabilidades.
- Monitore as implantações de patch com um processo de aprovação opcional para solicitações de patch enviadas por seus especialistas em correção.

Termos principais

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados no Configuration Management Database (CMDB).

Item vulnerável (VI)

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB. Itens vulneráveis (VITs) são agrupados em tarefas de correção, ou listas, de acordo com determinados critérios que especificam ações de correção para IVs.

Instância

Refere-se a uma conta distinta de uma aplicação do fornecedor de soluções. Por exemplo, cada conta de usuário pode ser uma instância na aplicação HCL BigFix. Este termo também se refere a um endereço da Web exclusivo e seguro para uma instância Now Platform®.

Solução

Existem dois tipos de soluções no contexto desta integração, potenciais e preferenciais. Uma possível solução é aquela que pode resolver uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis. Uma solução preferencial corresponde à solução mais eficaz para uma vulnerabilidade específica detectada.

Patch

Atualizações de software que corrigem vulnerabilidades. Os fornecedores de patch usam seus próprios nomes para patches, por exemplo, Na aplicação HCL BigFix, os patches são chamados de Fixlets.

Patch preferencial

Patches preferenciais são atualizações de software que têm como objetivo corrigir vulnerabilidades específicas. Os patches, uma vez implantados, são mapeados para os itens vulneráveis que estão relacionados a vulnerabilidades específicas e os corrigem.

Implantação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para fins desta integração, a implantação se refere a quando você aplica, inicia ou programa um patch em uma máquina.

A implantação no Now Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações de um scanner de terceiros ou uma integração de fornecedor de solução em seu ambiente.

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

- A aplicação Resposta a vulnerabilidades e os plug-ins de dependência, Security Support Common e Orquestração de suporte de segurança.
- Solução de gestão de vulnerabilidade.
- Resposta a vulnerabilidades Aplicação de Orquestração de patches disponível no ServiceNow® Store.
- Uma aplicação de fornecedor de patch de terceiros compatível, como a integração de orquestração de patches da Resposta a vulnerabilidades com HCL BigFix ou a integração de orquestração de patches da Resposta a vulnerabilidades com Microsoft SCCM.
- Integrações de scanner de terceiros compatíveis com a Resposta a vulnerabilidades.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para exibir dados e programar patches da aplicação Resposta a vulnerabilidades. Consulte as informações de configuração das integrações compatíveis que você está usando listadas abaixo para obter mais informações.

- Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades e a integração de orquestração de patches da Resposta a vulnerabilidades com o Microsoft SCCM.
- Nos espaços Resposta a vulnerabilidades e no ambiente clássico, a função sn_vul_patch_orch.read_patch, que permite que os usuários exibam, mas não editem dados, é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst.

  As funções que você precisa atribuir e que são necessárias para configurar as conexões com os fornecedores de patch e programar patches são específicas da integração. Consulte Configurar a integração de orquestração de patches Resposta a vulnerabilidades com HCL BigFix e Configurar a Orquestração de patches de resposta a vulnerabilidades com MS SCCM para obter mais informações.

Há um processo de envio e aprovação para solicitações de patch incluídas com as aplicações. Por padrão, uma propriedade do sistema é ativada [**sn_vul_patch_orch.patch_approval_required**] na aplicação Orquestração de patches de resposta a vulnerabilidades em sua instância Now Platform.

Esta propriedade do sistema é ativada para que, quando as implantações de patch forem programadas, elas sejam enviadas para revisão e aprovação dos usuários atribuídos ao Nível 1 - Grupo de aprovação de atualizações de patch. Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, poderá desativar a propriedade [**sn_vul_patch_orch.patch_approval_required**]. Você pode preferir deixar as aprovações ativadas para que os patches programados não entrem em

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

conflito com o horário comercial normal. Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Para obter mais informações e como desativar esta propriedade do sistema, consulte o tópico de configuração da sua integração compatível.

- Configurar a integração de orquestração de patches Resposta a vulnerabilidades com HCL BigFix.
- Configurar a Orquestração de patches de resposta a vulnerabilidades com integração de Microsoft SCCM.

Programar patches de Resposta a vulnerabilidades registros

Os especialistas em correção podem programar atualizações de patch para resolver itens vulneráveis e monitorar o andamento da correção a partir de registros na aplicação Resposta a vulnerabilidades.

Você pode programar patches dos seguintes registros:

- Atualização de patch
- Tarefa de correção
- Item descoberto

Registros que acumulam contagens de VI ativo em Resposta a vulnerabilidades

Para evitar possíveis problemas de desempenho com o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho agendado que seleciona mudanças modifica somente a contagem de VI ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros na aplicação Resposta a vulnerabilidades :

- VIT (item vulnerável)
- RT (tarefa de correção)
- Solução de vulnerabilidade
- Atualização de patch

Para obter mais informações sobre como exibir dados de patch e acúmulo de dados de patch para registros e como exibir patches sem soluções, consulte os tópicos a seguir.

- Dados de patch e rollup de estado para orquestração de patches no Resposta a vulnerabilidades.
- Exibição de dados de patch e programação de patches no Resposta a vulnerabilidades.
- Exibir patches sem soluções em Resposta a vulnerabilidades.

Edição em massa de itens vulneráveis com patches

Você pode editar em massa itens vulneráveis no ambiente clássico que tenham patches do ambiente clássico. Para obter mais informações sobre como a edição em massa funciona, consulte Editar itens vulneráveis em massa no Resposta a vulnerabilidades. Os patches preferenciais para todos os IVs selecionados para edição em massa. Esta opção de edição funciona somente se houver patches preferenciais mapeados para todos os IVs selecionados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral da Gestão de exceções

Quando sua organização não pode cumprir uma política de segurança ou gestão de vulnerabilidades, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável (VI) ou tarefa de correção (RT) que não pode ser corrigida de acordo com a política.

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade.

Ciclo de vida de uma exceção

Definição de uma exceção

Uma exceção é uma solicitação para adiar a correção de um VI ou RT por um período especificado. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Como solicitar uma exceção

Como responsável pela correção, você pode solicitar uma isenção para um VI ou RT usando o processo de gestão de exceções. Depois que o aprovador de exceção aprova esta solicitação, o VI ou RT é movido para um estado **adiado**.

Como aprovar uma solicitação de exceção

IVs ou RTs que não podem ser corrigidos imediatamente são revisados por analistas de vulnerabilidade, avaliados quanto ao risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se apenas o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção.

Nota:

- A partir da Resposta a vulnerabilidades v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

  Depois que uma solicitação de exceção para um VI ou RT for aprovada, você poderá executar as seguintes ações:

  - Reabrir
  - Excluir
  - Atualizar os campos **Atribuição a** ou **Grupos** de atribuição
- A partir da v23.0 de Resposta a vulnerabilidades, o fluxo de trabalho **de Aprovação do Estado da Regra de Exceção** foi descontinuado e substituído pelo fluxo de Aprovação de Regra de Exceção no Flow Designer.

Acompanhamento de uma solicitação de exceção

Tradução automática

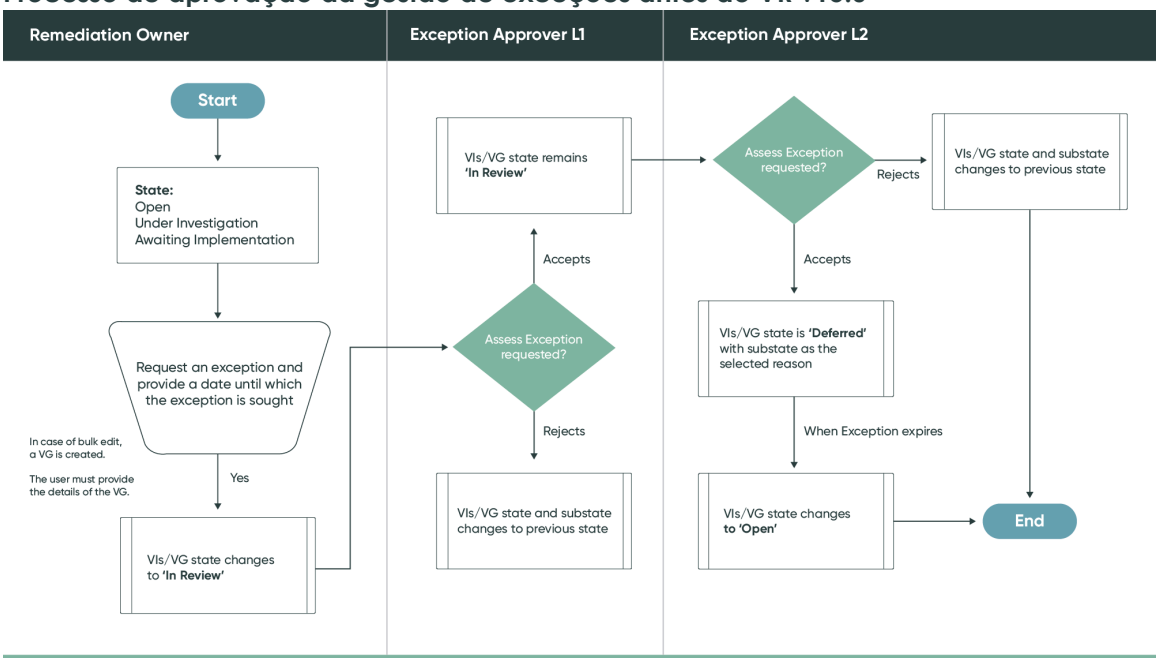
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** do VI ou RT. Se uma ação for realizada em um RT, você não poderá rastrear o status dos IVs individuais nesse RT.

Expiração de uma solicitação de exceção

Quando uma solicitação de exceção para um VI ou RT específico expira, o VI ou RT afetado é revertido para o estado **Aberto**.

Processo de aprovação da gestão de exceções antes do VR v15.0



Se um único VI ou todos os IVs em um RT forem aprovados na próxima verificação, os VIs e, quando aplicável, o campo **Estado** do RT mudarão para **Encerrado** com o subestado **Fixo**.

Vários adiamentos

Rastreie o número de vezes que um registro ou uma tarefa de correção é adiado. Um trabalho agendado, *`set deferral counts`*, é executado diariamente para publicar contagens dos registros que foram adiados mais de uma vez na coluna Contagem de adiamento no módulo Vários adiamentos para VR. Todas as contagens de registros associados a uma tarefa de correção serão coletadas e publicadas se uma tarefa de correção for adiada mais de uma vez.

Informações relacionadas

- Solicitar exceções para tarefas de correção e registros do Vulnerability Manager Workspace
- Solicitar uma exceção no Espaço de correção de problemas de TI
- Solicitar uma exceção usando GRC: Gestão de políticas e conformidade no Espaço de correção de problemas de TI

Visão geral das regras de exceção

As regras de exceção para Resposta a vulnerabilidades permitem automatizar o processo de adiamento de itens vulneráveis (IVs). Solicite uma exceção para os itens vulneráveis (IVs) que não podem ser corrigidos ou adiados imediatamente, identificando as vulnerabilidades, itens de configuração (ICs) ou IVs afetados. Adie os IVs correspondentes com base na regra quando o sistema os identificar, automatizando o processo de adiamento de VI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar regras de exceção em sua organização

Use regras de exceção para adiar automaticamente IVs novos e existentes por um período específico se eles corresponderem à condição de regra aprovada. A automação minimiza o risco de acordos de nível de serviço ausentes e facilita o gerenciamento de vários itens, pois você elimina a intervenção manual.

As regras de adiamento oferecem suporte à ordenação, ou seja, a regra com a prioridade mais alta é executada primeiro. Quando uma regra de alta prioridade é aplicada a um VI, nenhuma regra subsequente é aplicada novamente, mesmo se a condição corresponder ao VI.

Nota:

- Você só pode criar regras se selecionar Resposta a vulnerabilidades na configuração da Gestão de exceções. Para obter detalhes, consulte Configurar Gestão de exceções para Resposta a vulnerabilidades.
- Quando os IVs são adiados por uma regra de exceção, eles são copiados para o grupo de vulnerabilidade de adiamento (VG) criado. Os IVs continuam a fazer parte dos VGs dos quais faziam parte anteriormente.

O ciclo de vida de uma regra de exceção é o seguinte:

- Como criar uma regra de exceção
- Como aprovar uma solicitação de regra de exceção
- Ativação de uma regra de exceção
- Como adiar uma regra de exceção
- Expiração de uma regra de exceção

Como criar uma regra de exceção

Você pode criar uma regra de exceção para adiar automaticamente os IVs que correspondem às condições definidas para o período especificado. Depois de criar uma regra de exceção, envie-a para aprovação.

Como aprovar uma solicitação de regra de exceção

A aprovação de uma solicitação de regra de exceção é um processo de dois níveis. Se apenas o aprovador de primeiro nível estiver presente, a regra de exceção poderá ser avaliada e aprovada por uma única aprovação. No entanto, se não houver um aprovador de primeiro nível, uma aprovação de regra de exceção não poderá ser aprovada. Depois que a regra é aprovada, uma tarefa de correção (RT) é criada. Para obter mais informações, consulte Aprovar uma solicitação de regra de exceção.

Nota:

A partir da Resposta a vulnerabilidades v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Depois que uma solicitação de regra de exceção é aprovada, você pode executar as seguintes ações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Cancelar
- Excluir

Ativação de uma regra de exceção

Depois que uma regra de exceção é aprovada, uma tarefa de correção é criada em um estado Adiado por padrão. A partir da data "Válido a partir de", a regra de exceção é executada em todos os IVs criados e também naqueles que são movidos do estado Fechado para Aberto.

Nota: Se você habilitar a opção Executar em dados existentes, um trabalho agendado será executado uma vez nos dados existentes na data "Válido a partir de".

Como adiar uma regra de exceção

Você pode adiar IVs que correspondam às condições definidas nesta regra de exceção, até a data "Adiada até" definida para a regra. Nesta data, a tarefa de correção que você criou para a regra de exceção é encerrada e todos os IVs neste grupo voltam para o estado Aberto. Regras de grupo são aplicadas a eles novamente para alocá-los aos RTs necessários.

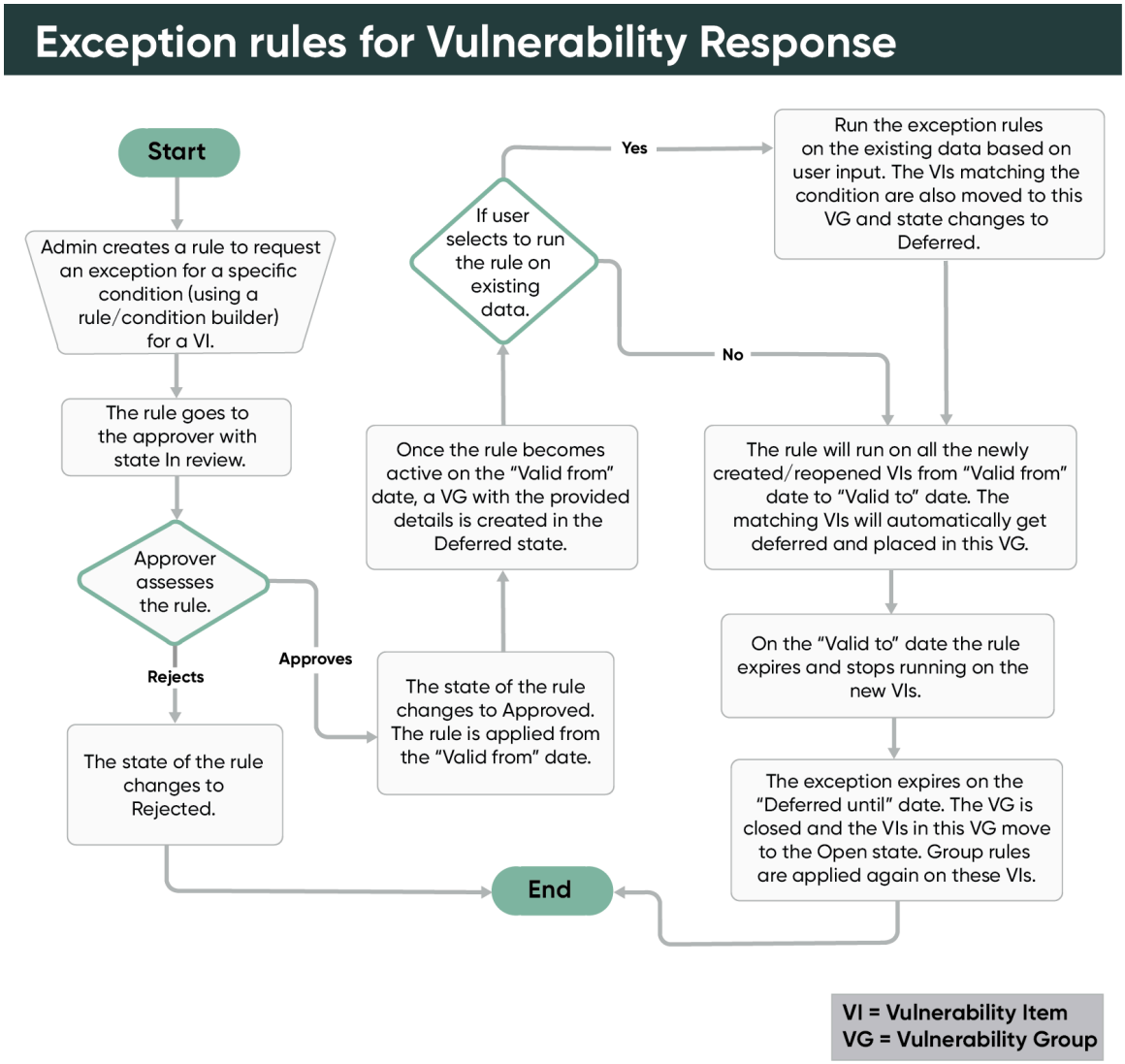
Expiração de uma regra de exceção

Depois que a regra de exceção expira, ela não é mais executada em IVs novos ou reabertos. O RT associado permanece no estado Adiado até a data "Adiado até".

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de regras de exceção anterior a v15.0



Visão geral das regras de exclusão

As regras de exclusão fornecem uma maneira de filtrar ou impedir que as detecções sejam convertidas em itens vulneráveis (VITs) durante o processo de ingestão em Resposta a vulnerabilidades.

Essas regras podem ser configuradas para lidar com vários cenários, como:

- Excluindo vulnerabilidades com baixa gravidade ou risco que não exigem correção imediata.
- Melhorar o processo de correção priorizando os VITs mais críticos para ação.
- Reduzindo o tempo de processamento durante a importação de dados excluindo uma porcentagem de detecções da conversão de VIT.

Durante o processo de ingestão de dados, há abordagens distintas para lidar com detecções novas e existentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para novas detecções:
  - Se uma nova detecção não atender às condições de uma regra de exclusão, uma detecção será criada com os VITs.
  - Se uma nova detecção atender às condições de uma regra de exclusão, a regra será associada à detecção, mas o VIT não será criado. Preencha a referência da regra de exclusão correspondente no registro de detecção. A coluna Regra de exclusão é preenchida com a referência da Regra de exclusão no registro de detecção.
- Para detecções existentes:
  - Se a detecção não atender às condições de nenhuma regra de exclusão, ela continuará com o fluxo de trabalho normal.
  - Se uma detecção existente corresponder às condições de uma regra de exclusão, o VIT associado a essa detecção permanecerá no estado atual, mas a regra será associada à detecção. O estado do VIT é regido pelo valor definido na propriedade *sn_vul.close_vit_with_excluded_detections*. Por padrão, o valor nesta propriedade é definido como falso. Se o valor estiver definido como Falso, as detecções em um VIT serão excluídas e o estado dos VITs permanecerá no estado atual. No entanto, se o valor estiver definido como Verdadeiro, os seguintes cenários poderão ocorrer:
    - Se todas as detecções em um VIT forem excluídas, o status do VIT será atualizado para Encerrado excluído.

      Nota: A partir da v22.1.2 de Resposta a vulnerabilidades, um novo subestado chamado Excluído foi adicionado,

    - Se uma detecção for marcada como encerrada enquanto as restantes forem excluídas, o VIT será designado como encerrado fixo.
    - Se o VIT tiver detecções em aberto, o VIT permanecerá Aberto.

Informações relacionadas

Criar uma regra de exclusão

Falso-positivo visão geral

Um falso-positivo é uma condição em que o scanner relata que existe uma vulnerabilidade no sistema, mas na verdade não há vulnerabilidade. Pode haver vários motivos, como classificação incorreta, lógica ou algoritmo inadequados no scanner. O responsável pela correção pode marcar itens vulneráveis (VIs) ou tarefas de correção (RTs) como falso-positivos.

Importante: Você pode marcar os itens vulneráveis de host como falso-positivos em massa no Vulnerability Manager Workspace. Para obter mais informações sobre como marcar os itens vulneráveis de host como falso-positivos em massa, consulte Edição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades.

Ciclo de vida de um falso-positivo

Significado de falso-positivo

O scanner às vezes emite um aviso quando, na verdade, não há vulnerabilidade. Por exemplo, se um item de configuração foi desativado, mas o scanner ainda está levantando um problema relacionado a ele, marque-o como um falso-positivo.

Marcar como falso-positivo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter detalhes sobre como marcar um VI ou RT como falso-positivo, consulte Marcar como falso-positivo.

Como trabalhar com o falso-positivo

Depois que um VI ou RT é marcado como falso-positivo, o estado é atualizado para Fechado e o subestado é alterado para Falso-positivo. As ações a seguir podem ser realizadas:

- Reabrir
- Excluir
- Atualize a data no campo **Até**. Esta data é usada como a data de vencimento para o falso-positivo.

Nota: Se não for aprovado, o VI ou RT será revertido para o estado anterior.

Como aprovar um falso-positivo

O aprovador pode aprovar o falso-positivo em seu fluxo de trabalho de aprovação.

Nota:

A partir da Resposta a vulnerabilidades v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Reabrir um falso-positivo

Um VI ou RT em um subestado falso-positivo pode ser reaberto a qualquer momento.

Como rastrear um falso-positivo

Use a seção **Aprovações de mudança de estado** para rastrear o status do falso-positivo. Depois de aprovado, o estado do VI ou RT é atualizado para Encerrado e o motivo é Falso-positivo.

Expiração de um falso-positivo

Somente o aprovador de falso-positivo pode definir uma data Até para o falso-positivo, para que o VI ou RT expire. Além disso, somente os falsos positivos para os quais o aprovador forneceu uma data Até podem expirar. Essa data pode ser fornecida após a aprovação do falso-positivo.

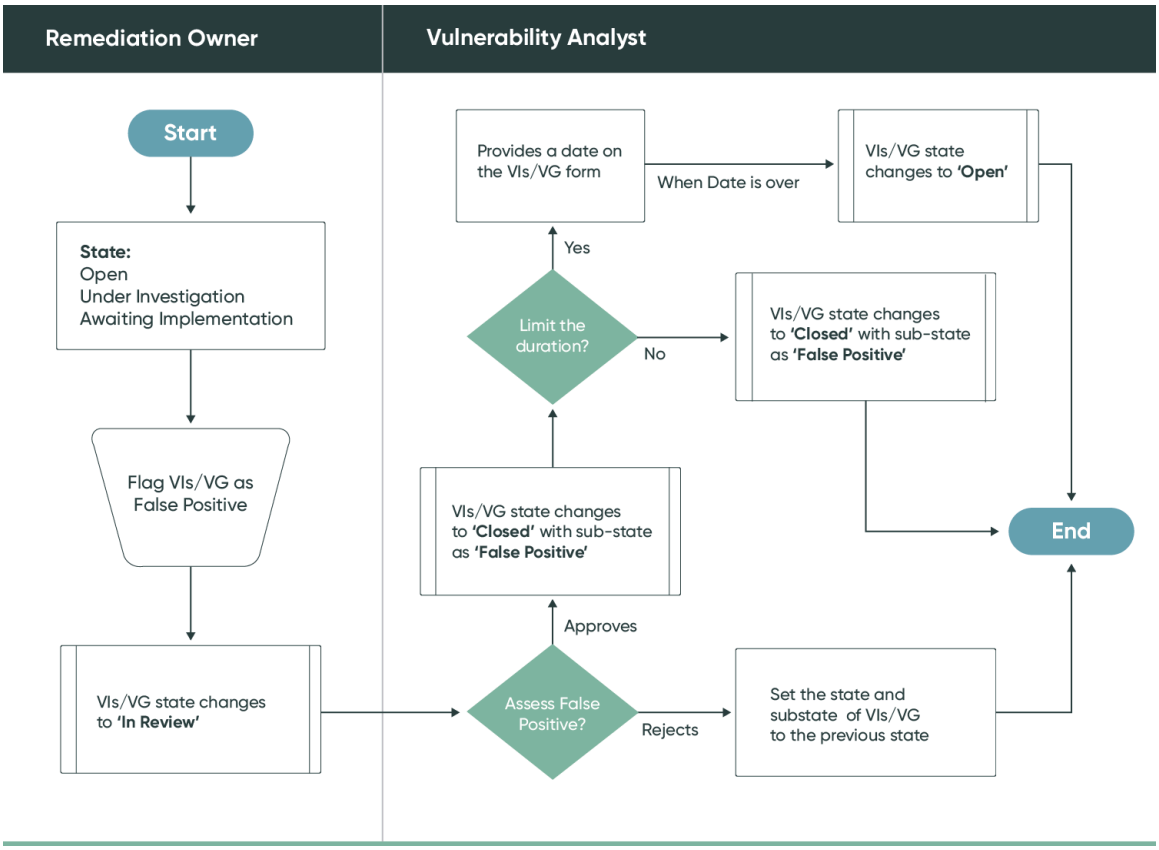
Um falso-positivo sem uma data Até é um falso-positivo permanente. Depois que o falso-positivo expirar, o estado do VI ou VR voltará para Aberto.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Processo de aprovação de falso-positivo anterior à v15.0



O processo de aprovação será automático se todos os IVs forem aprovados na próxima verificação. Os IVs são encerrados automaticamente, independentemente do estado atual. Os IVs ou, quando aplicável, os campos de **Estado** de RT mudam para **Encerrado** com o subestado **Fixo.**

Para obter mais informações, consulte Marcar e aprovar um falso-positivo.

Informações relacionadas

Solicitar um falso-positivo no Espaço de correção de problemas de TI

Watchdog para Resposta a vulnerabilidades

O watchdog é usado para rastrear tabelas com base nas condições especificadas. Por exemplo, ele pode ser usado para registrar detalhes de falhas de execução de integração em Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode optar por ser notificado sobre essas falhas. Com base nesta notificação, você pode planejar a correção. Os observadores padrão são:

- Falha na execução da integração: se o Estado de execução da integração estiver definido como Concluído e o Subestado estiver definido como Com falha, os usuários e grupos de usuários serão notificados se a condição retornar uma contagem maior que 0, ou seja, a execução da integração falhará.
- Integrações de longa execução: script para verificar se a execução da integração está excedendo o tempo definido. Este watchdog alerta proativamente sempre que houver um atraso na conclusão da execução da integração.

Log de observação

O watchdog vem com um log de observação, que fornece uma contagem do número de vezes que a condição foi atendida.

Painel Visão geral

Use o painel Visão geral para monitorar o cão de guarda nos últimos 30 dias. Você pode criar vários widgets para rastrear outros tópicos de monitoramento que está monitorando.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Relatório

Nome	Descrição
Falha no WatchDog nos últimos 30 dias	Todas as condições atendidas nos últimos 30 dias.

Para obter mais informações, consulte Configurar watchdog e Manipulação de erros para detecções.

Gestão de mudanças para Resposta a vulnerabilidades

Como responsável pela correção de TI, você pode criar e gerenciar solicitações de mudança (CHG) diretamente a partir das tarefas de correção (RT) na aplicação Resposta a vulnerabilidades. As solicitações de mudança ajudam a iniciar e rastrear atividades de mudança em seus ativos para que você possa corrigir suas tarefas de correção e os itens vulneráveis correspondentes.

Solicitações de mudança e o fluxo de trabalho de vulnerabilidade

Se você não estiver familiarizado com a aplicação Resposta a vulnerabilidades, consulte Explorar a aplicação Resposta a vulnerabilidadespara obter mais informações.

A imagem a seguir ilustra o fluxo de informações para Resposta a vulnerabilidades, desde a configuração da integração (scanner) até a triagem automatizada e a investigação.

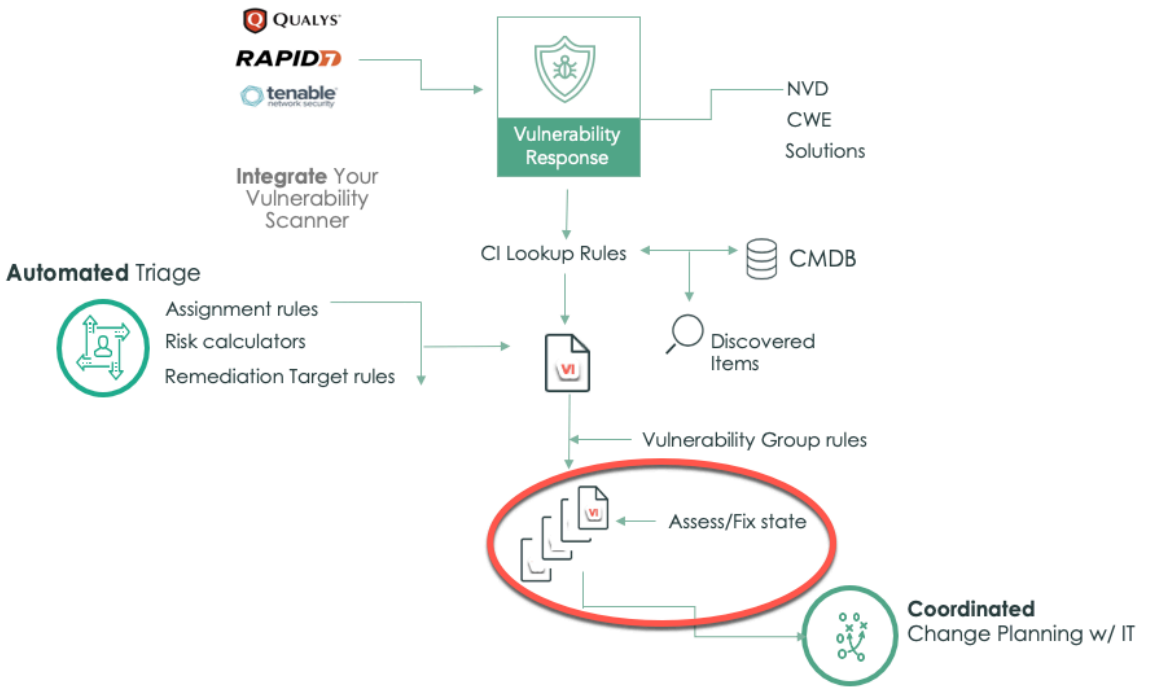
As solicitações de mudança e a gestão de mudanças fazem parte do processo de correção (estado Avaliar/Corrigir) no fluxo de trabalho Resposta a vulnerabilidades mostrado na figura a seguir. Durante esta fase, você pode usar solicitações de mudança para iniciar e rastrear a correção de vulnerabilidades. Você pode criar e gerenciar solicitações de mudança diretamente da tarefa de correção e listar tarefas de investigação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e correção que incluem soluções para ativos afetados para os itens de configuração (IC) no seu CMDB.

Solicitações de mudança na Resposta a vulnerabilidades



Quando usar solicitações de mudança na resposta a vulnerabilidades

Como proprietário de correção de TI, você pode criar solicitações de mudança a partir de uma tarefa de correção se um processo manual e controlado de qualquer tipo for necessário para modificação ou remoção de itens de configuração (ICs) compatíveis no seu CMDB. Criar e gerenciar solicitações de mudança diretamente de um registro de tarefa de correção ajuda a investigar e resolver vulnerabilidades rapidamente. Os IVs de tarefas de correção resolvidas podem ser verificados durante a próxima verificação programada na Now Platform e retornados para a triagem automatizada do fluxo de trabalho Resposta a vulnerabilidades. As intervenções manuais que podem exigir solicitações de mudança incluem os seguintes exemplos:

- Um patch de software, correção ou outra tarefa de TI que é necessária em itens vulneráveis antes da resolução de RT.
- Você determina que um subconjunto dos itens vulneráveis em uma tarefa de correção requer investigação adicional ou reatribuição a outro departamento.
- Você determina que um subconjunto de itens vulneráveis em um RT com um grande conjunto de itens vulneráveis pode ser movido para uma nova tarefa de correção.
- Você pode associar uma tarefa de correção a uma solicitação de mudança existente para evitar a duplicação de tarefas de correção.

Tipos de solicitações de mudança para um RT

A aplicação Resposta a vulnerabilidades utiliza os três tipos de mudanças de serviço compatíveis com o produto ITSM Gestão de mudanças em sua instância Now Platform® - padrão, de emergência e normal. O tipo de mudança selecionado determina qual modelo de estado é invocado e o processo de mudança que deve ser seguido. As solicitações de mudança registram as informações detalhadas sobre a mudança, como o motivo da

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mudança, a prioridade, o risco, o tipo de mudança e a categoria de mudança. Consulte Tipos de mudança .

Como um Resposta a vulnerabilidades proprietário de correção de TI, você tem as seguintes opções para criar solicitações de mudança normais, padrão e de emergência diretamente de uma tarefa de correção:

- Você pode criar solicitações de mudança que contêm informações preenchidas previamente da tarefa de correção para simplificar o processo e economizar tempo.
- Você pode associar uma tarefa de correção a uma solicitação de mudança existente para evitar a criação de solicitações de mudança duplicadas que compartilham informações semelhantes e itens vulneráveis.
- Usando um conjunto de condições, você pode filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para um novo RT.

Você pode filtrar itens vulneráveis usando valores de qualquer campo de uma tarefa de correção e aplicar a solicitação de mudança somente aos itens que correspondem aos seus critérios de filtro.

Informações relacionadas

Criar uma solicitação de mudança a partir de uma tarefa de correção

Associar uma tarefa de correção a uma solicitação de mudança existente

Dividir uma tarefa de correção

Sincronização de estado entre solicitações de mudança e tarefas de correção

Avaliação de exposição de software usando Software Asset Management (SAM Foundation)

Use a aplicação ServiceNow® Vulnerability Exposure Assessment para determinar a contagem total de software instalado para um pacote de software específico em seus ativos. Quando usado com a aplicação ServiceNow® Software Asset Management (SAM) Foundation, avalie sua exposição, crie itens vulneráveis e gerencie a correção do software vulnerável que você descobrir.

Importante: Você pode executar a avaliação de exposição por software e vulnerabilidades e exposições comuns (CVE) para aproveitar os recursos adicionais no espaço de avaliação de vulnerabilidade. Para obter mais informações, consulte Explorar o espaço de avaliação de vulnerabilidade.

Determine sua exposição a software vulnerável fornecendo as informações de software vulnerável (fornecedor, produto, edição e versão) sem usar o banco de dados de vulnerabilidades e exposições comuns (CVE). Avaliar casos de vulnerabilidades de dia zero (dia atual) para software para os seguintes casos:

- Quando os produtos ainda não têm dados de CVE.
- Quando há um atraso entre o momento em que uma vulnerabilidade se torna publicamente conhecida e os dados de CVE com a vulnerabilidade são atualizados no NVD.
- Quando você aprende sobre a vulnerabilidade entre as verificações programadas do seu scanner de vulnerabilidades.

Com a aplicação Vulnerability Exposure Assessment, se você conhece o fornecedor e o produto do software vulnerável, usando os registros que listam o software instalado em sua rede criada pela aplicação SAM Foundation, você pode avaliar sua exposição a software potencialmente mal-intencionado pacotes sob demanda.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conhecer a escala de sua exposição a esse tipo de vulnerabilidade permite que você responda proativamente implementando um alerta vermelho e desinstalando o software ou informando ao seu SOC (Security Operations Center, centro de operações de segurança) para procurar um patch específico. Você pode criar itens vulneráveis e atribuir tarefas ao especialista em correção para correção de investigação adicional. Exiba uma lista de tarefas de correção (VUL) para verificar se os itens vulneráveis que você deseja foram criados e associados corretamente à VUL.

Informações relacionadas

Configurar a avaliação de exposição de vulnerabilidade

Avalie sua exposição a software vulnerável

Gestão de crises de vulnerabilidade

Crie e rastreie eventos de vulnerabilidade críticos por meio do fluxo de trabalho da Gestão de crises de vulnerabilidade (VCM). Crie registros de avaliação de vulnerabilidade, registre os principais atributos da vulnerabilidade para calcular o risco, execute a avaliação para identificar o nível de exposição e envolva as partes interessadas para uma resposta coordenada e rápida às vulnerabilidades.

Gerenciamento de eventos de crise de vulnerabilidade

A Gestão de crises de vulnerabilidade é um fluxo de trabalho completo para lidar com eventos de crise de vulnerabilidade com os seguintes recursos.

- Identifique com eficiência itens de configuração vulneráveis correlacionando vulnerabilidades críticas com o inventário de instalação de software do inventário Gestão de ativos de software e Lista de materiais de software (SBOM), vulnerabilidades relatadas pelo scanner e Configuration Management Database (CMDB).
- Converta os resultados da avaliação em itens vulneráveis para correção.
- Inicie um incidente de segurança grave para garantir uma resposta rápida e coordenada à ameaça.
- Envolva-se e colabore com equipes em toda a organização, facilitando uma resposta unificada a vulnerabilidades.
- Forneça relatórios de status regulares às partes interessadas multifuncionais e às equipes envolvidas para manter a transparência e a comunicação durante a crise.

Gestão de crises de vulnerabilidade usando o espaço de avaliação de vulnerabilidade

Nota: A partir da v1.0.1 da Gestão de crises de vulnerabilidade, a aplicação está disponível como uma assinatura separada na loja. Você pode acessar a Gestão de crises de vulnerabilidade no espaço de avaliação de vulnerabilidade somente se tiver um direito refinado ou tiver instalado a aplicação da loja. Anteriormente, a Gestão de crises de vulnerabilidade era incluída com o plug-in Vulnerability Emergency Response. A partir da v3.2.2, o plug-in Vulnerability Emergency Response foi renomeado para Avaliação de exposição de vulnerabilidade.

Ao identificar uma vulnerabilidade de interesse, o gerenciador de eventos de vulnerabilidade cria um registro de avaliação de vulnerabilidade com informações sobre a origem da inteligência contra ameaças, características da vulnerabilidade e produtos afetados. Essas informações são usadas para análise adicional de impacto e exposição.

Depois que o registro de uma vulnerabilidade de interesse é criado, uma avaliação de risco é realizada. Essa avaliação compreende a pontuação de risco estruturada, a revisão

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do registro e as observações do analista que executa a tarefa. A pontuação de risco inicial para uma vulnerabilidade de interesse é calculada usando os atributos disponíveis no momento da criação do evento. A pontuação de risco da avaliação pode mudar conforme a inteligência adicional se torna disponível. Use a pontuação de risco para determinar o possível impacto da exploração e estabelecer prioridades de resposta.

Depois que a avaliação de uma vulnerabilidade de interesse tiver sido criada e determinada como apresentando risco à infraestrutura da organização, você poderá analisar a ameaça ainda mais atualizando a avaliação de risco com uma avaliação de exposição detalhada com o inventário de instalação de software de Gestão de ativos de software, Lista de materiais de software Inventário (SBOM), vulnerabilidades relatadas pelo scanner e Configuration Management Database (CMDB). Os itens de configuração e aplicações afetados são identificados automaticamente por meio da avaliação. Outros itens afetados podem ser adicionados manualmente.

Depois que a avaliação é concluída, os itens vulneráveis ou os itens vulneráveis de aplicação podem ser criados para os resultados da exposição que ainda não têm um item vulnerável associado. A calculadora de pontuação de risco de itens vulneráveis pode ser aproveitada/configurada para ajustar a pontuação de risco de itens vulneráveis vinculados a registros de avaliação de vulnerabilidade. O registro de Avaliação de vulnerabilidade pode ser atribuído a nível de exposição e prioridade de evento. Com base na prioridade do evento, o Gerenciador de eventos de vulnerabilidade pode optar por propor, promover ou vincular a avaliação de vulnerabilidade a um incidente de segurança grave.

Use Gestão de incidentes graves de segurança para rastrear e gerenciar atividades de correção, vincular incidentes de segurança em andamento, criar tarefas ad-hoc, envolver as equipes afetadas, enviar relatórios de status e colaborar usando integrações de colaboração disponíveis em Gestão de incidentes graves de segurança.

ServiceNow® Gestão de ativos de software e Lista de materiais de software (SBOM) lógica de processamento de avaliação

Usando os dados Gestão de ativos de software, os CPEs provenientes do NVD para o CVE e os modelos de descoberta são obtidos usando a lógica de correspondência de cadeia de caracteres. Depois de buscar os modelos de descoberta, uma verificação de instalações relacionadas é executada, os itens de configuração relacionados são obtidos e a tabela de itens de configuração afetados é preenchida. Você pode fornecer mais detalhes como Fornecedor, Produto, Versão e Edição. Com base neles, todos os modelos de descoberta correspondentes e as instalações de software do registro são obtidos. Posteriormente, os itens de configuração relacionados são obtidos e a tabela Item de configuração afetado é preenchida novamente.

Para SBOM, o software associado ao CVE da tabela relacionada (m2m) (entre CVE e Software) é obtido. Depois de extrair os detalhes do software, os componentes do SBOM relacionados são identificados pela correspondência do produto e da versão do componente do SBOM com o produto e a versão do software identificado.

Depois que os componentes associados são encontrados, as entidades relacionadas aos componentes são buscadas. O modelo de produto das entidades e o IC relacionado (se encontrado) são obtidos e o item de configuração é salvo na tabela Item de configuração afetado. Se o item de configuração não tiver itens vulneráveis, você poderá usá-lo para criar o item vulnerável. Se um item de configuração não for encontrado, o modelo de produto será salvo na tabela Modelo de software afetado e poderá ser usado para criar itens vulneráveis de aplicação.

Para obter mais informações sobre como usar o fluxo de trabalho Gestão de crises de vulnerabilidade, consulte Uso do espaço de avaliação de vulnerabilidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Explorando a avaliação de vulnerabilidade

Explorar o espaço de avaliação de vulnerabilidade

Guia Avaliação

Separação de domínios e Resposta a vulnerabilidades

Separação de domínios é compatível com Resposta a vulnerabilidades. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Resposta a vulnerabilidades

Com o Domain Separation, você pode padronizar procedimentos de VR (Resposta a vulnerabilidades) em toda a base de clientes que atende, com custos operacionais reduzidos e uma qualidade de serviço superior.

Separar espaços de trabalho do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínio na Resposta a vulnerabilidades por versões de versão

Versão	Nível de suporte	Anotações
Orlando	Padrão	
Paris	Padrão	
Quebec	Padrão	
Rome	Padrão	
San Diego	Padrão	
Tokyo	Padrão	
Utah	Padrão	
Vancouver	Padrão	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Suporte à separação de domínio na Resposta a vulnerabilidades por versões de versão

Versão	Nível de suporte	Anotações
Washingtondc	Padrão	

O Domain Separation para a aplicação Resposta a vulnerabilidades cobre a seguinte funcionalidade do produto:

- Ingere os itens vulneráveis de scanners de terceiros (por exemplo, Qualys, Rapid 7 ou Tenable) no domínio correto. Os dados são ingeridos no mesmo domínio do usuário de integração, cujas credenciais são usadas para integração.
- Verifica novamente ativos específicos de Resposta a vulnerabilidades no domínio do qual foi solicitado.
- Usa o processo de pesquisa de IC do CMDB para garantir que as informações de IC dos scanners correspondam aos ICs no CMDB do domínio do usuário de integração.
- Calcula pontuações de risco no nível do item vulnerável de acordo com a calculadora de pontuação de risco definida no mesmo domínio do usuário de integração.
- As regras de destino de correção são executadas em itens vulneráveis de acordo com as regras de destino de correção definidas no mesmo domínio do usuário de integração.
- As regras de tarefa de correção podem ser definidas e permanecer no mesmo domínio que o domínio do usuário de integração.
- As tarefas de correção criadas usando as regras de tarefa de correção permanecem no mesmo domínio em que as regras de grupo são criadas.
- O fluxo de trabalho de adiamento passa pelo processo de aprovação no mesmo domínio para o qual o adiamento é solicitado.
- Relatórios e painéis exibem os estados do item vulnerável, como idade do item vulnerável, itens vulneráveis em aberto por IC, vulnerabilidades por impacto e status da data da meta de correção no domínio ao qual pertence.
- O conhecimento de scanners de terceiros ou do banco de dados nacional de vulnerabilidades (NVD) pode ser ingerido no domínio global e os dados podem ser compartilhados entre vários clientes.

Nota: Em todos os casos acima, aplicam-se os princípios abrangentes de visibilidade na separação de domínios separados na NOW Platform.

Para obter mais informações sobre como criar e oferecer suporte a importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração e Criar e oferecer suporte a vários domínios na estrutura de trabalhos em segundo plano.

Casos de uso

A aplicação Resposta a vulnerabilidades gerencia o ciclo de vida de um item de vulnerabilidade de ponta a ponta. Os seguintes casos de uso reconhecem a separação de domínios:

- **Ingerir** itens vulneráveis (vulnerabilidades no ativo) da integração de terceiros.
  - Ingerir dados de várias instâncias
  - Desduplicar o item vulnerável
  - Corresponder ao IC do CMDB

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Aprimoramento** de item vulnerável com pontuações de risco e datas de meta de correção
  - Aprimoramento de ativos (CMDB)
  - Pontuação de risco e aprimoramento da data da meta de correção
- **Agrupar** itens vulneráveis e atribuir a tarefa de correção
  - Agrupar automaticamente os itens vulneráveis
  - Atribuir automaticamente a tarefa de correção
- **Corrigir**
  - Tarefas de correção
  - Ciclo de vida de correção abrangente
  - Fluxo de trabalho de adiamento
- **Medir** a postura de segurança da organização e do programa de gestão de vulnerabilidades
  - Tendência de vulnerabilidade, ativo mais vulnerável, vulnerabilidade por idade
  - Status da correção até a data da meta de correção

Configuração

A configuração do Domain Separation para Resposta a vulnerabilidades não requer etapas adicionais. Todas as tabelas Resposta a vulnerabilidades adquirem a coluna Domínio depois que a instância é separada por domínio. Você pode direcionar os dados de importação de integração de vulnerabilidade para domínios específicos. Para obter mais informações, consulte Criar importações separadas por domínio para uma integração.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- O item vulnerável ingerido de scanners de terceiros permanece no mesmo domínio que o domínio do usuário de integração e não pode ser acessado de nenhum outro domínio.
- Vulnerabilidades, itens vulneráveis (instâncias) ou ativos em um domínio não podem ser exibidos de outros domínios.
- O algoritmo de pontuação de risco, as regras de tarefa de correção e as regras de destino de correção não podem ser exibidas por ninguém fora do domínio.
- As informações de vulnerabilidade do NVD podem existir no domínio global e ser compartilhadas com todos os clientes.
- As tarefas de correção em um domínio não podem ser exibidas em outro domínio.
- Os fluxos de trabalho de adiamento criados em um domínio não são visíveis em outro domínio.
- Todas as notificações por e-mail estão contidas no domínio ao qual pertencem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como os analistas de vulnerabilidade gerenciam seus próprios dados de aplicação

- Os analistas criam suas próprias regras de instalação de aplicações, gerenciamento de aplicações de várias origens e pesquisa de IC.
- Os analistas podem configurar integrações específicas exclusivamente para uso no domínio.
- Os analistas podem criar seus próprios fluxos de trabalho de adiamento e gestão de mudanças.
- Os analistas podem criar suas próprias regras de tarefa de correção, lógica de pontuação de risco para priorizar vulnerabilidades com precisão, atribuir automaticamente tarefas de correção e atribuir ao grupo de atribuição correto.
- Os usuários do domínio criam um item de vulnerabilidade manual e fecham o item.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Resposta a vulnerabilidades usuários e grupos
- Integrações do Resposta a vulnerabilidades
- Conclua a configuração de configuração (gestão de usuários e grupos, instalação de aplicações, gestão de aplicações de várias origens, regras de pesquisa de IC, regras de tarefa de correção, calculadoras de risco, regras de meta de correção etc.)
- Concluir o ciclo de vida de correção, incluindo o adiamento
- Programar trabalhos

Informações relacionadas

Domain Separation para provedores de serviço

Mapeamento de serviços no Resposta a vulnerabilidades

O mapeamento de serviços ajuda as organizações a obter uma compreensão abrangente da infraestrutura de TI e dos relacionamentos entre vários componentes. Ele permite a descoberta e o mapeamento automáticos de serviços, aplicações e componentes de infraestrutura, fornecendo uma representação visual das dependências e relacionamentos.

Em Resposta a vulnerabilidades, o trabalho agendado *`Set related CI services`* estabelece conexões entre os serviços de negócio afetados e os itens de configuração (ICs) associados aos itens vulneráveis (VITs). O processo de vinculação ocorre quando a importação de integração é concluída e em um horário designado. Para aprimorar o desempenho deste trabalho agendado, várias mudanças foram implementadas, começando com a v21.1.2 de Resposta a vulnerabilidades. São eles:

- Cálculo de pontuação de risco: o processo de cálculo de pontuações de risco envolve a utilização do trabalho agendado *`Set related CI services`*. Depois que o IC é processado, este trabalho armazena os dados necessários na tabela Serviços relacionados [sn_vul_m2m_ci_services]. Anteriormente, em Conformidade de configurações, o cálculo de risco envolvia o acesso direto a Configuration Management Database (CMDB) *`CIUtils`* da API (Interface de programação de aplicações) para recuperar serviços para cada resultado de teste durante a importação. No entanto, o processo atual depende da saída do trabalho agendado da tabela Serviços relacionados [sn_vul_m2m_ci_services] para calcular a pontuação de risco em

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações. Além disso, a calculadora do sistema de base foi modificada para utilizar a tabela Serviços relacionados [sn_vul_m2m_ci_services].

- Tamanho dos serviços: o valor do serviço na propriedade do sistema *sn_sec_cmn.services_affected_by_CI_max_size*, que está relacionado ao trabalho agendado *Set related CI services*, foi reduzido de 1000 para 500.
- Profundidade dos serviços: a profundidade na propriedade do sistema *sn_sec_cmn.services_affected_by_CI_max_depth*, que está relacionada ao trabalho agendado *Set related CI services*, foi reduzida de 10 para 5. O valor do serviço também foi reduzido de 1000 para 500.
- Exclusão de classes CMDB : uma propriedade do sistema *sn_sec_cmn.ignoreCIClassForService* foi introduzida para habilitar a configuração de classes CMDB para as quais o cálculo de serviço deve ser ignorado. No sistema base, esta propriedade é definida para *cmdb_ci_unclassed_hardware*, *cmdb_ci_incomplete_ip*, *sn_sec_cmn_unmatched_ci*, pois essas classes são criadas por Resposta a vulnerabilidades e podem não ter nenhum mapeamento de serviço. Anteriormente, o cálculo do serviço era baseado no VIT. No entanto, a lógica foi modificada para usar o item descoberto. O item descoberto é usado para calcular o serviço, que é associado ao IC na mesma tabela.
- Trabalho agendado para atualização completa de serviços: um trabalho agendado sob demanda *Full refresh-related CI services for VI*, foi introduzido para executar uma atualização completa de serviços. Quando você faz upgrade para a v21.0 de Resposta a vulnerabilidades, o trabalho *Set related CI services* é executado por mais tempo no início, pois a tabela base usa itens descobertos em vez de itens vulneráveis. Como resultado, o trabalho deve processar todos os itens descobertos que foram verificados nos últimos 90 dias. Além disso, se você precisar de atualizações de serviço mais frequentes, isso poderá ser feito programando atualizações periódicas semanais ou executando uma atualização completa. Se você executou atividades que resultaram em mudanças nos serviços associados aos seus ICs e deseja que Resposta a vulnerabilidades reflita essas mudanças, é possível executar o trabalho agendado sob demanda *Full refresh related CI services for VI*. Este trabalho usa todos os itens descobertos registrados nos últimos 90 dias e atualiza os serviços associados de acordo.

Informações relacionadas

Mapeamento de serviços

CIUtils - Global

Implementação de Resposta a vulnerabilidades

Use as etapas ilustradas nas imagens a seguir para baixar a aplicação Resposta a vulnerabilidades do ServiceNow Store, instalá-la em sua instância Now Platform® e configurá-la usando o Assistente de configuração.

Um exemplo de instalação e configuração para instalar o sistema de base, a aplicação Resposta a vulnerabilidades e uma aplicação de scanner de terceiros, a aplicação Qualys, é ilustrado nas imagens a seguir. Funções e tarefas obrigatórias, bem como etapas opcionais, também são listadas.

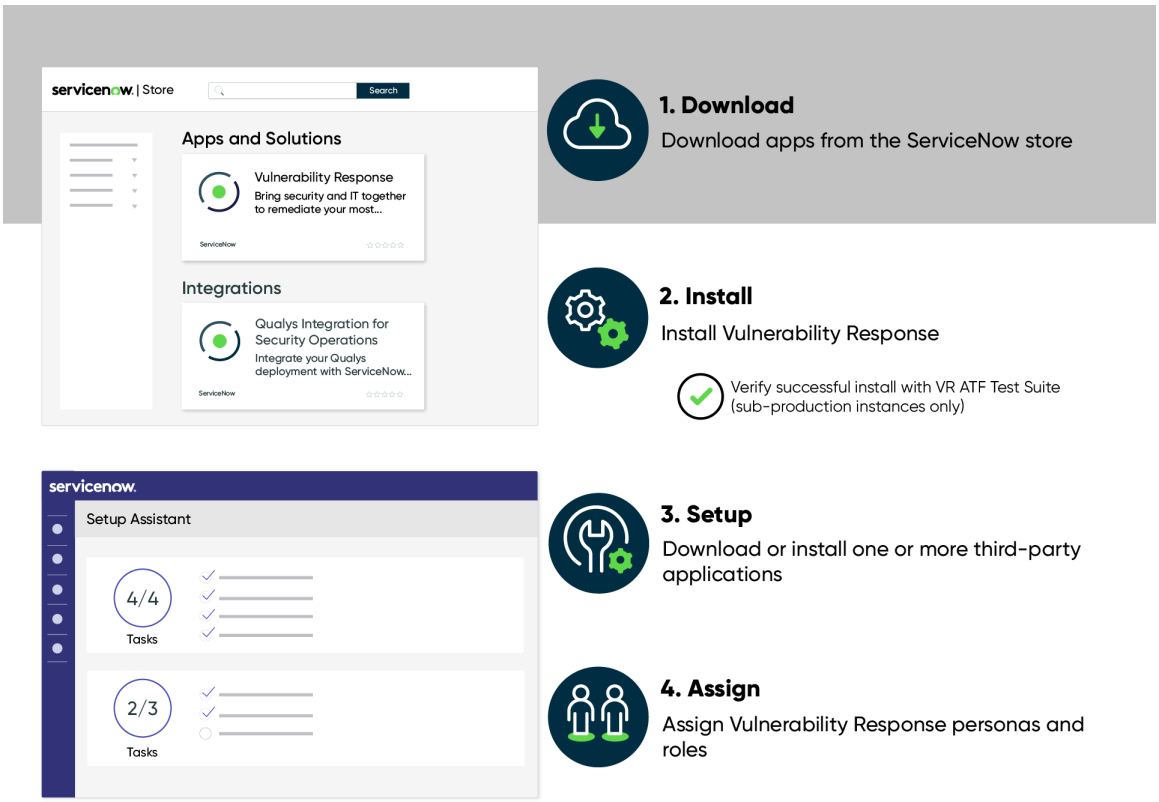
- Para obter mais informações sobre cada etapa ilustrada nas imagens a seguir e uma check-list com links para a documentação de suporte, consulte Check-list de implementação da aplicação Resposta a vulnerabilidades.
- Você pode estender os conceitos e a sequência de etapas apresentados neste exemplo para instalar e configurar outras aplicações compatíveis para Resposta a

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades. Para obter uma lista de aplicações de suporte, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

- A função de administrador é necessária para baixar e instalar a aplicação Resposta a vulnerabilidades e a aplicação de vulnerabilidade Qualys usadas neste exemplo.
- A função de administrador também atribui a persona de administrador de vulnerabilidade [sn_vul.vulnerability_admin] e outras funções de persona Resposta a vulnerabilidades a usuários e grupos.

Tarefas de administrador



A função sn_vul.vulnerability_admin configura as aplicações Resposta a vulnerabilidades e Qualys no Assistente de configuração e verifica os resultados esperados.

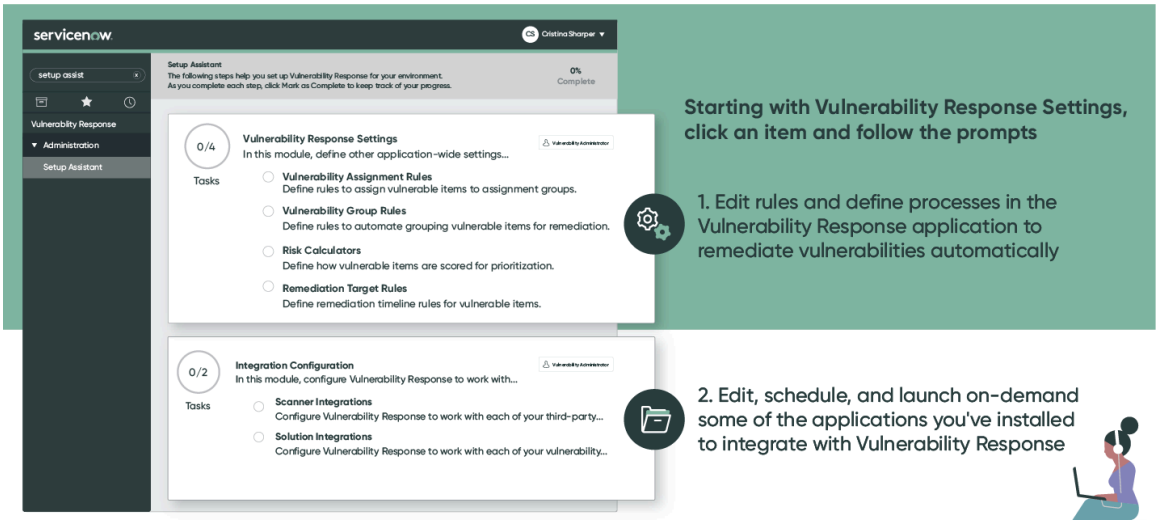
Siga as etapas e avisos no Assistente de configuração, começando com a seção Configurações da Resposta a vulnerabilidades, para continuar com a instalação e a configuração. A revisão dessas configurações ajuda a entender e verificar os processos de Resposta a vulnerabilidades à medida que você continua a configurar seu ambiente.

Função necessária: sn_vul.vulnerability_admin ou, alternativamente, admin.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de administrador de vulnerabilidade



Roles required: sn_vul.vulnerability_admin or admin

Revise as descrições, configurações padrão e dados de demonstração que você instalou com as aplicações nas seguintes seções:

- Regras de atribuição de vulnerabilidade: atribua automaticamente itens vulneráveis (VIs) ao grupo de atribuição apropriado.
- Regras de tarefa de correção - agrupe automaticamente os itens vulneráveis (IVs) conforme eles são importados com base em determinadas condições.
- Calculadoras de risco — A calculadora de risco padrão está habilitada.
- Regras de destino de correção — Defina linhas do tempo de correção para IVs e tarefas de correção (RTs).
- Revise e edite as configurações das aplicações de terceiros e soluções instaladas que você instalou e defina condições para suas importações de dados. Insira as informações da conta de terceiros e defina as configurações de importação e cronogramas, regras de pesquisa de item de configuração (IC), bem como outras configurações.

Para obter mais informações, consulte Check-list de implementação da aplicação Resposta a vulnerabilidades.

Para obter informações adicionais ao personalizar ou implementar a aplicação Resposta a vulnerabilidades, consulte KB1000704 .

Como instalar Resposta a vulnerabilidades

Antes de executar a aplicação Resposta a vulnerabilidades em sua instância Now Platform, você deve obter o direito e baixar a aplicação da ServiceNow Store, instalá-la em sua instância Now Platform e concluir algumas etapas de instalação no Assistente de configuração.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

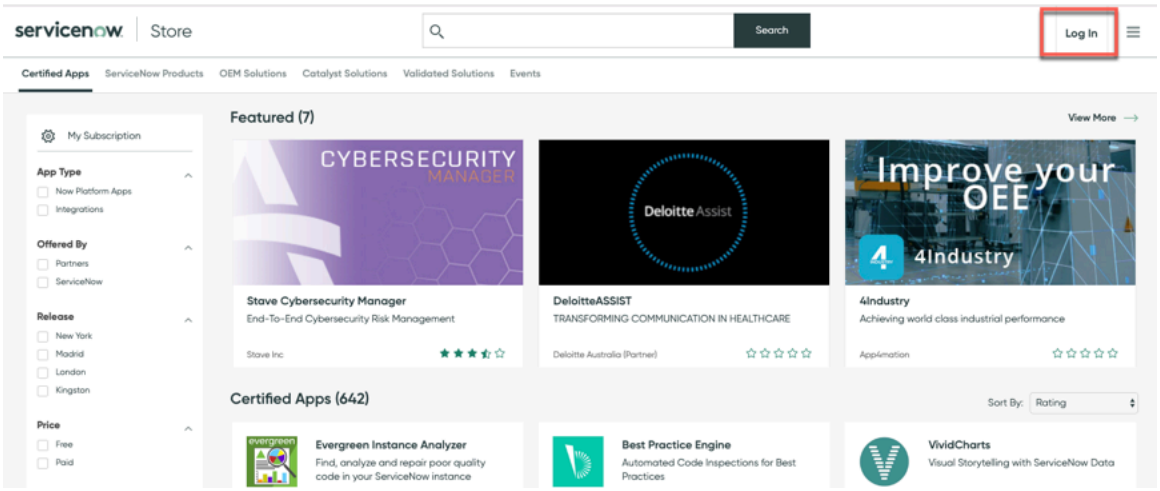
Tarefas de configuração	Descrição
Verifique se você tem as funções ServiceNow necessárias atribuídas para sua instância.	A função de administrador é necessária para a instalação. Se ainda não estiver atribuído, o Administrador do sistema [admin] também atribuirá a função Administrador de vulnerabilidade, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleta)].

Função necessária: administrador

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

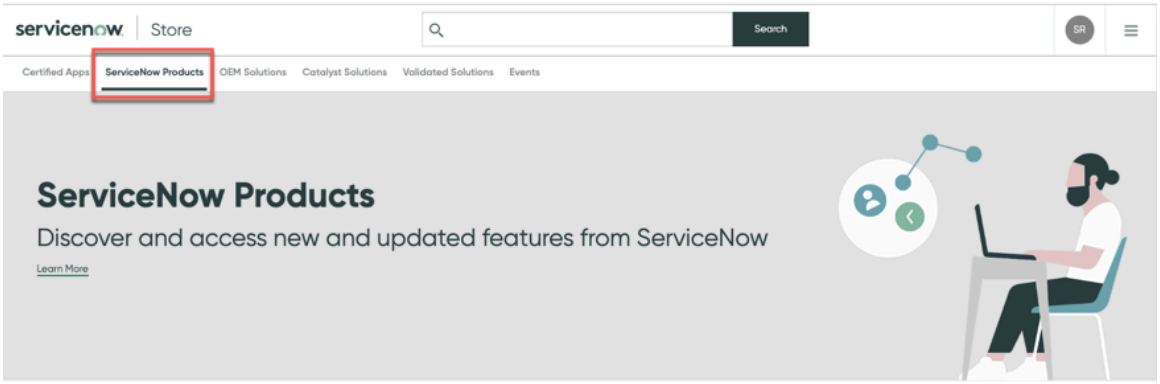
1. Para obter o direito e baixar a aplicação principal Resposta a vulnerabilidades, navegue até o ServiceNow Store.
2. No canto superior direito da página, clique em **Fazer login**.



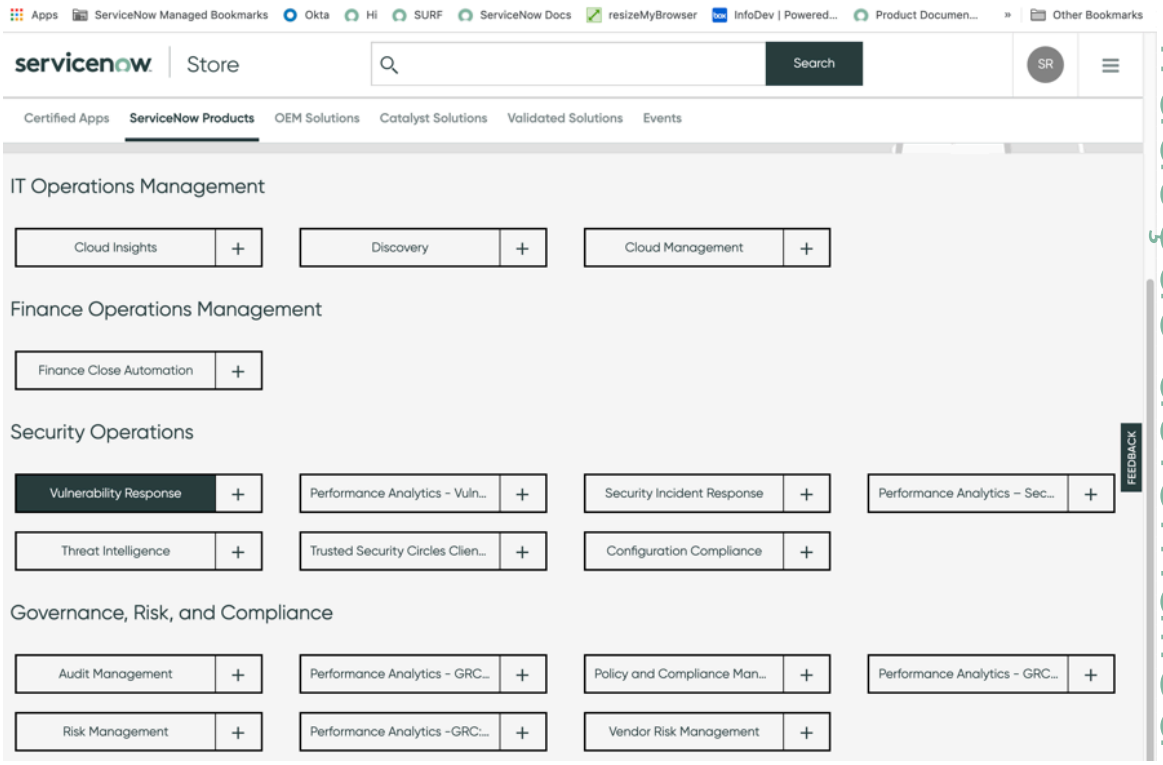
3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login**.
4. Na página exibida, se não estiver selecionado, clique na guia **Produtos da ServiceNow**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



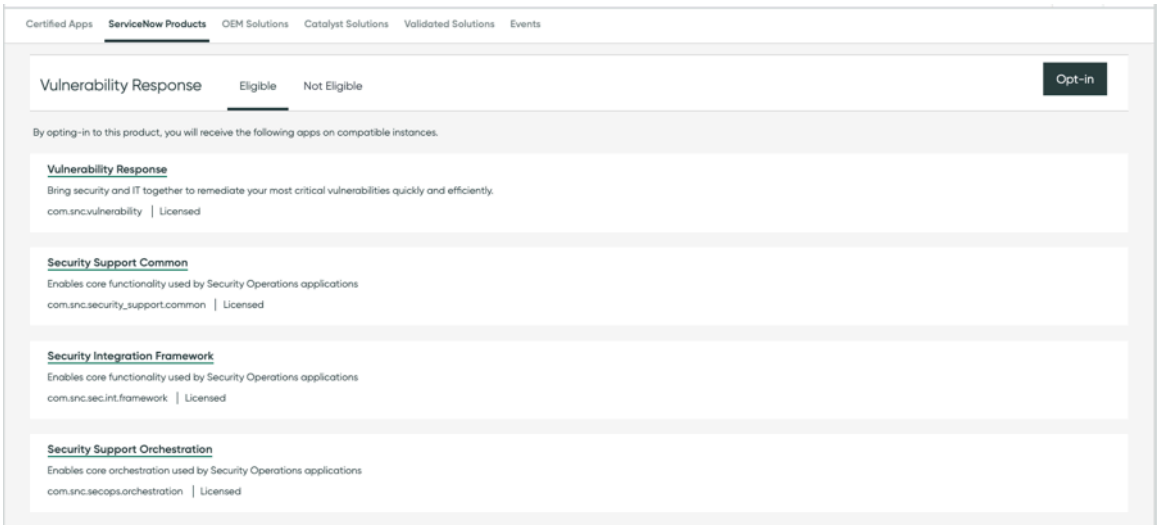
5. Para exibir as aplicações associadas para as quais você está qualificado com a aplicação Resposta a vulnerabilidades, na página da lista de produtos, clique no produto **Resposta a vulnerabilidades**.



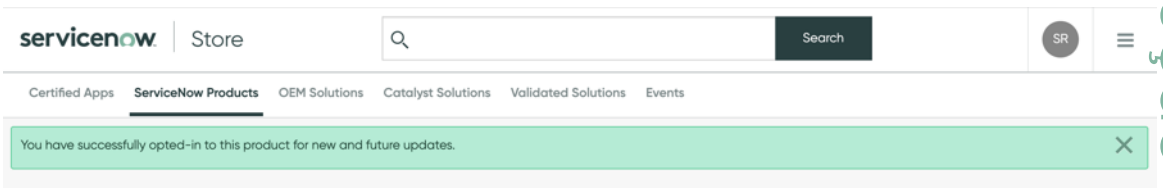
A guia Qualificado lista todas as candidaturas para as quais você está qualificado se aceitar. Para obter mais informações sobre uma aplicação, clique em um link.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Para obter a aplicação principal Resposta a vulnerabilidades, clique em **Aceitar**.
7. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.
   Uma mensagem é exibida indicando que você aceitou com sucesso a aplicação.



   Com a guia ServiceNow Produtos selecionada e exibida, uma marca de seleção verde substitui o sinal de mais à direita da aplicação Resposta a vulnerabilidades, conforme mostrado na figura a seguir.

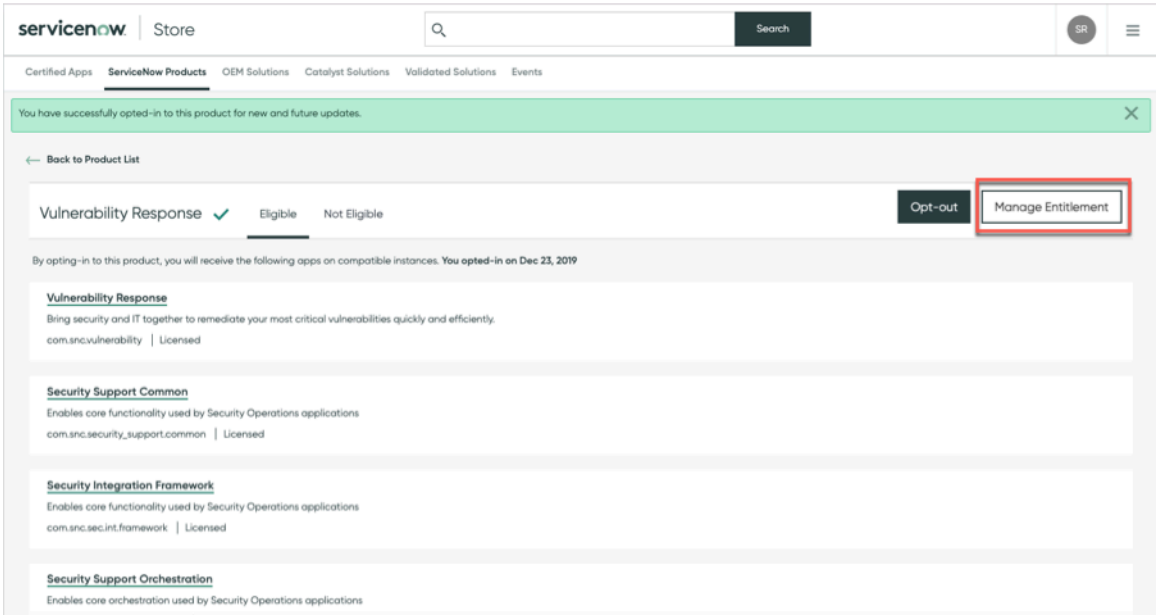
   Depois de aceitar os termos e condições e direitos gerenciados de qualquer uma das aplicações na guia **Produtos da ServiceNow**, na página Lista de produtos, você pode clicar no sinal de mais (+) para obter direitos e aceitar outras aplicações nesta página com um único clique.
8. Pule para a etapa 10 para instalar a aplicação em sua instância Now Platform.
9. Opcional: Como alternativa, para gerenciar seu direito da aplicação Resposta a vulnerabilidades em outras instâncias Now Platform, siga estas etapas.

   a. Se o botão Gerenciar direito não for exibido, clique na aplicação Resposta a vulnerabilidades na lista de produtos para exibi-la.

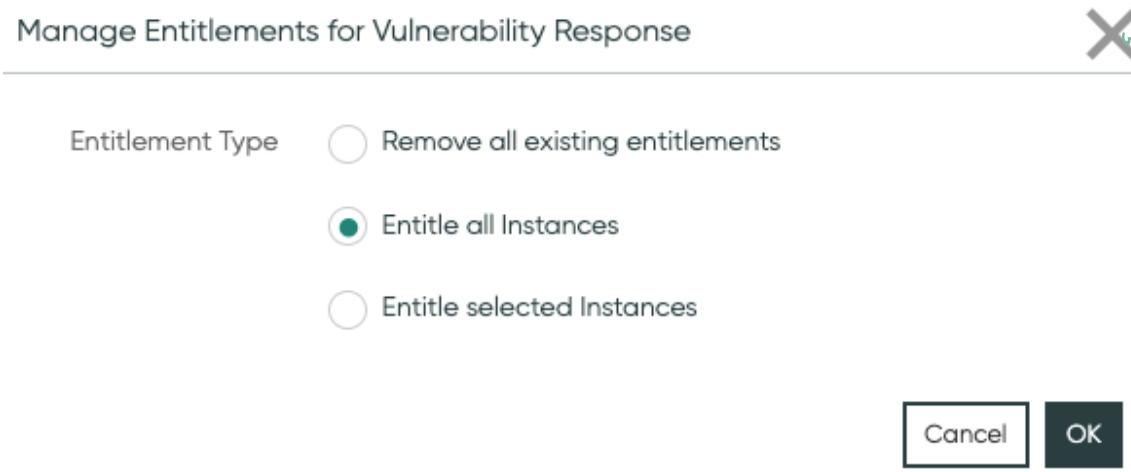
   b. Com a guia Qualificado selecionada, clique em **Gerenciar direito**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Na caixa de diálogo Gerenciar direitos para resposta a vulnerabilidades que é exibida, escolha uma:



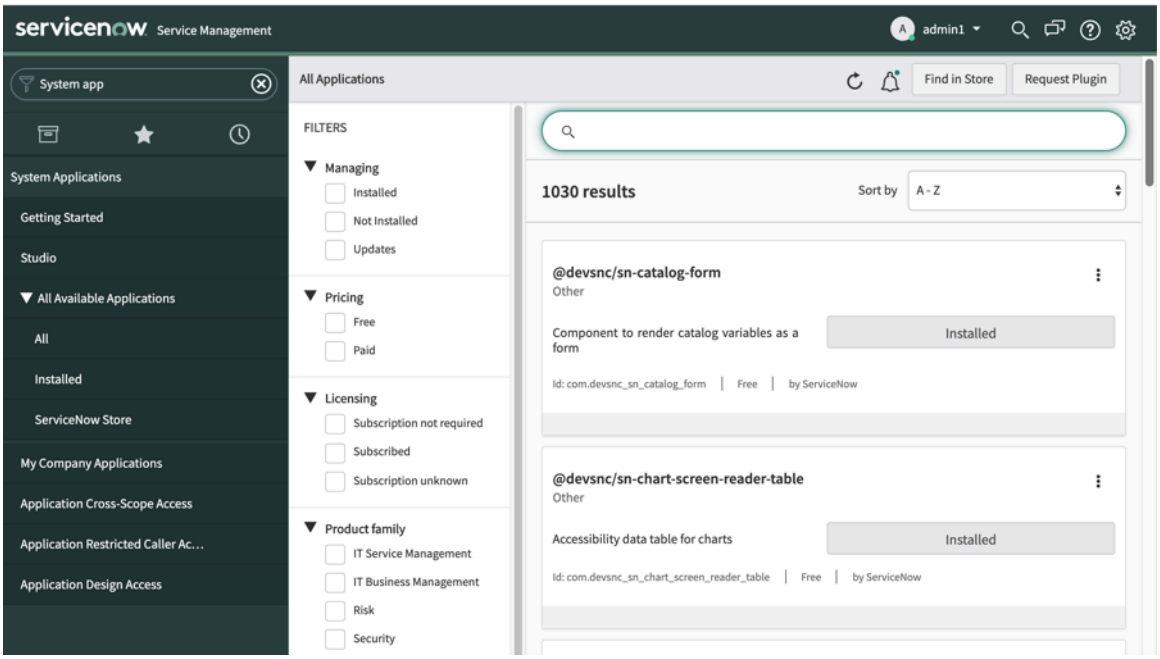
d. Clique em **OK** ou em **Cancelar** para continuar.
Você está pronto para ativar plug-ins e instalar a aplicação em sua(s) Now Platform instância(s).

10. Faça login na instância Now Platform na qual você deseja instalar a aplicação Resposta a vulnerabilidades.

11. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.

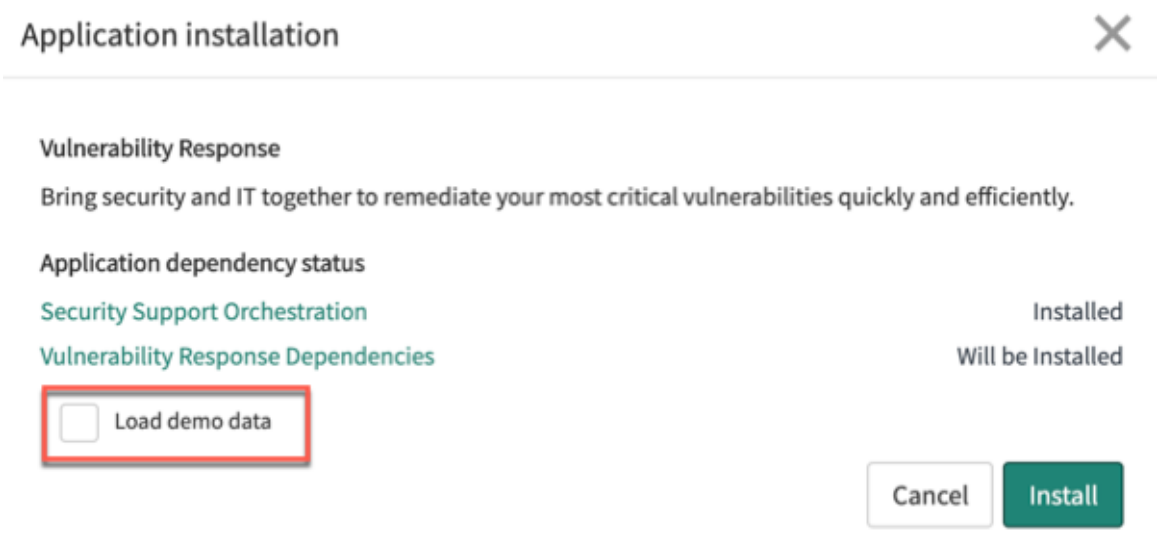
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. Nas aplicações listadas, localize a aplicação Resposta a vulnerabilidades (sn_vul), selecione uma versão na lista de seleção e clique em **Instalar**.
    A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas são exibidas.
13. Opcional: Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar**.

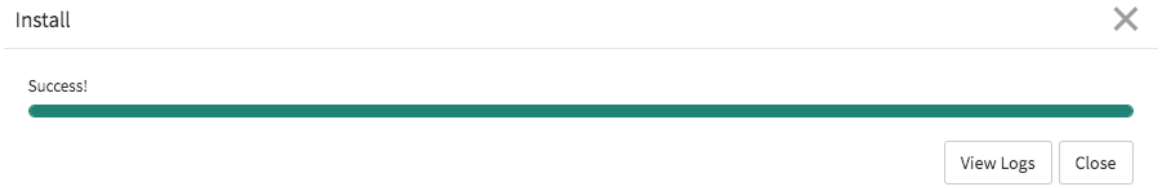
> **Nota:** Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não estarão disponíveis para instalação posterior no **Gerenciador de aplicações**. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.



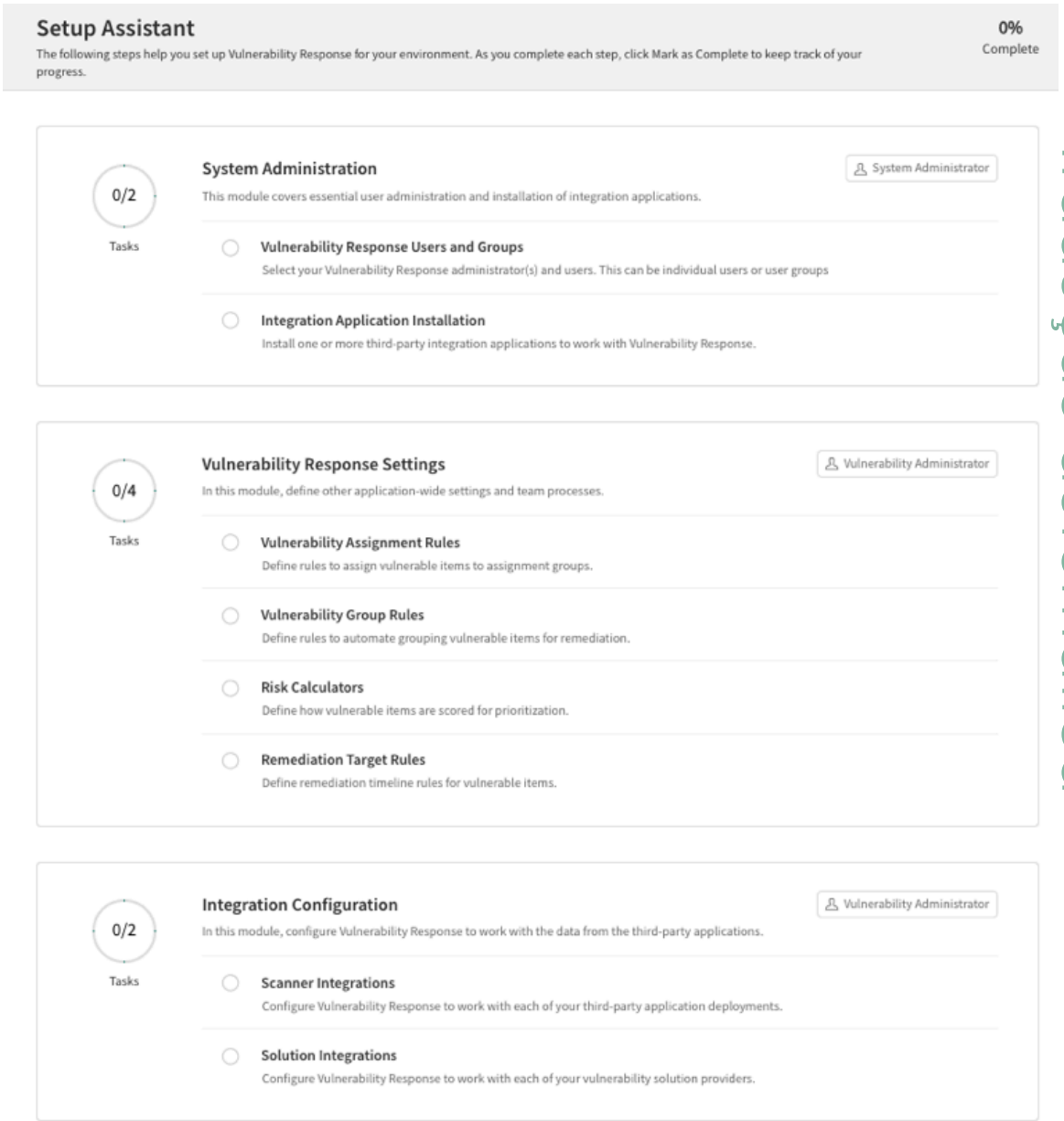
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta instalação pode levar algum tempo. Uma mensagem será exibida na caixa de diálogo Instalar depois que a aplicação for instalada com sucesso.



14. Clique em **Fechar**.
15. Depois que a instalação for concluída com sucesso, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.



16. Siga as instruções nos formulários de cada seção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Para obter mais informações sobre Resposta a vulnerabilidades configurações, instalação de aplicações, configuração, integrações, regras de grupo, calculadoras de risco e regras de destino de correção, consulte Configuração de Resposta a vulnerabilidades usando o Assistente de configuração.

Componentes instalados com Resposta a vulnerabilidades

Vários tipos de componentes são instalados com a ativação da aplicação Resposta a vulnerabilidades, incluindo tabelas, funções de usuário e trabalhos agendados.

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos agendados e as tabelas instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.
3. No Construtor de condições, para adicionar um segundo filtro, selecione **AND e**, em seguida, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, Trabalho **agendado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Nota: Funções, trabalhos agendados e tabelas para Resposta a vulnerabilidades de aplicações podem ser encontrados em Componentes instalados com Resposta a vulnerabilidades de aplicações.

Título da função [name]	Descrição	Contém as funções
v23.0: sn_vul.delete	Exclui registros de origem e itens vulneráveis. Antes da v23.0, a função de administrador tinha o privilégio de excluir os registros de origem.	• sn_vul_cmn.delete • sn_vul.delete_vulnerab
v23.0: sn_vul_cmn.delete	Exclui registros de origem.	
V23.0: sn_vulc.bulk_edit	Executa a operação de edição em massa nos resultados de testes.	
sn_vul.app_bulk_edit	Executa a operação de edição em massa em itens vulneráveis da aplicação (AVITs).	sn_vul.app_write_all
sn_vul_container.container_bulk_edit	Executa a operação de edição em massa em itens vulneráveis de contêiner (CVITs).	sn_vul_container.write_c

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
sn_vul_cisa.configure_intelligence_integration	Configura integrações de Inteligência.	
Gerentes de vulnerabilidade e analistas sênior [sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)]	Atualizar propriedades e integrações de vulnerabilidade. A função sn_vul.vulnerability_admin ou sn_vul.admin (obsoleta) é necessária para a administração Resposta a vulnerabilidades, incluindo integrações de vulnerabilidade, regras de tarefa de correção, calculadoras e regras e tarefas de destino de correção, relatórios e configuração de integração de terceiros.	• sn_vul.vulnerability_wri • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (integração de vulnera Qualys está instalada. • sn_vul_r7.admin (quan integração de vulnera Rapid7 está instalada. • sn_vul_shodan.admin integração do Shodan instalada.) • sn_vul.configure_nvd_ (quando as integraçõ estão instaladas). • treemap_admin (quan aplicação Performanc está instalada.)
Orquestração de patches	Configura integrações de fornecedor de patch de terceiros compatíveis. Exibir e aplicar dados de patch e registros de patch.	• sn_vul_patch_orch.co Configure e aplique p • sn_vul_patch_orch.rea Pode exibir registros e patch. • sn_vul_bigfix.configure Configura a aplicação BigFix Patch Orchestra Integration. Esta funçã contém as funções gr sn_vul_bigfix.read_inte connection_admin qu que o usuário se cone do BigFix. • sn_vul_sccm.configure Esta função contém as funções granulares sn_vul_sccm.read_inte connection_admin qu que o usuário se cone do SCCM. • sn_vul_bigfix.read_inte

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
		Usuários com esta fun visualizar (somente leit registros da aplicação vulnerabilidades e do Orchestration Integrat de orquestração de p • sn_vul_sccm.read_inte Usuários com esta fun exibir (somente leitura da Resposta a vulnera e da aplicação Integr Orquestração de pato Microsoft SCCM e os c orquestração de pato
Analistas de vulnerabilidade [sn_vul.vulnerability_write]	A função sn_vul.vulnerability_write é necessária para gerenciar tarefas de correção e itens vulneráveis e monitorar o andamento da correção.	• sn_vul.read_all • sn_sc_cmn.write • sn_vul_qualys.user (qu integração de vulnera Qualys está instalada. • sn_vul_shodan.write (c integração do Shodan instalada.)
V19.0: Gerenciador de eventos de vulnerabilidade [sn_vul_analyst.vul_event_manager]	A função sn_vul_analyst.vul_event_manager é usada para avaliar o impacto de uma nova vulnerabilidade ou software, ou adicionar uma vulnerabilidade de dia zero para identificar os ativos afetados e criar itens vulneráveis (IVs).	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emerge • sn_vul.manage_expos
Outros [sn_vul.read_all] A função sn_vul.vulnerability_read está obsoleta.	A função sn_vul.read_all é necessária para qualquer pessoa que precise de visibilidade na gestão de vulnerabilidades. Por exemplo, executivos de TI e segurança ou alguém que deseja detalhar os painéis de alto nível até os itens que compõem os elementos visuais do painel.	• sn_sec_cmn.read • sn_vul_qualys.read (qu integração de vulnera Qualys está instalada. • sn_vul_shodan.read (c integração do Shodan instalada.) • pa_viewer (quando a Performance Analytics instalada.)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
		• sn_vul_tenable.read_ir (quando a Integração vulnerabilidade da Te instalada.)
Administrador de importação do sistema VR [sn_vul.vr_import_admin]	Sistema executado como usuário. Executa trabalhos agendados. **Nota:** Este usuário é o padrão executar como usuário para cada registro de integração. Não mude.	• import_admin • sn_vul.vulnerability_wri
Responsável pela correção [sn_vul.remediation_owner]	Exiba e atualize a permissão para itens vulneráveis e tarefas de correção atribuídas a você ou ao seu grupo. Pode exibir todas as vulnerabilidades e soluções. Tem acesso de gravação ao**campo Anotações internas** no registro da solução.	Contido na função itil.
CISOs e executivos de vulnerabilidade [sn_vul.vulnerability_ciso]	Exiba o painel do CISO no Performance Analytics para Resposta a vulnerabilidades.	• sn_vul.ciso_read • sn_vul.read_all

Trabalhos agendados instalados

Trabalho agendado	Descrição
Preencher filtros OOTB salvos para o módulo Host e App	Migra módulos relacionados ao módulo Host e App.
Preencher filtros OOTB salvos para módulo CC	Migra módulos relacionados ao módulo CC.
Preencher filtros OOTB salvos para o módulo de contêiner	Migra módulos relacionados ao módulo de contêiner.
Atualizar filtros salvos relacionados ao host	Atualiza todos os dados de agregação relacionados a filtros salvos do módulo Host.
Atualizar filtros salvos relacionados a CC	Atualiza todos os dados de agregação relacionados a filtros salvos do módulo CC.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Atualizar filtros salvos relacionados ao contêiner	Atualiza todos os dados de agregação relacionados a filtros salvos do módulo Contêiner.
Atualizar filtros salvos relacionados ao app	Atualiza todos os dados de agregação relacionados a filtros salvos do módulo da aplicação.
Acionar criação e execução de agregação para filtro salvo	Cria, atualiza, executa e atualiza as agregações relacionadas ao filtro salvo.
Versão 19.0 do Vulnerability Response e v4.0 do Veracode Vulnerability Integration	A integração do Veracode CWE recupera Veracode - dados específicos de Enumeração de pontos fracos comuns (CWE) para obter informações sobre ameaças e recomendações de correção. A integração do Veracode SBOM ingere informações de versão, versão e vulnerabilidade que se originam em Veracode sobre os componentes em seus projetos de software. A integração gera SBOMs no formato CycloneDx JSON e os carrega em sua instância A integração de categorias do Veracode recupera dados de categorias aprimoradas de Veracode. A integração Veracode de DevOps permite que os usuários do DevOps exibam detalhes de resumo das verificações de vulnerabilidade de terceiros sem uma licença do SecOps. APIs baseadas em JSON para as seguintes integrações do Veracode: item vulnerável da aplicação, resumo de verificação, lista de aplicações. As versões de API baseadas em XML dessas integrações estão obsoletas.
Associar IVs existentes à regra de exceção automática	Associa automaticamente a regra de exceção automática aos IVs existentes.
Encerrar automaticamente detecções de vulnerabilidade	Encerra automaticamente as detecções vulneráveis obsoletas com base na configuração definida na tabela 'sn_vul_auto_close_config'.
Versão 16.1: HCL BigFix Collection, Fixlet e Integrações de Ações.	Gerencie patches e implantações de patch para vulnerabilidades com patches do produto HCL BigFix.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Calcular contagens relacionadas para todas as soluções	Inativo por padrão. Processa dados de soluções uma vez por noite em vez de continuamente. A partir da v22.0, você pode executar este trabalho somente sob demanda. Como este trabalho agendado processa todas as soluções, ele pode afetar o desempenho. Portanto, é recomendável executar este trabalho apenas uma vez se os dados da solução estiverem corrompidos.
Calcular contagens de IV relacionadas à tarefa de vulnerabilidade e correção	Captura mudanças de importação manuais e de IV do dia. Reconcilia relacionamentos de vulnerabilidade e solução e recalcula os totais. Os dados de soluções são enfileirados e processados separadamente pelo trabalho agendado **Processar fila de métricas de solução de vulnerabilidade**.
Verificar tempo limite do MID Server	Faz ping no MID Server e erra após 30 segundos.
V19.0: verificar possível exposição a vulnerabilidades	Processa os CVEs delta, o software e as instalações para obter a exposição.
Verificar estado de execução AguardarConcluído	Marca uma execução de integração como concluída depois que ela é verificada como totalmente concluída.
Expiração do adiamento de itens vulneráveis de verificação e grupos	Envia notificações se itens vulneráveis ou vulnerabilidades expirarem (e se expirarem em uma semana). Verifica se alguma regra de exceção é aplicável em um VI adiado e atualiza os campos **Motivo** e **Até** de acordo com a regra de exceção. O estado do IV permanece Adiado até a data de vencimento mais recente.
VITs de cancelamento de encerramento que não têm um IC associado	Encerra automaticamente itens vulneráveis que não têm um item de configuração (IC) associado e não são atualizados há três dias. O estado está definido como Encerrado/Cancelado.
Fechar VI na exclusão do registro de exp	Encerra um VI quando ele é excluído.
Integração de resultados de conformidade	Importa resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas para processamento na aplicação Conformidade de configuração.
Integração de preenchimento de resultados de conformidade	Parte de uma execução de integração encadeada com a Tenable.io Integração de ativos, importa dados de avaliação de configuração para ativos ignorados que são descobertos (importados por meio da integração de ativos).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Sincronização de estado de CR	O script adapta todas as tarefas de correção existentes aos relacionamentos CHG para que sejam sincronizados. Habilita a sincronização daqui para frente.
Integração de credencial de verificação da versão 15.0	Importa e armazena com segurança temporariamente Tenable.io credenciais usadas para acessar o scanner para novas verificações sob demanda.
Integração do CWE Abrange 2000	Integração de vulnerabilidade que extrai informações de vulnerabilidade do conjunto de dados de Enumeração de Fraqueza Comum (CWE), com curadoria da MITRE Corporação.
V18.0: excluir registros de ação de divisão obsoletos	Trabalho diário para limpar registros obsoletos em tabelas intermediárias de tarefa dividida.
Desabilitar soluções de VR quando a aplicação de soluções não estiver ativa	Desabilita e oculta o recurso Solução de gestão de vulnerabilidade quando a aplicação Solução de gestão de Resposta a vulnerabilidades não está instalada.
Avaliar metas de correção	Define ou atualiza datas de meta de correção em todos os itens vulneráveis. Determina o status das datas de meta de correção em relação às regras.
• Corrigindo as detecções de chave atualizada para Rapid7 • Corrigindo as detecções de chave atualizada para Qualys • Corrigindo as detecções da chave atualizada da Tenable	Limpa os dados de detecção automaticamente por um trabalho agendado específico de integração que é acionado após o upgrade para Resposta a vulnerabilidades.
Versão 16.1: gerar resumo de correção	Este trabalho gera automaticamente um resumo de e-mail para todos os usuários do grupo de usuários responsáveis pela correção. O trabalho é ativado por padrão.
V19.0: Inserir CVE explorado CISA na configuração de exposição	Insere CVEs CISA na tabela Configuração de exposição para calcular a exposição.
V18.0: inserir tarefas de correção clássicas na tarefa de correção unificada	Trabalho agendado único para inserir todas as tarefas de correção criadas na IU clássica na tarefa de correção unificada (sn_vul_remediation_task).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Integração da solução do Centro de Resposta de Segurança da Microsoft	Solução de gestão de vulnerabilidade integração que recupera soluções do Microsoft Security Response Center.
Versão 16.1: Integrações de coleta, atualização de patch e implantações do Microsoft SCCM	Gerencie patches e implantações de patch para vulnerabilidades com Microsoft patches do SCCM.
Retirar processo de integração limitado	Cria o processo de integração para o Integração com Shodan Exploits.
Preencher texto de produtos afetados	Após o upgrade, lida com as soluções existentes para preencher o texto dos produtos afetados. Este trabalho é executado uma vez.
Preencher nova coluna de contagem de CR	Preenche automaticamente a nova coluna de contagem de CR para clientes com dados existentes na tabela de tarefa de correção [sn_vul_vulnerability].
Processar fila de métricas de solução de vulnerabilidade	Processa os dados de soluções enfileirados da seguinte forma: • Acúmulo de soluções de entradas do NVD para entradas de terceiros • Preencher soluções preferenciais em vulnerabilidades e • Atualizando as métricas de status de correção nas soluções Além disso, ele também processa as soluções marcadas para status de atualização. **Nota:** Se você estiver usando apenas Rapid7, poderá desabilitar este trabalho agendado para melhorar o desempenho.
Preencher registros na tabela de mapeamento de fornecedor de vulnerabilidade Preencher registros na tabela de mapeamento de fornecedor de vulnerabilidades para vulnerabilidades do Rapid7	Insere registros na tabela de mapeamento de fornecedor de vulnerabilidades para vulnerabilidades existentes.
Reabrir grupos de vulnerabilidades adiados	Reabre tarefas de correção adiadas quando a data de adiamento tiver passado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Reaplicar todas as regras de atribuição de vulnerabilidade	Reavalia as regras de atribuição em relação a todos os VIs **abertos**.
Versão 16.5: contagem de reatribuições para regras de atribuição	É executado diariamente e publica o número total de IVs e tarefas de correção não atribuídas por este recurso para uma regra de atribuição específica.
Red Hat Solution Integration	Solução de gestão de vulnerabilidade integração que recupera soluções do Red Hat Security Advisory.
V17.1: atualizar e resolver VITs duplicados na tarefa de correção	Encontra itens vulneráveis duplicados para os itens na tarefa de correção com a opção "Atualizar automaticamente IVs duplicados" ativa.
Atualizar itens vulneráveis associados para tarefa de não correção baseada em regra da tarefa de correção	Atualiza a tarefa de correção com itens vulneráveis que correspondem aos critérios Grupo de filtros e Grupos de condições.
Reparar itens vulneráveis incorretos abertos e encerrados pela última vez	Repara dados de IU existentes corrompidos por defeitos corrigidos anteriormente.
Executar calculadoras novamente	Reaplica as calculadoras a todos os itens vulneráveis afetados pela mudança. Isso aciona um recálculo das pontuações de risco cumulativas de suas tarefas de correções. **Nota:** A reexecução de calculadoras pode levar muito tempo, dependendo do seu ambiente.
Repetir conjuntos para importação de integrações canceladas	Novas tentativas de conjuntos de importação de integração cancelados. Novas tentativas 5 vezes antes de retornar um erro.
Processos de integração de nova tentativa	Novas tentativas de processos de integração. Novas tentativas 5 vezes antes de retornar um erro.
Acumular valores de item vulnerável para vulnerabilidade e grupo	Calcula a pontuação de risco, o número de itens vulneráveis e o status da meta de correção para tarefas de correção, usando a calculadora de acúmulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
	Nota: A partir da v23.0 de Resposta a vulnerabilidades, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de vários threads. Esse upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.
Executar calculadora de gravidade após a promoção de entrada de vulnerabilidade	Executa a calculadora de gravidade depois que uma vulnerabilidade ausente anteriormente é atualizada com sua pontuação e outros dados de um provedor de terceiros, como Qualys Cloud Platform, Rapid7 Nexpose.
V19.0: executar avaliação de exposição para CVEs configurados	Calcula a exposição de todos os registros de CVE na tabela Configuração de exposição.
V19.0: executar exposição de software	Calcula a exposição de todos os registros de software na tabela Configuração de exposição.
Processador de Fonte de Dados de Vulnerabilidade Programada	Verifica a fila de importação em busca de entradas a serem processadas e atribui um trabalho de importação agendada com base nos recursos disponíveis.
Limpeza programada de anexos do processo de integração de vulnerabilidade	Remove anexos XML de integração quando eles completam 14 dias. Este tempo de retenção não é configurável.
Verificador de tempo limite de integração de vulnerabilidade programada	Cancela execuções de integração que levam mais de 60 minutos para serem concluídas.
Definir serviços de IC relacionados para VI	Depois que a importação de integração é concluída, ela vincula os serviços de negócio afetados aos ICs conectados a itens vulneráveis, no tempo especificado. Para obter mais informações, consulte Mapeamento de serviços no Resposta a vulnerabilidades.
Definir contagens de adiamento	Coleta o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou uma tarefa de correção foi adiado.
Acionar a próxima integração	Aciona a próxima integração em uma execução de integração em cadeia.
Integração de modelo	Um único registro de modelo é enviado para Tenable.io durante a nova verificação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Atualizar itens vulneráveis não agrupados	Determina se um item vulnerável está em umatarefa de correção e o adiciona ou remove da lista de **Itens vulneráveis** não agrupados. **Nota:** Este trabalho é executado após o upgrade e, dependendo do conjunto de dados, pode levar muito tempo para ser concluído.
Atualizar vulnerabilidade no VG	Atualiza o campo **Vulnerabilidade** na tabela Tarefa de correção (sn_vul_vulnerabilty) após o upgrade. Este trabalho é acionado uma vez e fica inativo depois.
Modelo de importação de vulnerabilidade	Mecanismo que processa a fila de importação. Um de 10.
Atualização encerrada de idade da Resposta a vulnerabilidades	Atualiza a coluna Idade fechada na tabela VI.
Contagem de IC de resposta a vulnerabilidades	Calcula o número de ICs verificados por scanners de terceiros nos últimos 30 dias.
Vulnerability Response Risk and Remediation Status Upgrade	Atualiza a classificação de risco nos dados quando você faz upgrade.
v20.0: verificar expiração da redução de risco	Verifica se os controles compensatórios expiraram para um item vulnerável e uma tarefa de correção. Se expirarem, ele reverterá a pontuação de risco para a pontuação de risco original e enviará uma notificação por e-mail indicando que os controles compensatórios expiraram. Também envia uma notificação por e-mail se os controles compensatórios estiverem definidos para expirar em 7 dias.

Tabelas instaladas

Tabela	Descrição
v22.0 sn_vul_cmn_auto_close_rule	Encerra detecções obsoletas automaticamente com base nas condições do filtro.
sn_vul_cmn_ws_saved_filter	Armazena os dados do filtro salvo.
sn_vul_licensing_usage	Contém o ativo duplicado, o ativo IP incompleto, as contagens totais de ativos do scanner e o uso final.
sn_vul_m2m_entry_compensating_control	Representa a associação entre entradas de vulnerabilidade e controles de compensação.
v21.0	Armazena os registros importados dos dados do Mecanismo de verificação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Mecanismo de verificação do Rapid7 [sn_vul_r7_scan_engine]	responsável por descobrir ativos durante uma verificação e verificar se há vulnerabilidades.
v21.0 Importação do mecanismo de verificação do Rapid7 [sn_vul_r7_scan_engine_import]	Usado pela integração do Rapid7 Scan Engine para preparar dados de importação antes do processamento.
Versão 19.0: [sn_vul_veracode_cwe_import]	Estende a tabela de categorias do Veracode para recomendações de correção do CWE.
Versão 19.0: [sn_vul_veracode_category_import]	Armazena dados de categoria importados.
Versão 19.0: [sn_vul_veracode_sbom_import]	Armazena dados SBOM importados originados do Veracode.
V17.1: Adicionar prova à chave VI [sn_vul_prova_key_vulnerability]	Vulnerabilidades do Rapid7 para as quais a prova deve ser incluída na chave IV.
Itens vulneráveis avaliados [sn_vul_m2m_exp_sw_vi]	Atribui uma tarefa de correção a um grupo de atribuição durante a criação da tarefa de correção.
Regra de atribuição [sn_vul_vgr_assignment_rule]	Atribui uma tarefa de correção a um grupo de atribuição durante a criação da tarefa de correção. Antes da v15.0: atribui uma tarefa de correção a um grupo de atribuição durante a criação da tarefa de correção [].
Associar Solicitação de Mudança [sn_vul_action_associate_cr]	Tabela de preparação usada para processar novas associações CHG da tarefa de correção. Antes da v15.0: tabela de preparação usada para processar novas associações VG-CHG.
Trabalho de Item Vulnerável Assíncrono [sn_vul_async_vi_job]	Contém trabalhos em segundo plano que processam itens vulneráveis. Somente um tipo de trabalho é compatível; usados para editar vulnerabilidades em massa.
Tipo de trabalho de item vulnerável assíncrono [sn_vul_async_vi_job_type]	Contém os tipos de trabalhos em segundo plano e faz referência ao script relevante. Tem apenas um processador, o **VulnerabilityBulkEditProcessor**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Encerrar automaticamente detecções obsoletas [sn_vul_auto_close_config]	Armazena a configuração de como as detecções obsoletas são fechadas automaticamente.
Configurar granularidade de item vulnerável [sn_vul_action_vi_granularity_config]	Armazena o formulário de IU usado para habilitar ou desabilitar a Porta de inclusão na página de configuração no módulo Configurar granularidade de IV.
Criar solicitação de mudança [sn_vul_action_create_cr]	Usado para criar solicitações de mudança a partir da tarefa de correção.
Criar Itens vulneráveis [sn_vul_action_create_vi]	Uma tabela de preparação que é usada como um espaço reservado para informações. Esta tabela não armazena nenhum registro.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
CWE [sn_vul_cwe]	Catálogo de vulnerabilidades de software de Enumeração e Fraqueza Comuns (CWE).
Plataforma aplicável do CWE [sn_vul_cwe_m2m_cwe_platform]	Contém os dados importados da plataforma aplicável do CWE.
Categoria CWE [sn_vul_cwe_category]	Contém os dados de categoria CWE importados.
Consequência CWE comum [sn_vul_cwe_conquence]	Contém os dados de consequência comuns do CWE importados.
Referência externa do CWE [sn_vul_cwe_reference]	Contém os dados de referência externa do CWE importados.
Exemplo observado do CWE [sn_vul_m2m_cwe_cve]	Contém os dados CVE do CWE importados.
Plataforma do CWE [sn_vul_cwe_platform]	Contém os dados importados da plataforma CWE.
Referência externa do CWE	Contém os dados de referência externa relacionados ao CWE importados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_cwe_reference]	
Relacionamento do CWE [sn_vul_m2m_cwe_relation]	Contém os dados de relacionamento do CWE importados.
Exibição do CWE [sn_vul_cwe_view]	Contém os dados de exibição do CWE importados.
Ponto fraco do CWE [sn_vul_cwe_weakness]	Contém os dados de fraqueza do CWE importados.
Versão 16.1: coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Versão 16.1: atualização de dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de itens descobertos.
Correspondência de software vulnerável do modelo de descoberta [sn_vul_discovery_model_software_match]	Complementa a correspondência de software vulnerável a um modelo de descoberta.
Configuração de gestão de exceções [sn_vul_exception_config]	Armazena as definições de configuração do recurso de gestão de exceções.
Regra de exceção [sn_vul_auto_exception_rule]	Contém o conjunto de regras avaliadas para Gestão de exceções.
Explorar [sn_vul_exploit]	Contém as definições de explorações: código disponível publicamente que aproveita uma vulnerabilidade.
Estrutura da Exploração sn_vul_exploit_framework	Contém os nomes das estruturas de exploração: pacotes de software completos que são capazes de executar muitas explorações.
Modelos de descoberta expostos [sn_vul_m2m_exp_sw_model]	Armazena o mapeamento entre o modelo de Descoberta e Vulnerabilidade Avaliação de exposição.
Avaliação de Exposição [sn_vul_exp_by_sw]	Armazena os registros para avaliação de exposição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
V19.0: Manifesto de exposição sn_vul_analyst_exposure_manifest	Tabela de manifesto para processamento delta.
Entradas de Vulnerabilidade de Exposição [sn_vul_m2m_entry_exp]	Armazena o mapeamento entre a avaliação de vulnerabilidade (sn_vul_entry) e de exposição.
Kit de malware [sn_vul_malware_Kit]	Contém os detalhes dos kits de malware: ferramentas pré-escritas que facilitam a execução de uma exploração ou de um conjunto de explorações relacionadas sem codificação adicional ou trabalho de configuração
Tabela de ativos ausentes [sn_vul_tenable_missing_asset]	Contém IDs de ativos temporários para dados de avaliação de conformidade de configuração ignorados com ativos incompatíveis.
Atualização da Solução do Microsoft Response Center [sn_vul_msrc_update]	Contém a última vez em que os dados da solução foram atualizados pela Microsoft. Usado para comparar com a importação noturna para determinar os dados delta para download.
Microsoft Security Response Center Importação de solução [sn_vul_msrc_solution_import]	Usado pela integração da Solução do Centro de Resposta de Segurança da Microsoft para preparar dados de importação antes do processamento.
Integração com a solução Microsoft Security Response Center [sn_vul_msrc_integration]	Estende a tabela Integração de vulnerabilidade [sn_vul_integration] para Integração com a solução Microsoft Security Response Center.
Entrada do Banco de Dados de Vulnerabilidades Nacionais [sn_vul_nvd_entry]	Vulnerabilidade documentada do banco de dados nacional de vulnerabilidades do NIST.
Importação de CVSS do NVD [sn_vul_nvd_cvss_import]	Contém dados de preparação que ainda não foram transformados para o esquema Resposta a vulnerabilidades durante a importação do NVD.
Versão 16.1 [sn_vul_patch_orch.patch_approval_required]	Quando as implantações de patch são programadas a partir de uma integração de patch, as solicitações são enviadas para revisão e aprovação aos usuários atribuídos ao Nível 1 - Grupo de aprovação de atualizações de patch. Esta propriedade é ativada por padrão.
Versão 16.1: implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre Coleções e ICs.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Versão 16.1: Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Versão 16.1: possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.
V19.0: possível exposição de vulnerabilidade sn_vul_analyst_m2m_pot_exp_sw_model	Tabela de avaliação de exposição para CVE.
Categoria do produto [sn_vul_product_category]	Contém os dados da categoria de produto importada.
Red Hat Security Advisory [sn_vul_rhsa_update]	Compara as soluções Red Hat com o trabalho noturno para determinar os dados delta para importação.
Red Hat Importações de solução [sn_vul_rh_solution_import]	Usado pelo Red Hat Solution Integration para preparar dados de importação antes do processamento.
Red Hat Solution Integration [sn_vul_rh_integration]	Estende a tabela Integração de vulnerabilidade [sn_vul_integration] para Red Hat Solution Integration.
Serviços de negócio relacionados [sn_vul_m2m_ci_services]	Vincula ICs a serviços de negócio para pesquisa de serviços afetados. Contém um sinalizador que indica se ele foi adicionado pelo Mapeamento de serviços.
V18.0: Contagens de esforço de correção [sn_vul_daily_count_re]	Contagem diária de esforços de correção. Esta tabela é atualizada diariamente.
V18.0: registro do esforço de correção [sn_vul_remediation_effort_record]	Rastreia o andamento da correção dos esforços de correção (RE). Contém referências aos REs.
Regra de meta de correção [sn_vul_ttr_rule]	Define o intervalo de tempo esperado para corrigir um item vulnerável. Estende o arquivo de aplicações.
V18.0: Tarefa de correção [sn_vul_remediation_task]	Armazena todas as tarefas de correção para VR, AVR, CVR e grupos de resultados de testes.
Integração REST [sn_vul_rest_integration]	Estende a tabela Integração de vulnerabilidade [sn_vul_integration] para as integrações baseadas em REST.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Detecção de vulnerabilidade do SAM NVD [sn_vul_sam_config]	Contém quais ICs e vulnerabilidades são monitorados com o SAM NVD e se a detecção de vulnerabilidades do SAM NVD está habilitada ou não.
Pool de importação agendada [sn_vul_sched_import_pool]	Coleção de registros de conjunto de importação programados usados para facilitar importações simultâneas de fontes de dados.
Selecionar item vulnerável [sn_vul_action_select_vi]	Tabela de preparação base usada para lidar com VG dividido, criar CHGs e associar CHGs
Status de configuração [sn_vul_setup_status]	Somente interno: usado pelo Assistente de configuração. Sempre que o Assistente de configuração é aberto, ele mostra o status das etapas Concluídas e a porcentagem no canto superior direito vem dessa tabela.
Mapa de Gravidade [sn_vul_severity_map]	Contém os mapeamentos da gravidade de origem para a gravidade normalizada.
Mapeamento do Scanner de Solução [sn_vul_solution_scanner_mapping]	Mapeia fornecedor, scanner e palavras-chave para exclusão ou inclusão.
Dividir grupo de vulnerabilidades [sn_vul_action_split_vg]	Tabela de preparação usada para dividir tarefas de correção.
Entrada de Vulnerabilidade de Terceiros [sn_vul_ third_party_entry]	Vulnerabilidade documentada de uma fonte de terceiros.
[sn_vul_tenable_io_template	Um registro de modelo é enviado para Tenable.io e importado durante a nova verificação para itens que têm Tenable.io como origem.
Atualizar manifesto [sn_vul_update_manifest]	Lista de tarefas de correção que foram atualizadas e exigem recálculo pela calculadora de acúmulo.
V17.1: Uso por classes de IC [sn_vul_licensing_usage_by_ci_classes]	Contém a contagem de uso agregada pela classe de IC.
Contagem de Itens de Configuração de VR [sn_vul_vr_configuration_item_count]	Contém a média cumulativa de 90 dias consecutivos de itens de configuração importados de integrações de terceiros.
Regras de Atribuição da Vulnerabilidade [sn_vul_assignment_rule]	Contém o conjunto de regras avaliadas para definir o grupo de atribuição nos IVs.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Calculadora de Vulnerabilidade [sn_vul_calculator_group]	Contém as regras da calculadora de vulnerabilidade. A ordem da calculadora determina qual calculadora é avaliada primeiro e, em cada calculadora, é usada no máximo uma regra de calculadora.
Regra da Calculadora de Vulnerabilidade [sn_vul_calculator]	Contém as regras para todas as calculadoras. Para cada calculadora, as regras da calculadora são revisadas em ordem. A primeira calculadora que corresponde à condição usa os valores dessa regra.
CVEs de vulnerabilidade [sn_vul_m2m_entry_cve]	Vincula os dados de CVE (Common Vulnerability Exposures, exposições de vulnerabilidade comuns) do NVD a entradas vulneráveis.
Entrada da Fila de Importação da Fonte de dados de Vulnerabilidade [sn_vul_ds_import_q_entry]	Fila para anexos antes que eles sejam processados por uma fonte de dados. Usado por integrações de vulnerabilidade.
Entrada de Vulnerabilidade [sn_vul_entry]	Vulnerabilidade documentada.
Verificação de entrada de vulnerabilidade [sn_vul_entry_scan]	Armazena o relacionamento entre uma verificação e a entrada de vulnerabilidade.
Estrutura de Exploração de Vulnerabilidade [sn_vul_m2m_framework_vul]	Contém o relacionamento entre estruturas de exploração e vulnerabilidades.
V19.0: avaliação de exposição de vulnerabilidade sn_vul_analyst_sam_config	Tabela de configuração de avaliação de exposição para CVE.
Configuração de granularidade de vulnerabilidade [sn_vul_granularity_config]	Armazena e mantém o estado de inclusão ou exclusão de porta para o módulo Configurar granularidade de VI.
Tarefas de correção [sn_vul_vulnerability]	Coleção de itens vulneráveis organizados para correção.
Solicitações de mudança de tarefa de correção [sn_vul_m2m_vg_change_request]	Armazena a associação de tarefas de correção e solicitações CHG.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Itens da Tarefa de correção [sn_vul_m2m_vul_group_item]	Associação de tarefas de correção e itens vulneráveis.
Regras de tarefa de correção [sn_vul_grouping_rule]	Contém as regras que definem os critérios com os quais os grupos são criados automaticamente para um conjunto de itens vulneráveis.
Integração de Vulnerabilidade [sn_vul_integration]	Registro programável para importar dados de vulnerabilidade de uma fonte externa. Estende a execução de script programada.
Fonte de dados de integração de vulnerabilidade [sn_vul_int_data_src]	Fonte de dados a ser usada com uma integração de vulnerabilidade.
Log de Integração de Vulnerabilidades [sn_vul_integration_log]	Registra a saída de informações de log por execuções de integração de vulnerabilidade.
Processo de Integração de Vulnerabilidades [sn_vul_integration_process]	Ocorrência de processo único para uma integração de vulnerabilidade.
Fila de Integração de Vulnerabilidade [sn_vul_integration_queue]	Enfileira as solicitações de importação para uma execução de integração quando todas as fontes de dados estão em uso.
Execução de Integração de Vulnerabilidades [sn_vul_integration_run]	Invocações de integração de vulnerabilidade. **Nota:** Se uma execução de integração estiver em andamento, somente uma integração poderá estar no estado pronto no backlog.
Estatísticas de execução de integração de vulnerabilidade [sn_vul_integration_stats]	Armazena o detalhamento de cada etapa: por exemplo, tempo de REST API, tempo de criação de VI e assim por diante para uma execução de integração
Tarefa de Item de Vulnerabilidade [sn_vul_m2m_item_task]	Itens vulneráveis associados a problemas, mudanças e incidentes de segurança.
Kit de Malware de Vulnerabilidade [sn_vul_m2m_malware_Kit_vul]	Contém os relacionamentos entre vulnerabilidades e kits de malware.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Solução de pré-requisitos de vulnerabilidade [sn_vul_m2m_solution_prerequisito]	Contém os pré-requisitos específicos da origem para aplicar uma solução, quando disponíveis.
Limite da taxa de vulnerabilidade [sn_vul_rate_limit]	Define um limite de taxa a ser usado em um scanner.
Referência de Vulnerabilidade [sn_vul_reference]	Referências externas para vulnerabilidades conhecidas.
Status de Correção de Vulnerabilidade [sn_vul_m2m_ttr_status]	Status do item vulnerável em relação à regra de meta de correção aplicada mais próxima.
Regra do Risco de Vulnerabilidade [sn_vul_calcul_risk]	Regra de calculadora especializada usada com as calculadoras de pontuação de risco. Usa pesos indicando quais valores, relacionados a um VI, serão usados para calcular a pontuação de risco.
Calculadora de Rollup de Vulnerabilidade [sn_vul_rollup]	Lista de calculadoras de acúmulo de vulnerabilidades.
Verificação de vulnerabilidades [sn_vul_scan]	Verificação de vulnerabilidades. Contém o que verificar, com qual scanner e um resumo dos resultados da verificação.
Item de configuração da Verificação de vulnerabilidades [sn_vul_m2m_scan_configuration_item]	Associa ICs do CMDB que estão na fila para serem verificados.
Entrada da fila de Verificação de vulnerabilidades [sn_vul_scan_q_entry]	Registro de verificação enfileirado para verificação ou processamento. Facilita as solicitações dentro dos limites de taxa declarados.
Origem da Verificação de vulnerabilidades [sn_vul_m2m_scan_source]	Associa origens a um registro de verificação e indica todos os registros que estão na fila para serem verificados.
Tarefa da Verificação de vulnerabilidades [sn_vul_m2m_scan_vulnerability]	Associa tarefas de vulnerabilidade às origens de um registro de verificação.
Verificador de vulnerabilidade [sn_vul_scanner]	Define scanners de terceiros a serem usados em verificações.
Limite de taxa do scanner de vulnerabilidades [sn_cmn_scanner_rate_limit]	Associa um scanner a um limite de taxa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Software de Vulnerabilidade [sn_vul_m2m_entry_software]	Contém associações entre vulnerabilidades e software vulnerável.
Solução de Vulnerabilidade [sn_vul_solution]	Contém os dados de relacionamento entre a vulnerabilidade e as possíveis soluções para ela.
Solução de Vulnerabilidade [sn_vul_m2m_vulnerability_solution]	Vincula a tabela de entrada de vulnerabilidade (sn_vul_entry) à tabela de solução de vulnerabilidade (sn_vul_solution).
Aprovação de Mudança do Estado de Vulnerabilidade [sn_vul_change_approval]	Rastreia o processo de aprovação de vulnerabilidades.
Solução de Substituição de Vulnerabilidade [sn_vul_m2m_solution_supersedence]	Contém o relacionamento específico de origem entre as soluções.
Manifesto de Atualização de Vulnerabilidade [sn_vul_vuln_update]	Contém uma lista de vulnerabilidades que precisam de seus dados de acúmulo atualizados depois que seus itens vulneráveis são atualizados, encerrados ou têm mudanças de pontuação de risco.
Mapeamento de Fornecedor de Vulnerabilidade [sun_vul_vulnerability_vendor_mapping]	Contém uma lista de vulnerabilidades e seus fornecedores.
Item Vulnerável [sn_vul_vulnerable_item]	Contém a ocorrência de uma vulnerabilidade em um item de configuração.
Detecção de Item Vulnerável [sn_vul_detection]	Contém as detecções de itens vulneráveis de integrações de terceiros.
Software Vulnerável [sn_vul_software]	Software que é conhecido por ter determinadas vulnerabilidades.

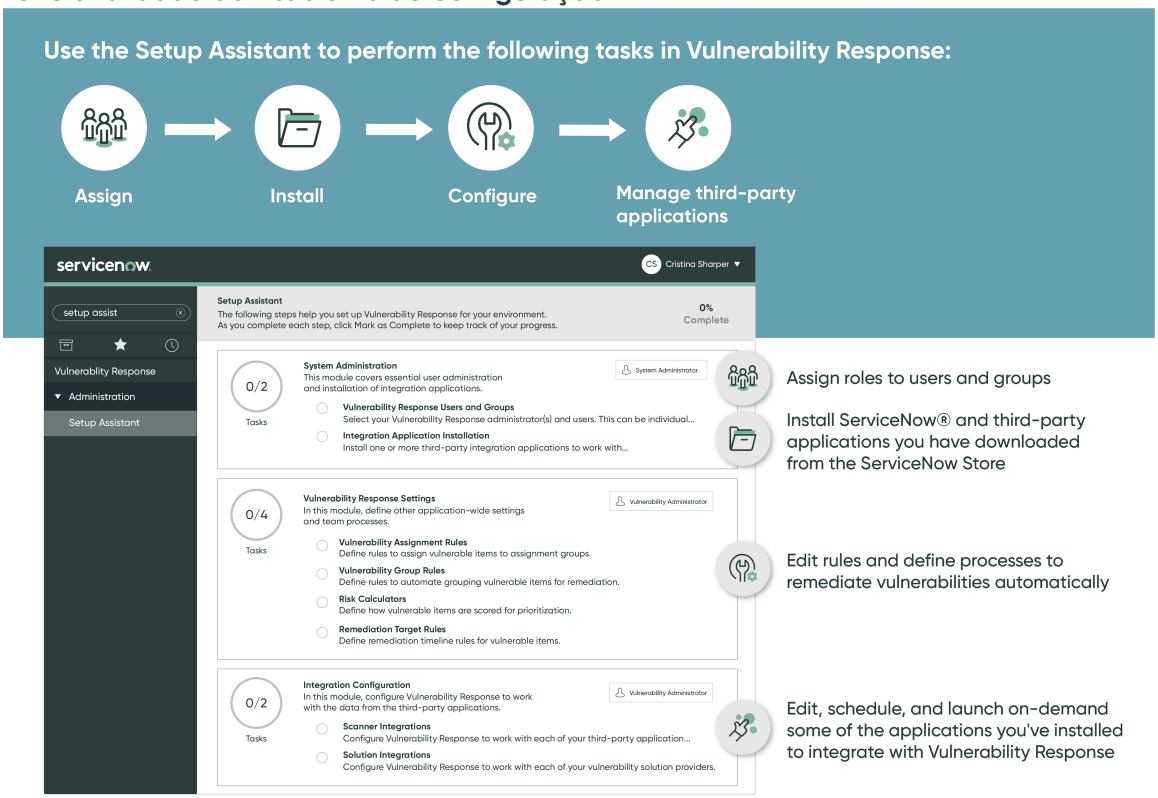
Configuração de Resposta a vulnerabilidades usando o Assistente de configuração

O Assistente de configuração orienta você na configuração de Resposta a vulnerabilidades e determinadas integrações de terceiros para seu ambiente. O Assistente de configuração fornece quase tudo o que você precisa para instalar e configurar seu ambiente para que você possa usar Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funcionalidade do Assistente de configuração



Now Platform® roles: admin and vulnerability admin

O uso do Assistente de configuração requer duas funções Now Platform® diferentes: administrador e administrador de vulnerabilidades.

Consulte as seções a seguir para complementar as instruções e os avisos fornecidos no Assistente de configuração.

Administração do sistema - atribuir usuários e grupos e instalar aplicações de integração

Função necessária: administrador

Uma lista de usuários e integrações deve ser obtida do Gerenciador de vulnerabilidades antes de iniciar essas tarefas.

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.
2. Na primeira seção, Administração do sistema, o administrador atribui funções a usuários e grupos e instala integrações compatíveis.

   Atribua Resposta a vulnerabilidades personas e funções a usuários e grupos no Assistente de configuração.

   Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Atribua funções no Assistente de configuração.
   - Atribua a função de sn_vul.admin a usuários ou grupos.
   - Atribua a função sn_vul.admin para administração e configuração da Resposta a vulnerabilidades, incluindo integrações de vulnerabilidade, regras de tarefa de correção, calculadoras e regras de tempo de correção.
   - Atribua a função sn_vul_vulnerability_write para a criação e atualização de tarefas de correção e itens vulneráveis.

     Nota: Todos os outros usuários recebem automaticamente o acesso de gravação somente para tarefas de correção atribuídas a eles.

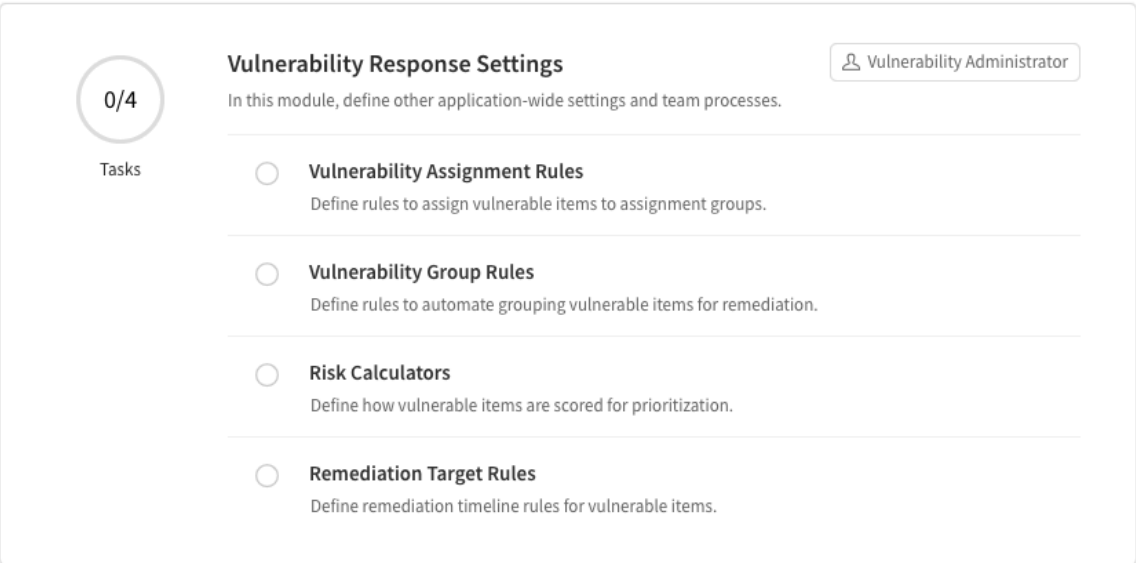
   - Atribua a função sn_vul_vulnerability_read para exibir tarefas de correção, itens vulneráveis e outras informações de vulnerabilidade.

     Nota: Usuários com a função itil recebem automaticamente a função sn_vul.remediation_owner, permitindo que eles vejam tarefas de correção e itens vulneráveis atribuídos a eles, entradas de vulnerabilidade e soluções na aplicação Resposta a vulnerabilidades em sua instância e na aplicação Mobile Agent. Nenhuma atribuição adicional é necessária.

4. Instale aplicações de integração de terceiros.
   - Consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis e Integrações do Resposta a vulnerabilidades para obter mais informações sobre aplicações compatíveis com Resposta a vulnerabilidades.
   - Para obter mais informações sobre como usar o assistente de configuração para instalar aplicações compatíveis, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

Resposta a vulnerabilidades Configurações

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou administrador



Em Configurações da Resposta a vulnerabilidades, o administrador de vulnerabilidades define configurações para toda a aplicação e define regras para Resposta a vulnerabilidades. Como alternativa, o administrador pode executar essas tarefas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Crie Regras de atribuição de vulnerabilidade.

   Crie regras que definam a atribuição automática de tarefas de correção para resolução. Pelo menos uma regra é enviada com o sistema de base. Para obter mais informações, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

   Nota:

   O recurso de reaplicação requer uma aplicação de linha de base das regras. Depois que suas regras forem criadas, ative o trabalho agendado *`Reapply all vulnerability assignment rules`* para executar, quando for mais conveniente. Caso contrário, será necessário reaplicar todas as regras a todos os IVs abertos antes de alterá-los.

   Quando o trabalho estiver concluído, defina o campo **Executar** no trabalho agendado para se adequar ao seu ambiente. Dependendo do número de IVs ativos que você tem, avaliá-los e atualizá-los diariamente pode ter um impacto não banal no desempenho. Para ambientes maiores, considere atualizar uma vez por semana ou até mesmo uma vez por mês.

   A reaplicação de regras de atribuição não reagrupa os itens vulneráveis.

2. Criar regras de tarefa de correção.

   Crie regras que definam a criação automática de tarefas de correção para resolução. Pelo menos uma regra, **Vulnerabilidade,** é enviada com o sistema de base. Você pode reaplicar as regras do formulário ou da exibição de lista.

   - Quando uma regra de grupo é excluída, no formulário ou na exibição de lista, você tem a opção de excluir todos os grupos **Abertos** criados por essa regra. Grupos que não estão no estado **Aberto** são excluídos.
   - Consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros para obter mais informações sobre como criar regras para o seu ambiente.
   - Consulte Explorar a aplicação Resposta a vulnerabilidades para obter mais informações sobre como usar Resposta a vulnerabilidades para corrigir vulnerabilidades.

3. Crie e habilite Calculadoras de risco.

   Habilite as calculadoras de risco que definem como os itens vulneráveis são pontuados para priorização. Várias calculadoras de risco são enviadas com o sistema de base. Consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade informações sobre como criar ou editar calculadoras de risco para o seu ambiente.

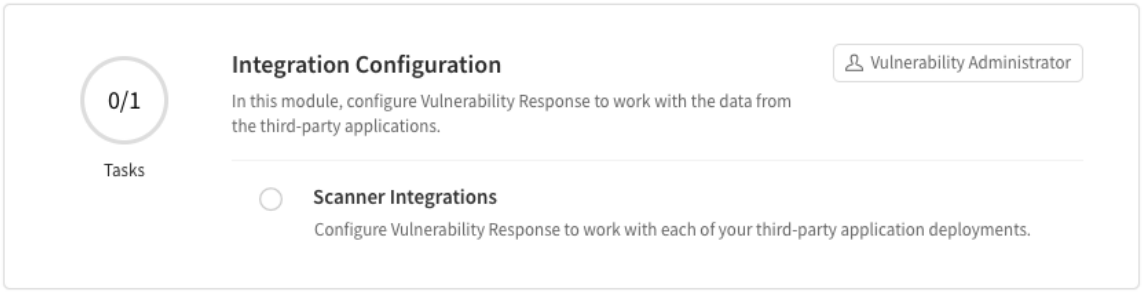
4. Crie Regras de destino de correção.

   Crie regras de destino de correção para categorias de correção. Pelo menos uma regra é enviada com o sistema de base. Consulte Resposta a vulnerabilidades regras de destino de correção para obter mais informações sobre como criar regras para o seu ambiente.

Configuração de Integração

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Na seção Configuração de integração, configure, programe, edite e inicie sob demanda as seguintes integrações de scanner de vulnerabilidade de terceiros e, se a aplicação Solução de gestão de Resposta a vulnerabilidades estiver instalada, provedores de soluções.

- Consulte Configurar o Qualys Vulnerability Integration usando o Assistente de configuração para obter mais informações sobre como configurar o Qualys Vulnerability Integration.
- A configuração da aplicação Integração de Resposta a vulnerabilidades com Tenable é compatível. Consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração.
- Depois de instalar a aplicação Solução de gestão de vulnerabilidade, a opção **Integrações de solução** é exibida abaixo **de Integrações de scanner**. Clique em **Integrações de solução** para configurar os provedores de soluções de vulnerabilidade instalados nesta seção do Assistente de configuração. Red Hat Solution Integration e Integração com a solução Microsoft Security Response Center são compatíveis.

  Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre as soluções instaladas. Consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades para obter mais informações sobre a instalação.

  Consulte Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade usando o Assistente de configuração para obter mais informações sobre como configurar as soluções instaladas.
- Se uma integração tiver várias origens, você poderá ter várias implantações da mesma integração de terceiros.
- As configurações da integração de terceiros original são usadas como modelo para as configurações de cada nova integração.

  Nota: Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

  Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Resposta a vulnerabilidades.

Nota: Várias integrações de vulnerabilidade para Rapid7 InsightVM não estão disponíveis no Assistente de configuração. Consulte Criar importações separadas por domínio para uma integração para obter informações sobre como configurar e criar várias integrações Rapid7 InsightVM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas adicionais

Consulte Tarefas adicionais Resposta a vulnerabilidades de instalação e configuração para obter mais informações sobre tarefas de configuração não incluídas no Assistente de configuração.

Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração

Atribua as funções de persona Resposta a vulnerabilidades a grupos ou usuários com o Assistente de configuração.

Antes de Iniciar

Se você já atribuiu funções de persona em Resposta a vulnerabilidades usando o Assistente de configuração e deseja obter mais informações sobre como editar e gerenciar suas funções granulares e atribuições de função no módulo Administração de usuários, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Se você for um cliente de upgrade, poderá continuar usando suas funções existentes para a aplicação Resposta a vulnerabilidades. O acesso para usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e funções de proprietário de correção disponíveis em versões anteriores de Resposta a vulnerabilidades não foi alterado.

No entanto, para obter mais controle sobre o que usuários e grupos podem fazer e ver na aplicação Resposta a vulnerabilidades no nível da tarefa, talvez você prefira usar funções granulares e de persona.

Se você ainda não atribuiu a função de persona sn_vul.vulnerability_admin usando o Assistente de configuração, siga as etapas abaixo para atribuí-la. Uma vez atribuído, o administrador de vulnerabilidade com esta função de persona tem permissão para concluir as tarefas do Assistente de configuração após a primeira seção e gerenciar regras e integrações de terceiros na aplicação Resposta a vulnerabilidades.

Para obter uma visão geral sobre funções de persona e funções granulares, consulte Resposta a vulnerabilidades personas e funções granulares.

Se você for um cliente de upgrade, use a tabela a seguir como referência.

Antes da v10.3	A partir da v10.3
Se você atribuiu sn_vul.admin	Você pode preferir atribuir sn_vul.vulnerability_admin - Administrador de vulnerabilidade a usuários ou grupos. Usuários com esta função têm acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Usuários com esta função configuram todas as aplicações e regras de VR e instalam integrações de terceiros.
Se você atribuiu sn_vulnerability_write para usuários e grupos.	Você pode preferir atribuir sn_vul.vulnerability_analyst - Analista de vulnerabilidade a usuários e grupos. Usuários e grupos com esta função exibem e atualizam todos os registros para correção de VI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes da v10.3	A partir da v10.3
Se você atribuiu sn_vul.remediation_owner	Você pode preferir atribuir sn_vul.remediation_owner - Proprietário da correção a usuários e grupos. Usuários e grupos com esta função corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem. Grupos ou usuários com esta função exibem e atualizam os registros atribuídos a eles ou a um grupo ao qual pertencem.
Se você atribuiu sn_vul.admin para gerenciamento de itens de configuração (ICs) incompatíveis	Você pode preferir atribuir sn_vul.ci- CI Manager a usuários e grupos. Usuários e grupos com esta função gerenciam itens de configuração (ICs) incompatíveis não encontrados no Configuration Management Database (CMDB). Grupos ou usuários com esta função atualizam itens descobertos.
Se você atribuiu sn_vul.admin para adiamentos e aprovações de exceção.	Você pode preferir atribuir sn_vul.exception_approver - Exception Approver a usuários e grupos. Usuários e grupos com esta função aprovam exceções, adiamentos e fechamentos de tarefas de correção e itens vulneráveis. A partir da v20.0, a função granular, sn_vul.read_all, foi removida para que você possa acessar os itens vulneráveis e as tarefas de correção atribuídos a você e seu grupo em vez de todos os itens vulneráveis e tarefas de correção.
Se você atribuiu sn_vul.vulnerability_read para fornecer visibilidade na gestão de vulnerabilidades.	Você pode preferir atribuir acesso de leitura a áreas específicas na aplicação por tarefa. Por exemplo, atribua sn_vul.read_all para que um usuário possa exibir todos os registros de VR. Para acesso de leitura para exibir regras de tarefa de correção, atribua sn_vul.read_group_rules. Usuários e grupos com esta função não atualizam registros.

Para exibir as funções granulares que um usuário ou grupos com uma função de persona herdam por padrão, navegue até **Todos** > **Administração de usuários** > **Funções**. Localize a função desejada e clique nela para abrir o registro. A guia Contém funções lista todas as funções granulares da função de persona, bem como todas as funções herdadas.

Você pode preferir verificar se todos os usuários e grupos necessários foram criados antes de atribuir funções no Assistente de configuração. Como alternativa, para adicionar novos usuários e grupos de dentro do Assistente de configuração, clique no link do **módulo Administração de usuários** no formulário mostrado na figura a seguir.

Tradução automática

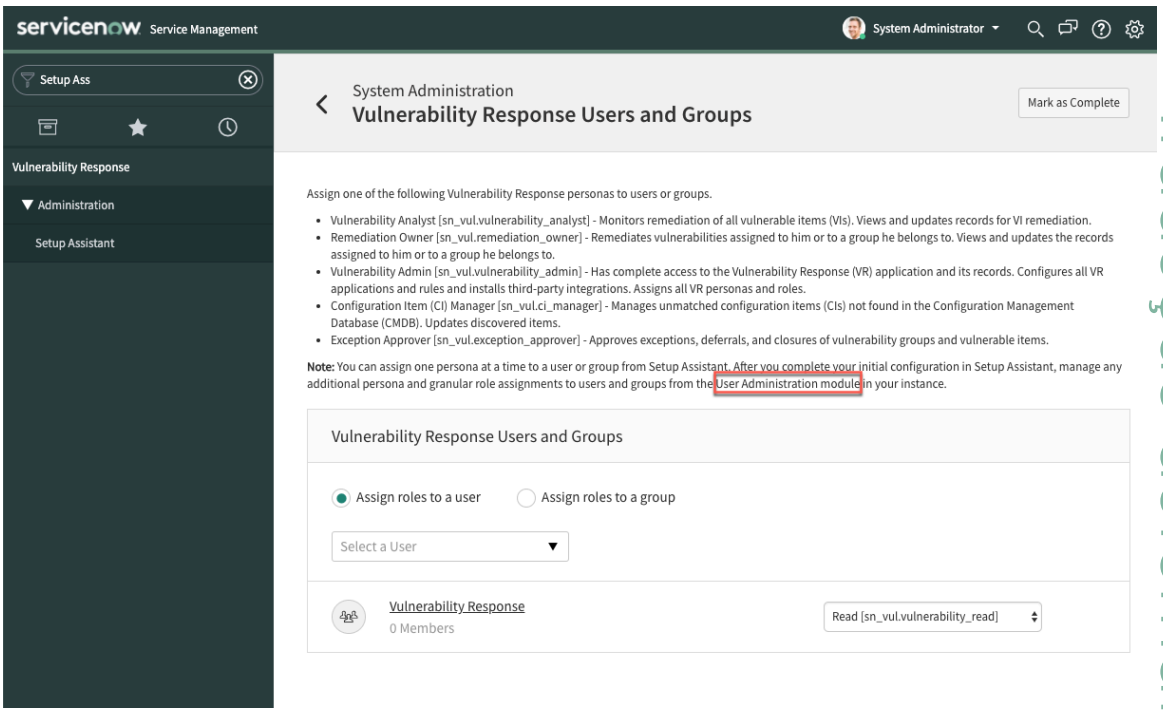
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para o exemplo a seguir, para limitar o acesso à aplicação Resposta a vulnerabilidades, este exemplo mostra como atribuir um usuário com a persona de administrador de vulnerabilidades. Normalmente, você pode preferir atribuir funções de persona diferentes de sn_vul.vulnerability_admin a grupos.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração Assistente de configuração**.
   A página do Assistente de configuração é exibida.
2. Clique em Usuários e grupos da Resposta a vulnerabilidades.
   A página Usuários e grupos da Resposta a vulnerabilidades do sistema é exibida.



3. Com Atribuir funções a um usuário selecionado, escolha um usuário existente na lista.

   Você só pode atribuir um usuário ou grupo com uma função de persona.

   À direita do formulário, depois de selecionar um usuário ou grupo, a persona padrão, Proprietário de correção [sn_vul.remediation_owner], é atribuída por padrão e permanece exibida na lista até que você a altere.

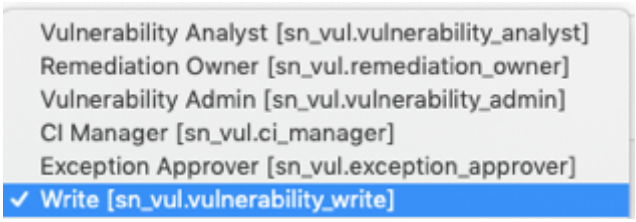
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você estiver atualizando para uma versão mais recente do Resposta a vulnerabilidades e tiver atribuído anteriormente a função sn_vul.vulnerability_read ou sn_vul.vulnerability_write a um usuário ou grupo antes do upgrade, ela será exibida junto com as novas funções de persona, conforme mostrado na figura a seguir .

Se você for um cliente de upgrade, poderá continuar usando suas funções existentes para a aplicação Resposta a vulnerabilidades. O acesso de usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e o proprietário de correção anteriores à v10.3 não foram alterados.

Observe que, para usuários existentes ou grupos atualmente atribuídos com as funções sn_vul.vulnerability_read ou sn_vul.vulnerability_write, essas funções são exibidas junto com as funções de persona na lista. Depois de atribuir uma função de persona, a função antiga não estará mais disponível. Por exemplo, conforme mostrado na figura a seguir, a função Gravação [sn_vul.vulnerability_write] não é mais exibida como uma opção para este usuário ou grupo depois que uma das funções de persona é atribuída a ele.

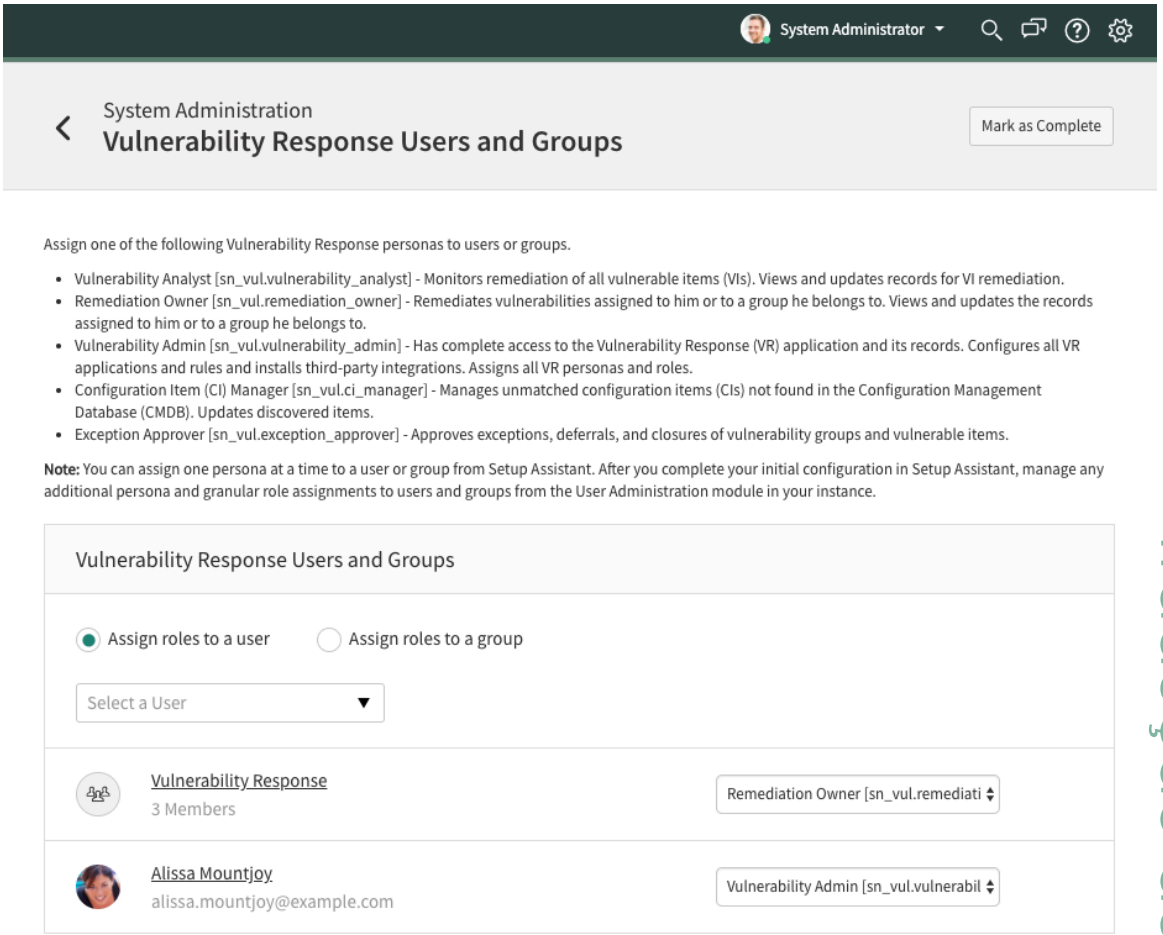


4. Na lista à direita do formulário, selecione **Administrador de vulnerabilidade [sn_vul.vulnerability_admin]**.
   Uma mensagem é exibida indicando que o usuário ou grupo foi atribuído com sucesso à persona.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona do responsável pela correção atribuída a um grupo e persona do administrador de vulnerabilidade atribuída a um usuário



5. Usando as descrições das funções de persona listadas acima, continue a atribuir usuários e grupos às funções de persona restantes: Proprietário de correção, Analista de vulnerabilidade, Gerente de IC e Aprovador de exceção.
   Você concluiu com sucesso a atribuição de funções de persona a usuários e grupos usando o Assistente de configuração.
6. Opcional: Para editar os usuários em um grupo do Assistente de configuração, siga estas etapas.

   a. Com o grupo exibido no formulário, clique no nome do grupo que você deseja editar.
   O registro do grupo é exibido.

   b. Com a guia Membros do grupo selecionada, clique em **Editar**.
   O formulário Editar Membros é exibido

   c. Use o slushbucket para selecionar ou remover usuários.

   d. Clique em **Salvar** para salvar suas mudanças e retornar ao registro do Grupo.

   e. Clique em **Atualizar** para retornar ao Assistente de configuração.

   f. Na página do Assistente de configuração, clique em **Usuários e grupos da Resposta a vulnerabilidades** para continuar com a configuração no Assistente de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Como administrador do sistema, continue com a configuração de Resposta a vulnerabilidades no Assistente de configuração. Observe que após a conclusão da primeira seção, você pode fazer com que um usuário atribuído com a função de persona de administrador de vulnerabilidades conclua as tarefas no Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares e exemplos, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Gerenciar persona e funções granulares para Resposta a vulnerabilidades

Depois de concluir a atribuição inicial de funções de persona usando o Assistente de configuração, gerencie atribuições de função granular adicionais a usuários ou grupos no módulo Administração de usuários em sua instância.

Antes de Iniciar

Se você ainda não concluiu a configuração inicial de Resposta a vulnerabilidades usando o Assistente de configuração ou atribuiu funções de persona a usuários e grupos, navegue até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**. Consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Para obter os principais termos e uma visão geral das funções de persona, consulte Resposta a vulnerabilidades personas e funções granulares.

Uma função de persona é uma função pré-configurada na aplicação que é composta por várias funções granulares. As funções de persona em Assistente de configuração, Administrador de vulnerabilidade, Analista de vulnerabilidade, Proprietário de correção, Gerenciador de itens de configuração e Gerenciador de exceções foram projetadas para corresponder a cargos comuns para gerentes, analistas e proprietários de serviço em uma organização de TI ou grupo de correção de vulnerabilidades.

Se você quiser que seus usuários e grupos tenham mais acesso do que uma das funções permite, você poderá adicionar funções mais granulares a usuários e grupos. Por outro lado, se você quiser limitar o acesso de usuários e grupos específicos no nível da tarefa, poderá remover funções granulares. Além disso, você pode criar funções personalizadas para atender às suas necessidades.

Função necessária: administrador

Procedimento

1. Para gerenciar funções granulares para usuários e grupos, escolha uma para continuar.

Opção	Descrição
Editar as funções granulares de um usuário ou grupo	Atribua ou remova funções granulares para usuários ou grupos ou edite funções granulares para que somente usuários selecionados em um grupo tenham permissões expandidas ou limitadas. Um exemplo segue a tabela.
Criar uma nova função	Crie uma nova função usando uma ou mais funções granulares da biblioteca para um cargo específico ou para atender a um requisito específico. Um exemplo segue a tabela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os nomes das funções granulares em Resposta a vulnerabilidades geralmente descrevem o que os usuários podem fazer e ver. Para exibir descrições de funções granulares específicas, navegue até **Todos** > **Administração de usuários** > **Funções** e localize a função desejada. A descrição da função, as funções que são herdadas automaticamente quando uma função é atribuída e todas as funções que dependem de outras funções também são listadas.

2. Para atribuir ou remover uma função granular de um usuário ou grupo, siga estas etapas.
   Por exemplo, suponha que você queira atribuir a um gerente de TI uma função que permita a esse gerente exibir registros, mas não atualizá-los ou editá-los. Para exibir registros em Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidadese para todas as integrações de terceiros, atribua a este usuário a função granular sn_vul.read_all.

   a. Navegar até **Todos** > **Administração de usuários** > **Usuários**.

   b. Localize o usuário e, na coluna Nome, clique no registro para abri-lo.
   O registro do usuário é exibido.

   c. Se não estiver selecionado, selecione a guia Funções.
   As funções atualmente atribuídas ao usuário são exibidas.

   d. Clique em **Editar**.
   O formulário Editar membros é exibido.

   e. No campo Coleção do slushbucket, insira o nome da função, se você souber, ou insira `*sn_vul` para exibir somente as funções granulares disponíveis para a Resposta a vulnerabilidades.

   f. Localize e mova sn_vul.read_all para a lista de funções.

   > **Nota:** Use o mesmo processo para remover funções granulares específicas de usuários no slushbucket movendo a função da lista Funções para a lista Coleção.

   g. Clique em **Salvar**.
   O registro do usuário é exibido com a nova função granular.

   h. Clique em **Atualizar** para salvar suas mudanças e retornar à lista Usuários.
   Você concedeu a um usuário permissão para ler, mas não atualizar registros em Resposta a vulnerabilidades, Performance Analytics para Resposta a vulnerabilidadese para integrações de terceiros.

3. Para editar um grupo para que somente membros específicos tenham acesso expandido com funções mais granulares, siga estas etapas.
   Por exemplo, suponha que você queira permitir que determinados usuários do grupo responsável pela correção (sn_vul.remediation_owner) criem itens vulneráveis manualmente, mas não queira expandir essa permissão para todos os usuários do grupo. A permissão para criar itens vulneráveis manualmente é concedida pela função granular sn_vul.create_vulnerable_items. Para conceder esta permissão somente para selecionar usuários deste grupo, siga estas etapas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Todos** > **Administração de usuários** > **Grupos**.

b. Localize o grupo responsável pela correção e, na coluna Nome, clique no grupo para abrir o registro.
O registro do grupo é exibido.

c. Se não estiver selecionado, selecione a guia Membros do grupo.
Os membros atuais do grupo são exibidos.

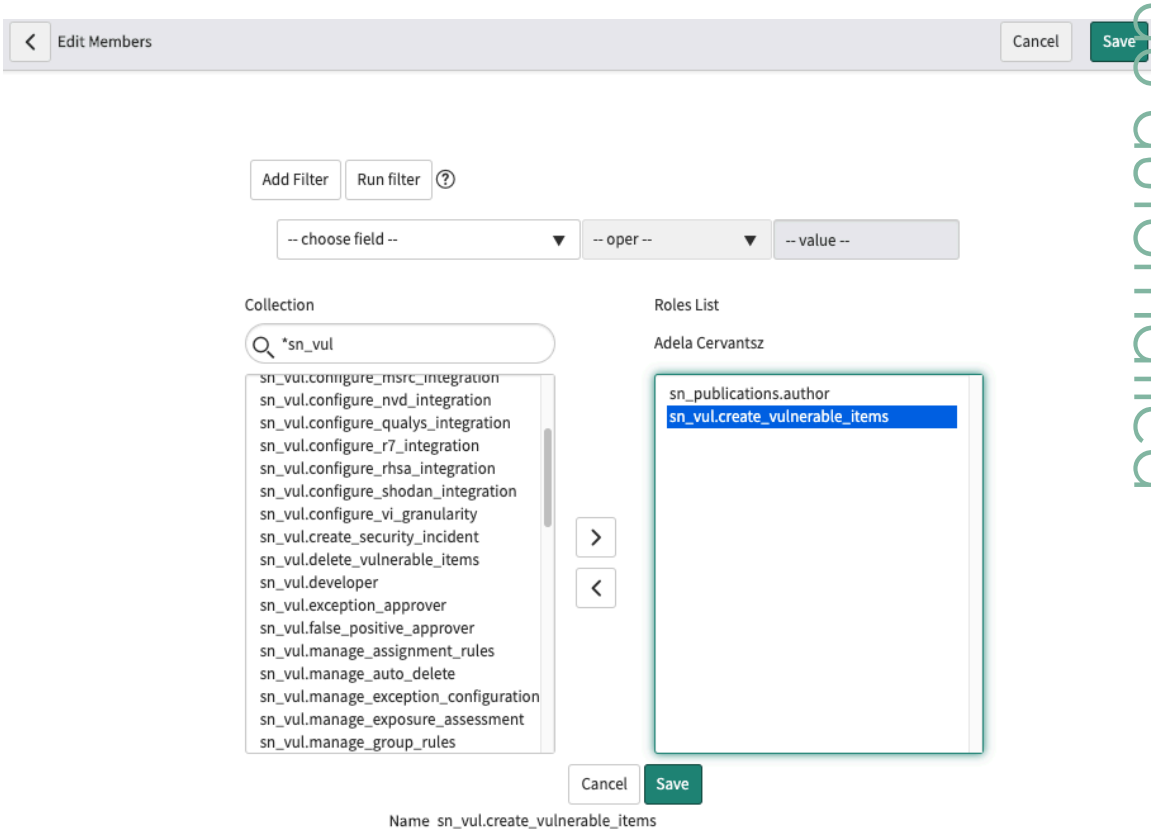
d. Clique em um nome na lista ao qual você deseja atribuir a função granular e abra o registro.

e. No registro, role até a guia Funções e selecione-a.
As funções atribuídas ao usuário são exibidas.

f. Clique em **Editar**.
O formulário Editar membros é exibido.

g. No campo Coleção, insira o nome da função, se você souber, ou insira `*sn_vul` para exibir todas as funções granulares disponíveis para a Resposta a vulnerabilidades.

h. Localize e mova sn_vul.create_vulnerable_items para a lista de funções.



i. Clique em **Salvar**.
O registro do usuário é exibido com a nova função granular.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

j. Clique na seta para voltar para exibir os usuários no registro do grupo de responsáveis pela correção

k. Clique nos nomes da lista aos quais você deseja atribuir esta função granular, abra seus registros e use o slushbucket para atribuir a função.

l. Depois de concluir as edições, clique em **Atualizar** para salvar as mudanças e retornar à lista de grupos.
Você concedeu a alguns usuários do grupo Proprietário de correção (sn_vul.remediation_owner) permissão para criar itens vulneráveis manualmente.

4. Para criar uma nova função usando somente as funções granulares selecionadas, siga estas etapas.
Para este exemplo, suponha que você queira criar uma função para um auditor de conformidade. Esta função funciona em conjunto com a Governança, risco e conformidade (GRC), e o trabalho requer as seguintes permissões e tarefas em Resposta a vulnerabilidades:

- Gerencia prazos de correção para itens vulneráveis e grupos de vulnerabilidades
- Aprova solicitações de exceção para estender prazos ou adiar correção
- Gerencia a limpeza de itens vulneráveis mais antigos com exclusão automática
- Definir pontuações de risco
- Lê todos os registros em Resposta a vulnerabilidades, mas não tem permissão para editá-los.

a. Navegar até **Todos** > **Administração de usuários** > **Funções**.

b. Na lista Funções, clique em **Novo**.

c. No registro Função, preencha os campos.

Crie um nome, selecione a aplicação que contém este registro e insira uma descrição resumida para sua nova função. Para obter mais informações sobre os outros campos do formulário, consulte Criação de uma função

Nota: Ao criar um nome para sua nova função, você pode preferir usar um nome que seja facilmente reconhecido na lista de funções e que descreva a funcionalidade da função. Para este exemplo, você pode preferir um título como Auditor de conformidade - GRC-VR.

d. Clique em **Enviar**.
A lista Funções é exibida.

e. Localize sua nova função e clique nela para abrir o registro.

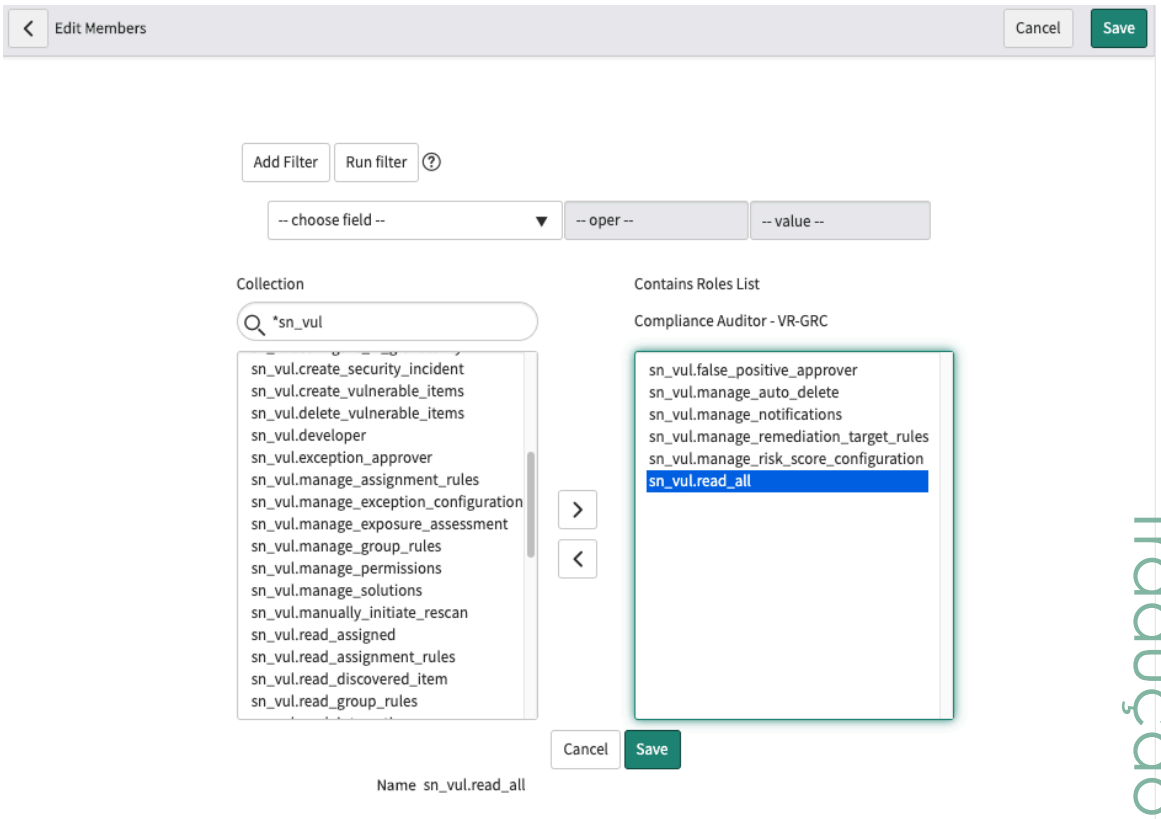
f. Clique em **Editar**.
O formulário Editar Membros é exibido.

g. Use o slushbucket para adicionar funções granulares à sua nova função.

Para este exemplo, as funções necessárias para esta nova função são exibidas na coluna direita na figura a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir somente as funções granulares da Resposta a vulnerabilidades, no campo Coleção, insira `*sn_vul`.



h. Clique em **Salvar**.
O registro da sua nova função é exibido. Começando com a guia Contém funções, continue editando a função conforme necessário.

i. Clique em **Atualizar** para salvar suas mudanças.
Sua nova função é exibida na lista Funções.

Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração

Instale as aplicações de integração de terceiros para as quais você tem direito em Resposta a vulnerabilidades usando o Assistente de configuração.

Antes de Iniciar

O Assistente de configuração oferece suporte à instalação da maioria das aplicações de integração de terceiros com Resposta a vulnerabilidades, mas você continua com a configuração de algumas aplicações instaladas a partir de módulos de configuração em sua instância. Consulte Integrações do Resposta a vulnerabilidades para obter uma lista de aplicações compatíveis com Resposta a vulnerabilidades.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Depois de instalado, o recurso [Solução de gestão de vulnerabilidade de Resposta a vulnerabilidades fornece acesso a Integração com a solução Microsoft Security Response Center e a Red Hat Solution Integration no Assistente de configuração.
- Solução de gestão de vulnerabilidade está disponível por assinatura separada. Consulte Solução de gestão de vulnerabilidade para obter mais informações sobre como Resposta a vulnerabilidades incorpora soluções.

Antes de instalar e ativar aplicações de terceiros no Assistente de configuração, execute as seguintes tarefas para garantir uma instalação sem problemas:

Tarefas de configuração	Descrição
Verifique se você tem direitos ServiceNow válidos para as aplicações de integração que deseja instalar.	Navegar até **Gestão de assinaturas** > **Assinaturas** em sua instância para verificar direitos. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre como obter direitos para uma aplicação Operações de segurança do ServiceNow Store, consulte .
(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros.	Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte Instalar e configurar a Resposta a vulnerabilidades.
Se ainda não estiver instalado e ativado, você deverá ativar e importar dados de vulnerabilidade com o trabalho agendado de integração do NVD e CWE antes de executar uma aplicação de scanner de terceiros para importar dados.	Execute as integrações de NVD e CWE como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.
Verifique se você concluiu todas as tarefas de configuração necessárias para as integrações de terceiros para Resposta a vulnerabilidades.	Revise todas as tarefas de configuração necessárias para cada integração que você deseja instalar em Integrações do Resposta a vulnerabilidades.

Função necessária: administrador

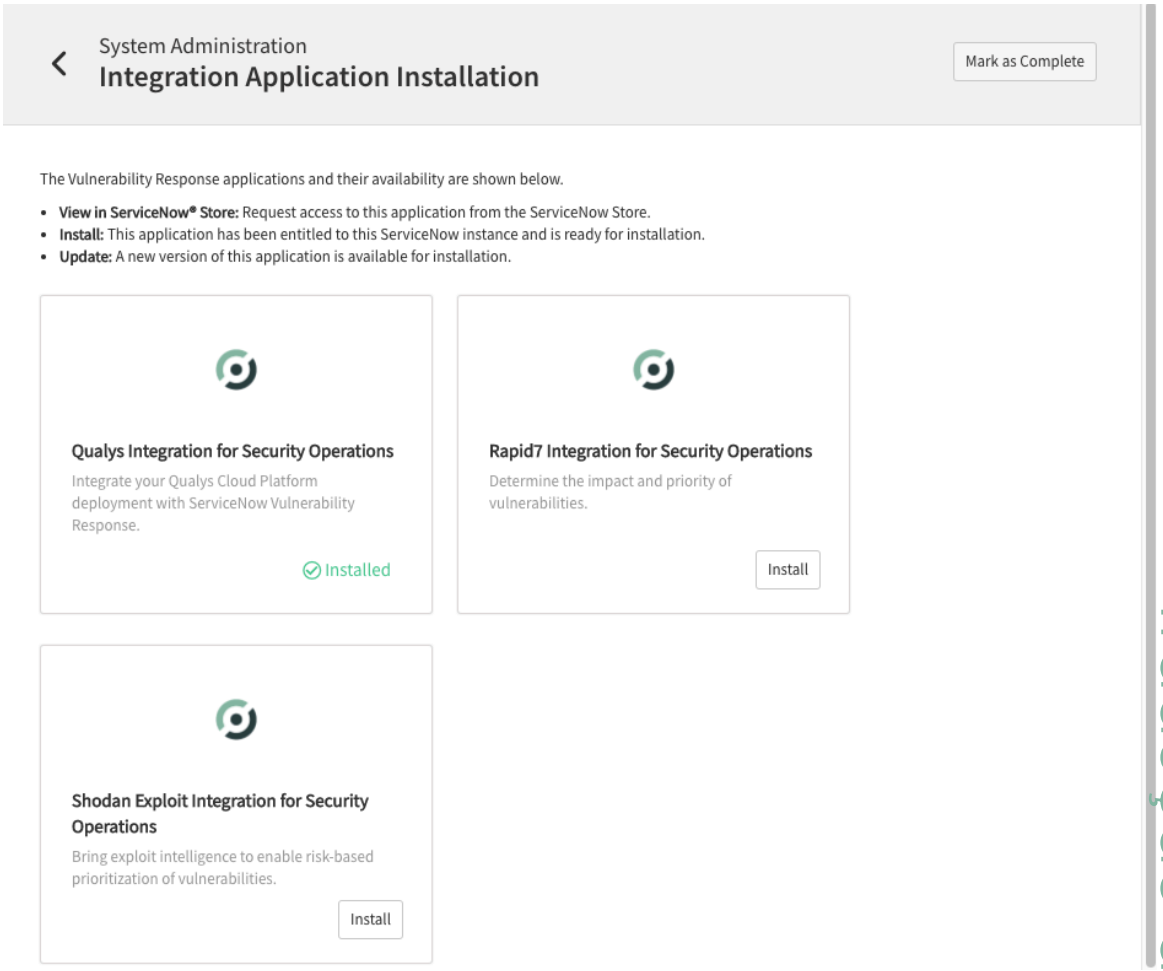
Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Administração do Sistema** > **Instalação de aplicação de integração**.

   Depois de alguns momentos, as aplicações para as quais você tem direito e que estão disponíveis para instalação em sua instância são exibidas.

Tradução automática

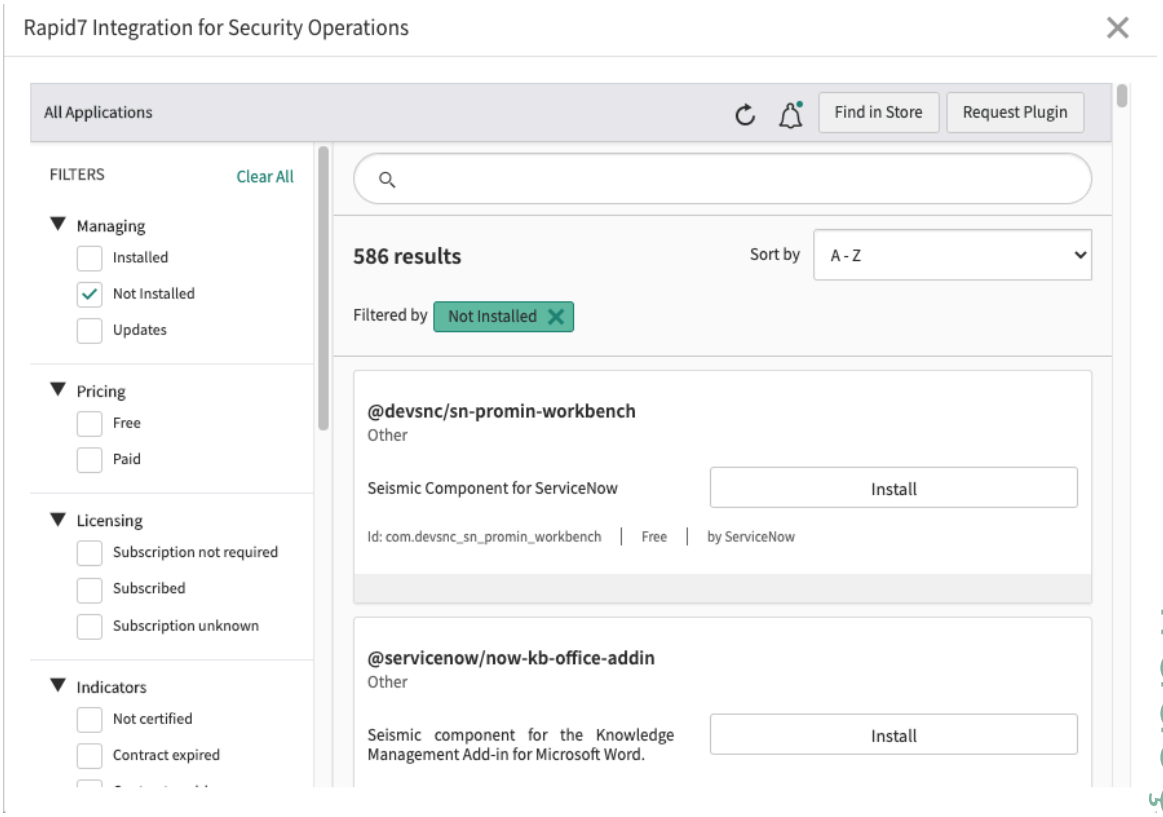
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Localize a aplicação que deseja instalar e clique em **Instalar** no bloco da aplicação. A caixa de diálogo Todas as aplicações é exibida com o nome do bloco da aplicação em que você clicou, por exemplo, Rapid7 Integration for Security Operations, conforme mostrado na figura a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

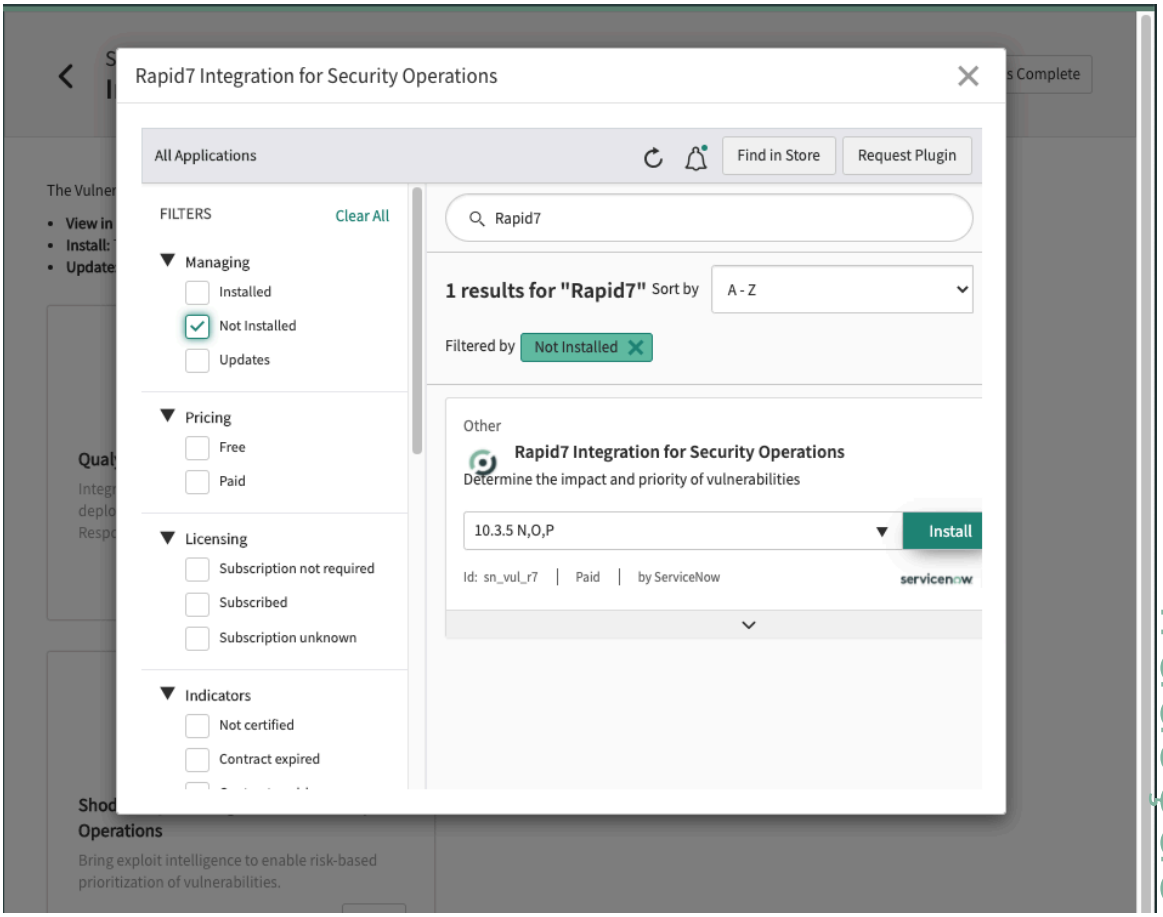


3. Localize a aplicação, selecione uma versão na lista de seleção e clique em **Instalar**.

Se uma atualização estiver disponível para a aplicação, o botão **Atualizar** será exibido.

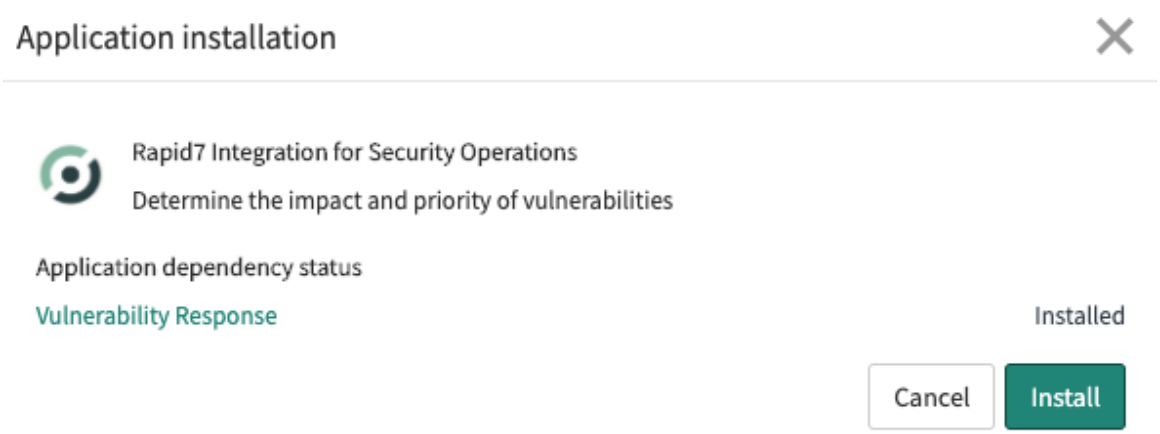
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo de instalação da aplicação exibe o status de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.

4. Na caixa de diálogo de instalação da aplicação, clique em **Instalar**.



A caixa de diálogo Instalar indica quando a instalação foi concluída com sucesso.

5. Feche a caixa de diálogo.
   A página Todas as aplicações é exibida, mostrando que sua aplicação foi instalada com sucesso.

Tradução automática

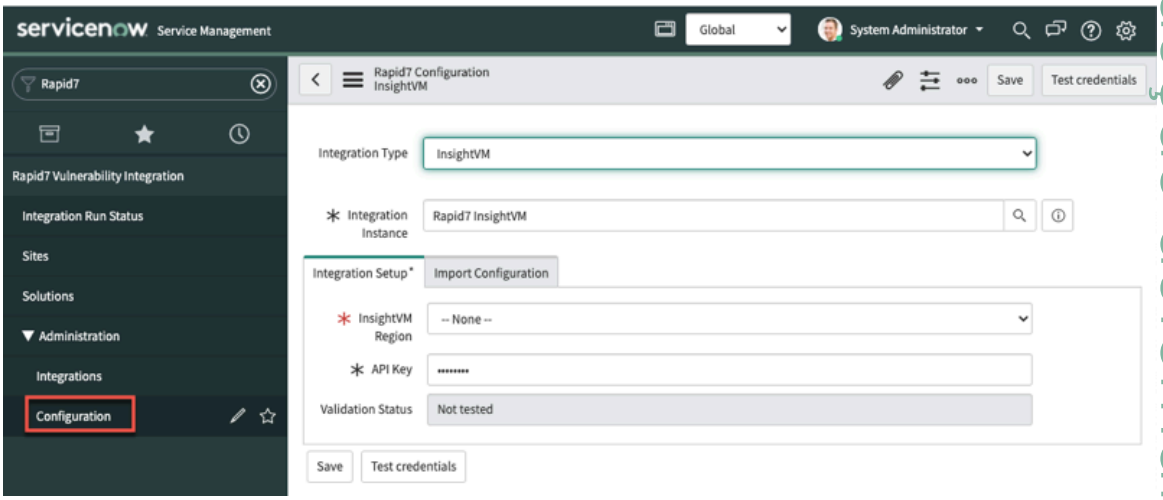
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a instalação e a ativação, você pode configurar, programar e iniciar as seguintes aplicações e soluções instaladas diretamente na seção Configuração de integração do Assistente de configuração:

- O Qualys Vulnerability Integration
- O Integração de Resposta a vulnerabilidades com Tenable.
- O Integração com a solução Microsoft Security Response Center
- O Red Hat Solution Integration
- Integração com a solução Microsoft Security Response Center
- A integração Gestão de ameaças e vulnerabilidades do Microsoft Defender

Para outras aplicações não listadas acima, navegue diretamente para o módulo de configuração da aplicação para continuar com a configuração e inserir as credenciais de terceiros necessárias. Por exemplo, a imagem a seguir mostra o local do módulo Configuração e para a aplicação Rapid7.

Para obter mais informações sobre como configurar aplicações específicas, consulte a documentação do produto de instalação e configuração pelo nome do produto fornecido para cada aplicação.



O que Fazer Depois

Continue com a configuração da sua aplicação no Assistente de configuração se a sua aplicação for compatível.

Se a sua aplicação não for compatível com a configuração no Assistente de configuração, navegue diretamente para o módulo de configuração da aplicação para continuar com a configuração. Para exibir as aplicações compatíveis no Assistente de configuração, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros

Se ainda não estiver instalado, baixe e execute a integração do NVD e execute o trabalho agendado do CWE como parte da configuração inicial da Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. A Integração de resposta a vulnerabilidades com NVD está disponível no ServiceNow Store.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ingestão de dados do CWE e do NVD

Os dados importados das integrações do NVD e do CWE são usados para aprimorar os dados de vulnerabilidade em sua instância e ajudar você a decidir se deve escalar a correção de uma vulnerabilidade, item vulnerável ou tarefa de correção. Após uma importação inicial, você pode atualizar os registros da biblioteca sob demanda ou configurar um trabalho agendado para atualizar os registros regularmente. Resposta a vulnerabilidades os armazena em **Bibliotecas**.

O Sistema de Pontuação de Vulnerabilidade Comum (CVSS), incluído no NVD e em entradas de terceiros, captura as principais características de uma vulnerabilidade. Resposta a vulnerabilidades usa dados do CVSS para produzir um valor normalizado que reflete a gravidade da vulnerabilidade. Quando a gravidade é calculada, a vulnerabilidade fornece uma melhor compreensão do risco representado por esta vulnerabilidade para sua organização. A gravidade ajuda a avaliar e priorizar a correção de vulnerabilidades.

Se esta for sua primeira instalação do Resposta a vulnerabilidadesou antes da ingestão de dados pela primeira vez com um produto de scanner de terceiros:

1. Execute uma importação inicial de dados do CWE com a Integração CWE Comprehense 2000.

   Para obter mais informações, consulte Configure e execute o trabalho agendado para atualizar registros de CWE. Por padrão, você executa atualizações de CWE **sob demanda** a partir do registro de integração e deve configurá-lo se quiser que ele seja executado como um trabalho agendado.

   > **Nota:** Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanal** na segunda- **feira**.

2. Verifique se a aplicação Resposta a vulnerabilidades Integration with NVD está instalada e se os dados da integração do banco de dados nacional de vulnerabilidades do NIST - API (somente CVE) ou da integração do banco de dados nacional de vulnerabilidades do NIST - API (CVE e CPE) foram importados com sucesso.

   A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Depois de instalada, a integração do NIST National Vulnerability Database Integration - API (somente CVE) é ativada por padrão. Ele é executado diariamente. Consulte Noções básicas sobre as integrações do NVD e Instalar a integração Resposta a vulnerabilidades com o banco de dados nacional de vulnerabilidades do NIST para obter mais informações.

3. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações do Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Exibição de dados de vulnerabilidade e itens vulneráveis importados

As seguintes bibliotecas estão disponíveis:

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, erros de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
	configuração, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de pontos fracos comuns, é apenas para referência.
Terceiro	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs.

Informações relacionadas

Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades

Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades

Antes de poder usar o recurso [Solução de gestão de Resposta a vulnerabilidades de Resposta a vulnerabilidades em sua instância, você deve concluir a instalação da aplicação Solução de gestão de vulnerabilidade. Esta aplicação está disponível como uma assinatura separada no ServiceNow Store.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Execute estas tarefas de configuração para uma instalação tranquila.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

O Integração com a solução Microsoft Security Response Center e o Red Hat Solution Integration são os aplicativos de solução disponíveis no Solução de gestão de Resposta a vulnerabilidades depois de instalar o Solução de gestão de vulnerabilidade.

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Solução de gestão de Resposta a vulnerabilidades requer a aplicação Resposta a vulnerabilidades. Para a versão mais atual de Solução de gestão de vulnerabilidade, verifique se você tem a versão mais atual de Resposta a vulnerabilidades instalada. Consulte KB0856498 Matriz de compatibilidade da Resposta a vulnerabilidades e mudanças no esquema da versão . Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem direito à aplicação.	Para verificar se você tem direito à aplicação Solução de gestão de vulnerabilidade, navegue até **Gestão**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	de assinaturas > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter o direito da aplicação Solução de gestão de vulnerabilidade do ServiceNow Store e baixá-lo na sua instância Now Platform, consulte .
Certifique-se de que seus registros do NVD estejam atualizados para os últimos 10 anos.	Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.
Certifique-se de que as vulnerabilidades de terceiros estejam atualizadas.	Consulte Integrações do Resposta a vulnerabilidades para obter informações sobre integrações de vulnerabilidade de terceiros.
Verifique se você tem as funções Now Platform necessárias atribuídas para sua instância.	As seguintes funções são necessárias para a instalação e verificação dos resultados esperados: Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades. • O administrador do sistema [admin] instala a aplicação. Se ainda não estiver atribuído, o administrador atribuirá a função de administrador de vulnerabilidades [sn_vul.vulnerability_admin or sn_vul.admin (obsoleto)]. • O administrador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Funções necessárias: administrador para instalar a aplicação Solução de gestão de vulnerabilidade e administrador de vulnerabilidade para configurá-la.

Procedimento

1. Navegue até o ServiceNow Store.

2. Clique **em Fazer login** e insira suas credenciais do HI.

3. Clique na guia **Produtos da ServiceNow** para exibir os produtos ServiceNow disponíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no sinal de mais (**+**) ao lado de **Gestão de soluções para vulnerabilidades** para exibir todas as aplicações associadas para as quais você está qualificado.
5. Clique **em Aceitar** para verificar se você tem direito a Solução de gestão de vulnerabilidade para a aplicação.
6. Se você já tiver um direito, pule para a etapa 10 para instalar a aplicação em sua instância Now Platform.
7. Marque a caixa de seleção e clique em **Aceitar** para concordar com os termos e condições no prompt.
   Uma mensagem é exibida indicando que você aceitou com sucesso a aplicação.
8. Opcional: Clique em Gerenciar direito se quiser gerenciar seu direito para Solução de gestão de vulnerabilidade em outras Now Platform instâncias.

   Nota: Se o botão **Gerenciar direito** não for exibido, clique na aplicação **Gestão de soluções de vulnerabilidade** na lista de produtos para exibi-lo.

   a. Escolha uma opção

   b. Clique em **OK** ou em **Cancelar** para continuar.
   Você está pronto para ativar plug-ins e instalar a aplicação em suas instâncias.

9. Faça login na instância Now Platform na qual você deseja instalar a aplicação Solução de gestão de vulnerabilidade.
10. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
11. Localize a aplicação Solução de gestão de vulnerabilidade (sn_vul_solution) e clique em **Instalar**.
    A caixa de diálogo de instalação da aplicação exibe o status do plug-in de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.
12. Clique em **Instalar**.
    Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.

    O administrador de vulnerabilidades agora pode configurar a aplicação de dentro do Assistente de configuração.

13. Clique em **Fechar**.

    O Integração com a solução Microsoft Security Response Center e o Red Hat Solution Integration são os aplicativos de solução disponíveis no Solução de gestão de Resposta a vulnerabilidades depois de instalar o Solução de gestão de vulnerabilidade.

    Exiba as Soluções de vulnerabilidade navegando até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções**. Para obter mais informações, consulte Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade usando o Assistente de configuração.

O que Fazer Depois

Depois de configurar a aplicação e as soluções disponíveis, verifique se os CVEs e as soluções concordam com o uso da tabela Solução de vulnerabilidade [sn_vul_m2m_vulnerability_solution].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades [PA]

Antes de poder usar a aplicação Performance Analytics para Resposta a vulnerabilidades, você deve obter o direito e baixar a aplicação do ServiceNow Store, instalá-la em sua instância Now Platform® e concluir algumas etapas de instalação e configuração. A aplicação PA não é instalada como parte da aplicação Resposta a vulnerabilidades. Ele está disponível com uma assinatura separada.

Antes de Iniciar

Se você já tiver a aplicação em sua instância e estiver atualizando para uma versão mais recente da aplicação, prossiga para a etapa 8 nas etapas a seguir para continuar com a atualização e a configuração.

Para uma nova instalação, conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Para verificar se os plug-ins e aplicações estão instalados e ativados, navegue até **Todos** > **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se o plug-in de dependências da Resposta a vulnerabilidades (com.snc.vul_dep) está instalado e ativado.	Dependências da Resposta a vulnerabilidades Este plug-in contém todos os plug-ins de dependência necessários para oferecer suporte à aplicação. Para verificar se o plug-in está instalado e ativado, em sua instância, você deseja que a aplicação navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**. Se você for solicitado a atualizar outros plug-ins de dependência, clique nos links das caixas de diálogo e siga as instruções para continuar.
Verifique se a aplicação ServiceNow Resposta a vulnerabilidades (sn_vul) está instalada e ativada.	Resposta a vulnerabilidades Para verificar se o plug-in está instalado e ativado, em sua instância, você deseja que a aplicação navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	Se você for solicitado a atualizar outros plug-ins de dependência, clique nos links das caixas de diálogo e siga as instruções para continuar. A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Entre em contato com a ServiceNow para obter mais detalhes.
Verifique se você tem as funções ServiceNow necessárias para sua instância. Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do Performance Analytics [pa_admin] ou o sistema [admin] instala a aplicação e verifica os resultados esperados. • O administrador de vulnerabilidade [sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)] supervisiona a configuração e verifica os resultados esperados com os painéis do PA. • O responsável pela correção [sn_vul.remediation_owner] supervisiona as tarefas de gestão de mudanças e lê e atualiza os registros atribuídos. A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a qualquer usuário.
Verifique se as aplicações Performance Analytics e Resposta a vulnerabilidades são compatíveis.	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

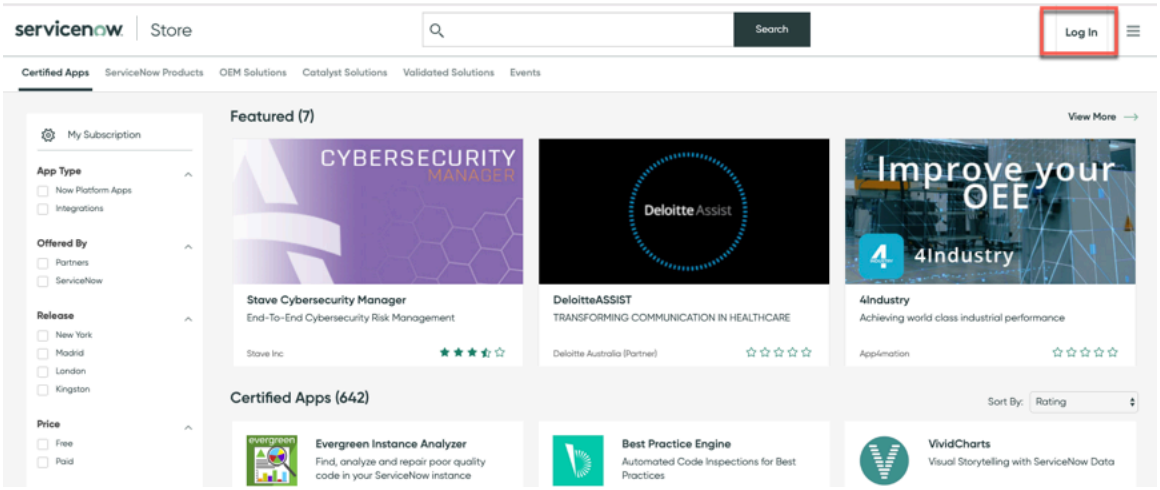
Função necessária: admin ou pa_admin

Procedimento

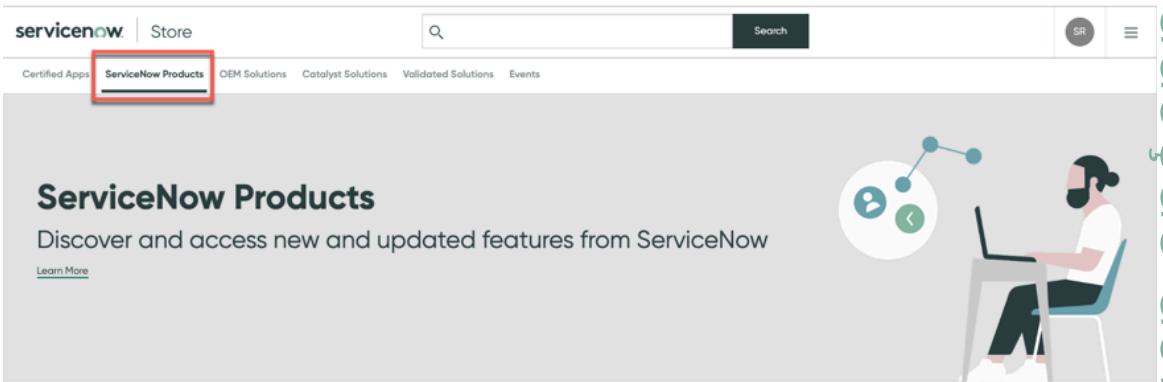
1. Para obter o direito e baixar a aplicação em sua instância Now Platform, navegue até ServiceNow Store.
2. No canto superior direito da página, clique **em Fazer login**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

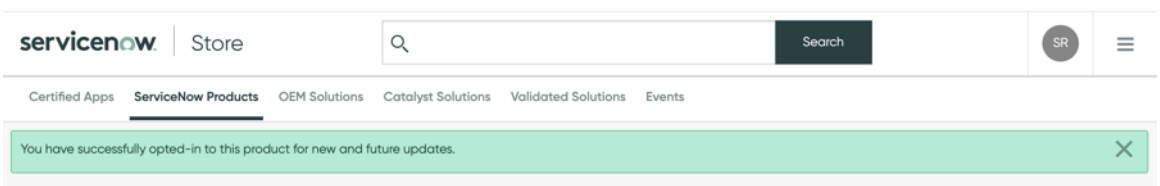


3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login**.
4. Na página exibida, se não estiver selecionado, clique na guia **Produtos da ServiceNow**.



5. Na página da lista de produtos, clique em **Análise de desempenho - Resposta a vulnerabilidades**.

6. Insira o **Nome** e **o motivo da instância**e clique em **Validar instância**.
   Uma página com o botão Aceitar será exibida.
7. Para obter a aplicação Performance Analytics para Resposta a vulnerabilidades, clique em **Aceitar**.
8. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.



Tradução automática

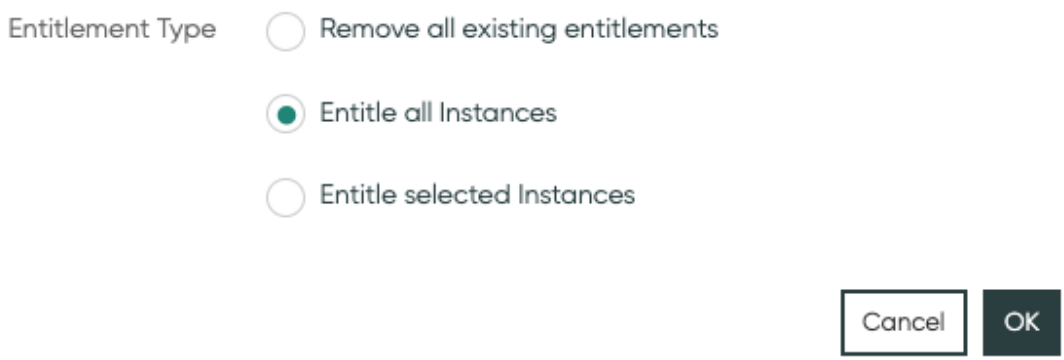
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Opcional: Como alternativa, para gerenciar seu direito da aplicação em outras Now Platform instâncias, siga estas etapas.

   a. Se o botão Gerenciar direito não for exibido, clique na aplicação Performance Analytics para Resposta a vulnerabilidades na lista de produtos para exibi-la.

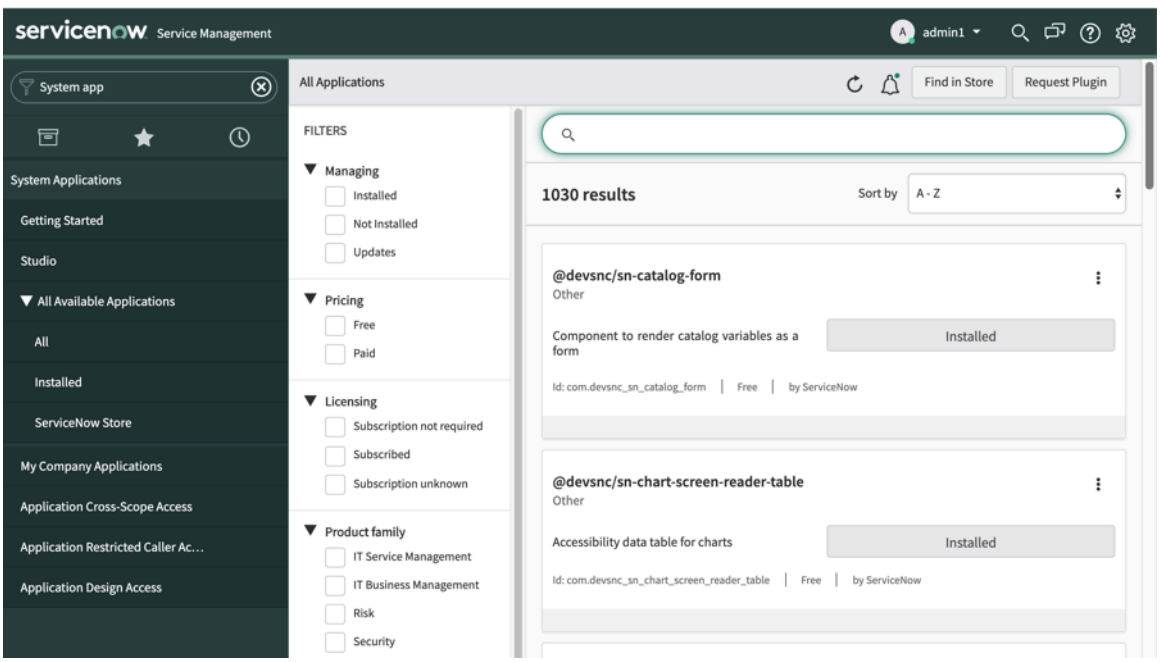
   b. Com a guia Qualificado selecionada, clique em **Gerenciar direito**.

   c. Na caixa de diálogo Gerenciar direitos para resposta a vulnerabilidades que é exibida, escolha uma:



   d. Clique em **OK** ou em **Cancelar** para continuar.
   Você está pronto para ativar plug-ins e instalar a aplicação em sua(s) Now Platform instância(s).

10. Faça login na instância Now Platform na qual você deseja instalar a aplicação Resposta a vulnerabilidades.
11. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

12. Nas aplicações listadas, localize a aplicação Performance Analytics - Pacote de conteúdo - Resposta a vulnerabilidades (sn_vul_analytics) e clique em **Instalar**.

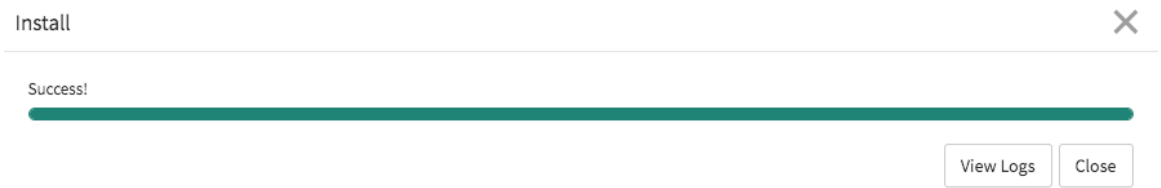
    Nota: Se você estiver atualizando para uma nova versão, selecione a versão desejada na lista de seleção.

    e clique em **Atualizar**.
    A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas automaticamente com a aplicação também são exibidas.

13. Opcional: Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar**.

    Nota: Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não estarão disponíveis para instalação posterior no **Gerenciador de aplicações**. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.

    Esta instalação pode levar algum tempo. Uma mensagem será exibida na caixa de diálogo Instalar depois que a aplicação for instalada com sucesso.



14. Clique em **Fechar**.

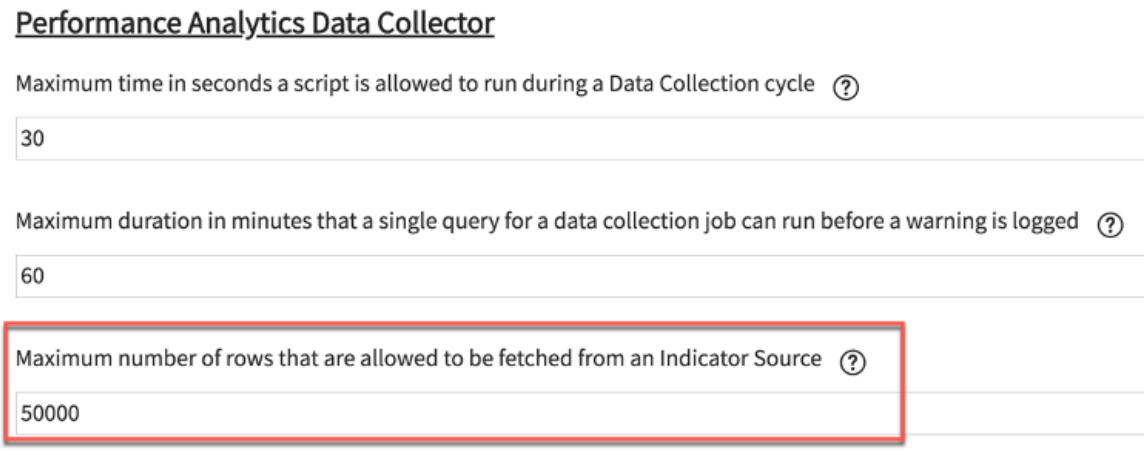
15. Opcional: Se você antecipar um grande número de itens vulneráveis ativos em seu ambiente, talvez prefira alterar a configuração padrão do número máximo de registros coletados, habilitar trabalhos agendados e definir horários de coleta fora do horário comercial.
    Para alterar essas e outras configurações da aplicação depois de instalada, siga estas etapas.

    a. Navegar até **Todos** > **Análise de desempenho** > **Console do administrador**.

    b. No bloco Configuração avançada, clique no link **Propriedades do Performance Analytics**.

    c. Na página do Console de administração [Performance Analytics], role até a seção Coletor de dados do Performance Analytics.
    A configuração padrão (50.000 registros) é exibida para o número máximo de linhas que podem ser obtidas de uma origem de indicador.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

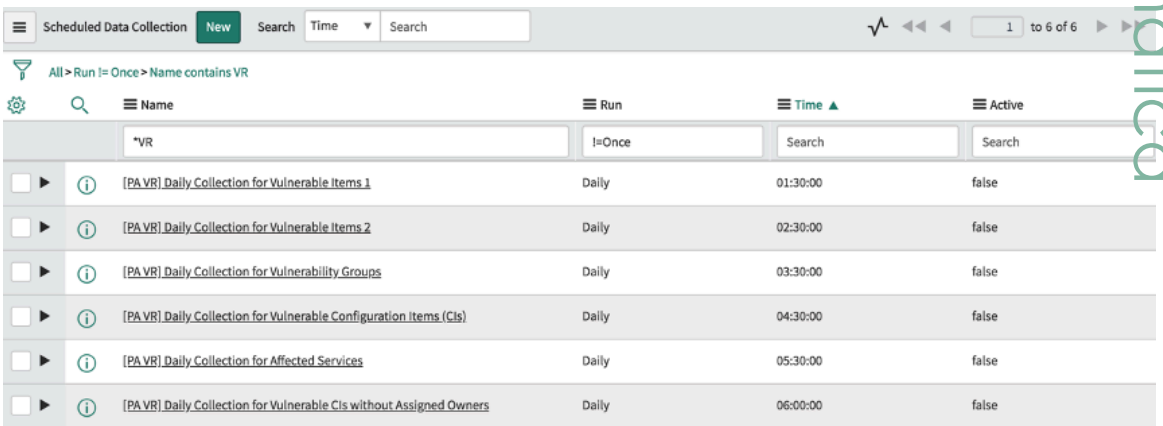


d. Você pode preferir aumentar esse número para um valor que seja aproximadamente 20% a mais do que o número total de itens vulneráveis (IVs) ativos que você antecipa em seu ambiente.

e. Clique em **Salvar**.

f. Para ativar trabalhos agendados, navegue até **Análise de desempenho** > **Coletor de dados** > **Trabalhos**.
A lista Coleta de dados programada é exibida. Na coluna Ativo, os trabalhos agendados listados na coluna Aplicação para Performance Analytics - Pacote de conteúdo - Resposta a vulnerabilidades por padrão estão desabilitados (`falso`).

> **Nota:** um trabalho agendado para coleta de dados históricos não é exibido na lista de trabalhos. Para grandes conjuntos de dados, você pode preferir começar a coletar dados e tendências ao longo do tempo, habilitando seus trabalhos diários ao configurar a aplicação Performance Analytics para Resposta a vulnerabilidades.



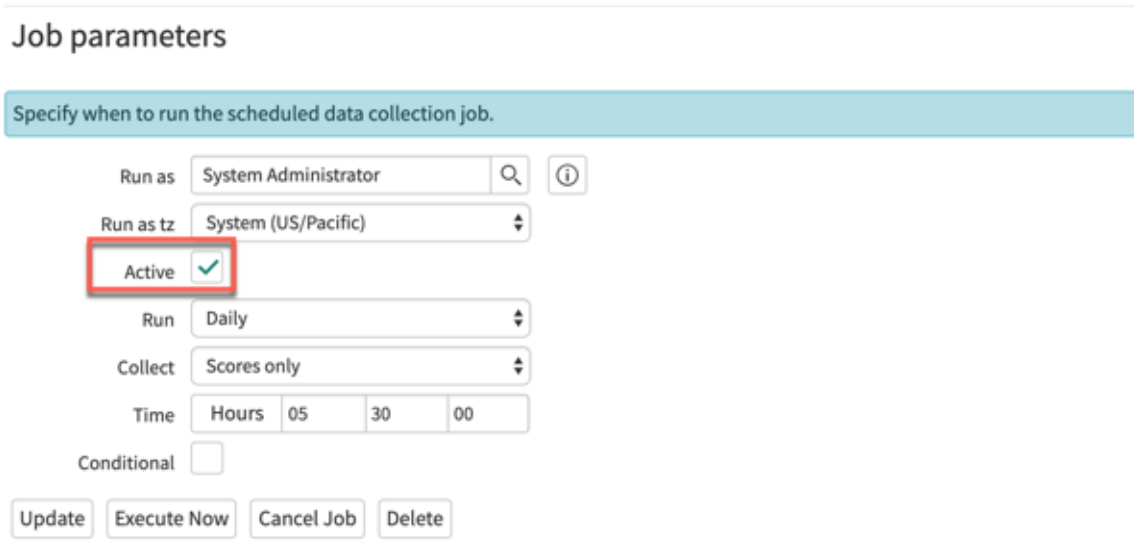
g. Na coluna Nome, clique em um link para abrir um registro de trabalho do PA_VR.

h. Se os campos não forem editáveis, clique no link **aqui** para editá-los.

i. Na seção Parâmetros de trabalho, clique na caixa de seleção Ativo para programar um trabalho.
Os campos de Tempo são exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



j. Insira a hora de início do trabalho.
Se você antecipar um grande volume, talvez prefira definir horários de coleta fora do horário comercial. Se você antecipar 10 milhões de IVs ativos ou mais em seu ambiente, entre em contato com seu parceiro de implementação ServiceNow® para obter mais informações sobre como configurar seu ambiente de coleta de dados.

Para obter mais informações sobre os indicadores usados para coleta de dados, consulte Exibir os indicadores [Performance Analytics para Resposta a vulnerabilidades [PA].

k. Depois de habilitar todos os trabalhos desejados, clique em **Atualizar**.
A lista Coleta de dados programada é exibida. Para obter mais informações, consulte Propriedades do Performance Analytics .

O que Fazer Depois
Navegar até **Resposta a vulnerabilidades** > **Visão geral** para exibir o painel.

Criar ou editar Resposta a vulnerabilidades regras de atribuição

Depois de concluir sua avaliação inicial de regras de atribuição usando o Assistente de configuração, você pode criar regras para atribuir automaticamente itens vulneráveis com base nas condições do filtro. Essas regras atribuem itens vulneráveis conforme eles são importados ou criados manualmente.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa
O sistema base é fornecido com uma regra de atribuição de vulnerabilidade, **Atribuir ao grupo de suporte de IC**, que atribui itens vulneráveis ao mesmo grupo de atribuição que o grupo de suporte de IC. Esta regra pode ser modificada usando condições de filtro ou você pode criar uma nova regra. Com regras de atribuição, você define as condições de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atribuição e a ordem de execução. Quando um VI corresponde a uma condição de regra, a pesquisa de atribuição é interrompida.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Abra a regra **Atribuir ao grupo de suporte de IC** ou clique em **Novo**.
3. Se for **Novo**, preencha os campos no formulário, conforme apropriado.

Regras de Atribuição da Vulnerabilidade

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se a regra de atribuição está ativa.
Ordem de execução	Ordem na qual as regras são avaliadas. Regras de alta prioridade, itens que precisam de tratamento especial, onde o risco é crítico ou um VI deve ser tratado pela conformidade regulatória, para ser executado primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é rnecessário, e você sabe quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir IVs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Descrição	Descrição da regra de atribuição.
Condição	
Visualização	Mostra quantos resultados esta consulta retornará.
Campos de condição	Condições que devem ser atendidas. **Nota:** Para disponibilizar Rapid7 InsightVM etiquetas do ativo para uso no filtro de condição para Regras de atribuição, você deve executar a integração da lista de ativos Rapid7 InsightVM antes das outras integrações Rapid7 InsightVM. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.
Novos critérios	Adiciona mais campos de filtro de condição para escolher.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ◦ Grupo de usuários: selecione um grupo de usuários na tabela de pesquisa. ◦ Campo de grupo de usuários: selecione um campo de grupo de usuários no menu suspenso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Script: crie ou edite um script. **Nota:** Criar ou editar um script requer ServiceNow conhecimento.

4. Clique em **Enviar**.
   Regras novas ou atualizadas são avaliadas na próxima importação.

Nota:

O recurso de reaplicação requer uma aplicação de linha de base das regras. Depois que suas regras forem criadas, se você ainda não tiver feito isso, ative o trabalho agendado *Reapply all vulnerability assignment rules* para executar, quando for mais conveniente. Aplica todas as regras a todos os VIs abertos, exceto aqueles atribuídos manualmente. Dependendo de quantos IVs ativos você tiver em seu ambiente, lembre-se de definir o campo **Executar** corretamente após a execução inicial para evitar impactos no desempenho.

Se você não executou este trabalho agendado, ao tentar usar o botão **Aplicar mudanças** no formulário Regras de atribuição, precisará fazê-lo. A reaplicação de regras de atribuição não reagrupa os itens vulneráveis.

Criar uma regra de atribuição Resposta a vulnerabilidades usando ML

Use o script a seguir para criar uma regra de atribuição de contato alternativo para itens vulneráveis que usa recomendações de ML da Inteligência preditiva para atribuí-los automaticamente para correção.

Antes de Iniciar

A aplicação Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades deve ser instalada e ativada. Esta aplicação está disponível no ServiceNow Store.

Uma solução de classificação deve ser definida, ativa e treinada. Você usa este modelo para ajudar a prever o grupo de atribuição apropriado para itens vulneráveis (VI) nos casos em que suas regras de atribuição não encontraram uma correspondência correta para os destinatários pretendidos.

Esta regra pode ajudar a reduzir o número de IVs não atribuídos depois que outras regras de atribuição já foram concluídas.

Para obter mais informações, consulte Instalar Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades e Criar e treinar uma definição de solução para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Talvez você prefira executar esta tarefa somente se tiver experiência avançada em codificação ou tiver conhecimento profundo sobre o Now Platform, seus recursos de Inteligência preditiva e como as regras de atribuição funcionam.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Selecione **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.
   Consulte Criar ou editar Resposta a vulnerabilidades regras de atribuição para obter mais informações sobre esses campos.
4. Na lista de seleção Atribuir usando, selecione **Script**.
5. No editor, copie e cole o script a seguir.

```
    /*
    * Catch-all assignment rule using ML recommendation
    * NOTE: Requires Vulnerability Assignment Recommendations for
 Vulnerability Response
    * Classification Solution must be active and trained
    */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
    var ARU = new sn_vul.AssignmentRecommendationUtils();
    ARU.initialize();

    var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
    /*
    *returns object containing array of predictions
    *payload structure:
    *
    {
        "predictions": [
            {
                "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
                "name": "Windows Server support ",
                "confidence_score": "57.54"
            },
            ...
        ],
        "exception": ""
    }
    */
    var viPredictionArray = viPredictionObj['predictions'];
    var topPredictionObj = viPredictionArray.shift();

    return topPredictionObj['sys_id'];
}
```

6. Selecione **Enviar**.

O que Fazer Depois

Revise Resposta a vulnerabilidades visão geral das regras de atribuição para obter informações mais gerais sobre regras de atribuição e o trabalho agendado *Reapply all vulnerability assignment rules*.

Criar uma regra de atribuição Resposta a vulnerabilidades para suporte de serviço

Use o script a seguir para criar uma regra que atribui itens vulneráveis para correção com base nos serviços de negócio que eles afetam.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode preferir executar esta tarefa somente se tiver experiência avançada em codificação ou tiver conhecimento profundo sobre o Now Platform e como as regras de atribuição funcionam.

Com esta regra, os IVs são atribuídos de acordo com o quanto correspondem aos serviços de negócio listados no seu CMDB. Se nenhum serviço, departamento ou grupo de suporte relacionado for correspondido, os IVs serão atribuídos ao grupo de analistas de vulnerabilidade.

Esta regra pode ajudar a reduzir o número de IVs atribuídos incorretamente ou que permanecem não atribuídos após a conclusão de outras regras de atribuição.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de atribuição**.
2. Selecione **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.
   Consulte Criar ou editar Resposta a vulnerabilidades regras de atribuição para obter mais informações sobre esses campos.
4. Na lista de seleção Atribuir usando, selecione **Script**.
5. No editor, copie e cole o script a seguir.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business
 Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
    var ci = vitGR.getValue('cmdb_ci');
    var defaultAssignmentGroup = 'Vulnerability Analyst';
    var defaultGR = new GlideRecord('sys_user_group');
    defaultGR.get('name', defaultAssignmentGroup);
    var defaultAssignmentGroupID = defaultGR.sys_id;

    var maxSizeValue =
 global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max
_size", 1000);
    var maxDepthValue =
 global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max
_depth", 10);
    var customValues = {
        "maxDepth": maxDepthValue,
        "maxSize": maxSizeValue
    };
    var ciu = new global.CIUtils();
    var services = ciu.servicesAffectedByCI(ci, customValues);
    var svc = new GlideRecord("cmdb_ci_service");
    var hasSvc = false;
    if (services && services.length > 0) {
        svc.addQuery("sys_id", "IN", services.join(",")); // returns
 the service with highest business criticality. Implement alternate
 logic here.
        svc.addNotNullQuery("busines_criticality"); // typo intended
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
        svc.orderBy("busines_criticality");
        svc.setLimit(1);
        svc.query();
        hasSvc = svc.next();
    }
    if (!hasSvc) {
        // If there are no services it should be assigned to a default
 assignent group
        return defaultAssignmentGroupID;
    } else {
        var serviceAssignmentGroup =
 hasSvc.getValue('support_group'); //Also consider managed_by_group,
 assignment_group, change_control
        return !gs.nil(serviceAssignmentGroup) ?
 serviceAssignmentGroup : defaultAssignmentGroupID; //Return the
 Service assignment group if it is not empty, return the default
 assignment group otherwise.
    }
}
```

6. Selecione **Enviar**.

O que Fazer Depois

Revise Resposta a vulnerabilidades visão geral das regras de atribuição para obter informações mais gerais sobre regras de atribuição e o trabalho agendado *`Reapply all vulnerability assignment rules`*.

Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção

Depois de concluir a avaliação inicial das regras de tarefa de correção usando o Assistente de configuração, você pode criar regras para agrupar automaticamente os itens vulneráveis com base nas condições do filtro. Essas regras agrupam automaticamente os itens vulneráveis à medida que são importados ou criados manualmente. Use o filtro para limitar os itens vulneráveis agrupados por esta regra, como selecionar todos os itens vulneráveis com explorações.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

O sistema base é fornecido com uma regra de tarefa de correção, **Vulnerabilidade**, que agrupa itens vulneráveis por vulnerabilidade e grupo de atribuição (de **Regras**de atribuição). Você pode reaplicar as regras do formulário ou da exibição de lista. Para algumas entradas de exemplo, Resposta a vulnerabilidades exemplos de regra de tarefa de correção.

Esta regra pode ser modificada da seguinte forma:

Usando condições de filtro e opções de Agrupar por.

Por padrão, as tarefas de correção usam **Regras de atribuição**, quando disponíveis, como parte dos critérios de filtro.

Nota: Se não houver regras de atribuição, você poderá selecionar um grupo usando o campo Grupo de **usuários**.

A partir da versão 18.0 de Resposta a vulnerabilidades, a regra da tarefa de correção de **vulnerabilidade** é desativada em Resposta a vulnerabilidades para novas implementações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de tarefa de correção**.
2. Abra a regra ou clique em **Novo**.
3. Se for **Novo**, preencha os campos no formulário, conforme apropriado.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra de tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condição	Condições de filtro opcionais para a regra. **Nota:** Para disponibilizar Rapid7 InsightVM etiquetas do ativo para uso no filtro de condição das Regras da tarefa de correção, você deve executar a integração da lista de ativos Rapid7 InsightVM antes das outras integrações Rapid7 InsightVM. Por padrão, (caixa de seleção que**diferencia maiúsculas de minúsculas** desabilitada), o texto de pesquisa que você insere no construtor de condições em registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefas.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis de	A tabela que a regra usa para agrupar IVs. Você pode ter até seis filtros. As opções são: ◦ Item vulnerável [sn_vul_vulnerable_item] ◦ Item vulnerável → Item de configuração [cmdb_ci] ◦ Item vulnerável → Vulnerabilidade [sn_vul_ third_party_entry] **Nota:** Se você escolher uma tabela estendida, o **campo Usando** será aplicado somente para itens vulneráveis que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar IVs.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir automaticamente tarefas de correção, a opção Atribuição é usada além das opções **Agrupar por** para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para garantir que cada

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	item vulnerável seja colocado em uma tarefa com um conjunto de grupo de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ◦ Agrupar por campo: se você selecionou qualquer campo de grupo de usuários nos valores de **campo Usando** na seção **Agrupar por**, eles serão exibidos no menu suspenso. ◦ Grupo de usuários: use a lista de pesquisa para selecionar um grupo de usuários estático.

Nota: Se você mudar de ideia sobre qualquer uma das configurações **de Agrupar por**, o link relacionado **Limpar agrupar por campos** redefinirá os campos **Agrupar por** no formulário.

Quando uma regra de grupo é excluída, no formulário ou na exibição de lista, você tem a opção de excluir todos os grupos **Abertos** criados por essa regra. Grupos que não estão no estado **Aberto** são excluídos.

Para algumas entradas de exemplo, consulte Resposta a vulnerabilidades exemplos de regra de tarefa de correção.

Definir campos e pesos para a regra de risco das Calculadoras de risco da Resposta a vulnerabilidades

Personalize os parâmetros e pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de vulnerabilidade e ativo exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Além disso, você pode usar atributos no configuration_item [cmdb_ci] no Configuration Management Database (CMDB) para ajudá-lo a criar lógica para suas calculadoras de risco da Resposta a vulnerabilidades. Se, por exemplo, você determinar que os ICs externos em sua organização são mais vulneráveis e podem precisar de correção imediata, você pode atribuir atributos como *Internet Facing* para esses ICs. Este atributo e outros estão listados nas notas de versão do Common Service Data Model para a versão da família Orlando. Para obter informações e orientações atuais sobre o CMDB, consulte os seguintes tópicos:

- Modelo conceitual do Common Service Data Model
- Modelo de esquema do CMDB

Função necessária: sn_vul.manage_risk_score_configuration

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Na página Calculadoras de vulnerabilidade, selecione **Calculadora de risco padrão**.
3. Navegar até **Página da Calculadora de vulnerabilidade** > **Guia Regras da calculadora de vulnerabilidade** > **Regra de Risco Padrão**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Opcional: Na seção Critérios da calculadora de risco da página Regra de risco de vulnerabilidade, defina o peso de cada critério de acordo com sua importância no cálculo de pontuação de risco geral.
5. Para desativar a regra, você deve desmarcar a caixa de seleção **Ativo**.
6. Para adicionar campos de regra de risco aos critérios da calculadora de risco, selecione **Adicionar critérios**.
7. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	Tabela que você usa para definir o peso da pontuação de risco. Você pode selecionar uma destas opções: ◦ **Item vulnerável**: adicione campos que são diretamente referência com pontos do item vulnerável (VI). ◦ **Item vulnerável - Item de configuração**: adicione campos de referência com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela base (cmdb_ci). ◦ **Item vulnerável - Vulnerabilidade**: adicione campos de referência com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, Entrada de terceiro. Esses campos não fazem parte da tabela base de entrada de vulnerabilidade. ◦ **Tabela de referência de item vulnerável**: adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao item vulnerável. Esses campos não são passíveis de referência com pontos diretamente do IV. ◦ **Tabela de referência de item de configuração**: adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não são passíveis de referência com pontos diretamente do IV. ◦ **Tabela de referência de vulnerabilidade**: adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vul_entry ou tabelas que têm uma referência a sn_vul_entry. Esses campos não são passíveis de referência com pontos diretamente do IV.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Condições personalizadas**: use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Tabela	Campo que aparece somente quando uma das seguintes opções é selecionada na tabela Escolher referência: ◦ **Item vulnerável -> Item de configuração** ◦ **Item vulnerável -> Vulnerabilidade** ◦ **Tabela de referência do item vulnerável** ◦ **Tabela de referência do item de configuração** ◦ **Tabela de referência de vulnerabilidade**
Campo	Campo a ser usado para cálculo de pontuação de risco para esta regra.
Agregação	Campo que aparece somente quando uma tabela de referência é selecionada em Escolher tabela de referência. Selecione o valor mínimo ou máximo a ser considerado para cálculos quando Campo for selecionado nas Tabelas relacionadas (m2m).
Ponderação	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Definir ponderação de valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, os valores de campo podem ser definidos como um intervalo (por exemplo, 1–5). Os pesos devem ser um número inteiro entre 0 e 100. **Nota:** Este campo não aparecerá se a opção Condições personalizadas for selecionada na tabela Escolher referência.
Tabela de condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Selecione uma condição na lista.
Nome do campo	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	referência. Insira um nome para os critérios de risco.
Condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Visualize os itens nesta tabela que correspondem às condições definidas.

8. Selecione **Enviar**.
9. Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco nos itens vulneráveis ativos.

Nota: A partir da versão 23.0 de Resposta a vulnerabilidades, no caso de:

- Regra da**calculadora de risco padrão** : sempre que a pontuação de risco em um item vulnerável (VIT) muda, os seguintes detalhes são documentados na seção Anotações do VIT:
  - Nome do grupo de calculadoras
  - Nome da calculadora
  - Valores de campo que têm um peso maior que 1 e sua contribuição de pontuação de risco.
  - Pontuação de risco final
- Regra de risco de**gravidade de vulnerabilidade** : sempre que a pontuação de risco é atualizada em um VIT, a seção **Anotações** é atualizada com os seguintes detalhes:
  - Nome do grupo de calculadoras
  - Nome da calculadora: dependendo se a regra da calculadora é baseada em um modelo ou em um script, o nome é acrescentado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e marque a caixa de seleção **Exibição avançada**. Na caixa suspensa **Tipo de valor**, selecione a opção necessária. Se o **modelo** for selecionado, a pontuação de risco será atualizada de acordo com a condição especificada na regra. Se **Script** estiver selecionado, você poderá adicionar ou atualizar o script existente.

Example:
Exemplo 1: adicione uma gravidade de origem como critério para uma regra de risco.

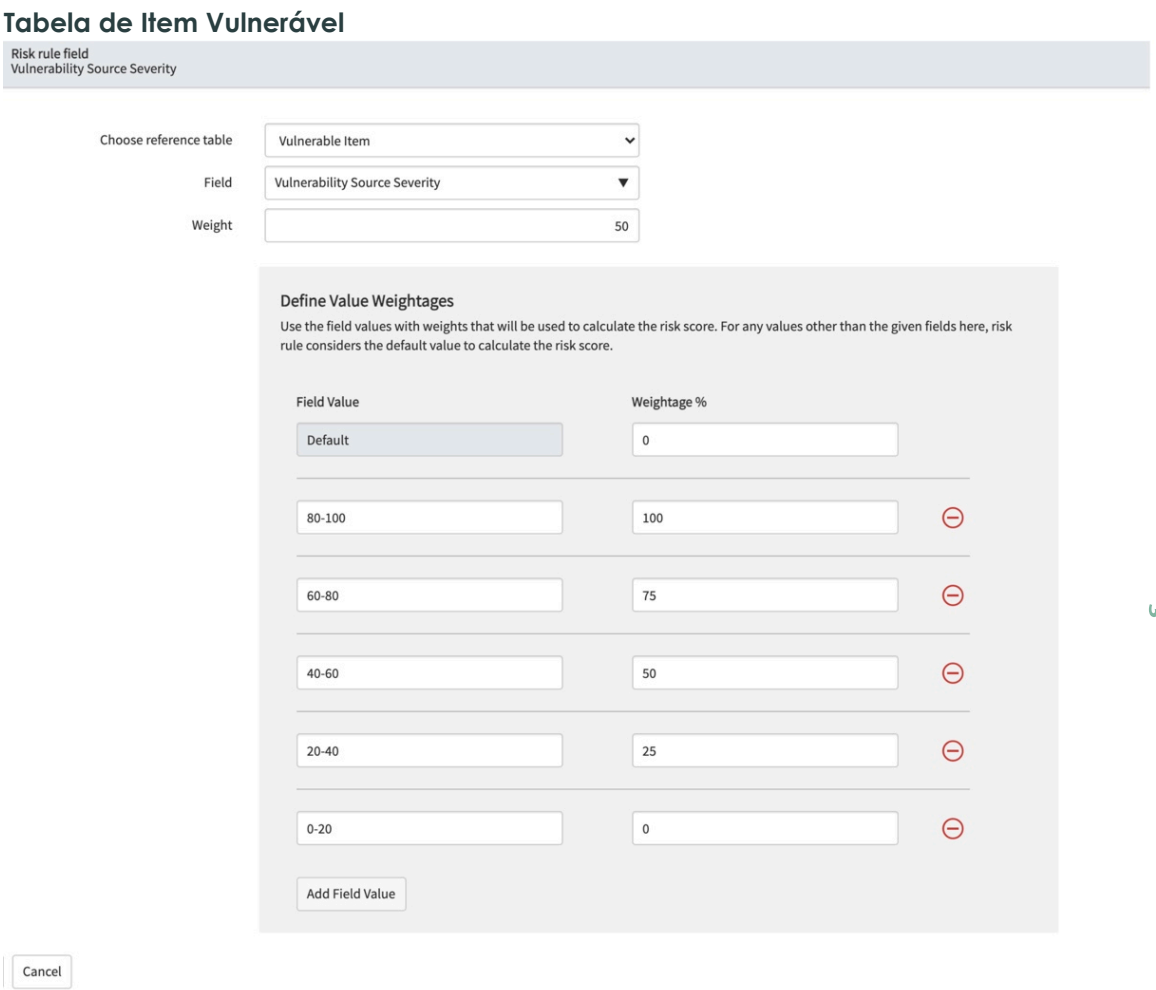
Caso de uso: fornecedores de terceiros, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo **Gravidade de origem** na tabela sn_vul_entry. Use este campo para cálculos de pontuação de risco. Para usar esta pontuação para calcular a pontuação de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos critérios da calculadora de risco, selecione **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione **Item vulnerável**.
5. Na lista Campo, selecione **Vulnerability.Source Severity**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
7. Na seção Definir ponderação de valor, adicione valores de campo e atribua um peso a eles.



8. Selecione **Enviar**.

Exemplo 2: adicione uma criticalidade de negócio como critério para uma regra de risco.

Caso de uso: suponha que sua organização tenha muitos serviços de negócio. O item de configuração (IC) LINUX-SF-6381 está sendo usado pelos seguintes serviços:

Criticidade dos serviços de negócio

Serviço de negócio	Criticidade
Gestão de nuvem	1 - Mais crítico
Comércio eletrônico	2 - Um pouco crítico
Serviços de cliente	3 - Menos crítico
Viagem e despesa	4 - Não crítico

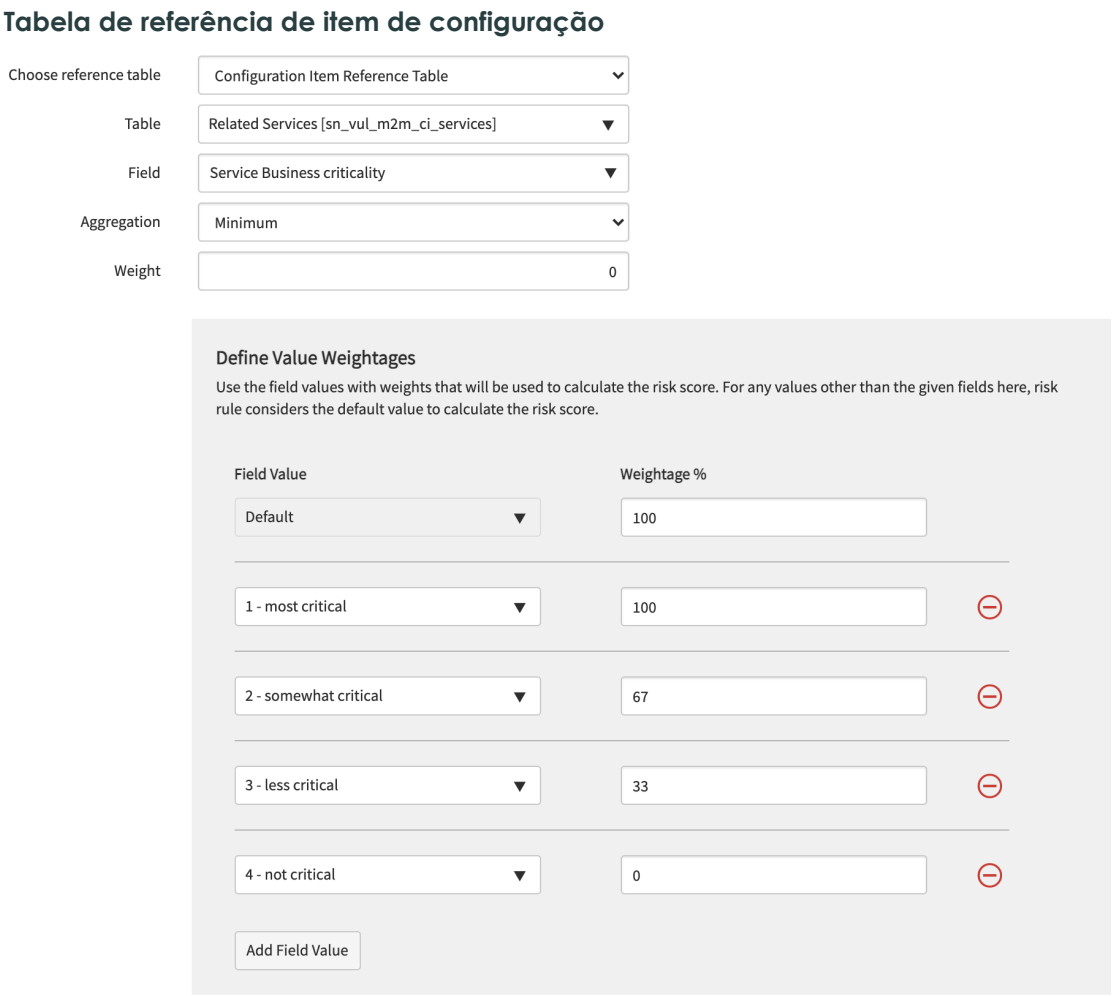
O mapeamento entre o IC e os serviços é armazenado na tabela Serviços relacionados [sn_vul_m2m_ci_services]. Quando uma vulnerabilidade é encontrada no ativo LINUX-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SF-6381, um item vulnerável (VI) é criado. Você pode usar o valor da criticalidade dos serviços afetados para calcular a pontuação de risco para este VI. Para usar o valor de criticalidade desses serviços para calcular a pontuação de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos critérios da calculadora de risco, selecione **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione **Tabela de referência do item de configuração**.
5. Na lista Tabela, selecione **Serviços relacionados [sn_vul_m2m_ci_services]**.
6. Na lista Campo, selecione **Serviço.Criticalidade**dos negócios .
7. No campo **Agregação**, selecione **Mínimo** para recuperar o serviço mais crítico deste caso de uso (**1 – Valor mais crítico**) ou Máximo para recuperar o serviço menos crítico deste caso de uso (**4 – Valor não crítico**) para este caso de uso.
8. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
9. Na seção Definir ponderações de valor, adicione valores de campo e atribua um peso a eles.



10. Selecione **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo 3: adicione um critério condicional à calculadora de risco.

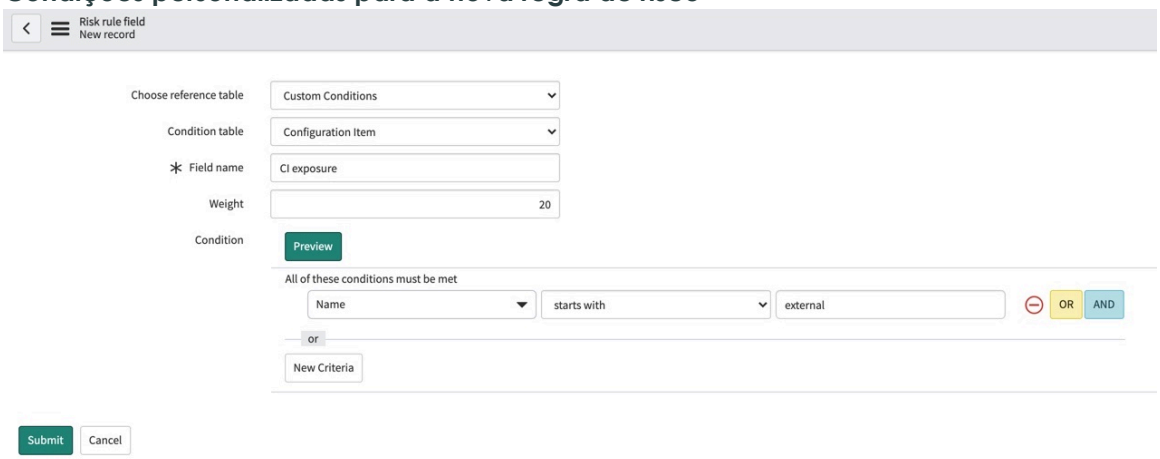
Vamos supor que uma organização tenha vários itens de configuração (ICs), dos quais apenas alguns podem ser acessados por um usuário externo. Os usuários podem adicionar ponderações de pontuação de risco para esses ICs externos.

Nota: Você pode identificar esses ICs pelo nome. Os nomes começam com "externo".

Para adicionar um critério condicional à regra de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos critérios da calculadora de risco, selecione **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione **Condições personalizadas**.
5. Na lista Tabela de condições, selecione **Item de configuração**.
6. No **campo Nome** do campo, insira o nome **Exposição de IC**.
7. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
8. No campo **Condição**, selecione **Nome** > **começa com** e insira o valor **externo**.

Condições personalizadas para a nova regra de risco



9. Selecione **Enviar**.

Nota: Adicionar critérios condicionais à regra de risco pode prejudicar o desempenho.

Informações relacionadas

- Calculadoras da Resposta a vulnerabilidades e regras da calculadora de vulnerabilidade
- Criar uma calculadora da Resposta a vulnerabilidades
- Filtrando na Resposta a vulnerabilidades

Resposta a vulnerabilidades Calculadoras de Acúmulo

Após a avaliação inicial das calculadoras de risco no Assistente de configuração, use as calculadoras de acúmulo de vulnerabilidades para configurar como a pontuação de risco cumulativo é calculada para tarefas de correção e vulnerabilidades importadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use as calculadoras de acúmulo de vulnerabilidades para configurar como a pontuação de risco cumulativo é calculada para tarefas de correção e vulnerabilidades importadas. As seguintes calculadoras de rollup são enviadas com o sistema de base:

- *Remediation Task Rollup*: acumula as pontuações de risco de todos os itens vulneráveis em tarefas de correção para fornecer uma pontuação de risco geral para todo o grupo de itens vulneráveis.
- *Patch Update Rollup*: acumula as pontuações de risco de todos os itens vulneráveis com a mesma atualização de patch para fornecer uma pontuação de risco geral para a atualização do patch.
- *Organization Risk Score Rollup*: acumula as pontuações de risco de todos os itens vulneráveis de host, itens vulneráveis de aplicação, itens vulneráveis de contêiner e problemas de configuração em uma organização para fornecer uma pontuação de risco geral para toda a organização no painel unificado.

  Nota: A partir da v22.0 de Resposta a vulnerabilidades, você pode configurar pesos de acúmulo para pontuação organizacional. Além disso, as calculadoras de acúmulo individuais foram removidas.

- *Vulnerable Item Rollup*: acumula as pontuações de risco de todos os itens vulneráveis de host em uma organização para contribuir com a pontuação de risco geral de toda a organização para o painel unificado.
- *Vulnerability Entry Rollup*: acumula as pontuações de risco de todos os itens vulneráveis com a mesma entrada de vulnerabilidade para fornecer uma pontuação de risco geral para a entrada de vulnerabilidade.
- *Rollup EPSS Scores from NVD to TPEs*: acumula as pontuações de EPSS de todos os itens vulneráveis/CVEs listados na tabela do NVD] para os TPEs existentes, para fornecer uma probabilidade geral da vulnerabilidade que está sendo explorada.
- *Remediation Effort Rollup*: acumula as pontuações de risco de todos os registros em um esforço de correção para fornecer uma pontuação de risco geral para o esforço de correção.

Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Calculadora de Rollup de Vulnerabilidade**.

Configure a calculadora de acúmulo para especificar quanto peso deve ser atribuído a cada um desses valores calculados na definição da pontuação de risco cumulativo. Quanto maior o peso, mais esse valor será usado para determinar a pontuação de risco acumulada nas tarefas de vulnerabilidade ou correção.

Nota: Quando **Incluir adiado** é selecionado, todos os itens vulneráveis adiados são incluídos no cálculo de acúmulo para as tarefas de correção. Certifique-se de entender o impacto no cálculo total antes de selecionar esta opção.

As calculadoras de acúmulo executam o trabalho agendado, *Rollup vulnerable item values to vulnerability and groups*, a cada 15 minutos para selecionar mudanças e acumular os detalhes e as pontuações de risco para tarefas de correção e vulnerabilidades. Esses trabalhos agendados também calculam valores cumulativos para o número de IVs, pontuação de risco máximo, data de meta de correção e status das tarefas de correção.

Nota: Os valores calculados para entradas de vulnerabilidade não incluem dados de meta de correção.

A pontuação de risco é calculada quando:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A pontuação de risco, a meta de correção, o status de correção ou as mudanças de vulnerabilidade nos itens vulneráveis.
- O estado do item vulnerável muda para Aberto, Adiado, Encerrado ou muda de Encerrado ou Adiado.
- Itens vulneráveis são excluídos.
- Itens vulneráveis são adicionados ou removidos da tarefa de correção.

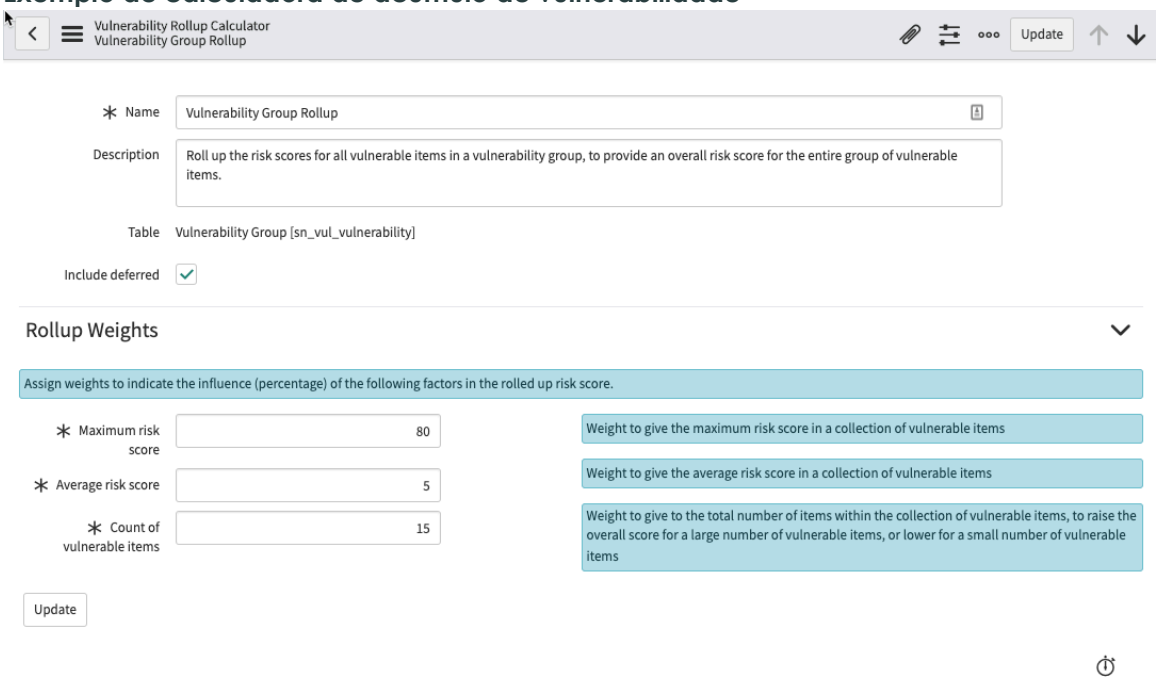
Exemplo de calculadora de acúmulo de vulnerabilidade: considere uma tarefa de correção VUL324567, que tem os seguintes itens vulneráveis:

- VIT1001 com pontuação de risco de 30
- VIT1002 com pontuação de risco de 40
- VIT1003 com pontuação de risco de 50

Além disso, considere os seguintes pesos na calculadora de acúmulo de vulnerabilidades:

- Pontuação de risco máximo: 80
- Pontuação de risco médio: 5
- Contagem de itens vulneráveis: 15

Exemplo de calculadora de acúmulo de vulnerabilidade



No exemplo da calculadora de acúmulo de vulnerabilidades, a fórmula para determinar a **pontuação de risco** da tarefa de correção é:

(**Pontuação de risco máximo**/100) * 80 + (**Pontuação de risco médio** /100) * 5 + (fator * 15)

O fator é determinado da seguinte forma:

Contagem de IV	Fator
< 10	0,2

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

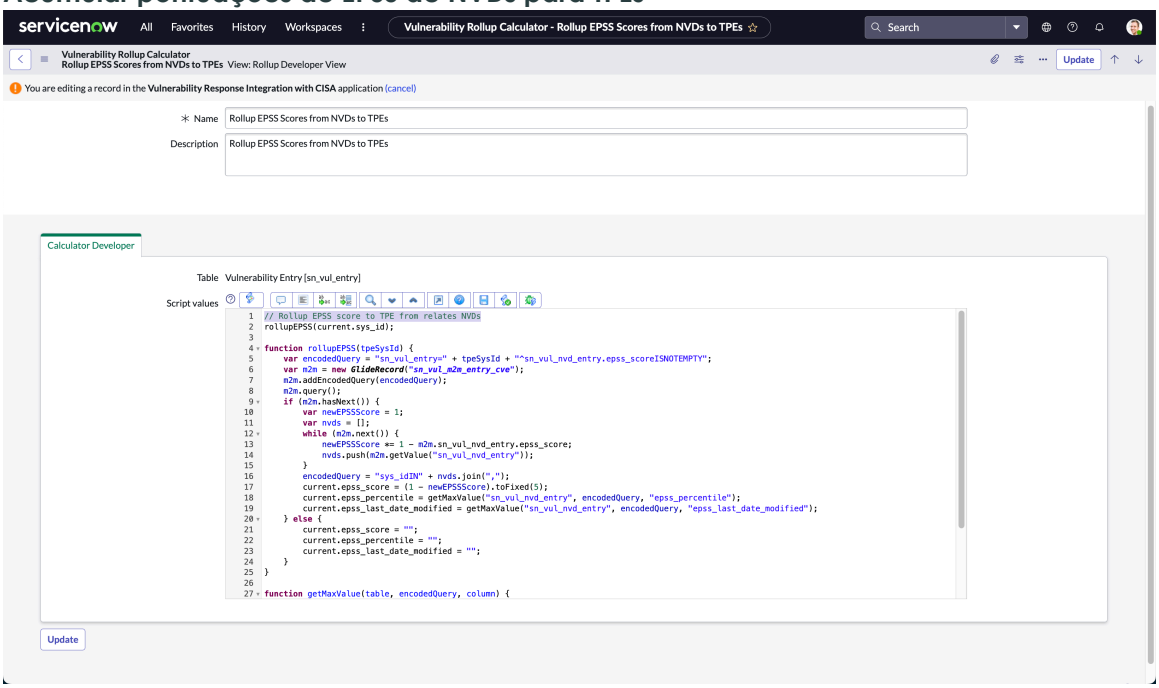
Contagem de IV	Fator
10-100	0,4
101-1000	0,6
1001-10000	0,8
> 10.000	1

Portanto, para a tarefa de correção, VUL324567:

- A pontuação média de risco é 40
- A pontuação de risco máximo é 50
- 50 (pontuação de risco máximo)
- O fator é 0,2

A **pontuação de risco** seria 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45]

Acumular pontuações de EPSS de NVDs para TPEs



Calculadora de acúmulo de EPSS - Exemplo

Por exemplo, considere uma organização com 100 vulnerabilidades, cada uma com 5% de chance de serem exploradas. A pergunta de grande interesse para um defensor de rede pode ser: qual é a probabilidade de que pelo menos uma dessas vulnerabilidades seja explorada e, portanto, qual é a minha ameaça geral? A probabilidade de pelo menos um evento ocorrer é simplesmente o complemento (oposto) de nenhum evento ocorrendo, ou seja:

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are
 exploited)
```

Em que, a probabilidade de não haver vulnerabilidades é o produto linear de cada vulnerabilidade não explorada. Neste exemplo, como cada vulnerabilidade tem 5% de chance de ser explorada, cada uma tem 95% de chance de não ser explorada. E como há 100 deles, podemos escrever isso como:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 -
 P(one vuln not exploited)^100 = 1 - 0.95^100 = 0.994
```

O que indica que a probabilidade de pelo menos uma das vulnerabilidades serem exploradas é de 99,4%.

Importante: Para modificar o *Rollup EPSS Scores from NVD to TPEs*, você precisa alternar a exibição do menu de contexto do formulário para **Acúmulo da Exibição do desenvolvedor** a partir da **exibição Padrão**.

Criar ou editar Resposta a vulnerabilidades regras de destino de correção

Depois de fazer a avaliação inicial das regras de destino de correção no Assistente de configuração, os gerentes de vulnerabilidade podem configurar uma regra de destino de correção no nível do item vulnerável para orientar a correção de vulnerabilidades de alto risco em tempo hábil. Quando a data de correção de um item vulnerável se aproxima, uma notificação é enviada aos usuários ou grupos especificados na regra.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de destino de correção**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	Nome da regra.
Meta (dias)	Especifique o número de dias em que os itens vulneráveis devem ser corrigidos, desde a última abertura.
V17.1: destino de (data)	Data a partir do momento em que os SLAs de destino são calculados. Você pode especificar somente a data ou os campos de tipo de data e hora. O valor padrão é Data da última abertura. Para personalizar os valores deste campo, consulte KB1642413 .
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra de meta de correção está ativa. Se esta caixa de seleção estiver desmarcada, esta regra não se aplicará a novos itens vulneráveis criados no sistema.
Notificar (dias antes do vencimento)	Número de dias antes do tempo de correção direcionado para o envio de uma notificação. A data de notificação calculada usando este valor é usada para mostrar o status de correção e a codificação de cores. Se a data for anterior à data de notificação, o status da correção será "Em andamento". Se já tiver passado da

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	data de notificação e for anterior à data da meta de correção, o status será mostrado como se aproximando da meta. **Nota:** Se este campo estiver definido como 0, somente uma notificação de **destino não atingido** será enviada.
Descrição	Texto que descreve a regra de meta de correção.
Condição	Usando o filtro de condição, selecione os critérios para aplicar a regra aos itens vulneráveis. Para evitar impacto no desempenho, teste suas condições em toda a escala de produção. Os testes permitem que você determine quanto tempo o trabalho **Avaliar metas de correção** leva para ser executado, de acordo com as condições e o tamanho do seu Configuration Management Database (CMDB). A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.
Notificações **Nota:** A contagem mostrada no e-mail de notificação não inclui itens vulneráveis no estado **Adiado**, **Resolvido**ou **Encerrado**.	
Usuários	As pessoas a serem notificadas quando o item vulnerável selecionado estiver se aproximando ou passar do tempo de meta de correção direcionado.
Grupo	O grupo a notificar quando o item vulnerável selecionado estiver se aproximando ou ultrapassar seu tempo de meta de correção.
Atualizar Histórico	
	Não usado para a criação inicial de uma regra. Posteriormente, as anotações de trabalho do sistema são registradas aqui.

4. Clique em **Enviar**.
   Esta regra entra em vigor durante a próxima execução do trabalho agendado, *Evaluate remediation targets* ou ao usar o botão **Aplicar mudanças** na exibição de lista Regras de destino de correção. O mesmo acontece quando uma regra existente é atualizada. Para obter mais informações sobre o trabalho agendado e **Aplicar mudanças**, consulte Resposta a vulnerabilidades regras de destino de correção.

Configurar integrações de terceiros instaladas usando o Assistente de configuração

Configure a Resposta a vulnerabilidades para funcionar com cada uma das implantações de aplicações de terceiros instaladas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração**.
2. Selecione **Integrações de scanner** para configurar implantações de aplicações de terceiros instaladas.
3. Se Solução de gestão de Resposta a vulnerabilidades estiver instalado, você poderá selecionar **Integrações de solução** para configurar seus provedores de soluções de vulnerabilidade.

Configurar integrações de soluções instaladas para Solução de gestão de vulnerabilidade usando o Assistente de configuração

Depois de instalar a aplicação Gestão de soluções para vulnerabilidades, você pode configurar seus provedores de soluções de vulnerabilidade usando o Assistente de configuração.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou admin
Use as seções a seguir para complementar as instruções e avisos fornecidos no Assistente de configuração para integrações de soluções instaladas para Solução de gestão de Resposta a vulnerabilidades.

- Verifique se você já instalou Solução de gestão de vulnerabilidade e as integrações de solução desejadas antes de começar. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.
- Consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades para obter mais informações antes de configurar as soluções instaladas.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções**.

   O Integração com a solução Microsoft Security Response Center requer uma chave de API e URL do Microsoft Security Response Center para configurá-lo.

   Nota: A inserção da chave de API é opcional para MSRC. Para obter a chave MSRC, você deve ter um ID da Microsoft de uma conta de e-mail do live.com, Outlook.com ou Microsoft.com, um número de telefone registrado na Microsoft ou um login do Skype.

2. Insira a URL.
   O URL no Assistente de configuração para MSRC é `https://api.msrc.microsoft.com`.
3. Clique em **Concluir**.
4. Opcional: Você pode executar importações sob demanda clicando **em Executar agora** na página de configuração depois de inserir suas credenciais.
5. O Red Hat Solution Integration também está disponível.
   Não requer uma chave de API.
6. No Assistente de configuração, à direita de Red Hat Solution Integration, clique em **Editar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Verifique se a URL no Assistente de configuração para RHSI é `https://access.redhat.com/Hidra/rest`
8. Opcional: Você pode executar importações sob demanda clicando **em Executar agora** na página de configuração.
9. Clique em **Concluir**, seguido por **Marcar como Concluído** para concluir a configuração. Uma marca de seleção é exibida no Assistente de configuração para integrações de solução quando você conclui a configuração.

Configurar a integração de vulnerabilidade do MS TVM usando o Assistente de configuração

Configure a integração Resposta a vulnerabilidades com a aplicação Gestão de ameaças e vulnerabilidades (MS TVM) da Microsoft depois de instalá-la usando o Assistente de configuração.

Antes de Iniciar

Além das instruções e avisos fornecidos no Assistente de configuração para a integração Resposta a vulnerabilidades com a integração da Gestão de ameaças e vulnerabilidades da Microsoft, execute as seguintes ações:

- Verifique se você já instalou a aplicação antes de começar. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.
- Consulte Preparação para a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft para obter mais informações antes de configurar a integração da Gestão de ameaças e vulnerabilidades da Microsoft para Resposta a vulnerabilidades.
- Verifique se você tem credenciais de conta do MS TVM disponíveis. Para obter essas credenciais, consulte Configurar o Microsoft Azure para a integração do MS TVM.

Funções necessárias: Administrador do sistema (admin) para instalação, Administrador de vulnerabilidade (sn_vul.vulnerability_admin) ou sn_vul.admin (descontinuado) e Configurar integração (sn_vul_msft_tvm.configure_integration) para configuração

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.

   O bloco Gestão de ameaças e vulnerabilidades da Microsoft é exibido.

   O MS TVM é uma integração de várias origens, o que significa que você pode ter várias implantações da mesma integração de terceiros. As configurações da integração de terceiros original são usadas como modelo para as configurações de cada nova integração.

   Nota: Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

   Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Resposta a vulnerabilidades.

2. Para configurar a integração da Gestão de ameaças e vulnerabilidades da Microsoft, clique em **Editar**.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Credenciais da conta

Campo	Descrição
Nome	Nome da instância.
Região de TVM	Região próxima ao local do servidor. Use o servidor mais próximo do seu local para obter o desempenho ideal da API.
Tipo de autenticação	Método para verificar a identidade. A autenticação de usuário controla a visibilidade de ativos específicos para usuários específicos. O MS TVM exporta os grupos de dispositivos atribuídos a este usuário. O valor padrão é Aplicação.
ID de locatário	Identidade do locatário da sua organização.
ID de cliente	Identidade do cliente gerada após o registro do MS TVM no Microsoft Azure.
Nome de usuário	Usuário que tem acesso ao grupo de dispositivos completo. Este campo aparece somente quando Usuário é selecionado no Tipo de autenticação.
Senha	Senha para o nome de usuário que tem acesso a todo o grupo de dispositivos. Este campo aparece somente quando Usuário é selecionado no Tipo de autenticação.
Segredo do cliente	Segredo do cliente gerado após o registro da aplicação MS TVM. Este campo aparece somente quando Aplicação é selecionado no Tipo de autenticação.

4. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Avançar**.
   O formulário Configuração de importação de vulnerabilidades é exibido.
5. Habilite ou desabilite a importação de vulnerabilidades, determine a data de início inicial das vulnerabilidades que você deseja importar e programe quando a importação de vulnerabilidades do MS TVM deve ser executada.
   Se você quiser importar todas as vulnerabilidades, deixe a data de início inicial em branco.
   a. Para importar dados sob demanda, clique em **Importar vulnerabilidades agora**.
   b. Para ver o registro de integração, clique **em Configurações avançadas**.
6. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Avançar**.
   O formulário Configuração de importação de recomendações é exibido.
7. Habilite ou desabilite a importação de recomendações e determine a programação em que a importação de vulnerabilidades do MS TVM deve ser executada.
   a. Para importar dados sob demanda, clique em **Importar recomendações agora**.
   b. Para ver o registro de integração, clique **em Configurações avançadas**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Avançar**.
   O formulário Configuração de importação de máquinas é exibido.
9. Habilite ou desabilite a importação de máquinas, determine a data de início inicial das máquinas que você deseja importar e programe quando a importação de máquinas do MS TVM deve ser executada.
   Se você quiser importar todas as máquinas, deixe a data de início inicial em branco.

   Nota: Os marcadores de máquina são importados por padrão e usados para organizar e rastrear as máquinas listadas no ambiente do MS TVM.

   a. Para exibir as regras de pesquisa de item de configuração (IC) padrão, clique em **Regras de pesquisa de IC**. As regras de pesquisa de IC definem como os dados da máquina de fontes de terceiros são usados para identificar itens de configuração (IC) no Now Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.

   b. Para importar dados sob demanda, clique em **Importar máquinas agora**.

      Nota: As máquinas com o status integrado no MS TVM são recuperadas pela aplicação ServiceNow.

   c. Para ver o registro de integração, clique **em Configurações avançadas**.
10. Para salvar suas mudanças e ir para o primeiro formulário de integração, clique em **Avançar**.
    O formulário Configuração de importação de vulnerabilidades da máquina é exibido.
11. Habilite as seguintes integrações e determine a data de início inicial das vulnerabilidades que você deseja importar.

Formulário de configuração de importação de vulnerabilidades da máquina

Integração	Descrição
Importação delta de vulnerabilidades da máquina com Microsoft TVM	Recupera vulnerabilidades que foram atualizadas durante a importação de vulnerabilidade completa, incluindo vulnerabilidades novas, corrigidas e atualizadas. Você só pode importar dados delta dos últimos 14 dias.
Importação completa de vulnerabilidades da máquina com Microsoft TVM	Recupera todas as vulnerabilidades em aberto. Devido ao alto volume de importação de dados, você pode programá-la para ser executada semanalmente.

Nota:

Execute a importação de máquinas antes da integração de vulnerabilidades de máquina. Caso contrário, os IVs não serão criados para as máquinas ausentes.

12. Para salvar suas mudanças e concluir a configuração no Assistente de configuração, clique em **Concluir**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Se você quiser ativar um agrupamento de itens vulneráveis no ambiente clássico, navegue até > **Resposta a vulnerabilidades** > **Administração** > **Regras de tarefa de correção** > **Recomendação do Microsoft TVM**.

No formulário exibido, selecione a opção **Ativo** para ativá-lo. Como alternativa, selecione **Novo** para criar uma nova regra.

Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral.

Configurar o Qualys Vulnerability Integration usando o Assistente de configuração

Depois de instalar a aplicação Qualys, configure-a usando o Assistente de configuração.

Antes de Iniciar

Use as seções a seguir para complementar as instruções e avisos fornecidos no Assistente de configuração para configuração do Qualys Vulnerability Integration.

- Verifique se você já instalou a aplicação antes de começar. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.
- Consulte Preparando para o Qualys Vulnerability Integration para obter mais informações antes de configurar o Qualys Vulnerability Integration.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas aplicações de terceiros.

Funções necessárias: administrador do sistema (admin) para instalação, administrador de vulnerabilidade (sn_vul.vulnerability_admin) ou sn_vul.admin (obsoleto) para configuração.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
   As integrações instaladas são exibidas.
2. Clique em **Editar** à direita de Qualys Vulnerability Integration que você deseja configurar.
3. No formulário Credenciais da conta, insira suas Qualys Cloud Platform credenciais.
   Suas credenciais são necessárias para configurá-lo.
4. Use as notas a seguir como um guia ao continuar com a configuração.
   - O link **Configurações avançadas** aponta para o registro de integração Qualys. Você pode adicionar parâmetros compatíveis com o produto Qualys para suas consultas programadas para ajudá-lo a filtrar os dados de vulnerabilidade importados. Consulte Definir parâmetros de filtro adicionais para Qualys importações para obter mais informações.
   - Se você tiver atualizado de uma versão anterior do Resposta a vulnerabilidades com uma versão do Qualys Vulnerability Integration que você já configurou, essa versão, com suas definições de configuração preservadas, ainda estará disponível.

     Em Configurações de importação em Configuração de detecção de host para Qualys Vulnerability Integration, há uma opção para exibir registros de detecção de vulnerabilidade Qualys. Se habilitado, permite que você crie itens vulneráveis a partir de registros de detecção em um status fixo (estado =**Fixo**). Para obter mais informações sobre detecções de itens vulneráveis, consulte Resposta a vulnerabilidades detecções de itens vulneráveis de integrações de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode ativar a caixa de seleção **Pesquisar por partição de rede** na página Configuração de detecção de host para incluir o identificador de partição de rede na pesquisa de endereço IP. Para obter mais informações, consulte Atualizar itens de configuração com o identificador de partição de rede para o Qualys Vulnerability Integration.

Todos os marcadores de host são importados como parte da integração Qualys de lista de hosts. Os marcadores de host são usados principalmente para filtragem em Resposta a vulnerabilidades Regras de atribuição e tarefa de correção. Eles são exibidos no formulário Item descoberto.

Nota: A integração Qualys da lista de hosts deve ser executada antes da criação de regras de atribuição ou de tarefa de correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

As Qualys **etiquetas** do ativo são armazenadas no módulo de etiquetas do host em Qualys Vulnerability Integration.

- O Qualys Vulnerability Integration oferece suporte a várias origens. Você pode ter várias implantações da mesma integração de terceiros. Para adicionar outra integração, na página Integrações de scanner, clique em **Adicionar integração**.

  As configurações da integração de terceiros original são usadas como modelo para as configurações de cada nova integração.

  Nota: Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

  Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Resposta a vulnerabilidades.

- Você pode executar importações sob demanda clicando **em Executar agora** em uma página de configuração.

5. Clique em **Concluir** para concluir a configuração no Assistente de configuração.

Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração

Depois de instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable, configure-a usando o Assistente de configuração.

Antes de Iniciar

Use as seções a seguir para complementar as instruções e avisos fornecidos no Assistente de configuração para a integração Integração de Resposta a vulnerabilidades com Tenable.

- Verifique se você já instalou a aplicação antes de começar. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.
- Consulte Preparação para a integração de vulnerabilidade da Tenable para obter mais informações antes de configurar o Tenable para Resposta a vulnerabilidades.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas aplicações de terceiros.

Tradução automática

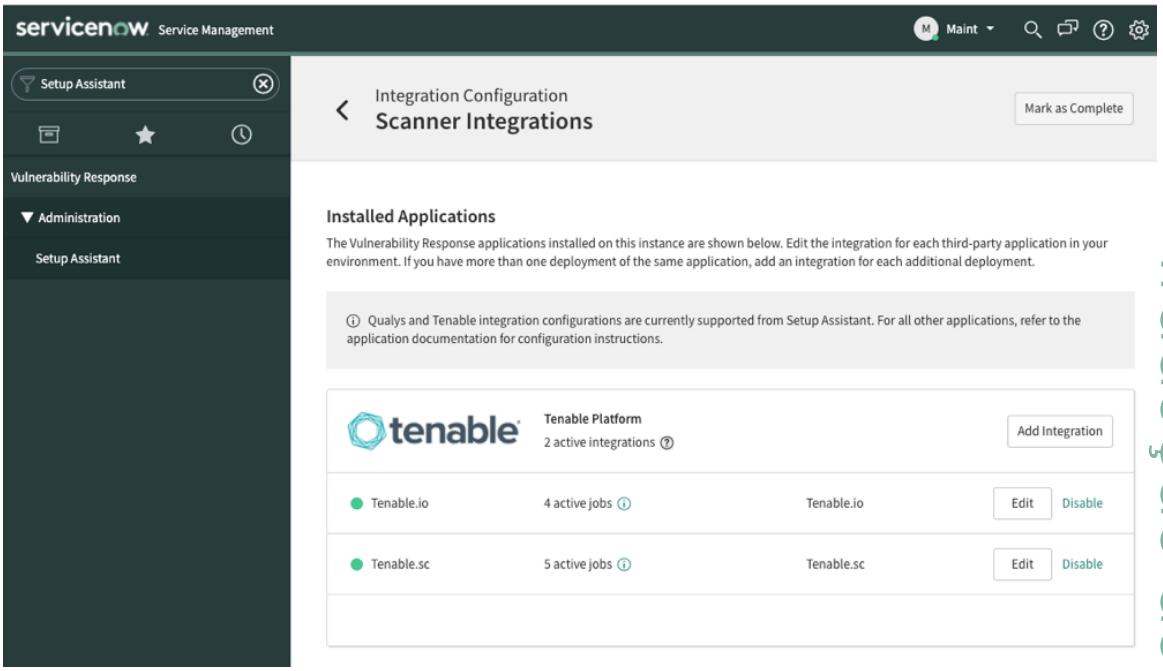
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias: Administrador do sistema (admin) para instalação, Administrador de vulnerabilidade (sn_vul.vulnerability_admin) ou sn_vul.admin (descontinuado) e Configurar integração (sn_vul_tenable.configure_integrations) para configuração.

Procedimento

1. Se não for exibido, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.

   As integrações Tenable.io e Tenable.sc são exibidas.



   A Tenable é uma integração de várias origens e você pode ter várias implantações da mesma integração de terceiros. As configurações da integração de terceiros original são usadas como modelo para as configurações de cada nova integração.

   Nota: Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

   Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Resposta a vulnerabilidades.

2. À direita da integração da Tenable que você deseja configurar, clique em **Editar**.
3. No formulário Credenciais da conta, preencha os campos.

   - Tenable.io requer acesso de administrador com um atributo de permissão maior ou igual a 64.

     Nota: A partir da versão 3.8 da Integração de resposta a vulnerabilidades com Tenable, o acesso ao Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

   - Tenable.sc requer acesso de Analista de segurança ou Gerente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

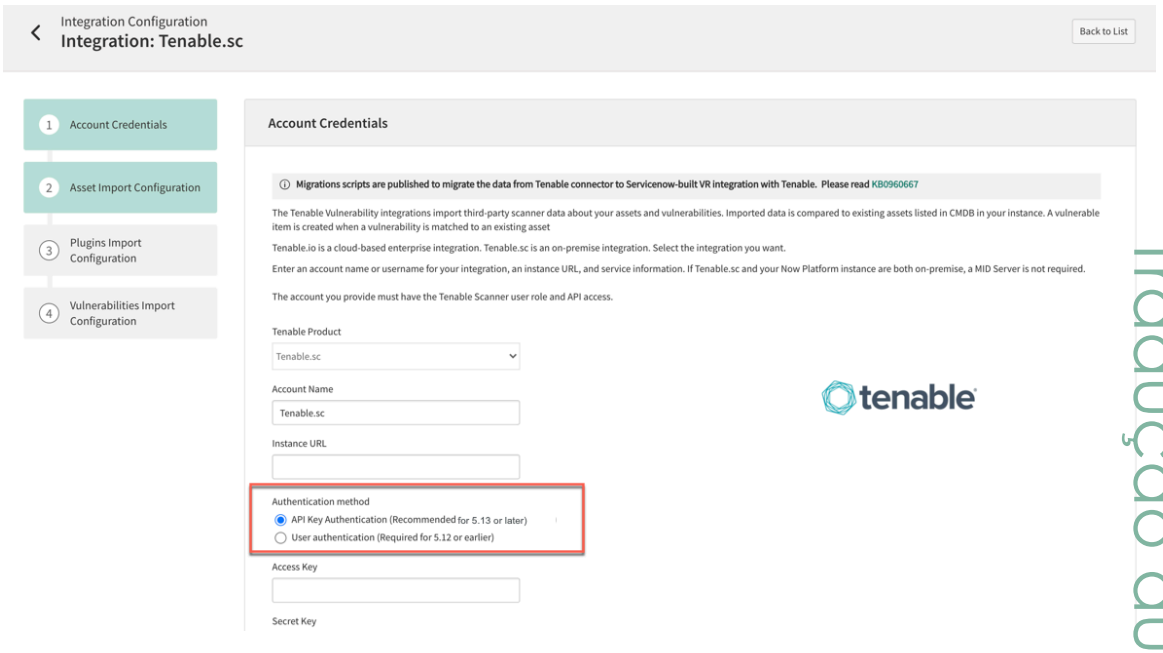
a. Selecione seu produto Tenable.

b. Insira o nome da sua conta da Tenable.

c. No campo URL da instância, insira o URL da sua plataforma Tenable.

d. Selecione um método de autenticação.

Com base na sua versão de Tenable.sc, você tem duas opções de autenticação:



i. A partir da v5.13 de Tenable.sc, selecione **Autenticação de chave de API**. Insira suas chaves secretas e de acesso da Tenable.

ii. Antes da v5.13, a autenticação de usuário era compatível com sua instância Now Platform® e era obrigatória. Insira seu Now Platform nome de usuário e senha.

Somente a autenticação de chave de API é compatível com Tenable.sc. Insira suas chaves secretas e de acesso da Tenable.

e. Opcional: Selecione um MID Server.

(Optional) Se sua instância Now Platform e sua aplicação Tenable.sc não estiverem no mesmo local, escolha um MID Server configurado na lista de seleção. Para obter mais informações, consulte MID Server .

- A partir da v15.0 de Resposta a vulnerabilidades e v3.0 de Integrações de vulnerabilidade da Tenable, você tem a opção de habilitar o parâmetro *Async_request* conforme descrito em Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable. Algumas configurações com a Tenable serão necessárias se você quiser fazer chamadas síncronas. Entre em contato com o produto da Tenable para obter ajuda. Depois de ativado, este parâmetro é aplicável a todas as integrações do Tenable.sc e há um tempo limite de 30

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

segundos. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Scripts de correção**.

- (Optional) Para clientes existentes, um script de correção estará disponível se você estiver usando chamadas assíncronas.

Se sua instância Now Platform e sua aplicação Tenable.sc estiverem no local, embora não sejam necessárias, você terá a opção de selecionar um MID Server configurado na lista de seleção.

Nota: Independentemente de você optar por empregar um MID Server ou não, as integrações expiram após cinco minutos e uma mensagem é exibida quando não há resposta do servidor.

Se você receber um erro de tempo limite, no Assistente de configuração, verifique se inseriu as credenciais e a URL corretas.

4. Clique em **Avançar** para salvar suas mudanças e prosseguir para o primeiro formulário de integração.
O formulário Configuração de importação de ativo é exibido.
5. Neste formulário, ative ou desative a Integração de importação de ativos, determine a data de início inicial dos ativos que você deseja importar e programe quando a importação de ativos da Tenable deve ser executada.

Para Tenable.io

- A integração de ativos pode ser usada com os resultados de conformidade Tenable.io e a integração de preenchimento de resultados de conformidade para importar dados de avaliação de configuração seguros sobre seus ativos para a aplicação Conformidade de configurações.
- A versão 12.2 da aplicação Conformidade de configurações é necessária em sua instância se você quiser importar e exibir esses dados de avaliação de configuração segura.

Consulte Conformidade de configurações dados importados para obter mais informações sobre quais dados são importados com essas integrações e onde eles são publicados.

- Os Tenable.io Resultados de conformidade e Integrações de preenchimento de resultados de conformidade não são ativados por padrão. Se você ativá-los, talvez prefira usar as configurações de programação padrão fornecidas. Consulte as etapas listadas abaixo para saber como localizar e ativar integrações para o Integrações de vulnerabilidade da Tenable.
- Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.io da sua instância. A integração de modelo Tenable.io e a integração de credencial de verificação Tenable.io precisam ser ativadas antes de iniciar novas verificações.

Por padrão, essas integrações estão desativadas. Quando você insere suas credenciais para Tenable.io, todas as integrações Tenable.io são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

a. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.

b. Na lista exibida, localize os registros de integração Tenable.io desejados.

c. Abra cada registro e marque a caixa de seleção **Ativo** para ativar a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Clique em **Atualizar** para salvar suas mudanças.

e. Retorne ao Assistente de configuração para continuar com a configuração para Integrações de vulnerabilidade da Tenable com Resposta a vulnerabilidades.

- Para a integração Tenable.io, você também tem a opção de ativar e desativar a importação de etiquetas do ativo. As etiquetas do ativo são importadas por padrão e usadas para organizar e rastrear os ativos listados em seu CMDB no ambiente Tenable.io.
- Para os produtos Tenable.io e Tenable.sc, se você selecionar **Habilitar pesquisa por partição de rede** em Pesquisar por partição de rede, poderá criar ICs individuais usando o mecanismo de identificação e reconciliação (IRE) para seus ativos que têm o mesmo endereço IP. Para obter mais informações, consulte Atualizar itens de configuração com o identificador de partição de rede para o Integrações de vulnerabilidade da Tenable e Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação.
- Na parte superior da tela, ao lado do link Importação de ativo, clique no link **Regras de pesquisa de IC** para exibir as regras de pesquisa de item de configuração (IC) padrão. As regras de pesquisa de IC definem como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (IC) no Now Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.
- Clique **em Importar ativos agora** para importar dados sob demanda.
- O link **Configurações avançadas direciona** você para o registro de integração de ativos. A partir da v3.3, você pode adicionar parâmetros que são compatíveis com o produto Tenable.io para suas consultas programadas para ajudá-lo a filtrar os dados de vulnerabilidade importados com os Ativos Tenable.io e as Integrações de vulnerabilidades fixas e abertas. Consulte Definir parâmetros de filtro adicionais para Tenable.io importações para obter mais informações.

6. Clique em **Avançar** para salvar suas mudanças e prosseguir para o próximo formulário. O formulário Configuração de importação de plug-ins é exibido.

7. Neste formulário, habilite ou desabilite a importação de plug-ins (entradas de vulnerabilidade de terceiros), determine a data de início inicial dos plug-ins que você deseja importar e programe quando a importação de plug-ins da Tenable deve ser executada.

Se você quiser importar todos os plug-ins, vulnerabilidades e ativos, deixe a data de início inicial em branco.

- Clique **em Importar plug-ins agora** para importar dados sob demanda.
- O link **Configurações avançadas direciona** você para o registro de integração de plug-ins.
- Para a importação de vulnerabilidades, você pode programar e definir níveis de gravidade para Tenable.io para as vulnerabilidades que deseja ingerir. Determine uma data para que somente as vulnerabilidades criadas ou atualizadas a partir de uma data específica sejam importadas.
- Para a integração Tenable.sc, você pode determinar um filtro de consulta e uma data para que somente as vulnerabilidades criadas ou atualizadas a partir de uma data específica sejam importadas.

8. Clique em **Avançar** para salvar suas mudanças e prosseguir para o próximo formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O formulário Configuração de importação de vulnerabilidades é exibido. Habilite ou desabilite a integração e determine a data de início inicial das vulnerabilidades que você deseja importar.

Para o produto Tenable.io :

- Importe somente as vulnerabilidades e IVs associados que correspondam às condições escolhidas com o filtro de gravidade.
- Para a integração de ativos [Tenable.io, *Last Scan Time* é importado e atualizado somente para ativos que têm vulnerabilidades.
- Habilite a opção **Vulnerabilidades corrigidas** para exibir IVs para registros de detecção corrigidos. Se este sinalizador estiver habilitado no Assistente de configuração, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância. Quando habilitado, este recurso pode afetar negativamente o desempenho de ingestão.
- O link **Configurações avançadas** ao lado de Importar filtros aponta para o registro de integração de vulnerabilidades.
- Clique no link **Importar cronogramas** na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.

Para o produto Tenable.sc :

- Importe somente as vulnerabilidades e IVs associados que correspondam aos filtros de condição definidos por uma consulta da Tenable na plataforma Tenable. Consulte a documentação da Tenable para obter mais informações sobre consultas da Tenable.

  O filtro de consulta da Tenable selecionado no Assistente de configuração também se aplica à integração de ativos Tenable.sc. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.

- Habilite a opção **Vulnerabilidades corrigidas** para exibir IVs para registros de detecção corrigidos. Se este sinalizador estiver ativo no Assistente de configuração, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância. Quando ativo, este recurso pode afetar negativamente o desempenho de ingestão.
- Para incluir o identificador de partição de rede na pesquisa de endereço IP, selecione **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede** seção. Para obter mais informações, consulte Atualizar itens de configuração com o identificador de partição de rede para o Integrações de vulnerabilidade da Tenable.
- Clique em **Importar cronogramas** na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.
- O link **Configurações avançadas** ao lado de Importar filtros aponta para o registro de integração de vulnerabilidades.
- A ServiceNow® Tenable.sc Integração de credencial de verificação é habilitada (`Ativo`) automaticamente no Assistente de configuração em sua instância quando você configura as Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades abertas e corrigidas).

  Esta integração importa e atualiza as credenciais do scanner do produto Tenable.sc em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable. Navegar até **Integração de**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidade Tenable > **Integrações** > **Integração de credencial de verificação da Tenable.sc** para exibir mais informações sobre a Integração de credencial de verificação.

9. Clique em **Concluir** para salvar suas mudanças e concluir a configuração no Assistente de configuração.

O que Fazer Depois

(Opcional) Navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Calculadoras de vulnerabilidade** > **Calculadora de Risco Padrão** > **Regra de risco da Tenable** para habilitar a regra de risco da Tenable.

No formulário Regra da calculadora de vulnerabilidade exibido, marque a caixa de seleção Ativo para habilitá-lo.

A Regra de risco da Tenable é instalada com a aplicação Integração de Resposta a vulnerabilidades com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade de Resposta a vulnerabilidades. A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com a nova calculadora de risco padrão. Esta regra de risco está desativada por padrão. Ao habilitar a regra da calculadora de risco da Tenable, os valores de VPR importados são usados para calcular a pontuação de risco dos itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR = 70%, Ativo = 15% e Criticalidade dos negócios = 15%. Habilitar esta regra da Calculadora de risco da Tenable pode afetar o desempenho de ingestão de dados.

Veja Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade

Configuração de provedores de soluções de vulnerabilidade

Configure provedores de soluções de vulnerabilidade seguindo a check-list e configurando os provedores no Assistente de configuração.

Preparar check-list de integração da solução

Use o Assistente de configuração para se preparar para a implementação de uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados do Common Vulnerability Reporting Framework (CVRF) ou do Common Security Advisory Framework (CSAF).

Preparando a integração da solução do Common Vulnerability Reporting Framework (CVRF)

Use o Assistente de configuração para se preparar para a implementação de uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados do Common Vulnerability Reporting Framework (CVRF).

Antes de começar

Para integrar com os fornecedores que fornecem as soluções, certifique-se de executar as tarefas na check-list a seguir. Você pode imprimir a check-list e verificar se os itens listados foram concluídos antes de instalar a aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Aplicações dependentes ☐	Verifique se as seguintes aplicações estão instaladas do ServiceNow Store: • Gestão de soluções de vulnerabilidade: para obter mais informações sobre como instalar Solução de gestão de vulnerabilidade, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração e Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades. • Resposta a vulnerabilidades: para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 16.1 de Resposta a vulnerabilidades ou posterior.
Credenciais de conta de terceiros ☐	Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.
Autenticação do fornecedor ☐	Verifique se você autenticou os fornecedores para importação de soluções usando as APIs. Para obter mais informações sobre como autenticar fornecedores, consulte Configurar aliases de conexão e credencial. Se você não quiser configurar um fornecedor baseado em API, poderá ignorar esta etapa.
Personalização de fluxo e ação de fluxo ☐	Se você quiser configurar um fornecedor baseado em API que não seja a Cisco, deverá personalizar o fluxo e a ação de fluxo para extrair uma chave exclusiva e um URL CVRF da resposta de um comunicado. **Nota:** A publicação da URL do CVRF não é padrão entre os fornecedores. Para personalizar o fluxo para fornecedores que não sejam a Cisco, consulte Configurar um fornecedor do Common Vulnerability Reporting Framework que não seja a Cisco. Você pode ignorar esta etapa se eles não quiserem configurar fornecedores diferentes da Cisco. Por padrão, o fluxo da Cisco foi enviado com a aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Funções ☐	Verifique se você tem um grupo de administradores ou usuário que possa gerenciar a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções.

Preparando a integração da solução CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum)

Use o Assistente de configuração para se preparar para a implementação de uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum).

Antes de começar

Para integrar com os fornecedores que fornecem as soluções, certifique-se de executar as tarefas na check-list a seguir. Você pode imprimir a check-list e verificar se os itens listados foram concluídos antes de instalar a aplicação.

Check-list de preparação da integração

Tarefa	Descrição
Aplicações dependentes ☐	Verifique se as seguintes aplicações estão instaladas do ServiceNow Store: • Gestão de soluções de vulnerabilidade: para obter mais informações sobre como instalar Solução de gestão de vulnerabilidade, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração e Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades. • Resposta a vulnerabilidades: para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 16.1 de Resposta a vulnerabilidades ou posterior.
Credenciais de conta de terceiros ☐	Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Autenticação do fornecedor ☐	Verifique se você autenticou os fornecedores para importação de soluções usando as APIs. Para obter mais informações sobre como autenticar fornecedores, consulte Configurar aliases de conexão e credencial para CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum). Se você não quiser configurar um fornecedor baseado em API, poderá ignorar esta etapa.
Personalização de fluxo e ação de fluxo ☐	Se você quiser configurar um fornecedor baseado em API diferente de Red Hat, deverá personalizar o fluxo e a ação de fluxo para extrair uma chave exclusiva e uma URL de CSAF da resposta de um comunicado. **Nota:** A publicação da URL de CSAF não é padrão entre os fornecedores. Para personalizar o fluxo para fornecedores diferentes de Red Hat, consulte Configurar um fornecedor da Estrutura consultiva de segurança comum que não seja Red Hat. Você pode ignorar esta etapa se eles não quiserem configurar fornecedores diferentes de Red Hat. Por padrão, o fluxo para Red Hat foi enviado com a aplicação.
Funções ☐	Verifique se você tem um grupo de administradores ou usuário que possa gerenciar a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções.

Configurar provedores de soluções de vulnerabilidade

Depois de instalar a aplicação Gestão de soluções para vulnerabilidades, configure os provedores de soluções de vulnerabilidade usando o Assistente de configuração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração**.
2. Clique **em Integrações de solução**.
3. Na seção Soluções instaladas , busque dados usando um URL, uma API ou uma importação.
   - Para buscar dados usando uma URL ou API, clique em **Adicionar integração**.
   - Para buscar dados carregando um arquivo do Common Vulnerability Response Framework (CVRF) ou do Common Security Advisory Framework (CSAF), clique em **Importar arquivo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Dependendo de qual formato você deseja importar os dados em, você pode executar uma das seguintes tarefas:

- Para CVRF:
  - Se você quiser importar um arquivo CVRF, consulte Importação de dados do Common Vulnerability Reporting Framework por meio da importação de arquivo.
  - Se você quiser importar dados do CVRF usando as APIs, consulte Importar dados do Common Vulnerability Reporting Framework (CVRF) por meio da URL do CVRF.
  - Se você quiser importar dados do CVRF por meio de consultorias, consulte Importar dados do Common Vulnerability Reporting Framework de consultorias.
- Para CSAF:
  - Se você quiser importar um arquivo CSAF, consulte Importar dados da Estrutura consultiva de segurança comum por meio da importação de arquivo.
  - Se você quiser importar dados de CSAF usando as APIs, consulte Importar dados do CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum) por meio do URL do CSAF.
  - Se você quiser importar dados de CSAF por meio de consultorias, consulte Importar dados da Estrutura consultiva de segurança comum de consultorias.

Common Vulnerability Reporting Framework (CVRF)

O Common Vulnerability Reporting Framework (CVRF) oferece uma estrutura padronizada para a criação de documentação de relatório de vulnerabilidade. É uma linguagem baseada em XML que simplifica o compartilhamento de informações cruciais relacionadas à segurança entre diversas partes interessadas em várias organizações. Ao utilizar o formato CVRF, a troca e o processamento de informações podem ser agilizados.

Importação de dados do Common Vulnerability Reporting Framework por meio da importação de arquivo

Importe um arquivo CVRF para exibir dados no formato CVRF. A importação é uma atividade única.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin.

Por Que e Quando Desempenhar Esta Tarefa

Depois de importada, uma entrada de fila é criada com um anexo, que é analisado quando a entrada é processada. Os dados são preenchidos nas respectivas tabelas. Antes de analisar os dados do CVRF, um registro de mapeamento de scanner é criado com base na configuração. Em seguida, os dados de mapeamento do scanner são transformados em dados de mapeamento do fornecedor.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique **em Importar arquivo**.

   Nota: Você pode carregar apenas um arquivo XML por vez com um tamanho máximo de arquivo de 1 GB.

3. No campo **Nome**, insira um nome exclusivo para a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O programador é criado com este nome.

4. No campo **Fornecedor**, insira o nome do fornecedor.
   O campo **Origem** das soluções é preenchido com o nome do fornecedor.
5. Clique em **Concluir**.

Resultados

Uma fila de importação foi criada. Clique no link na barra de informações para exibir as entradas da fila do fornecedor junto com a lista relacionada. Você também pode exibir o status do trabalho.

Depois que os dados são importados para o formato CVRF, eles são processados da seguinte forma:

1. Quando a fila é processada, o arquivo é analisado com uma fonte de dados dedicada.
2. Depois que o processamento é concluído, o log da aplicação é atualizado.
3. Depois que o arquivo XML CVRF é analisado, ele preenche as seguintes tabelas na aplicação ServiceNow® Resposta a vulnerabilidades.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Você pode ver as informações detalhadas relacionadas a erros ou exceções nos logs da aplicação.

Configurar aliases de conexão e credencial

Configure os aliases de conexão e credencial para autenticar fornecedores. Na análise de consultoria, os fornecedores de terceiros são autenticados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Procedimento

1. Criar autenticação OAuth.
   Consulte Criar um endpoint para que os clientes acessem a instância .
2. Crie um alias de conexão e credencial.
   Consulte Criação de um alias de conexão e credencial .
3. Crie uma conexão.
   a. Clique no nome do alias de conexão e credencial recém-criado.
   b. Na guia **Conexões**, clique em **Novo**.
   c. Se o tipo de autenticação for OAuth, selecione o perfil de registro da aplicação criado na etapa 1 como **perfil de entidade OAuth**.
   d. Crie um registro em Conexões a partir da lista relacionada do registro.
   e. No campo **Credencial**, selecione o registro de credencial criado na etapa 3d.
   f. No campo **URL de conexão**, insira a URL do fornecedor.
   g. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar um fornecedor do Common Vulnerability Reporting Framework que não seja a Cisco

Configure um fornecedor do Common Vulnerability Reporting Framework (CVRF) que não seja a Cisco com suporte de API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou administrador

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Conexão e Credencial** > **Aliases de conexão e credencial**.
2. Crie um registro com o tipo de autenticação compatível com o fornecedor.
   Para obter mais informações sobre como autenticar um fornecedor, consulte Configurar aliases de conexão e credencial.
3. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Flow Designer**.
4. Duplique o fluxo chamado "Análise de consultoria".

   Nota:
   - Se alguma das ações precisar ser alterada, copie a ação e use-a no novo fluxo.
   - Atualizar a lógica relacionada à paginação de acordo com o fornecedor

5. Se a lógica do parâmetro de intervalo de datas não for a mesma da Cisco, copie a ação **Atualizar parâmetros de paginação** e faça as mudanças conforme necessário para o fornecedor.
6. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Mapeamento de dados de aprimoramento**.
7. Crie um registro de acordo com a Cisco, alterando o valor **da chave de propriedade** de acordo com o fornecedor.
   Essa lógica serve para mapear campos obrigatórios de uma carga de consultoria para uma tabela ServiceNow.
8. Mapeie os seguintes marcadores de API da Carga de API.
   Esses marcadores precisam ser mapeados com detalhes a serem preenchidos na tabela Mapeamento de dados de aprimoramento. Por padrão, o mapeamento específico da Cisco é enviado.

   Nota: Você precisará criar um registro se precisar configurar vários fornecedores que publicam consultorias.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration_u	Descrição
URL do CVRF	cvrf_URL	Nome do marcador que contém a URL do CVRF.
ID da consultoria (chave exclusiva para resposta)	Id	Nome do marcador que contém um identificador exclusivo.
Data da última modificação	last_modified_date	Nome do marcador que contém a data em que o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration_u	Descrição
		registro foi atualizado pela última vez.
securityAdvisoryIntegrationSysId	Integração	Refere-se ao sysId do trabalho agendado de integração, que cria os registros de solução de vulnerabilidade.

9. Com base no formato de resposta, altere a lógica de análise copiando a ação **Recuperar lista** do fluxo de análise consultiva.

Importar dados do Common Vulnerability Reporting Framework de consultorias

Importe dados CVRF de consultorias configurando a URL do fornecedor com o tipo de importação como API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa

Quando a integração é executada, os relatórios são obtidos. A URL do CVRF e o ID dos consultivos são extraídos da carga útil. As chamadas de REST API são feitas para cada URL de CVRF e os dados são analisados e armazenados na tabela sn_vul_solution.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique **em Adicionar integração**.
3. No formulário, preencha os campos.

Importar formulário de consultoria de solução

Campo	Descrição
Tipo de importação	Opção para selecionar o tipo de importação. Selecionar **API**.
Nome	Nome exclusivo da integração.
Fornecedor	Nome do fornecedor **Nota:** O campo **Origem** das soluções é preenchido com o nome do fornecedor.
Alias de conexão	Opção para selecionar uma credencial autenticada. **Nota:** A tabela sys_alias armazena credenciais e o URL base para consultorias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Programação	Frequência na qual os dados devem ser atualizados.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Configuração de APIs	
Fluxo	Opção para selecionar o fluxo. O fluxo é acionado quando o programador é executado. O fluxo cuida da análise dos consultores, extrai a URL do CVRF e armazena esses detalhes nas tabelas de atualização. Você pode copiar o fluxo existente e editá-lo conforme necessário. Por exemplo, você pode fazer mudanças relacionadas à paginação.
Ação de fluxo	Opção para selecionar a ação de fluxo. As ações de fluxo cuidam da capacidade da janela deslizante. Você pode atualizar as ações de fluxo e adicionar o parâmetro de consulta diretamente à ação, arrastando.
Tabela de mapeamento	Opção para selecionar a tabela de mapeamento. O registro da tabela Mapeamento de dados de aprimoramento é usado para extrair a URL do CVRF e o ID da consultoria da carga de consultoria.
Consultas de resposta	Opção para inserir o nome do marcador da carga de consultoria de onde a lista de consultoria pode ser extraída.
Critérios de filtro	
Parâmetros de intervalo de tempo	Opção para selecionar o intervalo de tempo para a solicitação e o formato de data para chamadas de API. O parâmetro Solicitação de data de início/ data de término é o nome do parâmetro usado para a data de início e a data de término durante chamadas de API. Por exemplo, StartDate, start_date, endDate, end_date.
Formato de data	Opção para inserir o formato de data, como `mm/dd/yyyy`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O formato de data é o formato que a API precisa para filtragem. Os formatos que não são compatíveis com GlideDate não funcionam.
Intervalo inicial em dias	Einsira os dias para os quais os dados devem ser obtidos quando o programador é executado pela primeira vez. Para execuções subsequentes, o mecanismo de janela deslizante é seguido. **Nota:** Se você não quiser selecionar um intervalo de tempo, selecione **Sem parâmetros**.
Mapeamentos do scanner	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Clique em **Concluir**.

Importar dados do Common Vulnerability Reporting Framework (CVRF) por meio da URL do CVRF

Importe dados CVRF configurando a URL do fornecedor no Assistente de configuração.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa
Quando a integração é executada, os dados são obtidos do URL que é analisado. Os dados são armazenados na tabela sn_vul_solution com a origem como o nome do fornecedor.

Nota: A Oracle publica diretamente o URL do CVRF para fornecer soluções. Portanto, se você quiser configurar a integração para importar dados do Oracle, certifique-se de ter o URL do CVRF para o Oracle e siga as etapas a seguir.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique **em Adicionar integração**.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar formulário CVRF

Campo	Descrição
Tipo de importação	Tipo de importação. Selecione **URL**.
Nome	Nome exclusivo da integração.
Fornecedor	Nome do fornecedor **Nota:** O campo **Origem** das soluções é preenchido com o nome do fornecedor.
URL	URL do qual você deseja buscar os dados da solução no formato CVRF.
Programação	Frequência na qual os dados devem ser atualizados. **Nota:** Se o marcador de status do CVRF mostrar "FINAL", o campo será definido automaticamente como **Sob demanda** para evitar execuções desnecessárias.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.

4. Clique em **Concluir**.

Solução de problemas de importação de dados do Common Vulnerability Reporting Framework

As ações de solução de problemas podem ajudar a resolver problemas comuns ao importar dados CVRF na aplicação Resposta a vulnerabilidades.

Problema	Ação
A duração da execução da integração é longa	Se a integração for executada por um período mais longo do que o esperado, faça o seguinte: 1. Navegue até a tabela sn_vul_ds_import_q_entry. 2. Agrupe pelo campo **Status**. Você pode ver as entradas, que estão nos estados Concluído, Em andamento ou Na fila.
Falha na integração na importação baseada em API	Se a integração falhar na importação baseada em API, faça o seguinte:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Problema	Ação
	1. Navegue até **Flow Designer**. **2.** Abra o fluxo selecionado na configuração. **Nota:** No caso da Cisco, abra o fluxo de Análise de consultoria. **3.** Clique **em Execuções**. **4.** Abra a execução mais recente ou a execução que deve ser depurada. **5.** Verifique o fluxo em cada fase.
Falha na integração na importação baseada em API com um erro de tempo limite	Se a integração falhar em uma importação baseada em API devido ao tempo limite no fluxo de análise de consultoria, faça o seguinte: **1.** Aumente o tempo limite abrindo `sys_properties.LIST`. **2.** Na coluna Nome, pesquise `sn_vul.CVRFFlowTimeout (inMiliSeconds)`. **Nota:** O tempo é mostrado em milissegundos. **3.** Abra o registro e atualize o valor com um número grande. **4.** Salve o registro e execute novamente a integração.
Falha na integração com o erro "O mapeamento do scanner para a transformação de dados de mapeamento do fornecedor está em andamento"	Verifique se a integração falha durante a importação baseada em URL ou API, com o seguinte erro:`O mapeamento do scanner para a transformação de dados de mapeamento do fornecedor está em andamento. Os dados serão preenchidos somente após a conclusão da transformação. Tente executar após algum tempo.` Se você tiver este erro, aguarde um pouco e execute a integração novamente.
Fila de importação não criada durante a importação de arquivo	Durante uma importação de arquivo, às vezes a fila de importação não é criada. Esta falha significa que a transformação que mapeia os dados de mapeamento do scanner para os dados de mapeamento do fornecedor está em andamento. A

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Problema	Ação
	entrada da fila é criada quando o processo é concluído.

CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum)

Quando usado com Solução de gestão de vulnerabilidade, o CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum) permite notificações de segurança de automação por meio de um formato JSON legível por máquina.

O CSAF permite a integração com qualquer fornecedor de inteligência de solução usando a estrutura de gestão de soluções para importar os dados de inteligência. As notificações de segurança de CSAF podem ser de um dos tipos a seguir.

- Consultorias de segurança
- Vulnerability Exploitability Exchange (VEX)
- Resposta a incidentes de segurança
- Consultoria informativa

O CSAF oferece suporte somente a importações de arquivos, importações de URL e importações de API de consultorias de segurança de fornecedores.

Importar dados da Estrutura consultiva de segurança comum por meio da importação de arquivo

Importe um arquivo CSAF para exibir dados no formato CSAF. A importação é uma atividade única.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou administrador

Por Que e Quando Desempenhar Esta Tarefa

Depois de importada, uma entrada de fila é criada com um anexo, que é analisado quando a entrada é processada. Os dados são preenchidos nas respectivas tabelas. Antes de analisar os dados de CSAF, um registro de mapeamento de scanner é criado com base na configuração. Em seguida, os dados de mapeamento do scanner são transformados em dados de mapeamento do fornecedor.

O mapeamento do scanner não é aplicável a vulnerabilidades baseadas no banco de dados nacional de vulnerabilidades (NVD), que são vulnerabilidades com uma entrada de vulnerabilidade comum (CVE) no banco de dados do NVD.

Se você tiver apenas uma solução de substituição mais alta e ela for distribuída para os itens vulneráveis, a solução preferencial será preenchida. Quando há várias soluções de fornecedor incluídas em uma entrada do NVD, a solução preferencial não é preenchida porque há mais de uma solução de substituição mais alta. Nesse caso, você deve selecionar uma solução manualmente. Para vulnerabilidades de terceiros, a solução preferencial será preenchida somente se você adicionar o mapeamento de scanner correspondente.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Security Advisory Framework**.
2. Selecione **Importar arquivo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode carregar apenas um arquivo JSON por vez com um tamanho máximo de arquivo de 15 MB.

3. No campo **Nome**, insira um nome exclusivo para a integração.
   O programador é criado com este nome.
4. No campo **Fornecedor**, insira o nome do fornecedor.
   O campo **Origem** das soluções é preenchido com o nome do fornecedor.
5. Selecione **Concluir**.

Resultados

Uma fila de importação foi criada. Selecione o link na barra de informações para exibir as entradas da fila do fornecedor junto com a lista relacionada. Você também pode exibir o status do trabalho.

Depois que os dados são importados para o formato CSAF, eles são processados da seguinte forma:

1. Quando a fila é processada, o arquivo é analisado com uma fonte de dados dedicada.
2. Depois que o processamento é concluído, o log da aplicação é atualizado.
3. Depois que o arquivo CSAF JSON é analisado, ele preenche as seguintes tabelas na aplicação ServiceNow® Resposta a vulnerabilidades.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Você pode ver as informações detalhadas relacionadas a erros ou exceções nos logs da aplicação.

Configurar aliases de conexão e credencial para CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum)

Configure os aliases de conexão e credencial para autenticar fornecedores. Na análise de consultoria, os fornecedores de terceiros são autenticados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Procedimento

1. Criar autenticação OAuth.
   Consulte Criar um endpoint para que os clientes acessem a instância .
2. Crie um alias de conexão e credencial.
   Consulte Criação de um alias de conexão e credencial .
3. Crie uma conexão.
   a. Selecione o nome do alias de conexão e credencial recém-criado.
   b. Na guia **Conexões**, selecione **Novo**.
   c. Se o tipo de autenticação for OAuth, selecione o perfil de registro da aplicação criado na etapa 1 como **perfil de entidade OAuth**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Crie um registro em Conexões a partir da lista relacionada do registro.

e. No campo **Credencial**, selecione o registro de credencial criado na etapa 3d.

f. No campo **URL de conexão**, insira a URL do fornecedor.

g. Selecione **Enviar**.

Configurar um fornecedor da Estrutura consultiva de segurança comum que não seja Red Hat

Configure um fornecedor de CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum) diferente de Red Hat com suporte de API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou administrador

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Conexão e Credencial** > **Aliases de conexão e credencial**.
2. Crie um registro com o tipo de autenticação compatível com o fornecedor.
   Para obter mais informações sobre como autenticar um fornecedor, consulte Configurar aliases de conexão e credencial para CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum).
3. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Flow Designer**.
4. Duplique o fluxo chamado "Análise de consultoria".

   Nota:
   - Se alguma das ações precisar ser alterada, copie a ação e use-a no novo fluxo.
   - Revise os parâmetros page_index_key e page_size_key de acordo com a API do fornecedor.
   - Atualizar a lógica relacionada à paginação de acordo com o fornecedor

5. Se a lógica do parâmetro de intervalo de datas não for a mesma que Red Hat, copie a ação **Atualizar parâmetros de paginação** e faça as mudanças conforme necessário para o fornecedor.
6. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Mapeamento de dados de aprimoramento**.
7. Crie um registro de acordo com Red Hat, alterando o valor **da chave de propriedade** de acordo com o fornecedor.
   Essa lógica serve para mapear campos obrigatórios de uma carga de consultoria para uma tabela ServiceNow.
8. Mapeie os seguintes marcadores de API da Carga de API.
   Esses marcadores precisam ser mapeados com detalhes a serem preenchidos na tabela Mapeamento de dados de aprimoramento. Por padrão, o mapeamento específico Red Hat é enviado.

   Nota: Você precisará criar um registro se precisar configurar vários fornecedores que publicam consultorias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration_u	Descrição
URL de CSAF (URL do recurso que aponta para a carga de CSAF)	cvrf_URL	Nome do marcador que contém a URL do CSAF.
ID da consultoria (chave exclusiva para resposta)	Id	Nome do marcador que contém um identificador exclusivo.
Data da última modificação	last_modified_date	Nome do marcador que contém a data em que o registro foi atualizado pela última vez.
csaf (valor estático)	formato_consultoria	Valor do formato de consultoria para cargas de CSAF. Observe que este é um valor estático aplicável a todas as integrações de CSAF.
securityAdvisoryIntegrationSysId	integração	Refere-se ao sysId do trabalho agendado de integração, que cria os registros de solução de vulnerabilidade.

9. Com base no formato de resposta, altere a lógica de análise copiando a ação **Recuperar lista** do fluxo de análise consultiva.

Importar dados da Estrutura consultiva de segurança comum de consultorias

Importe dados de CSAF de consultorias configurando a URL do fornecedor com o tipo de importação como API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa

Quando a integração é executada, os relatórios são obtidos. A URL de CSAF e o ID dos consultivos são extraídos da carga útil. As chamadas de REST API são feitas para cada URL de CSAF e os dados são analisados e armazenados na tabela sn_vul_solution.

O mapeamento do scanner não é aplicável a vulnerabilidades baseadas no banco de dados nacional de vulnerabilidades (NVD), que são vulnerabilidades com uma entrada de vulnerabilidade comum (CVE) no banco de dados do NVD.

Se você tiver apenas uma solução de substituição mais alta e ela for distribuída para os itens vulneráveis, a solução preferencial será preenchida. Quando há várias soluções de fornecedor incluídas em uma entrada do NVD, a solução preferencial não é preenchida porque há mais de uma solução de substituição mais alta. Nesse caso, você deve selecionar uma solução manualmente. Para vulnerabilidades de terceiros, a solução preferencial será preenchida somente se você adicionar o mapeamento de scanner correspondente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Security Advisory Framework**.
2. Selecione **Adicionar Integração**.
3. No formulário, preencha os campos.

Importar formulário de consultoria de solução

Campo	Descrição
Tipo de importação	Opção para selecionar o tipo de importação. Selecionar **API**.
Nome	Nome exclusivo da integração.
Fornecedor	Nome do fornecedor **Nota:** O campo **Origem** das soluções é preenchido com o nome do fornecedor.
Alias de conexão	Opção para selecionar uma credencial autenticada. **Nota:** A tabela sys_alias armazena credenciais e o URL base para consultorias.
Programação	Frequência na qual os dados devem ser atualizados.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Configuração de APIs	
Fluxo	Opção para selecionar o fluxo. O fluxo é acionado quando o programador é executado. O fluxo cuida dos consultores de análise, extrai a URL do CSAF e armazena esses detalhes nas tabelas de atualização. Você pode copiar o fluxo existente e editá-lo conforme necessário. Por exemplo, você pode fazer mudanças relacionadas à paginação.
Ação de fluxo	Opção para selecionar a ação de fluxo. As ações de fluxo cuidam da capacidade da janela deslizante. Você pode atualizar as ações de fluxo e adicionar o parâmetro

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de consulta diretamente à ação, arrastando.
Tabela de mapeamento	Opção para selecionar a tabela de mapeamento. O registro da tabela Mapeamento de dados de aprimoramento é usado para extrair a URL de CSAF e o ID de consultoria da carga de consultoria.
Consultas de resposta	Opção para inserir o nome do marcador da carga de consultoria de onde a lista de consultoria pode ser extraída.
Critérios de filtro	
Parâmetros de intervalo de tempo	Opção para selecionar o intervalo de tempo para a solicitação e o formato de data para chamadas de API. O parâmetro Solicitação de data de início/ data de término é o nome do parâmetro usado para a data de início e a data de término durante chamadas de API. Por exemplo, StartDate, start_date, endDate, end_date.
Formato de data	Opção para inserir o formato de data, como `mm/dd/yyyy.`. O formato de data é o formato que a API precisa para filtragem. Os formatos que não são compatíveis com GlideDate não funcionam.
Intervalo inicial em dias	Einsira os dias para os quais os dados devem ser obtidos quando o programador é executado pela primeira vez. Para execuções subsequentes, o mecanismo de janela deslizante é seguido. **Nota:** Se você não quiser selecionar um intervalo de tempo, selecione **Sem parâmetros**.
Mapeamentos do scanner	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Selecione **Concluir**.

Importar dados do CSAF (Common Security Advisory Framework, Estrutura consultiva de segurança comum) por meio do URL do CSAF

Importe dados de CSAF configurando a URL do fornecedor no Assistente de configuração.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (descontinuado) ou admin

Por Que e Quando Desempenhar Esta Tarefa
Quando a integração é executada, os dados são obtidos do URL que é analisado. Os dados são armazenados na tabela sn_vul_solution com a origem como o nome do fornecedor.

Nota: A URL pode ser uma carga de CSAF direta, que contém os detalhes da consultoria, ou uma URL de feed de ROLIE (Resource-Oriented Lightweight Information Exchange, troca de informações peso-leve orientada para recursos). Em qualquer um dos casos, a carga útil é analisada de acordo e os registros de solução são criados. Conclua as etapas a seguir para importação de URL de CSAF.

Você também pode importar soluções de vulnerabilidade de agregadores de CSAF ou provedores confiáveis por meio de uma importação de URL que oferece suporte ao feed ROLIE. Essas soluções de vulnerabilidade são mapeadas automaticamente para o fornecedor correto e os itens vulneráveis (VITs) com base nas vulnerabilidades e exposições comuns (CVEs).

O mapeamento do scanner não é aplicável a vulnerabilidades baseadas no banco de dados nacional de vulnerabilidades (NVD), que são vulnerabilidades com uma entrada de vulnerabilidade comum (CVE) no banco de dados do NVD.

Se você tiver apenas uma solução de substituição mais alta e ela for distribuída para os itens vulneráveis, a solução preferencial será preenchida. Quando há várias soluções de fornecedor incluídas em uma entrada do NVD, a solução preferencial não é preenchida porque há mais de uma solução de substituição mais alta. Nesse caso, você deve selecionar uma solução manualmente. Para vulnerabilidades de terceiros, a solução preferencial será preenchida somente se você adicionar o mapeamento de scanner correspondente.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Security Advisory Framework**.
2. Selecione **Adicionar Integração**.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar formulário de CSAF

Campo	Descrição
Tipo de importação	Tipo de importação. Selecione **URL**.
Nome	Nome exclusivo da integração.
Fornecedor único	Selecione esta opção se estiver importando CSAF de um fornecedor.
Fornecedor	Nome do fornecedor Este campo só estará disponível se você selecionar **Fornecedor único**. **Nota:** O campo **Origem** das soluções é preenchido com o nome do fornecedor.
Multifornecedor	Selecione esta opção se estiver importando CSAF de vários fornecedores.
Agregador	Um provedor confiável cuja solução você pode importar.
URL	URL do qual você deseja buscar os dados da solução no formato CSAF.
Programação	Frequência na qual os dados devem ser atualizados. **Nota:** Se o marcador de status do CSAF mostrar "FINAL", o campo será definido automaticamente como **Sob demanda** para evitar execuções desnecessárias.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Mapeamentos do escâner **Nota:** A seção Mapeamentos do scanner é opcional para CSAF.	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Selecione **Concluir**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução de problemas de importação de dados do Common Security Advisory Framework

As ações de solução de problemas podem ajudar a resolver problemas comuns ao importar dados de CSAF na aplicação Resposta a vulnerabilidades.

Problema	Ação
A duração da execução da integração é longa	Se a integração for executada por um período mais longo do que o esperado, faça o seguinte: **1.** Navegue até a tabela sn_vul_ds_import_q_entry. **2.** Agrupe pelo campo **Status**. Você pode ver as entradas, que estão nos estados Concluído, Em andamento ou Na fila.
Falha na integração na importação baseada em API	Se a integração falhar na importação baseada em API, faça o seguinte: **1.** Navegue até **Flow Designer**. **2.** Abra o fluxo selecionado na configuração. **Nota:** No caso de Red Hat, abra o fluxo de análise de consultoria. **3.** Selecione **Execuções**. **4.** Abra a execução mais recente ou a execução que deve ser depurada. **5.** Verifique o fluxo em cada fase.
Falha na integração na importação baseada em API com um erro de tempo limite	Se a integração falhar em uma importação baseada em API devido ao tempo limite no fluxo de análise de consultoria, faça o seguinte: **1.** Aumente o tempo limite abrindo `sys_properties.LIST`. **2.** Na coluna Nome, pesquise `sn_vul.CVRFFlowTimeout (inMiliSeconds)`. **Nota:** O tempo é mostrado em milissegundos. **3.** Abra o registro e atualize o valor com um número grande. **4.** Salve o registro e execute novamente a integração.
Falha na integração com o erro "O mapeamento do scanner para a	Verifique se a integração falha durante a importação baseada em URL ou API,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Problema	Ação
transformação de dados de mapeamento do fornecedor está em andamento"	com o seguinte erro:`O mapeamento do scanner para a transformação de dados de mapeamento do fornecedor está em andamento. Os dados serão preenchidos somente após a conclusão da transformação. Tente executar após algum tempo.` Se você tiver este erro, aguarde um pouco e execute a integração novamente.
Fila de importação não criada durante a importação de arquivo	Durante uma importação de arquivo, às vezes a fila de importação não é criada. Esta falha significa que a transformação que mapeia os dados de mapeamento do scanner para os dados de mapeamento do fornecedor está em andamento. A entrada da fila é criada quando o processo é concluído.

Tarefas adicionais Resposta a vulnerabilidades de instalação e configuração

Para ajudá-lo na correção, você pode executar essas tarefas de configuração administrativa adicionais como parte de sua configuração fora da configuração básica. Você executa essas tarefas fora do Assistente de configuração.

Você pode usar a emissão de relatórios padrão fornecida com Resposta a vulnerabilidades para supervisionar sua postura de segurança. Você pode editar esses relatórios se eles não forem adequados ao seu ambiente ou usá-los como modelos para criar o seu próprio.

Se a aplicação Performance Analytics para Resposta a vulnerabilidades estiver instalada, você poderá criar relatórios, painéis dinâmicos e muito mais. Consulte Introdução a relatórios para obter mais informações.

As notificações por e-mail aumentam a produtividade e facilitam o fluxo de trabalho.

Com a Avaliação de exposição de software, pesquise o fornecedor, o nome do produto e o número da versão na Software Asset Management (SAM Foundation) para determinar sua exposição a software vulnerável.

A visibilidade das bibliotecas de vulnerabilidades pode fornecer flexibilidade com tarefas de agrupamento e correção.

Configure a Gestão de exceções para ajudá-lo quando sua organização não puder cumprir uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz, você pode solicitar uma exceção.

Para obter mais tarefas de configuração adicionais, consulte os tópicos que seguem esta visão geral.

Testes de início rápido para Resposta a vulnerabilidades

Valide se Resposta a vulnerabilidades ainda funciona depois de fazer qualquer alteração na configuração, como aplicar um upgrade ou desenvolver um aplicativo. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A propriedade de execução de testes está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se forem criados dados de demonstração ou contas de demonstração, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção. Consulte Executar o pacote de testes Automated Test Framework (ATF) para Resposta a vulnerabilidades para obter mais informações sobre como configurar e executar o pacote de testes para Resposta a vulnerabilidades.

Os testes de início rápido Resposta a vulnerabilidades exigem a ativação da aplicação Resposta a vulnerabilidades (sn_vul) e o carregamento dos dados de demonstração.

Testes Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
VR: criar regras de destino de correção	Crie regras de destino de correção.	Madrid
VR: criar regras do grupo de vulnerabilidades	Crie regras do grupo de vulnerabilidades.	Madrid
VR: criar item vulnerável por meio de formulário	Determine se um usuário pode criar com êxito um item vulnerável a partir do formulário de Item vulnerável.	Madrid
VR: ciclo de vida do grupo de vulnerabilidades	Determine se um usuário pode resolver com êxito um grupo de vulnerabilidades.	Madrid
VR: ciclo de vida do item vulnerável	Determine se um usuário pode mover com sucesso um item vulnerável durante o ciclo de vida e também se um item vulnerável encerrado pode ser reaberto.	Madrid
VR: calculadora de acúmulo	Determine se a calculadora de risco de acúmulo pode fornecer uma pontuação de risco geral para um grupo inteiro de itens vulneráveis usando as pontuações de todos os itens vulneráveis em um grupo de vulnerabilidade.	New York
VR: regras de atribuição de Resposta a vulnerabilidades	Determine se um conjunto de exemplo de regras de atribuição pode atribuir automaticamente itens vulneráveis a um grupo de atribuição para correção.	New York
VR: calculadoras de vulnerabilidade	Teste as calculadoras de vulnerabilidade.	New York

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
VR: Pesquisa de IC - Qualys	Crie uma nova regra de pesquisa com o método "field_matching" chamada "Pesquisa por adaptador de rede" para Qualys. Determine se um item de configuração foi correspondido com êxito na tabela Item descoberto por adaptador de rede e endereço IP com a nova regra de pesquisa.	Orlando
VR: criar solicitação de mudança normal e de emergência	Determine se o usuário pode criar com êxito solicitações de mudança normais e de emergência a partir de um grupo de vulnerabilidades.	Orlando
VR: dividir grupo de vulnerabilidade	Determine se um usuário pode dividir com êxito um grupo de vulnerabilidades.	Orlando
VR: atualize o estado do VG quando um CHG é cancelado.	Determine se o campo Estado em um grupo de vulnerabilidades muda com êxito quando uma solicitação de mudança associada ao grupo de vulnerabilidades é cancelada.	Orlando
VR: atualize o estado do VG quando um CHG muda para revisão.	Determine se o campo Estado em um grupo de vulnerabilidades muda com êxito quando uma solicitação de mudança associada a ele é movida para o estado revisão.	Orlando
VR: Pesquisa de IC - Rapid7	Teste a pesquisa de IC usando a regra de pesquisa Integração com Rapid7 Vulnerability existente **IP Address**.	Orlando
VR: Pesquisa de IC - Qualys	Teste a pesquisa de IC criando uma nova regra de pesquisa para o Qualys Vulnerability Integration	Orlando
VR: fluxo de trabalho de aprovação de exceção para VI	Crie uma solicitação de exceção e verifique se o processo de aprovação está funcionando.	Orlando

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
VR: fluxo de trabalho de aprovação falso-positivo para VI	Crie uma solicitação de exceção de falso-positivo e verifique se o processo de aprovação está funcionando.	Orlando
VR: AVR (Resposta a vulnerabilidades de aplicações)	Determine se suas regras e calculadoras estão funcionando corretamente. Verifique se as atualizações estão funcionando.	Orlando
Regras de destino de correção: teste de importação de VI	Teste as regras de destino de correção de VR durante a importação.	Paris
VR: regra de classificação	Um exemplo de regra de classificação que classifica uma vulnerabilidade automaticamente.	Tokyo

Informações relacionadas

Testes de início rápido

Executar o pacote de testes Automated Test Framework (ATF) para Resposta a vulnerabilidades

Execute o pacote de testes do Automated Test Framework (ATF) depois de instalar ou fazer upgrade da aplicação Resposta a vulnerabilidades.

Antes de Iniciar

Confirme uma instalação bem-sucedida e se sua instância funciona conforme projetado.

A propriedade de execução de testes está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se forem criados dados de demonstração ou contas de demonstração, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção.

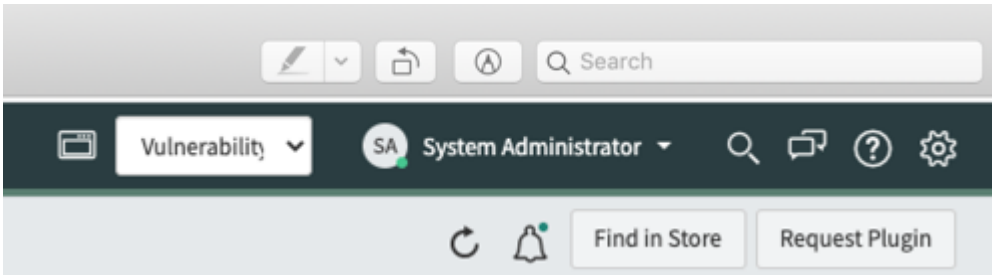
- Verifique se você instalou os dados de demonstração ao instalar Resposta a vulnerabilidades. Os dados de demonstração são necessários para executar o pacote de testes Resposta a vulnerabilidades.
- Para habilitar o teste, siga estas etapas:
  1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Administração** > **Propriedades**.
  2. Se não estiver selecionado, marque a caixa de seleção **Habilitar execução de pacote de testes/teste**.
  3. Clique em **Salvar**.
  4. Se o escopo não estiver definido como **Resposta a vulnerabilidades** no cabeçalho ou se o escopo não for exibido no cabeçalho, clique no ícone de configurações na parte superior da página na janela do navegador .
  5. Na janela Configurações do sistema, clique em **Desenvolvedor**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Se não estiver selecionado, clique em **Mostrar seletor de aplicações no cabeçalho** e feche a janela.
7. Na lista exibida ao lado de `Administrador do sistema`, clique em **Resposta a vulnerabilidades** para o campo.

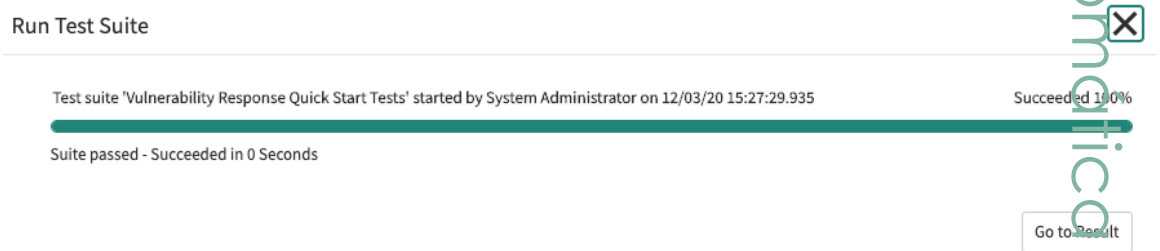
   O campo é exibido conforme mostrado na imagem a seguir.



Função necessária: admin ou atf_test_admin

Procedimento

1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Pacotes**.
2. Na lista Pacotes de testes, localize **Testes de início rápido de Resposta a vulnerabilidades**.
3. Selecione-o para abrir o registro.
4. No registro aberto, marque a caixa de seleção **Ativo**.
5. Clique em **Atualizar**.
6. Se o botão **Executar pacote de testes** não for exibido, atualize a tela, abra o registro novamente e clique em **Executar pacote de testes** para iniciar o teste.
   Depois de alguns momentos, a caixa de diálogo Executar pacote de testes indica um teste bem-sucedido. Clique **em Ir para o resultado** para obter mais



   informações.

O que Fazer Depois

Parabéns! Você pode continuar com a configuração de Resposta a vulnerabilidades.

Para obter mais informações sobre testes automatizados para Resposta a vulnerabilidades e testes automatizados, pacotes de testes e criação de testes automatizados, consulte Automated Test Framework (ATF) .

Instalar Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades

Instale Recomendações de atribuição de vulnerabilidade para que você possa reduzir o tempo gasto na identificação de proprietários para descobertas de vulnerabilidades não atribuídas ou atribuídas incorretamente. Esta aplicação está disponível como uma assinatura separada no ServiceNow Store.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Antes de executar o recurso [Recomendações de atribuição de vulnerabilidade de Resposta a vulnerabilidades em sua instância Now Platform®, você deve primeiro baixar e instalar a aplicação Recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades. Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Para obter mais informações, consulte Ativação de uma aplicação da ServiceNow Store.

Função necessária: administrador

Tarefas de configuração	Ação
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações** > **Instalado em sua instância**. Resposta a vulnerabilidades será mostrado nesta lista se estiver instalado. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se a aplicação Inteligência preditiva está instalada e ativada.	Navegar até **Aplicações do sistema** > **Todas as aplicações** > **Instalado em sua instância**. Inteligência preditiva será mostrado nesta lista se estiver instalado. Se a aplicação não estiver instalada e ativada, consulte Como instalar Inteligência preditiva .
Verifique se você tem as funções ServiceNow necessárias para sua instância.	Verifique se você tem estas funções necessárias para instalação e verificação dos resultados esperados: • vulnerabilidade_admin: necessário para habilitar e configurar Recomendações de atribuição de vulnerabilidade. Você também pode usá-lo para exibir e selecionar recomendações de atribuição para itens vulneráveis e tarefas de correção. • ServiceNow admin: necessário para instalar aplicações.

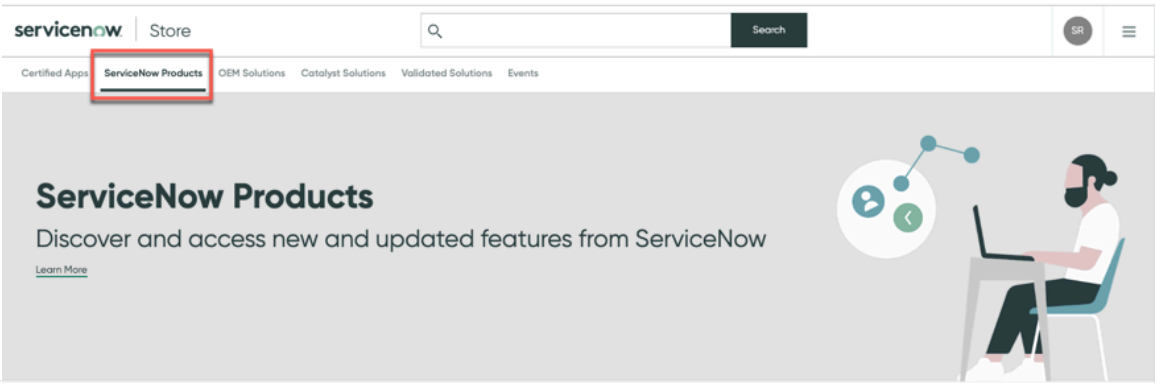
Procedimento

1. Navegue até o ServiceNow Store.
2. Clique **em Fazer login** e insira suas credenciais do HI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Para exibir os produtos ServiceNow disponíveis, clique na guia ServiceNow **Produtos**.



4. Para exibir todas as aplicações associadas que você está atribuindo para Recomendações de atribuição de vulnerabilidade, clique no produto Resposta a vulnerabilidades.

   A página lista todas as aplicações para as quais você está qualificado se aceitar. Para obter informações sobre uma aplicação, clique no link da aplicação.

5. Para verificar se você tem direito a Recomendações de atribuição de vulnerabilidade, clique em **Aceitar**.
6. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.
   Uma mensagem é exibida indicando que você aceitou a aplicação com sucesso.
7. Pule para a etapa 10 para instalar a aplicação em sua instância Now Platform.
8. Opcional: Se você quiser gerenciar seu direito da aplicação Recomendações de atribuição de vulnerabilidade em outras instâncias Now Platform, clique em **Gerenciar direito**.

   Nota:

   Se o botão **Gerenciar direito** não for exibido, clique na aplicação Recomendações de atribuição de vulnerabilidade na lista de produtos para exibi-la.

   a. Escolha uma opção.

   b. Clique em **OK** ou em **Cancelar** para continuar.
   Você está pronto para ativar plug-ins e instalar a aplicação em suas instâncias Now Platform.
9. Faça login na instância Now Platform na qual você deseja instalar a aplicação Recomendações de atribuição de vulnerabilidade.
10. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
11. Nas aplicações listadas, localize a aplicação Recomendações de atribuição de vulnerabilidade (sn_vul_recom) e clique em **Instalar**.
    A caixa de diálogo de instalação da aplicação é exibida e todas as dependências instaladas são exibidas.
12. Opcional: Se você quiser dados de demonstração, marque a caixa de seleção **Carregar dados de demonstração** e clique em **Instalar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não estarão disponíveis para instalação posterior no Gerenciador de aplicações. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.

Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.

13. Clique em **Fechar**.
14. Para configurar Recomendações de atribuição de vulnerabilidade, consulte Configurar recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades.

Configurar recomendações de atribuição de vulnerabilidade para Resposta a vulnerabilidades

Habilite Recomendações de atribuição de vulnerabilidade para reduzir o tempo gasto na identificação dos responsáveis pelas descobertas de vulnerabilidades não atribuídas ou atribuídas incorretamente.

Antes de Iniciar
Função necessária: sn_vul.manage_assignment_recom_config

Por Que e Quando Desempenhar Esta Tarefa
Esta aplicação não está habilitada por padrão.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Recomendações de atribuição**.
2. Selecione **Habilitar recomendações de atribuição**.
   O **campo de definição da solução Inteligência preditiva é** exibido. O valor padrão é **Atribuição de item vulnerável**.
3. Clique em **Salvar**.

Criar e treinar uma definição de solução para Resposta a vulnerabilidades

Crie e treine um modelo de definição de solução para Resposta a vulnerabilidades usando Inteligência preditiva. Você pode usar este modelo para prever o grupo de atribuição de um item vulnerável (VI) ou tarefa de correção (RT) com base nos dados existentes.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Inteligência preditiva** > **Classificação** > **Definições de solução**.
2. No formulário Definições de classificação, clique em **Atribuição de item vulnerável**.
   Esta é a definição de solução padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- A frequência de treinamento padrão é de 30 dias. Isso significa que a cada 30 dias, o modelo é treinado novamente automaticamente usando o conjunto de dados VI que corresponde à condição de filtro configurada.
- Os campos da tabela Item vulnerável podem ser usados para treinamento. A definição de solução padrão é treinada em dois campos de VI: **Vulnerability.Summary** e **Configuration item.Name**. Você pode personalizar os campos usados para treinamento, dependendo de quais campos você considera úteis para prever a propriedade da vulnerabilidade em sua organização.

3. Para criar e treinar a solução de classificação, consulte Criação e treinamento de uma solução de classificação .

Nota: Você também pode criar e treinar uma semelhança ou uma solução de clustering. Para obter mais informações, consulte:

- Crie e treine uma solução de semelhança .
- Crie e treine uma solução de cluster .

4. Clique em **Atualizar e treinar novamente**.

Nota: Para definir configurações avançadas para soluções de ML, consulte Definição de configurações avançadas para suas soluções de ML .

Criar uma calculadora Resposta a vulnerabilidades

Uma calculadora de vulnerabilidade é uma fórmula predefinida para calcular um campo de destino quando determinados critérios são atendidos. As calculadoras, que calculam a **pontuação de risco**do item vulnerável, podem conter **regras de risco**.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Nota: Você pode notar uma degradação no desempenho ao executar calculadoras de vulnerabilidade que contêm scripts.

Ordene suas regras para executar as regras mais simples primeiro e somente executar scripts nos itens que não podem ser tratados com uma condição e valor de modelo ou uma regra de risco.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de calculadora de vulnerabilidade

Campo	Descrição
Nome	O nome da calculadora de vulnerabilidade.
Tabela	Preenchido automaticamente com o nome da tabela de itens vulneráveis.
Aplicação	Preenchido automaticamente com Resposta a vulnerabilidades.
Campo de destino	Campo a ser calculado.
Descrição	Descrição de texto da calculadora.
Ativo	Ligue ou desligue a calculadora.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar**.
   A seção **Regras da calculadora de vulnerabilidade** é exibida.
5. Crie uma regra para a calculadora clicando em **Novo**.

   Nota: Para o formulário **Novas regras de risco** (disponível somente quando o **campo Destino** é **Pontuação de risco**), consulte a etapa 10.

6. Preencha os campos, se for o caso.

Formulário Regra da calculadora de vulnerabilidade

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionadas, as condições com script e os valores com script podem ser selecionados em Tipo de **condição** e **Tipo de valor**.

7. Preencha os campos na guia **Quando esta condição for atendida**, conforme apropriado.

Guia Quando esta condição for atendida

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionado, selecione condições com script e valores com script em Tipo de **condição e Tipo** de **valor**.
Tipo de condição	Disponível quando você seleciona a **exibição Avançada**. As opções incluem: ◦ Filtro: usa condições de filtro. ◦ Grupo de filtros: consulte criar um novo grupo de filtros para definir os critérios da calculadora. ◦ Script: condição de script usada para determinar quando aplicar esta calculadora. **Nota:** Antes de escrever scripts para determinar quando aplicar as calculadoras, retorne à lista de **Calculadoras de vulnerabilidade**. Explore os registros da calculadora de vulnerabilidade enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada ou não. A seleção dos tipos **Grupo de filtros** ou Condição de **script** oculta este campo. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.

8. Clique na guia **Definir estes valores** e preencha os campos no formulário, conforme apropriado.

Guia Definir estes campos

Campo	Descrição
Tipo de valor	Disponível quando você seleciona a **exibição Avançada**. As opções incluem: ◦ Modelo: defina os valores a serem definidos em cada campo. ◦ Script: usado para definir os valores em cada campo.
Valores de Script	Disponível se você selecionou o tipo de valor **Script**. Define a quais valores os cálculos serão aplicados.
Modelo	Selecione os campos e valores que você deseja usar para a calculadora. A seleção do tipo de valor **Script** oculta este campo.

9. Quando tiver concluído todas as entradas, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao editar uma calculadora existente e quiser atualizar todas as pontuações existentes, você pode usar o botão **Reaplicar calculadora**. Ele é executado em todos os itens vulneráveis (IVs) ativos e, se essa calculadora for usada para definir seu valor, recalculará o valor desses IVs. Como a reaplicação de uma calculadora pode levar muito tempo, um trabalho agendado lida com isso.

10. Para o formulário **Novas regras de risco**, preencha os campos conforme apropriado.

    Defina cada peso de acordo com a porcentagem do resultado que deve vir desse valor. Para todos os dados que o scanner não fornecer ou para dados que não devam fazer parte da pontuação de risco, defina o peso como zero.

    Você pode adicionar, excluir ou atualizar os campos. Você também pode configurar a porcentagem de ponderação dos valores de campo. Para obter mais informações, consulte Definir campos e pesos para a regra de risco das Calculadoras de risco da Resposta a vulnerabilidades.

    Conforme você atualiza os pesos, os cenários exibem os pesos restantes, bem como os resultados de **pontuação de risco** antecipados.

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada. A seleção dos tipos **Grupo de filtros** ou Condição de **script** oculta este campo.
Pesos	
Severidade da Vulnerabilidade	Percentual do resultado proveniente da gravidade.
Pontuação de EPSS de vulnerabilidade	Probabilidade de exploração da vulnerabilidade. Por padrão, o peso desses critérios é zero. Se você quiser usar isso para o cálculo da pontuação de risco, defina um peso apropriado em relação a esses critérios.
Explorar itens existentes	Percentual do resultado proveniente da existência de uma exploração. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Explorar nível de habilidade	Porcentagem do resultado que vem do nível de habilidade exigido pela exploração. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.

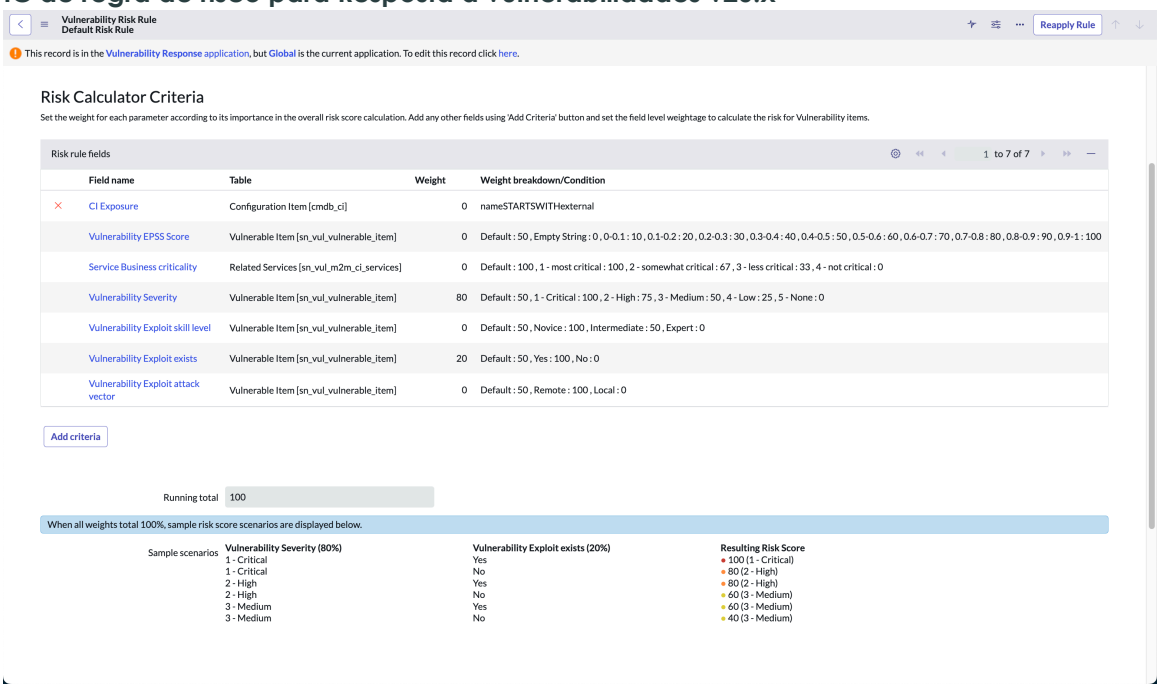
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Explorar vetor de ataque	Porcentagem do resultado que vem de onde o ataque é direcionado. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Criticidade do negócio de serviços	Percentual do resultado proveniente da criticidade dos negócios. Se você não vinculou seus ICs a serviços de negócio, defina o peso como zero.
Exposição de IC	Percentual do resultado obtido se o IC for voltado para a Internet. Se o peso for diferente de zero, um filtro de condição será exibido para definir quais ICs são voltados para a Internet. Defina o filtro para selecionar os itens de configuração voltados para a Internet. Você pode visualizar quais registros correspondem à condição.
Total da execução	Percentuais totais calculados automaticamente. Quando esse valor atinge 100, a visualização do cenário mostra amostras de pontuações de risco em diferentes cenários.
Cenários de pontuação de risco	Quando todos os pesos totalizam 100%, os cenários de pontuação de risco são exibidos, fornecendo uma visualização da pontuação de risco em alguns dos cenários possíveis.

Você pode adicionar ou remover critérios e ajustar o peso de cada critério usando a lista integrada.

IC de regra de risco para Resposta a vulnerabilidades v20.x



11. Clique em **Enviar**.

Desabilitar a calculadora de vulnerabilidade padrão se não for usada

Se você não usar calculadoras de vulnerabilidade, desabilite a calculadora padrão, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Abra a calculadora relevante.
3. Desmarque a caixa de seleção **Ativo** para desativar a calculadora.
4. Clique em **Atualizar**.

Criar, habilitar ou modificar Resposta a vulnerabilidades regras de exclusão automática

Você pode criar, habilitar ou modificar as regras de exclusão do item de vulnerabilidade (VI) e da tarefa de correção (RT). Use a exclusão automática para remover registros mais antigos das tabelas VI e RT.

Antes de Iniciar
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Funções necessárias:

- administrador: modificar as regras de exclusão automática
- sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto): exibir o módulo de exclusão automática

Por Que e Quando Desempenhar Esta Tarefa
Com o tempo, é provável que uma grande quantidade de registros encerrados se acumule nas tabelas VI e VUL da sua instância. Muitos desses registros podem ter sido encerrados por mais de 365 dias, mas não foram removidos. Use regras de exclusão automática para remover muitos desses registros encerrados mais antigos. A remoção desses registros não apenas reduz significativamente o número de registros nas tabelas VI e VUL, como também ajuda a manter o alto desempenho.

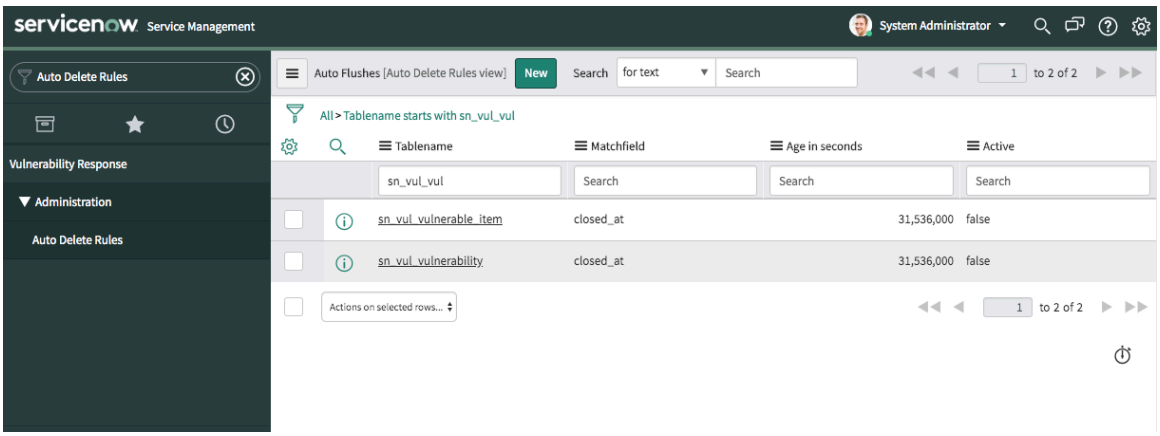
Embora a exclusão automática de metas de registros por padrão esteja fechada há 365 dias, a primeira execução pode tentar limpar muitos registros em uma única transação. Dependendo do tamanho do seu ambiente, talvez você prefira escalonar o processo de exclusão para limitar o escopo da consulta. Por exemplo, você pode iniciar sua primeira execução para registros encerrados com mais de 450 dias. Depois que essa execução for concluída, você poderá trabalhar em incrementos menores (425, 400, 375) até reduzir o número de registros com mais de 365 dias.

Há duas regras fornecidas com seu Now Platform® que excluem automaticamente os registros encerrados que atendem às condições especificadas junto com todos os registros que se referem a eles. Uma regra exclui itens vulneráveis e a outra regra exclui tarefas de correção. Por padrão, essas regras de exclusão automática estão desabilitadas, portanto, você precisa ativá-las manualmente antes de excluir quaisquer registros. Você pode escolher as duas regras pré-configuradas fornecidas com sua instância ou pode criar a sua própria.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exclusão automática**.
   A exibição de lista é exibida.

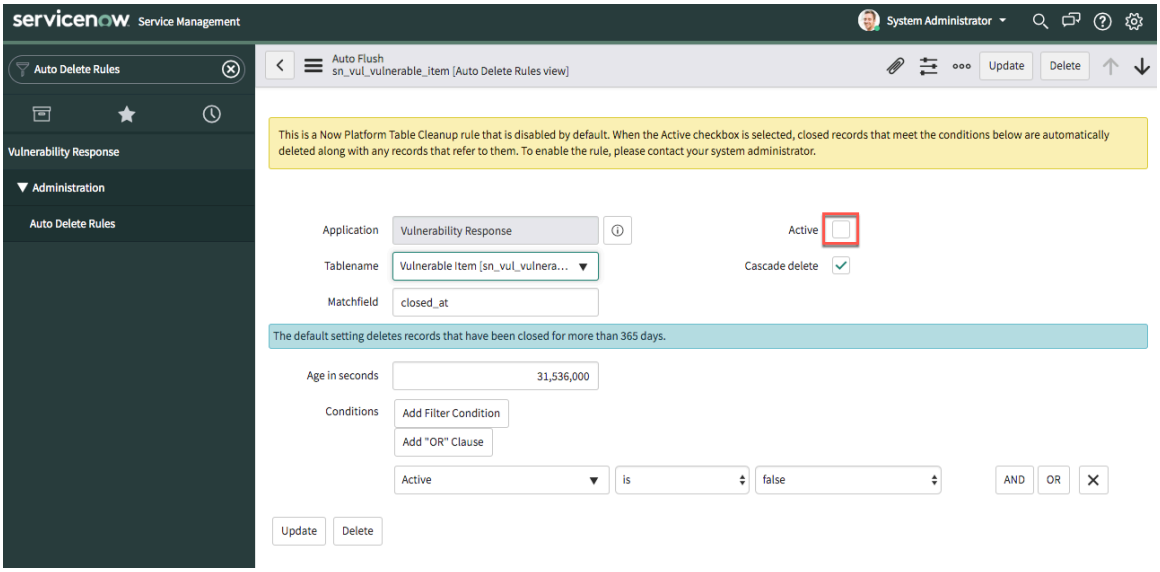


2. Para editar, selecione a regra de exclusão para itens vulneráveis (sn_vul_vulnerable_item) ou a regra para tarefas de correção (sn_vul_vulnerability).
3. Para criar uma nova regra, clique em **Novo**.
4. Preencha ou edite os campos no formulário, conforme apropriado.

Campo	Descrição
Aplicação	Nome da aplicação na qual os registros estão sendo excluídos. O valor padrão é Resposta a vulnerabilidades.
Nome da tabela	Nome da tabela para a qual a regra está sendo aplicada.
Campo de correspondência	Campo para o qual o sistema monitora a duração.
Ativo	Opção para ativar a regra. Depois de ativado, o registro pode ser excluído.
Exclusão em cascata	Opção para excluir todos os registros correspondentes, além de todos os registros que se referem a eles. Se esta opção não estiver selecionada, somente os registros correspondentes serão excluídos, mas não os registros que se referem a eles.
Idade em segundos	Idade do registro de vulnerabilidade a ser excluído. Para as regras de VI e RT, a idade é de 365 dias. Essa idade é exibida em segundos.
Condições	Condições de filtro que definem os registros nas tabelas VI e RT (VUL) às quais as regras se aplicam.

5. Marque a caixa de seleção **Ativo** para ativar uma regra.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que a regra é ativada, a função da plataforma por hora, **Limpeza automática**, exclui os registros da tabela para a qual a regra está ativada.

Se o seu ambiente tiver milhões, ou dezenas de milhões, de registros que correspondem aos seus critérios de exclusão, convém consultar o suporte ao cliente ServiceNow antes de habilitar as regras de exclusão automática para ajudá-lo a excluir registros usando um processo em fases.

Adicionar gráficos de significância de vulnerabilidade à página inicial da Resposta a vulnerabilidades

Você pode adicionar gráficos de definição de significância de vulnerabilidade e outras visualizações à Visão geral.

Antes de Iniciar

- Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.
- O plug-in Análise de vulnerabilidades deve ser ativado.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Visão geral**.
   Alguns relatórios são adicionados ao painel por padrão. Para obter mais informações sobre esses relatórios, consulte Usando os painéis padrão Resposta a vulnerabilidades.
2. Próximo ao cabeçalho do painel, clique no ícone de exibição de cartão ícone + de adição **Adicionar conteúdo** para abrir a caixa de diálogo e adicionar mais widgets.
3. Nas listas na caixa de diálogo **Adicionar widgets**, selecione **Relatórios** para exibir mais Resposta a vulnerabilidades relatórios.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conteúdo	Opções
Detalhes da tarefa de correção	**Mapa de Árvore** > **Significância da vulnerabilidade** > **Significância da vulnerabilidade**
Relatório de pontuação de significância de vulnerabilidade	**Análise de desempenho** > **Pontuação** > **Serviços com significância de vulnerabilidade**
Entrada vulnerável	**Relatórios** > **Entrada vulnerável** > **Vulnerabilidades por impacto, pontuação, semana**
Tarefa de Correção	**Relatórios** > **Tarefa de Correção** > **Tarefa de correção por tempo para corrigir status**
Item da Tarefa de correção	**Relatórios** > **Item da Tarefa de correção** > **Novos itens vulneráveis**
Execução de Integração de Vulnerabilidades	**Relatórios** > **Execução de Integração de Vulnerabilidades** > **Duplicatas da Qualys nos últimos 30 dias, novos IVs, resultados, IVs atualizados, execuções de integração da Qualys**
Item Vulnerável	**Relatórios** > **Item Vulnerável** > **Uma extensa lista de filtros de itens vulneráveis, incluindo IVs da Qualys em aberto.**.

4. Clique no local na tela em que você deseja adicionar o medidor.
5. Feche a caixa **Adicionar conteúdo**.

Definir Resposta a vulnerabilidades notificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações de falso-positivos. Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas sobre como criar notificações por e-mail, consulte Criar uma notificação por e-mail .

Resultados
A partir da v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os links são abertos em Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos em Vulnerability Manager Workspace para os usuários com as funções sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Links abertos em Espaço de correção de problemas de TI para os usuários com a função sn_vul.remediation_owner.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Definir Resposta a vulnerabilidades modelos de e-mail

Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas sobre como criar modelos de e-mail, consulte Criar uma mensagem de e-mail com um modelo .

Criar ou editar notificações de meta de correção

Os administradores de vulnerabilidade podem editar a notificação de meta de correção ou adicionar novas, especificando quando enviar a notificação, quem a recebe e qual conteúdo está na notificação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de meta de correção ou escolha **Novo**.
3. Preencha os campos no formulário, conforme apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultados
A partir da v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos em Vulnerability Manager Workspace para os usuários com as funções sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Links abertos em Espaço de correção de problemas de TI para os usuários com funções, sn_vul.remediation_owner.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configurar a avaliação de exposição de vulnerabilidade

Avalie a exposição de dia zero (dia atual) de seus ativos a software vulnerável com a aplicação Vulnerability Exposure Assessment.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Você pode executar a avaliação de exposição por software e vulnerabilidades e exposições comuns (CVE) para aproveitar os recursos adicionais no espaço de avaliação de vulnerabilidade. Para obter mais informações, consulte Explorar o espaço de avaliação de vulnerabilidade.

Função necessária: administrador

Compatibilidade e requisitos do sistema

A aplicação Resposta a vulnerabilidades está disponível no ServiceNow Store. A aplicação Gestão de ativos de software (SAM) Foundation [com.snc.asset_management] é instalada como parte da aplicação Resposta a vulnerabilidades. Para verificar se a aplicação SAM Foundation está instalada em sua instância, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e pesquise `com.snc.asset_management`. Se a aplicação não estiver instalada, selecione **Instalar**. Para obter mais informações, SAM Foundation consulte Plug-in Software Asset Management Foundational .

Como a aplicação Avaliação de exposição de vulnerabilidade requer acesso aos dados de ativos em sua instância Now Platform®, as aplicações de gestão de ativos devem ter dados para fazer referência. A tabela Modelos de descoberta de software [cmdb_sam_sw_discovery_model] e as Instalações de software [cmdb_sam_sw_install] exigem dados.

A aplicação Vulnerability Exposure Assessment também funciona com as aplicações SAM Foundation ou SAM Pro Now Platform®. A aplicação SAM Pro não faz parte do produto principal Resposta a vulnerabilidades do ServiceNow Store e requer uma assinatura separada.

Nota: A aplicação SAM Pro é necessária somente para a Biblioteca de conteúdo, que pode gerar melhores resultados.

A partir da v23.0 de Resposta a vulnerabilidades, se você tiver a assinatura Pro ou Enterprise, será redirecionado para a página **Avaliação de exposição** nos espaços com base na sua função ao clicar no link **Avaliação de exposição** no menu **Todos** :

Como acessar a página Avaliação de exposição nos espaços

Função	Espaço
Gerenciador de vulnerabilidades	Espaço para gerentes de vulnerabilidades
Gerenciador de eventos [sn_vul_analyst.vul_event_manager] ou Resposta de emergência [sn_vul_analyst.emergency_response]	Espaço de avaliação de vulnerabilidade

Para evitar ser redirecionado para os espaços e permanecer na página Avaliação de exposição clássica, defina o **Tipo de link** como *Lista de registros* na guia Tipo de link na página Módulo - Avaliação de exposição. Você pode acessar a página Módulo - Avaliação de exposição selecionando o ícone **Editar módulo** ao lado do link **Avaliação de exposição** no menu **Todos**.

Com a função de gravação de vulnerabilidade [sn_vulnerability_write], você pode exibir o módulo Avaliação de exposição e criar e editar registros de avaliação de exposição sob demanda para software vulnerável em sua instância com a aplicação Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Avalie sua exposição a software vulnerável

Configurar Gestão de exceções para Resposta a vulnerabilidades

Quando sua organização não pode cumprir uma política de segurança ou gestão de vulnerabilidades, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável (VI) ou tarefa de correção (RT) que não pode ser corrigida de acordo com a política.

Antes de Iniciar

Limite a duração de uma exceção solicitada e adicione um questionário à exceção ou à solicitação de falso-positivo usando o módulo Resposta a vulnerabilidades. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Resposta a vulnerabilidades. Você também pode solicitar uma exceção usando a integração GRC: Gestão de políticas e conformidade.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Resposta a vulnerabilidades estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Gestão de políticas e conformidade estiver instalado, você poderá selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica o objetivo de Política e Controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que gerou a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista **Gerenciar exceções usando**. Você pode selecionar Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade. Você deve ativar o plug-in GRC para usar GRC: Gestão de políticas e conformidade para solicitar uma exceção. Alterar a configuração não afeta os dados existentes.
3. Se você selecionou a opção Resposta a vulnerabilidades, insira as seguintes informações:

Configurações do formulário Gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Exibe o questionário selecionado por você para solicitar uma exceção. O **Questionário de exceção** é exibido por padrão. **Nota:** Este campo aparece somente quando você marca a caixa de seleção **Habilitar questionário para solicitar exceção**.
Questionário para controle de compensação	Exibe o questionário que um proprietário de correção deve responder para solicitações de redução de risco. A partir da v20.0 de Resposta a vulnerabilidades, você pode definir o questionário para solicitações de redução de risco. O **Questionário de controle de remuneração** é selecionado por padrão. **Nota:** Este campo aparece somente quando você marca a caixa de seleção **Habilitar questionário para solicitar exceção**.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Exibe o questionário selecionado por você para marcar como falso-positivo. O questionário para solicitação de falso-positivo é exibido por padrão. **Nota:** Este campo aparece somente quando a caixa de seleção **Habilitar questionário para marcar falso-positivo** está marcada.

Se você personalizou o questionário existente e fez upgrade para a v20.0, esse questionário personalizado será exibido para a solicitação de redução de risco em vez do **Questionário de controle de remuneração**padrão .

4. Se você selecionou a opção GRC: Gestão de políticas e conformidade, insira as seguintes informações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações do formulário Gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Exibe o questionário selecionado por você para marcar como falso-positivo. O questionário para solicitação de falso-positivo é exibido por padrão.

5. Para configurar questionários com base em condições para solicitações de exceção e falso-positivo:

   a. Na seção Configuração do questionário de VR, selecione **Novo**.

   b. No formulário Configuração do questionário - Novo registro, preencha os campos e selecione **Enviar**.
   Para obter mais informações sobre os campos de formulário Configuração de questionário, consulte Campos de formulário de configuração de questionário.
   O questionário criado aparece na seção Configuração do questionário de VR do formulário Configurações para gestão de exceções de VR.

   Por exemplo, se você quiser configurar o questionário para solicitações de falso-positivo para itens vulneráveis críticos, selecione a regra de aprovação **Falso-positivo para itens vulneráveis**, forneça a condição como Classificação de `risco é 1 - Crítico` e selecione o questionário desejado no formulário Configuração do questionário.

6. Selecione **Salvar**.

Adicionar um aprovador de exceção

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção.

Antes de Iniciar

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Até Resposta a vulnerabilidades v14.0, uma solicitação de exceçãopara um item vulnerável ou tarefa de correção é aprovada usando o fluxo de trabalho de aprovação padrão de dois níveis. A solicitação deve ser aprovada por dois níveis de aprovadores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Até Resposta a vulnerabilidades v14.0, se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada. No entanto, a partir da Resposta a vulnerabilidades v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na coluna Nome, pesquise por **Exceção**e clique em **Aprovador de exceção - nível 1**.

   Nota: A partir de Resposta a vulnerabilidades v12.8.1, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de falso-positivo ou exceção é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *sn_vul.exception_approver_L1*, *sn_vul.exception_approver_L2*ou *sn_vul.false_positive_approver_group* para alterar o valor da propriedade.

3. No formulário Aprovador de exceção de grupo - Nível 1, clique na lista relacionada Membros do grupo.
4. Clique em **Novo** para criar uma lista.
5. No formulário, preencha os campos.

Formulário do usuário

Campo	Descrição
ID do Usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear o usuário fora da instância e encerrar todas as sessões ativas do usuário. O sistema evita que usuários com a função de administrador se bloqueiem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ◦ Listas de usuários ◦ Lista de seleção em campos de referência (ícone de lupa) ◦ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço Web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário para o local deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...**.

6. Clique em **Enviar**.
7. Repita as etapas 1 a 5 para criar um Aprovador de exceção - Nível 2.
   O aprovador deve navegar até **Resposta a vulnerabilidades** > **Minhas aprovações** e aprovar as solicitações.

> **Nota:** Para aprovar uma exceção para GRC: Gestão de políticas e conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Configurar regras de aprovação para Gestão de exceções

A partir da Resposta a vulnerabilidades v15.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Resposta a vulnerabilidades (VR) pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Se você já for um usuário de VR, a opção padrão será fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você implantou Resposta a vulnerabilidades v15.0 ou posterior, o valor da propriedade do sistema *sn_vul.flow_designer_activation* será definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Resposta a vulnerabilidades antes da v15.0, o valor desta propriedade do sistema será definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota: Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso positivo para itens vulneráveis

Nota: Você também pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Resposta a vulnerabilidades.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso-positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Expiração da aprovaçãoy (dias) A partir da v21.0 de Resposta a vulnerabilidades	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v21.0 de Resposta a vulnerabilidades	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Criar configurações para uma regra de aprovação.

   Nota: Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para Gestão de exceções.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Criar configurações para uma regra de aprovação

Defina as condições para filtrar itens vulneráveis, tarefas de correção ou regras de exceção correspondentes a um nível de aprovação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
No módulo Configurações de aprovação, você pode configurar vários níveis de aprovação para diferentes configurações. Defina regras baseadas em condição, com cada regra contendo vários níveis de aprovação.

Nota: Use o módulo Regras de aprovação para configurar regras de aprovação para os fluxos de trabalho de gestão de exceções. Para obter informações sobre como configurar regras de aprovação, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Configuração de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Ativo	Habilitado por padrão, o que significa que a configuração de aprovação está em uso.
Descrição	Descrição resumida dos níveis de configuração de aprovação.

5. Defina uma condição para os itens vulneráveis ou tarefas de correção de uma das seguintes maneiras:

Campo	Descrição
Condição	Identifica os itens vulneráveis ou as tarefas de correção correspondentes.
Condição avançada	Script que define a condição dos itens vulneráveis ou tarefas de correção. **Nota:** Este campo aparece quando você marca a caixa de seleção **Avançado**.

6. Selecione **Atualizar**.
   Você pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para Gestão de exceções.

Example:
Você pode definir diferentes caminhos de aprovação para:

- Exemplo 1: diferentes tipos de vulnerabilidades ou itens de configuração (voltados para a internet ou internos).
- Exemplo 2: solicitações de adiamento e redução de risco quando um proprietário de correção gera essas solicitações simultaneamente para itens vulneráveis de host (VITs) ou tarefas de correção (VUL).

  A coluna Aprovação de mudança contém os registros de aprovação de mudança do estado de adiamento. Quando você define uma condição na coluna Aprovação de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mudança usando o Construtor de condições, o registro de aprovação de adiamento é considerado, mas não o registro de aprovação de redução de risco. Portanto, para definir a condição no registro de aprovação de mudança do estado de redução de risco, use o campo **Condição avançada**.

Para a **solicitação de exceção para regra de aprovação de itens vulneráveis**, a **solicitação para configuração de aprovação de classificação de risco de média a baixa** é enviada com o sistema de base. Essa configuração é definida como falsa por padrão. Você pode usar esta configuração para definir um caminho de aprovação para as solicitações de redução de risco de médio a baixo. Você também pode atualizar o script nesta configuração para que ele seja aplicável a várias mudanças de classificação de risco nas solicitações de redução de risco.

Solicitação de classificação de risco da configuração Média a Baixa:

```
function evaluate() {
    var gr = new GlideRecord("sn_vul_change_approval");
    gr.addQuery("sys_id", approval);
    gr.addQuery("current_value", "3 - Medium");
    gr.addQuery("desired_value", "4 - Low");
    gr.query();
    if (gr.next()) {
        return true;
    }
    return false;
}
evaluate();
```

Defina a configuração anterior como verdadeira com a ordem mais baixa e defina a **configuração Padrão - Solicitação de exceção para VI** como verdadeira.

Resultado: quando um proprietário de correção gera um adiamento e solicitações de redução de risco simultaneamente no Espaço de correção de TI, as solicitações de aprovação de adiamento são redirecionadas para os aprovadores definidos em **Configuração padrão - Solicitação de exceção para VI** e as solicitações de aprovação de redução de risco são redirecionadas para os aprovadores definido na **solicitação para configuração de classificação de risco de médio a baixo**.

Criar níveis de aprovação para Gestão de exceções

Defina os níveis de usuários e grupos de usuários que aprovarão as solicitações de exceção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. Na seção Níveis de aprovador, selecione um nível de aprovador.
5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Nível do aprovador

Campo	Descrição
Nome	Nome do nível de aprovação.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ◦ Um aprovador necessário ◦ Todos os usuários devem aprovar
Ativo	Habilitado por padrão, o que significa que o nível de aprovação está em uso.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção de: ◦ Usuário e grupo de usuários ◦ Campo da tabela de aprovação ◦ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções: ◦ sn_vul.exception_approver: para gestão de exceções e regras de exceção ◦ sn_vul.false_positive_approver: para falso-positivo
Usuários	Edite os usuários listados nos grupos.

Tradução automática

6. Para salvar as mudanças, selecione **Atualizar**.

Nota: Antes da v15.0, o processo de fluxo de trabalho era funcional se houvesse usuários somente no nível de exceção 1. No entanto, a partir da v15.0, deve haver pelo menos um usuário em cada nível.

Antes da v15.0, no fluxo de trabalho, se não houvesse usuário no segundo nível, o item de vulnerabilidade ou o grupo vulnerável era adiado. No entanto, da v15.0 em diante, se não houver usuário no segundo nível, a solicitação de aprovação será rejeitada automaticamente.

Example:
Pode haver diferentes níveis de aprovação para vulnerabilidades de servidores Linux e Windows.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de gestão de exceções versus Flow Designer

A partir da Resposta a vulnerabilidades v15.0, se você estiver implantando Resposta a vulnerabilidades (VR) pela primeira vez, o Flow Designer para aprovação de solicitações de exceção na gestão de exceções será habilitado por padrão. Se você já for um usuário de VR, a opção padrão será fluxo de trabalho.

Nota: A partir da Resposta a vulnerabilidades v19.0, somente o Flow Designer é compatível com novos clientes. Se você for um usuário existente e fizer upgrade para Resposta a vulnerabilidades v19.0, o Flow Designer e o fluxo de trabalho de gestão de exceções serão compatíveis.

Fluxo de trabalho versus Flow Designer

Considerações	Fluxo de trabalho	Flow Designer
Versão	Antes da v15.0 de Resposta a vulnerabilidades.	A partir da v15.0 de Resposta a vulnerabilidades.
Opção padrão	Opção padrão se você for um usuário de VR existente.	Opção padrão para novos usuários de VR a partir da v15.0.
Como definir o processo de aprovação	A gestão de exceções inclui solicitações de exceção e falso-positivo junto com regras de exceção.	Inclui a definição de vários níveis e a adição de diferentes aprovadores para diferentes casos de uso. Mais fácil de implementar do que o fluxo de trabalho. A gestão de exceções inclui solicitações de exceção e falso-positivo junto com regras de exceção.
Atualizando para o Flow Designer	Você pode fazer upgrade para o Flow Designer a partir do fluxo de trabalho. No entanto, as solicitações existentes só podem ser aprovadas usando o fluxo de trabalho.	O Flow Designer está habilitado por padrão.
Propriedade do sistema *sn_vul.flow_designer_activation*	Se você estiver usando o fluxo de trabalho para gestão de exceções antes da v15.0, a propriedade do sistema será definida como falsa. Para ativar o Flow Designer, defina esta propriedade como verdadeira. **Nota:** Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer.	Se você estiver usando o VR pela primeira vez para v15.0 ou posterior, o valor da propriedade do sistema será definido como verdadeiro por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho versus Flow Designer

Considerações	Fluxo de trabalho	Flow Designer
Módulo de regras de aprovação	Depois de definir a propriedade do sistema como verdadeira, o trabalho agendado **Habilitar regras de aprovação do módulo** é executado em 24 horas. Este trabalho agendado habilita o módulo **Regras de aprovação**. Para ativar este módulo instantaneamente, execute este trabalho manualmente.	Se você implantou o VR pela primeira vez a partir do VR v15.0, este módulo estará disponível por padrão.
Níveis de aprovação	Fornece a opção de definir apenas dois níveis de aprovadores.	Fornece várias opções, como definir qualquer número de configurações, níveis de aprovador e adicionar dinamicamente aprovadores para cada regra.

Adicionar um aprovador de falso-positivo

Somente usuários adicionados ao grupo de aprovadores de falso-positivo podem aprovar falso-positivos para itens vulneráveis (VIs) e tarefas de correção (VULs). A concessão de um falso-positivo é um processo de aprovação de nível único.

Antes de Iniciar

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Nota:

A partir da Resposta a vulnerabilidades v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > > **Administração de usuários** > **Grupos**.
2. Na coluna **Nome**, pesquise **Falso-positivo** e clique na opção.
3. No formulário Grupo, navegue até **Membros do grupo** > **Novo** (ou **Editar**).
4. No formulário Usuário, crie um registro inserindo os detalhes do usuário e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Todas as funções são concedidas ao usuário. Os usuários selecionados são adicionados à lista Membros do grupo. Esses membros podem aprovar solicitações para marcar IVs ou tarefas de correção como falso-positivos. Depois de aprovado, o estado do registro é atualizado para Encerrado e ele é reaberto somente na data especificada.

Configurar questionário para redução de risco

A partir da Resposta a vulnerabilidades v20.0, você pode personalizar o questionário da solicitação de redução de risco para um conjunto de itens vulneráveis filtrados ou tarefas de correção.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O **Questionário para controles de compensação para itens vulneráveis** e **o Questionário para controles de compensação para regras de aprovação de grupo vulnerável** são enviados com o sistema de base.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Gestão de exceção**.
2. No formulário Configurações para Gestão de exceções de VR, marque a caixa de seleção Habilitar questionário para solicitar exceção.
3. Para configurar questionários com base nas condições das solicitações de redução de risco:

   a. Na seção Configuração do questionário de VR, selecione **Novo**.

   b. No formulário Configuração do questionário - Novo registro, selecione o **Questionário para controles de compensação para grupos vulneráveis** ou **Questionário para controles de compensação para regra de aprovação de itens vulneráveis** e forneça a condição.

   c. Selecione o questionário desejado e selecione **Enviar**.
   Para obter mais informações sobre os campos de formulário Configuração de questionário, consulte Campos de formulário de configuração de questionário.
   O questionário criado aparece na seção Configuração do questionário de VR do formulário Configurações para gestão de exceções de VR.

4. Selecione **Salvar** no formulário Configurações para Gestão de exceções de VR.

Exibir ANS de Resposta a vulnerabilidades para tarefas de correção

Para garantir que os itens vulneráveis sejam processados corretamente, você pode definir um Acordo de nível de serviço (ANS) para Resposta a vulnerabilidades tarefas de correção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

As definições do ANS nesta lista são um subconjunto da lista de ANS da plataforma, específica para Resposta a vulnerabilidades.

Para obter instruções detalhadas, consulte Criação de uma definição do ANS .

Se você estiver acompanhando o tempo necessário para corrigir IVs, talvez prefira usar Resposta a vulnerabilidades regras de destino de correção. As regras de destino de correção definem os intervalos de tempo esperados para corrigir itens vulneráveis (VI) especificamente no contexto da Resposta a vulnerabilidades, enquanto os SLAs podem fornecer um intervalo de tempo para corrigir a própria vulnerabilidade.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Definições do ANS**.
2. Clique em uma definição.
   Os SLAs de tarefa são mostrados nas listas relacionadas de **Tarefas**de correção.

Configurar watchdog

Use a página de configuração do watchdog para criar novos ou atualizar os existentes com as condições que você deseja especificar. Você pode habilitar a notificação para cada cão de guarda e ser notificado quando as condições forem atendidas.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **WatchDog** > **Configuração**.
2. Selecione o watchdog que você deseja implementar.
3. No formulário, preencha os campos.

Formulário de integração do Watchdog

Campo	Descrição
Nome	Nome do cão de guarda.
Ativo	Defina a caixa de seleção como *true* para habilitar o cão de guarda.
Tipo de condição	Escolha entre Filtro ou Script.
Condição avançada	Este campo aparece somente quando Script é selecionado em Tipo de condição.
Tabela	Selecione a tabela para executar a condição de monitoramento.
Condição	Condição para avaliar o cão de guarda.
Notificar	Caixa de seleção para notificar os grupos ou usuários se a condição de monitoramento for atendida.
Usuários	Lista de usuários a serem informados se a condição de monitoramento for atendida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupos	Grupo a ser informado se a condição de monitoramento for atendida.
Log de observação	
Watchdog	Referência à tabela de monitoramento.
Contagem	Número de registros que atendem aos critérios de monitoramento.
Anotações	Anotações adicionais para os logs de Watchdog.

4. Selecione **Atualizar**.

Tarefas de configuração avançadas Resposta a vulnerabilidades

As tarefas de configuração a seguir exigem codificação ou conhecimento avançado ServiceNow e não são consideradas parte da configuração básica.

Talvez você prefira executar essas tarefas somente se tiver experiência avançada em codificação ou tiver um conhecimento avançado do Now Platform.

Criar importações separadas por domínio para uma integração

Se você precisar que os dados importados estejam em um domínio específico, o usuário atribuído para executar as integrações deverá pertencer a esse domínio.

Antes de Iniciar

Função necessária:
import_admin e a função de configuração de integração para sua integração específica, por exemplo, sn_vul.configure_r7_integration ou sn_vul_tenable.configure_integration.

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação ou conhecimento avançado ServiceNow.

As filas de importação contêm anexos de dados que os trabalhos agendados (integrações) processam. Em um ambiente separado por domínio, você deve corresponder o trabalho agendado à fila de importação correta.

Procedimento

1. Crie um domínio.
2. Para cada domínio criado, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um espaço reservado **run_as** para o domínio em sua integração de vulnerabilidade. É o equivalente ao usuário **VR.System** no domínio global. Este usuário precisa de acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota: Não use este usuário para qualquer outra finalidade.

3. Crie um trabalho agendado em cada domínio.
   Para obter mais informações sobre cuidados e configurações adicionais, consulte Configurações adicionais para Separação de domínios.

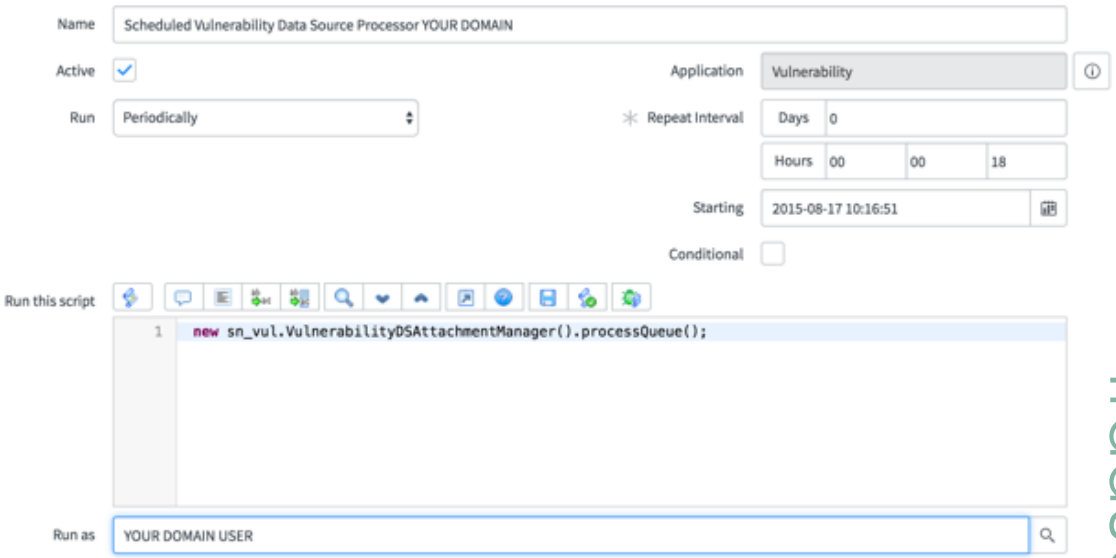
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos agendados**.

b. Copiar **Processador da Fonte de Dados de Vulnerabilidade Programada** para o domínio.

c. Para identificar o trabalho agendado, acrescente o domínio ao nome.



d. No campo **Executar como**, altere o usuário **run_as** para o usuário que você criou na Etapa 2.

A partir da v20.1 de Resposta a vulnerabilidades, as seguintes mudanças de script são enviadas com o sistema de base.

4. **Nota:** Edite a ação de IU a seguir para que a integração seja executada no domínio do usuário **run_as**.

   Edite a ação de IU **Executar agora** no trabalho de integração **de detecção de host da Qualys** para adicionar este bloco de código à parte superior do arquivo.

   Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

5. **Nota:** Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário **run_as**.

   Edite o método de inclusão de script **VulnerabilityIntegrationUtilsaddIntegrationRun** para adicionar o código realçado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Edite o método de inclusão de script **VulnerabilityIntegrationUtils**, **addProcessRun** para adicionar o código realçado na imagem a seguir.
   Código addProcessRun

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Edite o método de inclusão de script **VulnerabilityIntegrationUtils**, **copyProcess** para adicionar o código realçado na imagem a seguir.
   Código copyProcess

Script

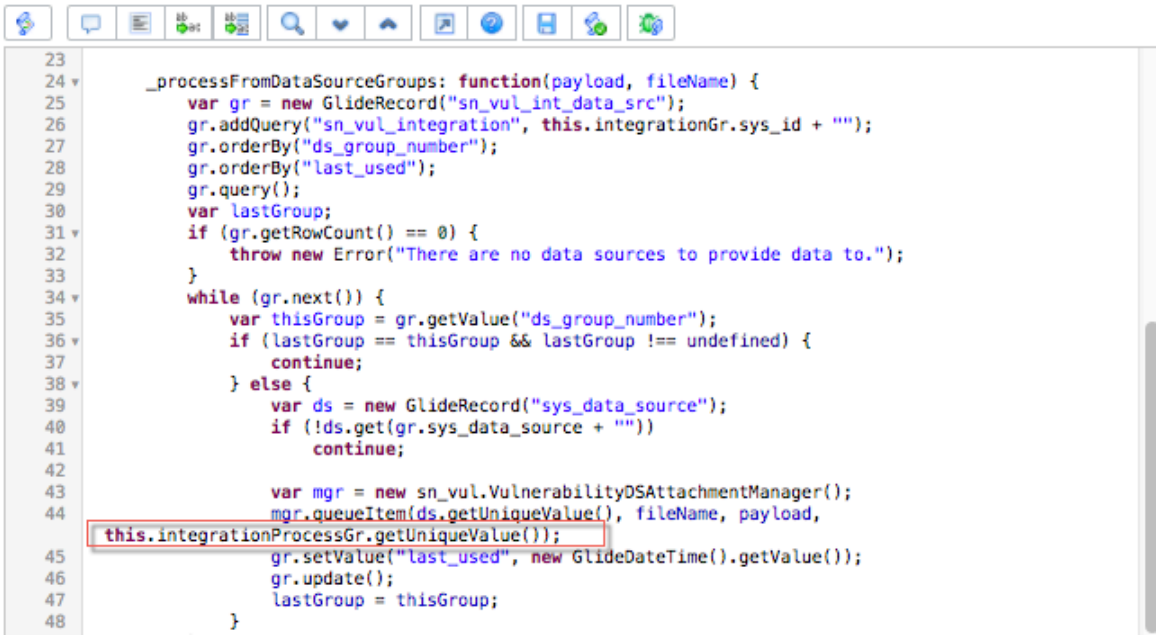
```
_copyProcess: function(intProcGr, isProcessErrored) {
    var copy = new GlideRecord('sn_vul_integration_process');
    copy.initialize();
    copy.setValue('integration_run', intProcGr.getValue('integration_run'));
    copy.setValue('parameters', intProcGr.getValue('parameters'));
    copy.setValue('state', 'new');
    copy.setValue('notes', '');
    copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
    if (isProcessErrored) {
        copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
        var nextRetryDueOn;
        if (intProcGr.getValue('next_retry_due_on') != '')
            nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
        else
            nextRetryDueOn = new GlideDateTime();

        var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
        var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
        nextRetryDueOn.addSeconds(nextRetryDelay * 60);
        if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
            copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
    } else
        copy.setValue('retries', intProcGr.retries + 1);

    copy.insert();
    return copy;
},
```

8. Edite o método de inclusão de script **DataSourceVulnReportRefreshProcessor_processFromDataSourceGroups** para alterar este código original:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

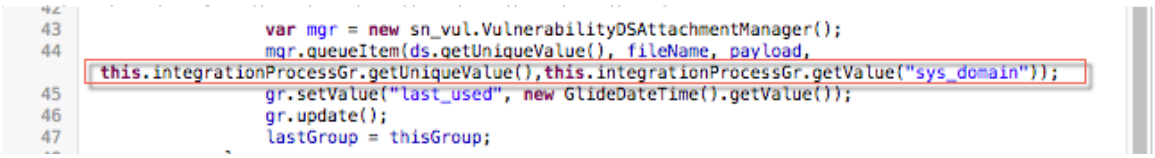
Código original _processFromDataSourcesGroups



```
23
24      _processFromDataSourceGroups: function(payload, fileName) {
25          var gr = new GlideRecord("sn_vul_int_data_src");
26          gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27          gr.orderBy("ds_group_number");
28          gr.orderBy("last_used");
29          gr.query();
30          var lastGroup;
31          if (gr.getRowCount() == 0) {
32              throw new Error("There are no data sources to provide data to.");
33          }
34          while (gr.next()) {
35              var thisGroup = gr.getValue("ds_group_number");
36              if (lastGroup == thisGroup && lastGroup !== undefined) {
37                  continue;
38              } else {
39                  var ds = new GlideRecord("sys_data_source");
40                  if (!ds.get(gr.sys_data_source + ""))
41                      continue;
42
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
48              }
```

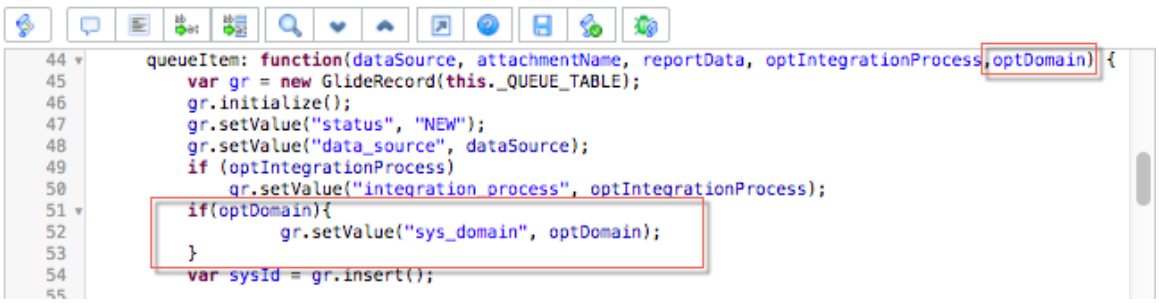
Para:

Código _processFromDataSourcesGroups editado



```
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
```

9. Edite o método de inclusão de script **VulnerabilityDSAttachmentManager**, **queueItem** para adicionar os seguintes blocos de código realçados
queueItem



```
44      queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
45          var gr = new GlideRecord(this._QUEUE_TABLE);
46          gr.initialize();
47          gr.setValue("status", "NEW");
48          gr.setValue("data_source", dataSource);
49          if (optIntegrationProcess)
50              gr.setValue("integration_process", optIntegrationProcess);
51          if(optDomain){
52                  gr.setValue("sys_domain", optDomain);
53          }
54          var sysId = gr.insert();
```

_obterPróximo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
156     _getNext: function() {
157         // First go through the retries, if any
158         var gUser = new GlideRecord("sys_user");
159         gUser.get(gs.getUserID());
160         var sysDomainUser = gUser.getValue("sys_domain");
161         var gr = new GlideRecord(this._QUEUE_TABLE);
162         gr.addQuery("status", "RETRY");
163         gr.addQuery("sys_domain", sysDomainUser);
164         gr.orderBy("queued_on");
165         gr.query();
166         if (gr.next()) {
167             return gr;
168         }
169
170         // Then handle the regular queued items
171         gr = new GlideRecord(this._QUEUE_TABLE);
172         gr.addQuery("status", "QUEUED");
173         gr.orderBy("queued_on");
174         gr.addQuery("sys_domain", sysDomainUser);
175         gr.query();
176         if (gr.next()) {
177             return gr;
178         }
179
```

Função _processQueueEntry

```
182     _processQueueEntry: function(entry) {
183         var schedGrId = this._getScheduledImportSet(entry.data_source);
184         if (gs.nil(schedGrId)) {
185             return;
186         }
187
188         var dataSourceGr = new GlideRecord("sys_data_source");
189         if (!dataSourceGr.get(entry.data_source)) {
190             gs.warn("Non existent data source - marking as complete");
191             entry.setValue("status", "COMPLETE");
192             entry.setValue("processing_notes", "Data source does not exist, could not process.");
193             entry.update();
194             return;
195         }
196
197         try {
198             this._deleteDataSourceAttachments(entry.data_source);
199             if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
200                 gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
201                 throw "Attachments not deleted";
202             }
203             var attachmentApi = new GlideSysAttachment();
204             attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
205             var schedGr = new GlideRecord("scheduled_import_set");
206             schedGr.get(schedGrId);
207             schedGr.setValue("data_source", entry.data_source);
208             schedGr.setValue("run_as", gs.getUserID());
209             schedGr.update();
```

Neste ponto, você está pronto para importações separadas por domínio.

Nota: Se você tiver várias implantações de uma integração Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações, repita este processo para cada implantação.

Criar e oferecer suporte a vários domínios na estrutura de trabalhos em segundo plano

Os trabalhos em segundo plano em produtos de resposta a vulnerabilidades são projetados para serem executados por longos períodos de tempo para executar vários processos em seus registros. Os processadores de trabalho em segundo plano são enviados com o sistema de base que é executado por meio do usuário do sistema e cria registros no domínio global.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administrador de Domínio** > **Domínios**.
2. Crie um domínio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como criar um domínio, consulte Criação de um domínio .

Para cada domínio criado, crie um usuário e atribua o usuário ao domínio. Suponha que este usuário seja um espaço reservado run_as para o domínio. É o equivalente ao usuário VR.System no domínio global. Este usuário precisa de acesso aos dados de vulnerabilidade.

3. Mude o run_as dos trabalhos agendados *Scheduled Background Job Manager*e *Close the parent background job*.

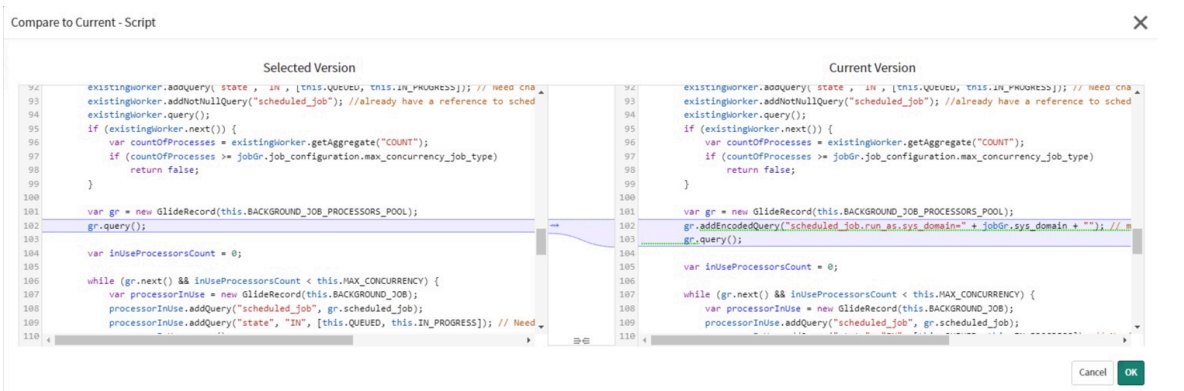
   Se você tiver vários domínios criados, duplique este trabalho e altere o usuário run_as de acordo. Você também pode manter uma cópia dos trabalhos anteriores com o usuário run_as do domínio global em um modo inativo.

   Dez trabalhos de processador (por exemplo, *Background job processor 10*) são enviados com o sistema base. Altere a execução a partir desses trabalhos para o usuário separado por domínio. Se vários domínios estiverem presentes, dois trabalhos por domínio serão suficientes, mas esses trabalhos também poderão ser duplicados, se necessário. Mantenha dois trabalhos de processador com o usuário run_as no domínio global.

   A partir da v20.0 de Resposta a vulnerabilidades, as seguintes mudanças de script são enviadas com o sistema de base.

4. Modifique a inclusão de script *BackgroundJobManager*e adicione a seguinte linha, conforme mostrado na imagem a seguir.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" +
 jobGr.sys_domain + "");
```



Nota: Acione a reaplicação sob demanda de quaisquer regras do domínio correto.

Criar uma regra de pesquisa de IC de resposta a vulnerabilidades

O módulo **Regras de pesquisa de IC** contém regras que são usadas para encontrar o registro correspondente para informações de host recebidas durante as importações de integração de vulnerabilidade de terceiros. As informações do host são correspondidas com os itens descobertos, classes de item de configuração incompatíveis e o Configuration Management Database (CMDB).

Antes de Iniciar

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

A criação de regras de pesquisa de IC requer conhecimento avançado de ServiceNow e Resposta a vulnerabilidades. Em vez de modificar uma das regras de pesquisa existentes, considere copiá-la e modificar a cópia. Quando você estiver satisfeito com a nova regra fazendo o que você deseja, desative a original.

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **CMDB** > **Regras de Pesquisa de IC**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regra de pesquisa de IC

Campo	Descrição
Nome	Nome da regra.
Método de pesquisa	Método usado para correspondência. As opções são: ◦ **Script**: pré-criado (endereço IP, nome DNS e assim por diante) ou script personalizado. ◦ **Correspondência de campo**: pesquise na tabela ou no campo no CMDB.
Tipo	Tipo usado com o **método Pesquisa**de script.
Ordem	Ordem de precedência da regra. Regras com a ordem mais baixa são avaliadas primeiro.
Ativo	Caixa de seleção para saber se a regra está ativa ou desabilitada.
Origem	Origem usada como entrada para esta regra.
Campo de origem	Campo de origem usado como entrada para esta regra. Selecione qualquer campo, mas ele é tratado como um valor de cadeia de caracteres.
Condição	Condição com base na qual a regra de pesquisa de IC é aplicada. Esta condição depende do atributo do scanner de terceiros. **Nota:** O atributo de ativo faz parte da carga útil. Ele é recebido do scanner de terceiros. Consulte a tabela Itens descobertos para obter exemplos de carga.
Script	O script de amostra editável, com base no **Tipo**, é mostrado. Implemente o script personalizado seguindo os comentários incluídos no modelo da função padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A função de processo tem três parâmetros: *rule*, *sourceValue* e *sourcePayload*
Pesquisar na tabela	Tabela a ser pesquisada no CMDB. Usado com campo correspondente ao **Método de pesquisa**.
Pesquisar no campo	Campo que contém informações que podem ser usadas para localizar um IC. Usado com o campo correspondente ao **Método de pesquisa**. Este campo pode estar no registro de IC ou em um registro relacionado, como um adaptador de rede.

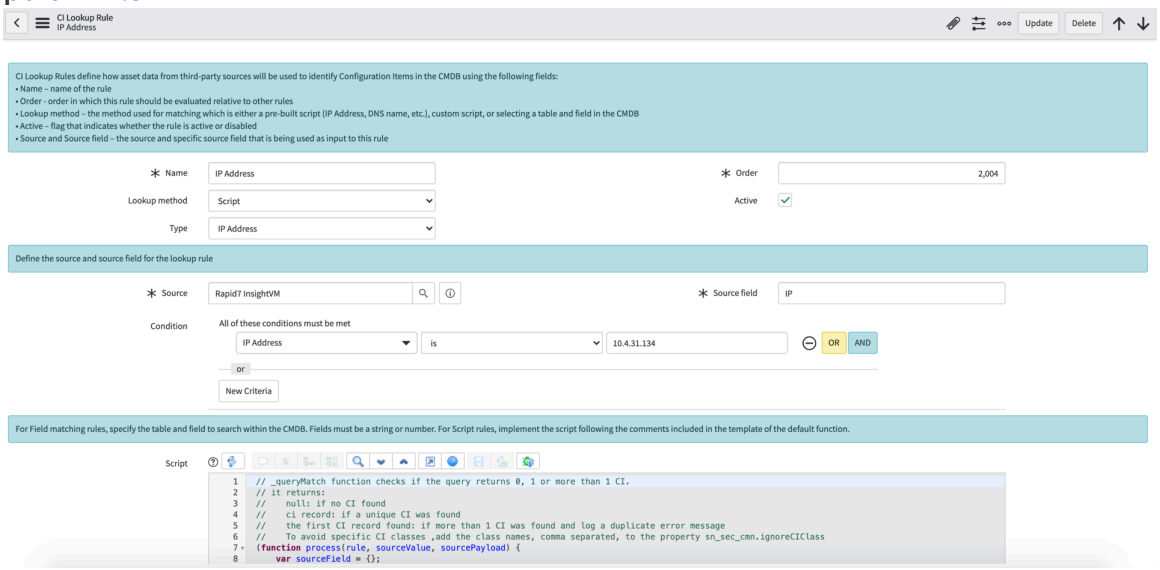
4. Clique em **Enviar**.

Para obter mais informações sobre implementação de regras de pesquisa de IC, consulte Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Resposta a vulnerabilidades regras de pesquisa de IC.

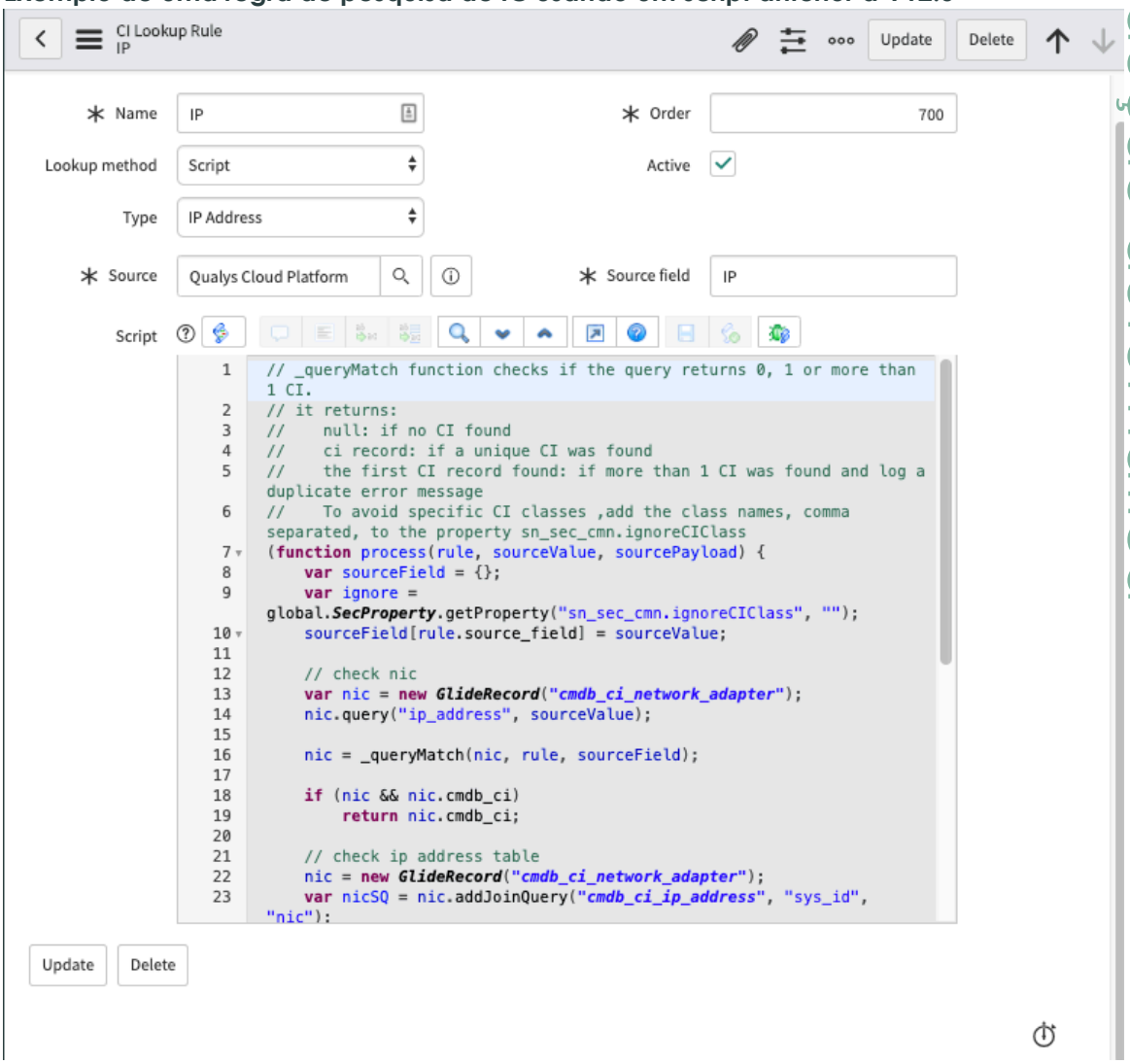
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de uma regra de pesquisa de IC usando um construtor de condições para V12.0



Exemplo de uma regra de pesquisa de IC usando um script anterior à V12.0



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Resposta a vulnerabilidades campos de formulário de item vulnerável

Ignorar classes de IC

Para ignorar algumas classes de item de configuração (IC), por exemplo, Balanceador de Carga [cmdb_ci_lb], ao executar Regras de Pesquisa de IC, defina a propriedade do sistema **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*.

Antes de Iniciar

Função necessária: administrador

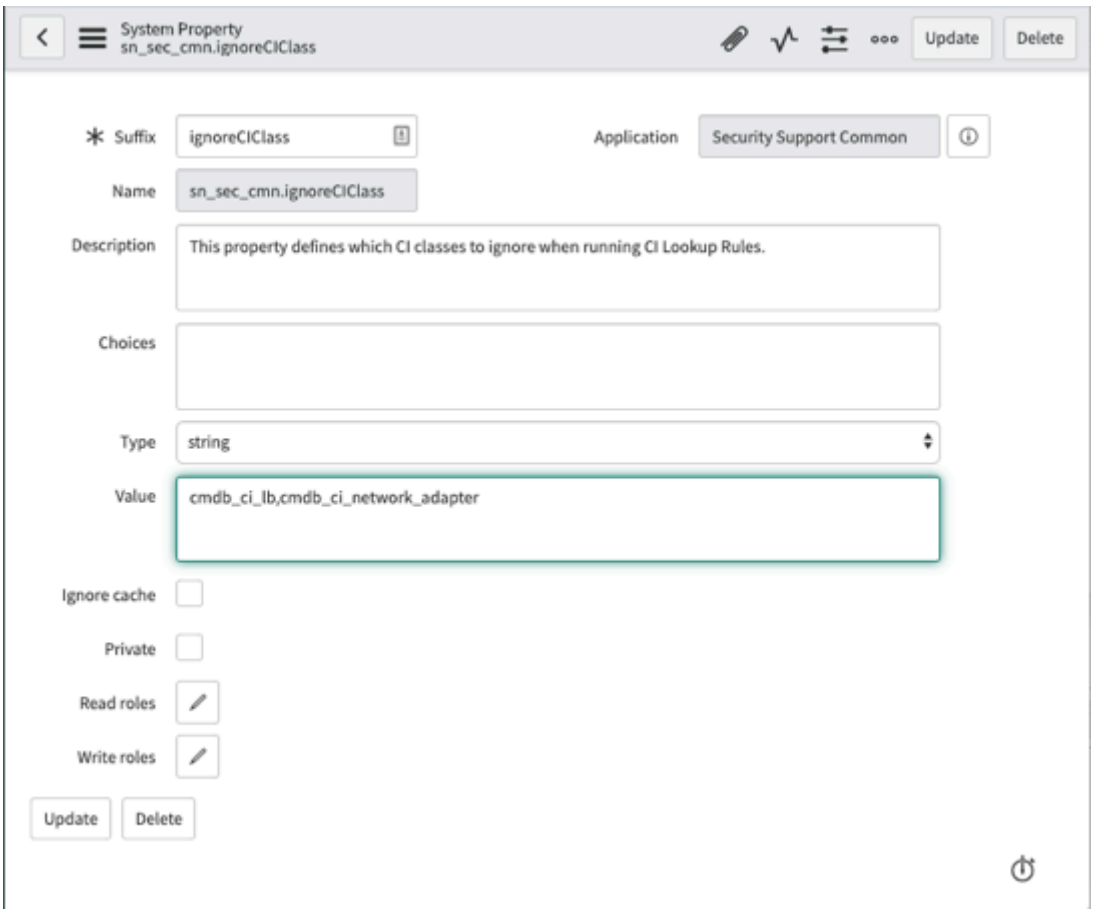
Nota:

A propriedade do sistema **ignoreCIClass** está disponível a partir da Resposta a vulnerabilidades v9.0. No entanto, a funcionalidade da propriedade não está disponível no upgrade de qualquer versão anterior.

Se você tiver atualizado de qualquer aplicação Operações de segurança, anterior à versão 9.0, consulte KB0788209 para obter instruções sobre como habilitar essa funcionalidade.

Procedimento

1. Insira `sys_properties.list` na barra de navegação à esquerda.
2. Clique **em Enter**.
3. No menu **Pesquisar**, em **Nome**, insira `sn_sec_cmn.ignoreCIClass`.
4. Na caixa de texto **Valor**, insira as classes de IC a serem excluídas em uma lista separada por vírgulas.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Atualizar**.
   Esta lista é usada pelas Regras de pesquisa de IC durante a próxima importação. Itens vulneráveis criados durante a importação não são associados a um IC de nenhum tipo listado no campo **Valor** da propriedade do sistema `sn_sec_cmn.ignoreCIClass`.

Filtrar ICs desativados

Filtrar itens de configuração (ICs) desativados ao executar as regras de pesquisa de IC. Para filtrar ICs desativados ao executar as regras de pesquisa de IC do CMDB das Operações de segurança, defina a propriedade do sistema **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] como verdadeira.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
O valor padrão da propriedade do sistema é verdadeiro. Esta propriedade só se aplica a regras de pesquisa de IC em Resposta a vulnerabilidades e não afeta a lógica de pesquisa do IRE.

Procedimento

1. Insira `sys_properties.list` na barra de navegação à esquerda.
2. Selecione **Enter**.
3. No menu **Pesquisar**, em **Nome**, insira `sn_sec_cmn.filterOutDecommissionedCI` para filtrar os ICs desativados.
4. Na caixa de texto **Valor**, insira o valor verdadeiro ou falso.
   O valor padrão é verdadeiro.
5. Selecione **Atualizar**.
   Este valor é usado pelas Regras de pesquisa de IC durante a próxima importação. A propriedade do sistema `sn_sec_cmn.filterOutDecommissionedCI` filtra os ICs desativados ao executar essas regras de pesquisa.

Promover ICs automaticamente

Edite a cadeia de caracteres JSON na propriedade do sistema **autoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] para que as regras de pesquisa de item de configuração (IC) promovam automaticamente todos os ICs do CMDB das Operações de segurança para entradas correspondentes na tabela [cmdb_ci].

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
O tipo de propriedade do sistema é "cadeia de caracteres" e requer que você insira uma cadeia de caracteres JSON. Esta propriedade é ativada por padrão e promove ICs correspondentes ao executar as regras de pesquisa de IC.

Scripts de pesquisa personalizados podem retornar registros de tabela secundária do script. Para esta propriedade, a função *`_autoPromoteCI`* no *`CIIdentify Script Include`* usa o IC retornado pelo script de pesquisa e percorre automaticamente os relacionamentos para chegar à entrada *`cmdb_ci`* e retorná-la.

Para substituir a lógica de promoção automática, ou seja, para adicionar ou atualizar novas classes de IC, adicione o objeto JSON no campo Valor na propriedade do sistema [**sn_sec_cmn.autoPromoteFields**].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Insira `sys_properties.list` na barra de navegação à esquerda.
2. Selecione **Enter**.
3. Localize a propriedade do sistema `[`**sn_sec_cmn.autoPromoteFields**`]` e selecione o registro para abri-lo.

   Cadeia de caracteres padrão:

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. Na caixa de texto **Valor**, edite a cadeia de caracteres usando o formato de emparelhamento padrão.
5. Selecione **Atualizar**.
   Este valor é usado pelas Regras de pesquisa de IC durante a próxima importação.

Configurar a chave de item vulnerável

Configure a granularidade da chave do item vulnerável (VI) na aplicação Resposta a vulnerabilidades para definir o que torna um item vulnerável (VI) em sua organização.

Antes de Iniciar

Função necessária: administrador
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Termos-chave:

IC (Configuration Item, item de configuração)

Um ativo existente listado no seu CMDB.

Vulnerabilidade

Um registro de uma vulnerabilidade conhecida importada do Instituto Nacional de Padrões e Tecnologia (NIST), Banco de Dados Nacional de Vulnerabilidade (NVD), Vulnerabilidades e exposições comuns (CWE) ou integrações de terceiros com Resposta a vulnerabilidades.

Item vulnerável

Um item vulnerável é criado quando uma vulnerabilidade importada corresponde a um item de configuração no seu CMDB.

Detecção

Uma ocorrência única e distinta de uma vulnerabilidade conforme relatada pelos scanners de suas integrações de terceiros. As detecções são importadas e exibidas nos registros de detecção e de item vulnerável em sua instância. Também conhecido como Detecção de item vulnerável.

Por padrão, um item vulnerável é uma combinação exclusiva de um item de configuração (IC), uma vulnerabilidade e uma instância de integração. Para criar itens vulneráveis com

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mais granularidade, adicione portas exclusivas de detecções de itens vulneráveis para ajudá-lo a gerenciar a correção de vulnerabilidades no nível que você considera mais eficaz para sua organização.

Se você quiser criar itens vulneráveis com mais granularidade, configure a chave do item vulnerável para que ela inclua a porta. Quando a porta Incluir está habilitada, os itens vulneráveis são criados por portas exclusivas a partir das detecções de itens vulneráveis.

A partir da Resposta a vulnerabilidades V17.1, você pode identificar e corrigir vulnerabilidades do Rapid7 adicionando a prova como a chave VI. Para obter mais informações, consulte Como adicionar prova às chaves de item vulnerável do Rapid7.

Escolha uma opção na tabela a seguir para habilitar a opção Incluir porta.

Três cenários para habilitar a opção Incluir porta com a chave VI pela primeira vez

Se...	Descrição
Uma ou mais das seguintes condições são verdadeiras: • Você está atualizando de uma versão do Resposta a vulnerabilidades anterior à v10.0 que não era compatível com detecções de itens vulneráveis. • Você é um novo cliente e não tem dados da Resposta a vulnerabilidades (itens vulneráveis ou detecções de itens vulneráveis) em sua instância Now Platform®. • Você já excluiu todos os registros de item vulnerável e dados relacionados em sua instância e está pronto para criar todos os dados da Resposta a vulnerabilidades, começando com uma nova importação para incluir IVs diferenciados por uma porta exclusiva.	Habilite a Porta de inclusão. Depois que a porta de inclusão estiver habilitada, as detecções importadas criarão itens vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.
Ambas as condições são verdadeiras: • Você tem a v10.0 ou posterior de Resposta a vulnerabilidades e tem dados existentes da Resposta a vulnerabilidades (itens vulneráveis ou detecções de itens vulneráveis) em sua instância que deseja preservar. • Você deseja começar a criar novos itens vulneráveis para incluir IVs diferenciados por uma porta exclusiva.	Habilite a porta de inclusão. Suas detecções existentes e os itens vulneráveis associados serão preservados. Depois que a porta de inclusão estiver habilitada, novas detecções criarão novos itens vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.
Ambas as condições são verdadeiras: • Você tem a v10.0 ou posterior de Resposta a vulnerabilidades. • Você tem dados existentes da Resposta a vulnerabilidades (itens vulneráveis ou	**1.** Exclua todos os registros de item vulnerável e dados relacionados da sua instância. **2.** Habilite a porta de inclusão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Três cenários para habilitar a opção Incluir porta com a chave VI pela primeira vez

Se...	Descrição
detecções de itens vulneráveis), mas não deseja preservar os dados existentes, pois prefere criar os dados de vulnerabilidade a partir de uma nova importação e deseja incluir IVs diferenciados por uma porta exclusiva.	Depois que a porta de inclusão estiver habilitada, novas detecções criarão novos itens vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.

Nota:

Se a opção Incluir porta estiver habilitada, mais de um item vulnerável poderá ser criado para um item de configuração. Por exemplo, se houver uma vulnerabilidade para duas portas em um item de configuração, portas 80 e 443, dois IVs exclusivos serão criados, um para cada porta começando com a próxima importação.

Nota: Certifique-se de criar IVs para incluir VIs por portas exclusivas antes de habilitar este recurso. Depois de habilitar a chave VI para incluir a porta, você deve primeiro excluir os dados da Resposta a vulnerabilidades antes de desabilitar a porta Incluir e retornar à importação de dados de vulnerabilidade usando a granularidade de chave VI padrão, ou seja, em que os IVs são criados para a porta, mas não são diferenciados por uma porta exclusiva. Para obter mais informações sobre como excluir seus dados de vulnerabilidade, consulte Excluir todos os registros de itens vulneráveis e dados relacionados em Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV**.

   O campo Última atualização exibe a data em que a chave VI foi configurada pela última vez.

2. Clique na caixa de seleção Incluir porta para habilitá-la.

3. Clique em **Salvar**.
   A caixa de diálogo Confirmação é exibida.

   Se você não tiver registros de detecção de item vulnerável em sua instância, as detecções de item vulnerável e os itens vulneráveis serão criados por porta exclusiva, começando com sua próxima importação.

   Se você tiver detecções de item vulnerável e itens vulneráveis em sua instância, as detecções existentes e os itens vulneráveis associados serão preservados. Novas detecções criam novos vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.

O que Fazer Depois

Verifique se os itens vulneráveis por porta são exibidos na detecção de itens vulneráveis e nos registros de itens vulneráveis. Para obter mais informações, consulte Exibir Resposta a vulnerabilidades dados de detecção de itens vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como adicionar prova às chaves de item vulnerável do Rapid7

Adicione a prova como uma chave de item vulnerável (VI) para os Rapid7 VIs. Incluir a prova de vulnerabilidades específicas permite que a integração do scanner Rapid7 crie IVs para cada prova recebida de Rapid7.

Uma chave de VI é a combinação de vulnerabilidade, item de configuração (IC) e instância de integração. Dividir as detecções em diferentes VIs com base na prova cria vários IVs. Você pode atribuir as vulnerabilidades aos proprietários de correção apropriados.

Por exemplo, pode haver duas detecções com a mesma vulnerabilidade e IC, mas com provas diferentes, levando à criação de um IV. A partir da Resposta a vulnerabilidades V17.1, você pode identificar e corrigir vulnerabilidades adicionando provas como a chave VI.

Você pode adicionar a prova como uma chave VI da seguinte forma:

Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV** e selecione a opção para incluir prova.

Caso de uso: inclusão de prova na chave VI para VIs existentes ou divisão de VIs existentes com base na prova de detecção

Para criar IVs com base em provas, você pode usar as vulnerabilidades log4j do R7. Por exemplo, você pode usar uma das várias vulnerabilidades log4j do R7, como `R7-apache-log4j-core-cve-2021-44228`, `R7-amazon_linux-cve-2021-44228` ou `R7-amazon-linux-ami-2- cve-2021-44228`.

Se todas as detecções em um VI tiverem a mesma prova, o VI existente será atualizado para incluir "Prova na chave de VI (external_id)". Se houver várias detecções com provas diferentes, o VI existente será encerrado. As detecções são divididas nos novos IVs com "Prova na chave de VI (external_id)".

Nota:

Se você fornecer o ID da vulnerabilidade, os IVs existentes serão divididos com base na prova. As novas vulnerabilidades para este ID de vulnerabilidade também têm a prova como uma das chaves VI.

Excluir todos os registros de itens vulneráveis e dados relacionados em Resposta a vulnerabilidades

Remova permanentemente todos os dados da Resposta a vulnerabilidades (itens vulneráveis ou detecções de itens vulneráveis) e dados e registros relacionados da aplicação Resposta a vulnerabilidades em sua instância Now Platform®.

Antes de Iniciar

Exclua registros de detecção de item vulnerável, itens vulneráveis, grupos de vulnerabilidades e todos os registros relacionados na aplicação Resposta a vulnerabilidades da sua instância. Use este processo para limpar sua instância para importar dados com um novo início de suas integrações de terceiros ou, como um pré-requisito para retornar a configuração de chave do item vulnerável (VI) à sua configuração padrão. Para obter mais informações sobre como configurar a chave VI, consulte Configurar a chave de item vulnerável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esta ação exclui todos os registros de itens vulneráveis e todos os dados relacionados da sua instância. Depois de excluídos, esses dados não podem ser recuperados. Ele também requer que você suspenda a importação de dados e desabilite suas integrações ativas de terceiros com Resposta a vulnerabilidades.

É necessário excluir os dados do item vulnerável com este processo antes de alterar a configuração da chave VI. A remoção de todos os dados garante que todos os itens vulneráveis e detecções de itens vulneráveis sejam mapeados e atualizados com os dados mais atuais, começando com a próxima importação.

Verifique se as seguintes condições se aplicam antes de excluir seus dados:

- Você tem a v10.0 ou posterior de Resposta a vulnerabilidades instalada. Para obter mais informações, consulte Resposta a vulnerabilidades detecções de itens vulneráveis de integrações de terceiros.
- Você deseja desabilitar a porta de inclusão e retornar a configuração da chave VI à sua configuração padrão.
- Você tem itens vulneráveis existentes e detecções de itens vulneráveis, mas não deseja ou precisa atualizá-los e mantê-los.
- Você determinou que deseja remover todos os dados existentes da Resposta a vulnerabilidades e registros relacionados para limpar sua instância.

Função necessária: sn_vul.vulnerability_admin

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Integrações de Vulnerabilidade**.
2. Registre todas as integrações ativas exibidas.

   Todas as integrações ativas listadas com trabalhos agendados são desabilitadas antes da exclusão de todos os itens vulneráveis e dados relacionados para que nenhum dado novo seja importado durante a remoção de dados. Registrar esta lista ajuda a ativar suas integrações após a conclusão da exclusão.

3. Revise o artigo Como excluir dados de resposta a vulnerabilidades existentes para reimportação na Base de conhecimento HI.
4. Se for exibida uma mensagem de aviso que o impeça de gravar na coluna Ativo, para desabilitar integrações ativas, siga estas etapas.

   a. Na coluna Nome, clique em um item para abrir o registro.

   b. Se você não puder editar a caixa de seleção Ativo, clique no link **aqui** para editar o registro.

   c. Clique na caixa de seleção **Ativo** para desabilitar a integração e cancelar o próximo trabalho agendado.

   d. Clique em **Atualizar** para salvar suas mudanças e retornar à lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Verifique se você desativou todas as integrações ativas da lista Integrações.
Depois de desabilitar uma integração, ela não será mais exibida na lista de integrações ativas. Para exibir uma lista de integrações inativas e localizar todas as integrações que você desativou após excluir todos os dados de vulnerabilidade, na coluna Ativa na parte superior, insira `=false`.

5. Continue com as etapas no artigo da base de conhecimento para excluir seus dados de vulnerabilidade existentes.
6. Depois de confirmar que todos os dados foram excluídos com sucesso, navegue até **Resposta a vulnerabilidades** > **Administração** > **Configurar granularidade de IV**.
7. No formulário:
   - Se você excluiu dados porque prefere criar seus dados de vulnerabilidade para incluir a porta de uma nova importação, habilite Incluir porta e clique em **Salvar**.
   - Se você excluiu dados porque deseja retornar a chave VI à sua configuração padrão, desabilite Incluir porta e clique em **Salvar**.

   Para obter mais informações, consulte Configurar a chave de item vulnerável.

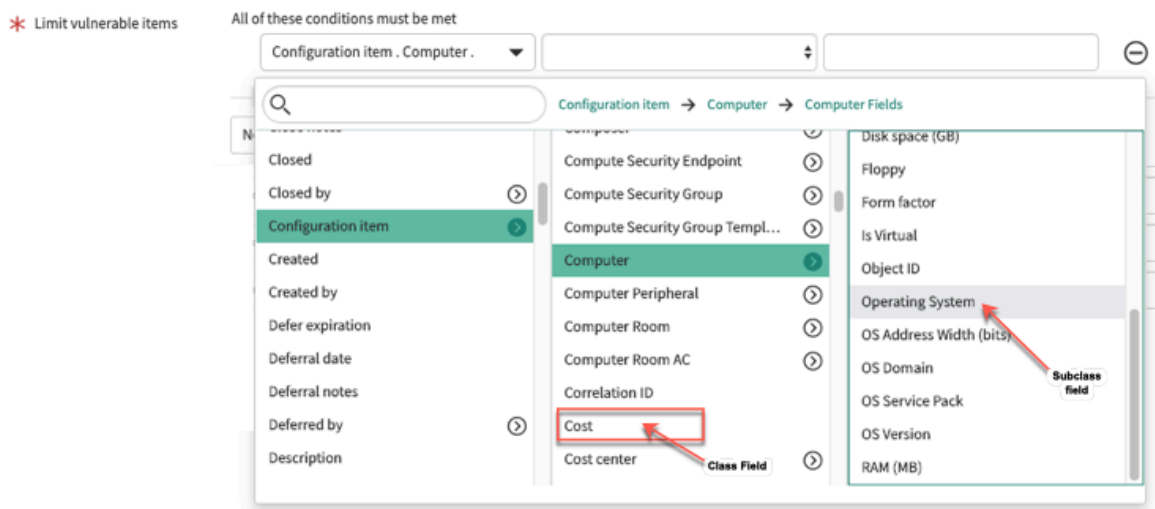
Filtrando em Resposta a vulnerabilidades

Regras de tarefa de correção, calculadoras e regras de atribuição usam condições durante a importação, criadas usando o **Construtor de condições**. As mudanças nos critérios podem afetar o desempenho, já que cada registro é avaliado usando esses filtros.

As regras e calculadoras enviadas com o sistema base são otimizadas para desempenho. A edição ou criação de regras ou calculadoras é cuidadosa e pode exigir a experiência de ServiceNow e Resposta a vulnerabilidades.

Evite filtrar com base em campos de subclasse

Algumas tabelas oferecem suporte à extensão. Um exemplo disso é a tabela IC do CMDB [cmdb_ci]. Tabelas como cmdb_ci_hardware e cmdb_ci_computer estendem esta tabela. Se você filtrar com base em um campo que não está na tabela primária, esse filtro pode ser caro para construir e avaliar.



Por exemplo, filtrar em **Item de Configuração** > **Custo** não afetaria negativamente o desempenho porque **Custo** é um campo de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

classe, e não um campo de subclasse, do **Item de configuração**.

Item de Configuração > **Computador**, no entanto, é uma subclasse que requer uma referência com pontos para outro campo, neste caso, **Sistema operacional**. Esse processo pode levar muitos milissegundos, o que aumenta rapidamente quando milhões de itens vulneráveis estão sendo importados e afetam o desempenho.

Nota: O uso da condição [contém] é como uma pesquisa de caracteres curinga e pode causar impacto no desempenho. Usar [is], sempre que possível, é mais eficiente.

Mapeamento de gravidade para Resposta a vulnerabilidades

A Resposta a vulnerabilidades é fornecida com o Banco de dados nacional de vulnerabilidades (NVD) para o mapeamento de severidade normalizado da ServiceNow. As integrações de terceiros da ServiceNow fornecem mapeamentos de gravidade após a instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

Mapeamento de gravidade da integração de vulnerabilidade da Rapid7

Normalized_Severity

Calcule normalised_severity na entrada de terceiros usando a severidade proveniente da tabela **sn_vul_nvd_entry**. Isso é definido usando Regras de negócio para severidade normalizada de pesquisa na tabela **sn_vul_entry**.

Source_severity

Os dados da tabela **sever_score** são mapeados para a tabela **source_severity** enquanto a **API Rapid7 Vulnerability Integration-** está em execução.

Prioridade

Este campo está vazio.

Mapeamento de severidade de integração de vulnerabilidade da Qualys

Normalized_Severity

Calcule normalised_severity na entrada de terceiros usando a severidade proveniente da tabela **sn_vul_nvd_entry**. Isso é definido usando Regras de negócio para severidade normalizada de pesquisa na tabela **sn_vul_entry**.

Source_severity

Os dados de **SEVERITY_LEVEL** são mapeados para a tabela **source_severity** enquanto a **integração da base de conhecimento da Qualys** está em execução.

Prioridade

Os dados do campo Prioridade são obtidos da **tabela SEVERIDADE** e mapeados para a tabela de **prioridade** enquanto a **Integração de detecção de host da Qualys** está em execução usando a regra de negócio mapeada para os dados da Qualys.

Nota: As regras de negócio são executadas em segundo plano e verificam a prioridade da Qualys e, consequentemente, mapeiam a prioridade. Portanto, para mapear os dados da Qualys, BR é responsável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de gravidade da integração de vulnerabilidade da Tenable.io

Normalized_Severity

Calcule normalised_severity na entrada de terceiros usando a severidade proveniente da tabela **sn_vul_nvd_entry**. Isso é definido usando Regras de negócio para severidade normalizada de pesquisa na tabela **sn_vul_entry**.

Source_severity

Os dados da **tabelarisk_factor** são mapeados para a tabela **source_severity** enquanto a integração do **plug-in Tenable.io** está em execução.

Prioridade

Os dados de **sever_id** são mapeados para **source_severity** enquanto a **Integração de vulnerabilidades abertas da Tenable.io** está em execução.

VPR

Os dados da **pontuação** são mapeados para **Source_risk_score** enquanto **a integração de plug-in Tenable.io** está em execução.

Os dados de **Calculated from score** são mapeados para **Source_risk_rating** enquanto **a integração de plug-in Tenable.io** está em execução.

Mapeamento de gravidade da integração de vulnerabilidade da Tenable.sc

Normalized_Severity

Calcule **normalised_severity** na entrada de terceiros usando a severidade proveniente da tabela sn_vul_nvd_entry. Isso é definido usando Regras de negócio para severidade normalizada de pesquisa na tabela **sn_vul_entry**.

Source_severity

Os dados da **tabelariskFactor** são mapeados para **source_severity** enquanto a integração do **plug-in Tenable.io** está em execução.

Prioridade

Dados de **gravidade** recebidos como **"severity": { "id": "0", "name": "Info", "description": "Informative" }** são mapeados para **source_severity** enquanto a **Integração de vulnerabilidades abertas da Tenable.io** está em execução.

VPR

Os dados do **vprScore** são mapeados para **Source_risk_score** enquanto **a integração de plug-in Tenable.io** está em execução.

Os dados de **Calculated from vprScore** são mapeados para **Source_risk_rating** enquanto **a integração de plug-in Tenable.io** está em execução.

Mapeamento de gravidade do TVM

Normalized_Severity

Calcule normalised_severity na entrada de terceiros usando a gravidade proveniente da tabela **sn_vul_nvd_entry**. Isso é definido usando Regras de negócio para severidade normalizada de pesquisa na tabela **sn_vul_entry**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Source_severity

Os dados da tabela de **gravidade** são mapeados para **source_severity** enquanto a integração do **Microsoft TVM Vulnerability (CVE)** está em execução.

Prioridade

Este campo está vazio.

Criar um Resposta a vulnerabilidades mapa de severidade

Resposta a vulnerabilidades mapeamento de severidade transforma campos de severidade de origem de terceiros em campos reconhecíveis em Resposta a vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades é fornecido com o banco de dados nacional de vulnerabilidades (NVD) para mapeamento de severidade ServiceNow normalizado. ServiceNow integrações de terceiros, como Qualys Vulnerability Integration, fornecem mapeamentos de gravidade após a instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

A criação ou edição de um mapa de severidade se destina somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Mapeamento de gravidade normalizada**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Mapeamento de campo

Campo	Descrição
Origem	O nome da origem do mapeamento de gravidade.
Valor de origem	O valor da severidade de origem.
Valor de meta	O valor da severidade desejada. As opções são: ◦ 1- Crítica ◦ 2 - Alto ◦ 3 – Médio ◦ 4 - Baixo(a) ◦ 5 - Nenhum

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Repita a Etapa 3 para cada nível de severidade de origem.
5. Clique em **Enviar**.

Definir classificações de serviço para Resposta a vulnerabilidades relatórios e listas relacionadas

Traga mais foco para a emissão de relatórios e listas relacionadas em Resposta a vulnerabilidades definindo classificações de serviço. Além disso, a redução do número de classificações de serviço solicitadas pode melhorar o desempenho da Resposta a vulnerabilidades coleta de dados.

Antes de Iniciar
Função necessária: administrador

Nota:

A edição de propriedades do sistema requer conhecimento de ServiceNow e Resposta a vulnerabilidades.

Procedimento

1. Insira `sys_properties_list.do` na barra de navegação à esquerda.
2. Clique **em Enter**.
3. No menu **Pesquisar**, em **Nome**, insira `sn_vul.service_classifications`.
4. Abra a propriedade do sistema *`sn_vul.service_classifications`*.
5. Na caixa de texto **Valor**, insira a lista separada por vírgulas das classificações de serviço desejadas.

   Nota: Quando esta configuração está vazia, todos os serviços são listados.

   Exemplos:

   Para ver Serviços de negócio, Serviços técnicos e Serviços de aplicações e excluir Ofertas de serviço, Serviços compartilhados e serviços não classificados, defina o valor como: **Serviço de negócio, Serviço técnico, Serviço de aplicações**.

   Para ver os Serviços de aplicações, defina o valor como: **Serviço de aplicações**.

6. Clique em **Atualizar**.
   Os dados em cada relatório e lista relacionada a itens vulneráveis são filtrados pela classificação de serviço durante a próxima execução do trabalho de análise de desempenho noturno.

Auditar campos selecionados na tabela de itens vulneráveis

Habilite a auditoria para os campos especificados na tabela Item vulnerável [sn_vul_vulnerable_item]. Este método de auditoria é útil quando você deseja auditar campos que não podem ser auditados por padrão.

Antes de Iniciar
Função necessária: administrador

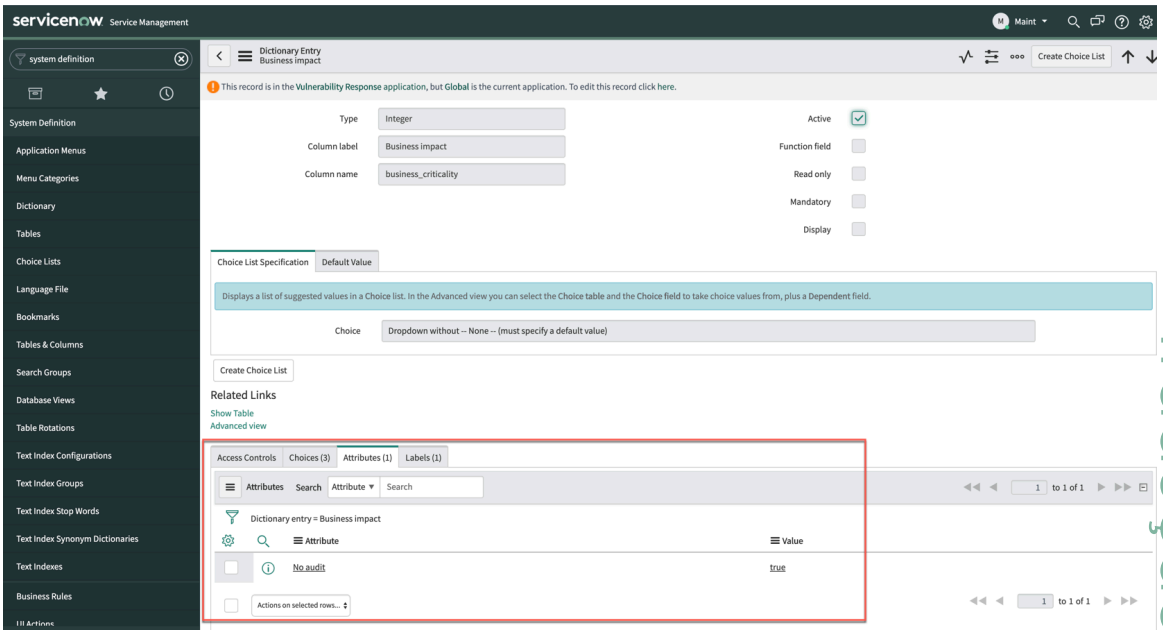
Por Que e Quando Desempenhar Esta Tarefa
A tabela sn_vul_vulnerable_item é auditável por padrão. Campos que têm o atributo no_audit definido como verdadeiro não são auditáveis. Para obter mais informações sobre como auditar tabelas, consulte Habilitar auditoria para uma tabela .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Definição do Sistema** > **Tabelas** e pesquise a tabela sn_vul_vulnerable_item.
   A lista de entradas de dicionário para a tabela é exibida.
2. Para habilitar a auditoria de um campo, clique no nome da entrada.
   A página Entrada de Dicionário dessa entrada é exibida.



3. Navegar até **Atributos** > **Sem auditoria**.
   A página Atributo do dicionário é exibida.
4. Para remover o atributo no audit=true, clique em **Excluir**.
   A auditoria para este campo está habilitada.

Resposta a vulnerabilidades configuração da estrutura de trabalho em segundo plano

Defina a estrutura de trabalho em segundo plano na sua instância Now Platform®. Essas mudanças de configuração podem ajudar a melhorar o desempenho, reduzindo a quantidade de recursos do sistema usados para executar seus trabalhos em segundo plano.

O que você pode editar na estrutura de trabalho em segundo plano

Com o módulo de configuração de trabalho em segundo plano, você tem as seguintes opções de configuração na estrutura:

- Você pode definir o número de trabalhos em segundo plano que são executados simultaneamente para Resposta a vulnerabilidades processos.
- Para trabalhos longos que são executados em segundo plano e processam grandes quantidades de dados, você pode criar partições para processar dados em blocos menores.
- Você pode cancelar um trabalho.

Por que configurar a estrutura de trabalho em segundo plano

Os trabalhos em segundo plano em seu Now Platform® foram projetados para serem executados por longos períodos de tempo para executar vários processos em seus registros em Resposta a vulnerabilidades. Esses trabalhos eram baseados anteriormente em regras

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de negócio que são executadas de forma assíncrona. Não há limite para o número desses trabalhos que podem ser executados em segundo plano em sua instância para que as grandes quantidades de registros afetados por esses trabalhos possam ser processadas. Quando vários trabalhos que demoram muito para serem concluídos são executados simultaneamente em segundo plano, os recursos do sistema usados para executar os trabalhos agendados são afetados, o que, por sua vez, pode afetar negativamente o desempenho.

Configurar a estrutura de trabalho em segundo plano pode ajudar a melhorar seu desempenho, reduzindo a quantidade de recursos do sistema usados para executar seus trabalhos em segundo plano.

Termos principais

Capacidade do trabalho

Descreve os trabalhos específicos. Por exemplo, um trabalho específico pode incluir os seguintes recursos:

- O trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo.
- O trabalho pode ser particionado.
- O trabalho pode ser cancelado durante a execução.

Simultaneidade

Refere-se a trabalhos ou partes de trabalhos que são executados em paralelo.

Partição

As partições são partes de trabalhos que podem ser divididas para que possam ser processadas em paralelo para obter melhor desempenho. Geralmente se refere a trabalhos com tempos de execução longos.

Configuração do trabalho

Refere-se às configurações de um trabalho agendado específico.

Trabalho agendado

Trabalhos agendados são trabalhos automatizados que podem ser realizados em um horário específico ou em uma programação recorrente.

Recursos do sistema

Refere-se à quantidade de recursos do sistema para os quais você deve oferecer suporte a um determinado número de trabalhos em segundo plano e trabalhos agendados em seu ambiente.

Propriedade do sistema

As propriedades do sistema armazenam informações de configuração que raramente ou nunca mudam. Cada vez que você altera ou adiciona uma propriedade do sistema, o sistema limpa o cache para manter todos os nós no cluster sincronizados. Essa limpeza de cache afeta o desempenho.

Regra de negócio

Uma regra de negócio é um script do lado do servidor que é executado quando um registro é exibido, inserido, atualizado ou excluído, ou quando uma tabela é consultada. As regras de negócios realizam tarefas como alterar valores automaticamente em campos de formulário quando determinadas condições são atendidas ou criar eventos para notificações por e-mail e ações de script.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

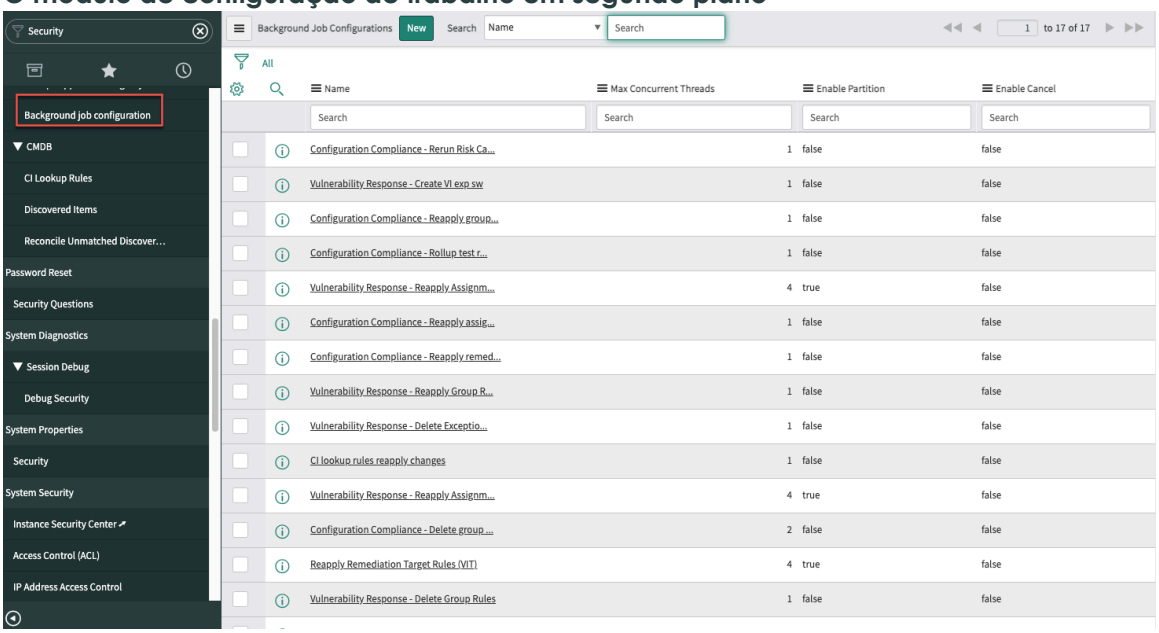
Caso de uso para definir a estrutura de trabalho em segundo plano

Por exemplo, o trabalho em segundo plano que aplica regras de destino de correção para registros de itens vulneráveis (VITs) e registros de itens vulneráveis da Resposta a vulnerabilidades da aplicação (AVITs) processa simultaneamente grandes quantidades de registros com várias tarefas.

Dependendo do tamanho da importação e do número de registros que você tem em seu ambiente, este trabalho pode usar uma grande quantidade de recursos do sistema disponíveis e levar muito tempo para ser concluído com sucesso. Os trabalhos de manutenção do sistema ou outros trabalhos agendados podem ser executados mais lentamente.

No módulo de configuração de trabalho em segundo plano, os trabalhos são listados por nome e um ID de configuração exclusivo. Nesses registros, você pode definir quantas tarefas deseja executar simultaneamente para um determinado trabalho em segundo plano. Você também pode definir o trabalho para processar partições de dados para que as tarefas sejam concluídas com mais rapidez e facilidade e usem menos recursos do sistema. Você também pode cancelar um trabalho se determinar que ele está sendo executado por muito tempo.

O módulo de configuração de trabalho em segundo plano



Para obter mais informações sobre as etapas necessárias para definir as configurações do trabalho em segundo plano, consulte Definir configurações de trabalho em segundo plano no Resposta a vulnerabilidades.

Definir configurações de trabalho em segundo plano no Resposta a vulnerabilidades

Defina quantas tarefas você deseja executar simultaneamente para um determinado trabalho em segundo plano. Você também pode definir o trabalho para importar partições de dados para que as tarefas sejam concluídas com mais rapidez e facilidade e usem menos recursos do sistema. Você também pode cancelar um trabalho se determinar que ele está sendo executado por muito tempo.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou gerenciadores de vulnerabilidade com a função granular sn_sec_cmn.manage_background_job

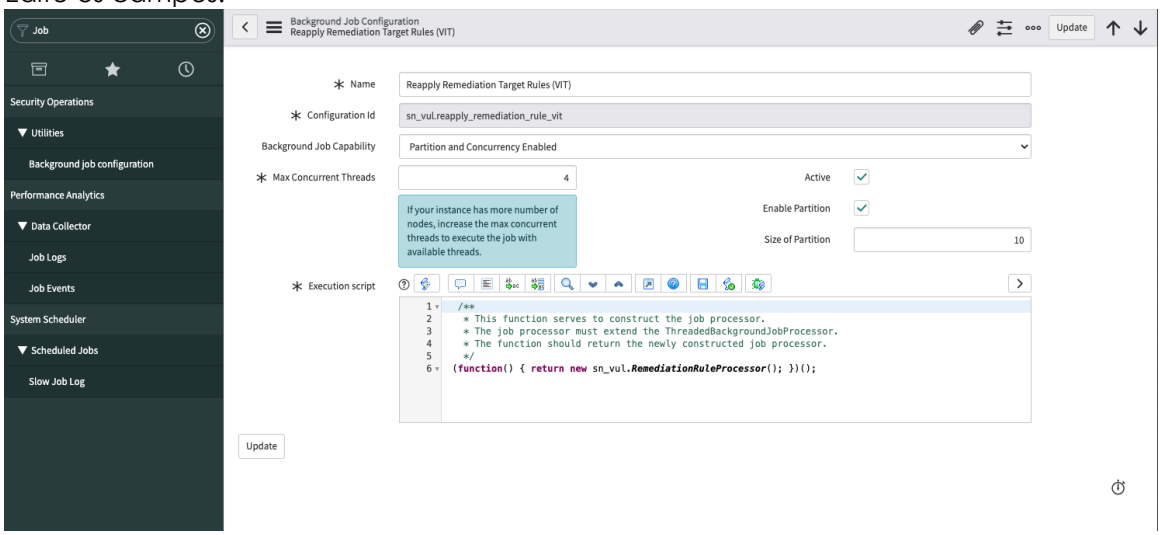
Consulte a seção abaixo das etapas para obter um exemplo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Configurações de trabalho em segundo plano**.
2. Na coluna Nome, clique em um registro para abri-lo.
3. Edite os campos.



Campo	Descrição
Nome	Nome do trabalho.
ID da configuração	Somente leitura. ID exclusivo usado para identificar o trabalho.
Capacidade de trabalho em segundo plano	Escolha um. ◦ Partição e simultaneidade habilitadas - Um trabalho com um longo tempo de execução pode ser dividido e o trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo. ◦ Simultaneidade habilitada — O trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo. ◦ Cancelamento habilitado — O trabalho pode ser cancelado. ◦ Simultaneidade e cancelamento habilitados — O trabalho pode ser executado em paralelo com outro trabalho e ser cancelado. ◦ Partição, simultaneidade e cancelamento habilitados — Um trabalho com tempo de execução longo pode ser dividido, o trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo e o trabalho pode ser cancelado. ◦ Classe primária1

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor exibido indica se um trabalho oferece suporte ao particionamento, simultaneidade e cancelamento.
Máximo de threads simultâneos	Este campo será exibido somente se a simultaneidade for compatível. Insira o número máximo de trabalhos que você deseja que esta configuração execute em paralelo. O número de trabalhos agendados compatíveis com sua instância é, por padrão, 10. Você pode diminuir esse valor se achar que pode usar ou tem recursos do sistema inferiores disponíveis para executar seus trabalhos em segundo plano.
Ativo	Habilitar ou desabilitar o trabalho Se um trabalho estiver desabilitado, você não poderá criar trabalhos desse tipo. Os trabalhos existentes na fila não serão processados.
Habilitar partição	Este campo será exibido somente se o particionamento for compatível. Esta opção permite limitar e definir o número de itens que este trabalho pode processar de uma só vez. O campo Tamanho da partição também é exibido. Se você deixar este campo desabilitado, os trabalhos em segundo plano que oferecem suporte ao particionamento processarão todos os itens em sua instância com este trabalho.
Tamanho da partição	Este campo será exibido somente se o particionamento for compatível. O padrão é 10.000 itens. Insira um valor para o número de itens por bloco de dados que você deseja que este trabalho processe. Esta opção está disponível para trabalhos que processam um grande número de registros, como IVs, tarefas de correção, resultados de testes e grupos de resultados de testes.
Script de execução	Exibe o processador de trabalho usado para executar este trabalho. É fornecido um método padrão para trabalhos que oferecem suporte ao particionamento.
Habilitar cancelamento	Este campo só será exibido se o cancelamento do trabalho for compatível. Esta op-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	ção é compatível com trabalhos que processam itens descobertos e reaplicam regras de IC.

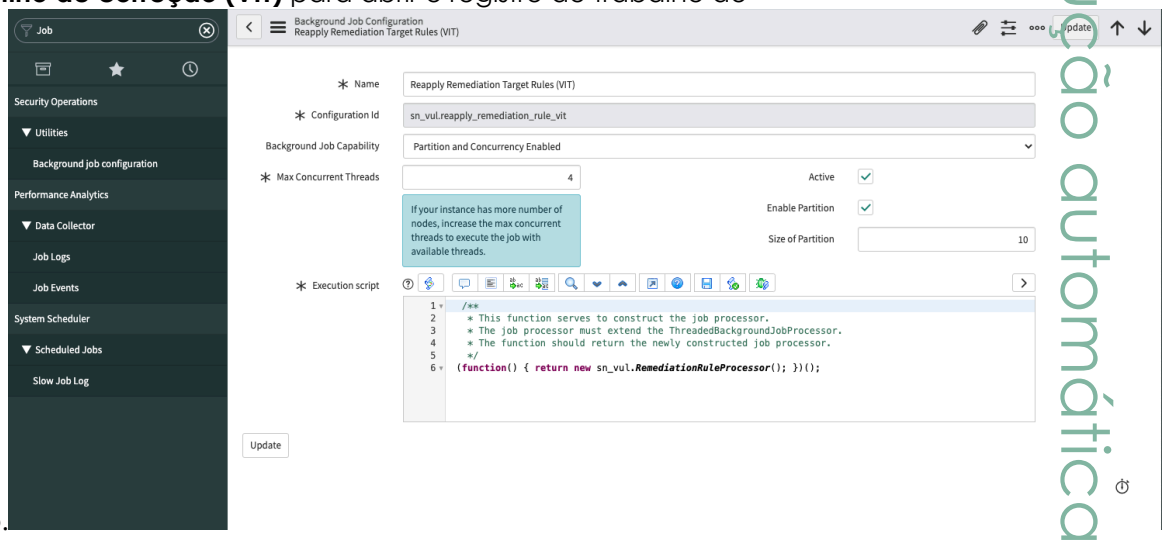
4. Clique em **Atualizar** para salvar suas mudanças.
   Consulte o exemplo a seguir para saber como verificar os resultados das mudanças de configuração.

   Há duas configurações de trabalho de Regras de meta de correção incluídas na aplicação, uma para itens vulneráveis e uma para itens vulneráveis de aplicação:

   - Reaplicar regras de destino de correção (VIT)
   - Reaplicar regras de destino de correção (AVIT)

   Suponha que você mude para as regras de destino de correção e queira reaplicá-las sem usar a maioria dos recursos de processamento do sistema disponíveis. Para ajudá-lo a limitar os recursos de processamento, você pode controlar o número de trabalhos em segundo plano executados e o número de itens processados por trabalho no módulo Configurações de trabalho em segundo plano.

5. Para definir essas configurações, navegue até **Operações de segurança** > **Configurações de trabalho em segundo plano** e clique em **Reaplicar regras de destino de correção (VIT)** para abrir o registro do trabalho de configuração.

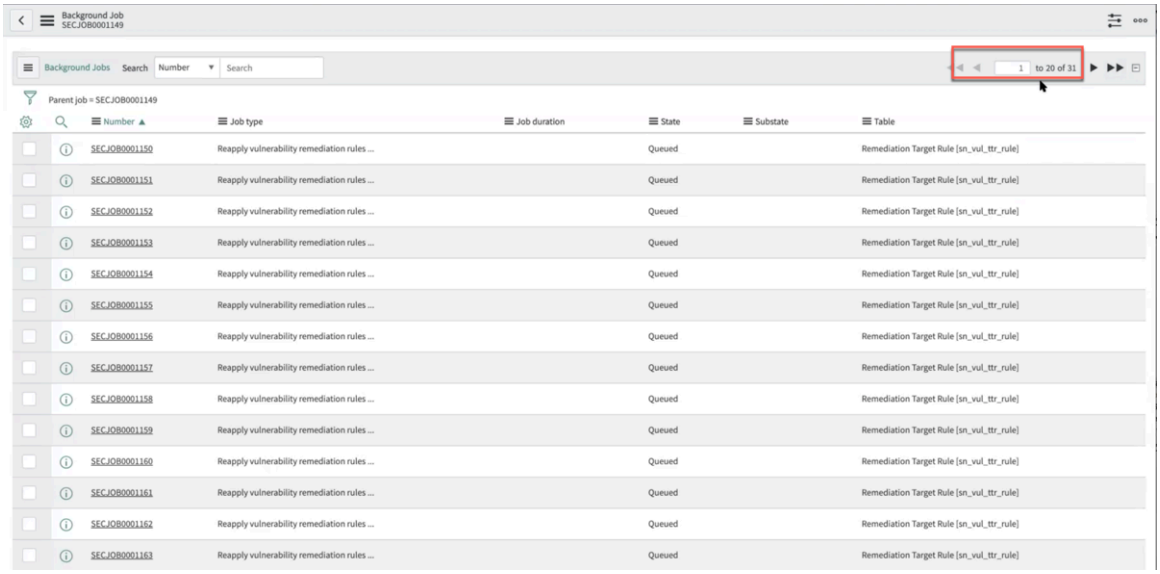


   Para fins de exemplo, digamos que você saiba que tem pouco mais de 300 IVs.

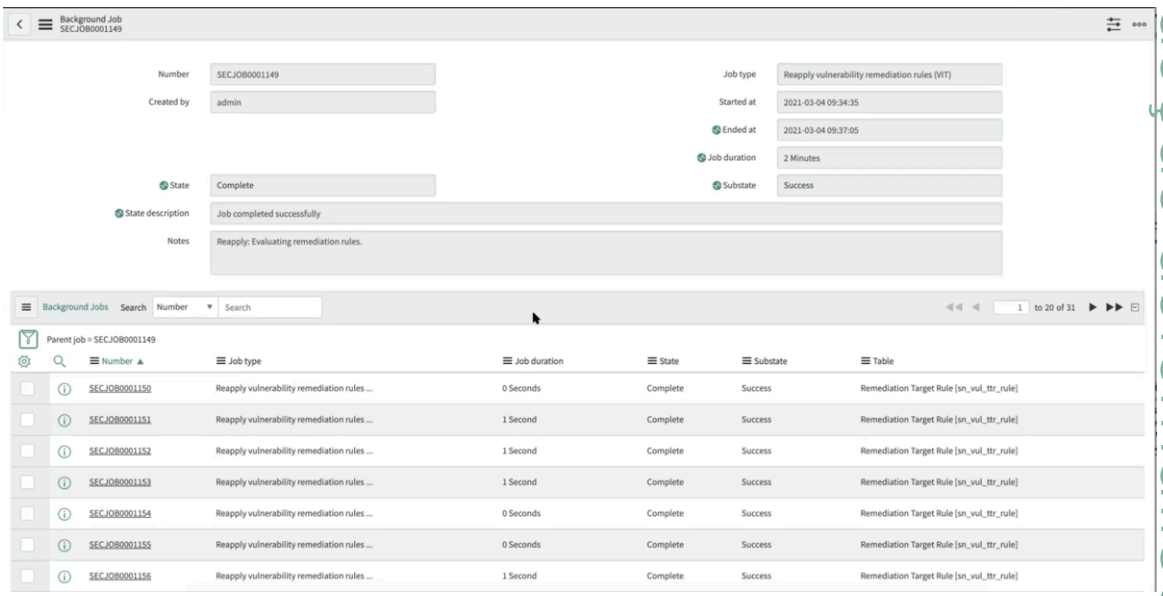
6. No registro de trabalho de configuração aberto, altere o valor do Tamanho da partição de **4** para **10**.
7. Navegar até **Resposta a vulnerabilidades** > **Regras de destino de correção**, localize Reaplicar regra de correção de vulnerabilidade que você alterou, selecione o registro na lista e clique em **Aplicar mudanças** para reavaliar as regras de destino para os VIs existentes.
   O trabalho Reaplicar regras de correção de vulnerabilidade (VIT) está na fila.
8. Clique no link **Exibir status** para exibir o registro do trabalho em segundo plano e verificar se os trabalhos estão na fila, conforme mostrado na imagem a seguir.
   Para este exemplo, 31 trabalhos são criados para processar regras de destino para 307 IVs (máximo de 10 itens por trabalho). Esses trabalhos são trabalhos secundários do trabalho primário em segundo plano. Os trabalhos secundários processam os registros sequencialmente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando todos os trabalhos forem concluídos com sucesso, os campos serão atualizados no registro de trabalho em segundo plano.



Tradução automática

9. Navegue até seus itens vulneráveis e verifique se eles refletem sua nova mudança de regra.

Processamento paralelo avançado para trabalhos em segundo plano no Resposta a vulnerabilidades

Com esta configuração avançada, controle o número total de trabalhos em segundo plano que estão sendo processados paralelamente, independentemente do tipo de trabalho.

Antes de Iniciar

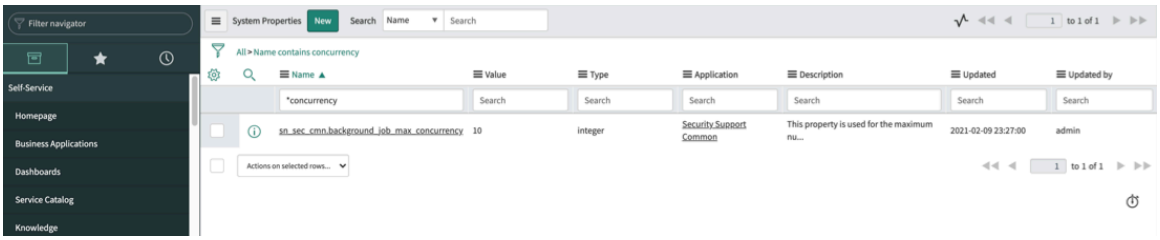
Função necessária: sn_vul.vulnerability_admin ou gerenciadores de vulnerabilidade com a função granular sn_sec_cmn.manage_background_job

Nota: Este procedimento requer conhecimento avançado de programação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No Navegador de filtros, insira **sys_properties.list** e localize a propriedade do sistema *sn_sec_cmn.background_job_max_concurrency*.



2. Clique nele para abrir o registro.

   Por padrão, a propriedade do sistema *sn_sec_cmn.background_job_max_concurrency* executa no máximo 10 trabalhos em segundo plano em paralelo.

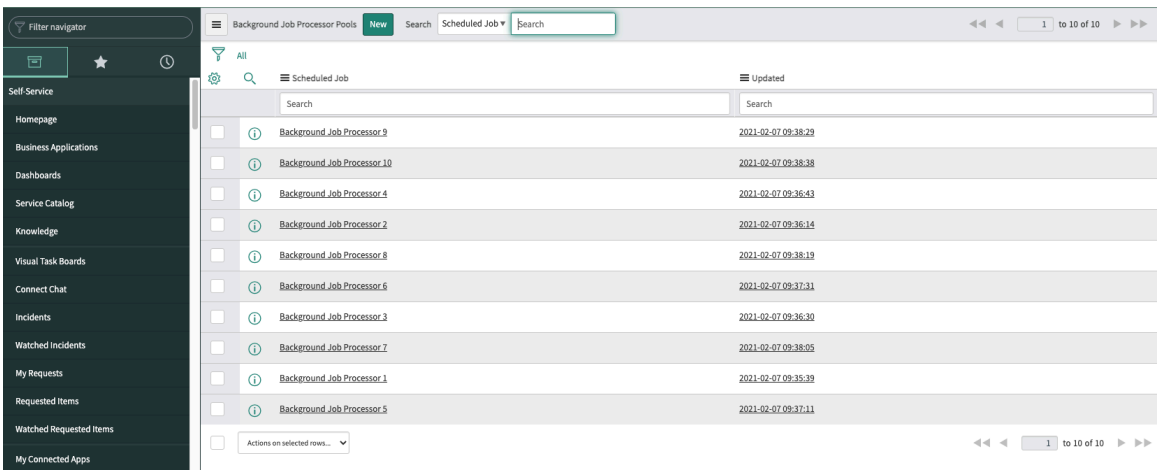
   Se sua instância tiver um número baixo de nós, você poderá reduzir esse valor na propriedade do sistema. Por exemplo, digamos que você tenha sete regras de atribuição em sua lista de Regras de grupo. No registro de configuração do trabalho Reaplicar regras de atribuição, três trabalhos são definidos para o máximo de threads simultâneos. O valor de simultaneidade da estrutura é 10, mas o sistema é uma instância de nó único, portanto, você pode processar dois trabalhos particionados do trabalho Regras de atribuição de reaplicação simultaneamente. Se você definir o Máximo de threads simultâneos como um registro de trabalho de Regras de atribuição, todos os tipos de trabalho Reaplicar regras de atribuição serão processados sequencialmente.

   Por outro lado, se sua instância tiver mais nós, você poderá aumentar esse valor, mas também deverá adicionar mais trabalhos agendados para fazer essa mudança.

   Para aumentar o número de trabalhos agendados, duplique um trabalho agendado quantas vezes forem necessárias para corresponder ao valor em que você aumentou a propriedade do sistema. Por exemplo, por padrão, há 10 trabalhos agendados. Portanto, se você quiser 20 trabalhos, deverá duplicar um trabalho 10 vezes.

   Os dez trabalhos agendados incluídos com Now Platform® para processamento são exibidos na tabela sn_sec_cmn_background_job_processor_pool.

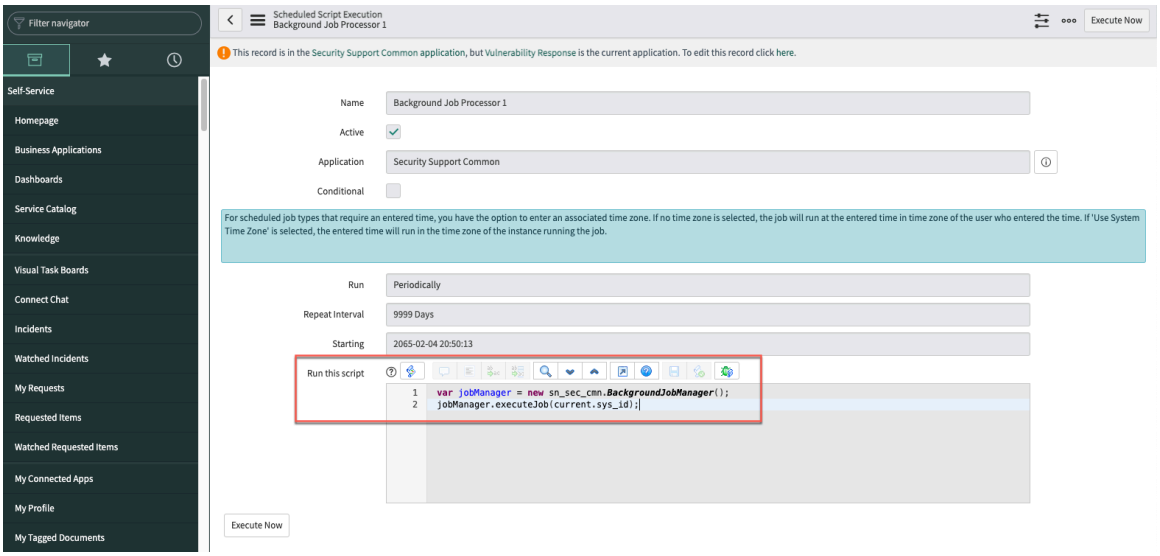
3. No Navegador de filtros, insira **sn_sec_cmn_background_job_processor_pool.list**



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em um trabalho para copiá-lo e duplicá-lo quantas vezes forem necessárias para que o número de trabalhos corresponda ao valor que você aumentou na propriedade do sistema.



5. Depois que o trabalho agendado for definido, adicione uma referência clicando em **Novo** na lista sn_sec_cmn_background_job_processor_pool do trabalho que você copiou.

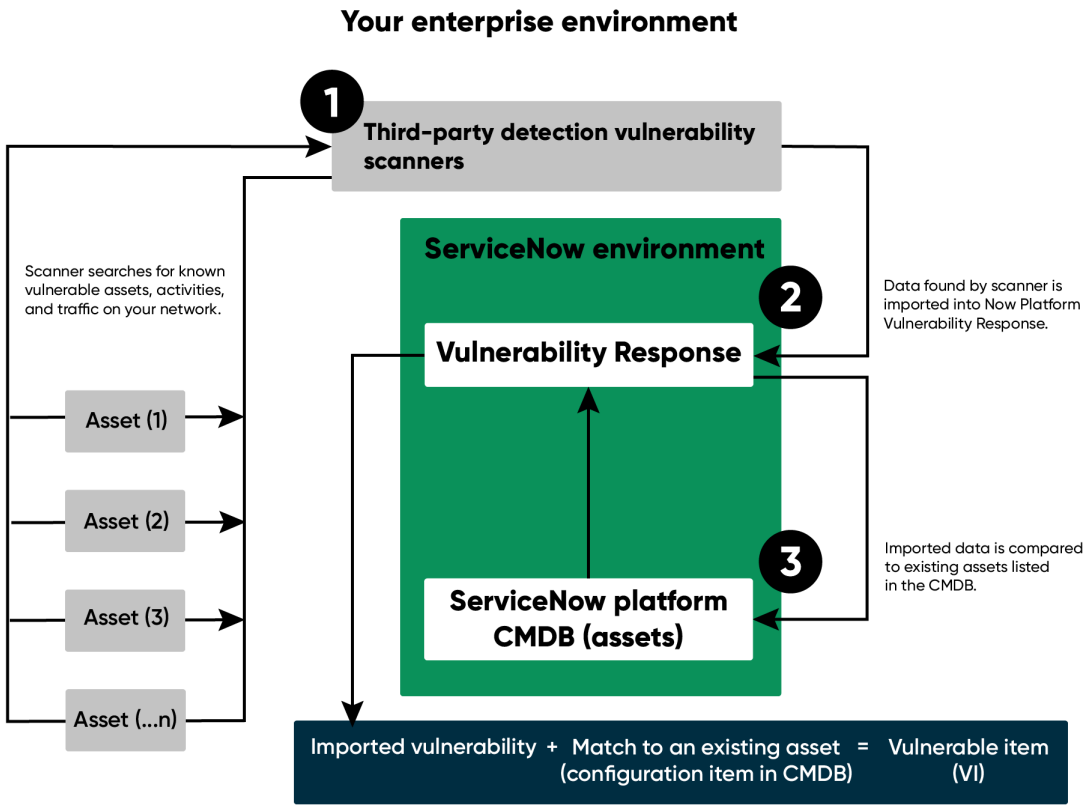
Integrações do Resposta a vulnerabilidades

Resposta a vulnerabilidades inclui suporte para integrações de terceiros. Incluídas nesta seção estão algumas diretrizes básicas para desenvolver suas próprias integrações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de terceiros



As vulnerabilidades importadas do banco de dados nacional de vulnerabilidades (NVD) e os dados de detecção de scanners de terceiros são reconciliados com os ativos no seu CMDB. Quando uma vulnerabilidade importada corresponde a um ativo existente, um item vulnerável é criado. Itens vulneráveis são agrupados automaticamente em tarefas para correção, pontuados de risco com contexto de negócios, priorizados e atribuídos às equipes apropriadas para correção.

Nota:

As integrações de terceiros são tratadas separadamente. Se mais de uma aplicação de integração de terceiros estiver em uso em seu ambiente, não haverá desduplicação de item vulnerável (VI) entre as integrações. Por exemplo, a desduplicação de VI entre Rapid7 e Qualys não está disponível.

No entanto, incompatibilidades na contagem de detecção entre um scanner de terceiros (por exemplo, Qualys) para IVs em sua instância ServiceNow são esperadas, já que deduplicamos em IPs, portas e assim por diante.

Para obter informações sobre integrações de terceiros compatíveis com Resposta a vulnerabilidades de aplicações, consulte, Integração do Resposta a vulnerabilidades de aplicações a outras aplicações

- CISA - Integração de vulnerabilidade de exploração conhecida (KEV)
- Noções básicas sobre a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft
- Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Noções básicas sobre a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM
- Noções básicas sobre as integrações do NVD
- Integração da vulnerabilidade da Qualys
- Noções básicas sobre Integração com Rapid7 Vulnerability
- Shodan Exploit Integration
- Noções básicas sobre a integração de vulnerabilidade da Tenable
- Integrações da Solução do Microsoft Security Response Center Solution Integration

  O Integração com a solução Microsoft Security Response Center está disponível com Solução de gestão de vulnerabilidade. Para obter informações sobre a instalação e a configuração do Integração com a solução Microsoft Security Response Center e do Red Hat Solution Integration, consulte Instalar a aplicação Solução de gestão de Resposta a vulnerabilidades. Você pode configurar, editar, programar e iniciar sob demanda o Integração com a solução Microsoft Security Response Center e o Red Hat Solution Integration de dentro do Assistente de configuração.

Anotações adicionais para integrações

Se várias implantações forem compatíveis com uma integração, consulte Criar importações separadas por domínio para uma integração.

- Você pode instalar, configurar, programar e iniciar sob demanda muitas das aplicações de integração no Assistente de configuração.
- Você pode instalar a aplicação Integração com Rapid7 Vulnerability do Assistente de configuração, mas a configuração não é compatível com esta integração de dentro do Assistente de configuração. Para obter mais informações, consulte Instalar o Integração com Rapid7 Vulnerability.
- A aplicação Tenable para Resposta a vulnerabilidades da Tenable é criada e mantida pela Tenable. Consulte a documentação em Tenable para Resposta a vulnerabilidades.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

A partir do VR v17.1, os seguintes nomes de estado do processo de integração foram atualizados:

Nome do estado anterior a V17.1	Nome do estado V17.1 em diante
Processando	Recuperando
AguardarConcluído	Aguardando/Processando

Nota: Você pode exibir os anexos que são baixados e processados. Quando o status da execução da integração é `esperaconcluído`, ele exibe a porcentagem de integração que está concluída.

Integrações criadas manualmente

Você pode adicionar outras integrações que não estão disponíveis como aplicações ServiceNow Store, conforme necessário. Para obter mais informações, consulte Criar manualmente uma integração de vulnerabilidade.

Noções básicas sobre as integrações do NVD

As integrações do NVD usam dados importados do produto National Vulnerability Database (NVD) do National Institute of Standards and Technology (NIST) para ajudá-lo a determinar o impacto e a prioridade das falhas no seu código. Execute esta integração como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

O NIST NVD coleta dados de vulnerabilidades e exposições comuns (CVE) e de enumeração de plataforma comum (CPE) e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente com Resposta a vulnerabilidades para mapear vulnerabilidades de CVE e CPE, enriquecendo os dados em sua instância.

Importante: Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Depois de instalada, a integração do NIST National Vulnerability Database Integration-API (somente CVE) é invocada automaticamente como um trabalho agendado e é executada diariamente. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dica: A ativação desse plug-in em instâncias de produção pode exigir uma licença separada.

Versões disponíveis

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades Integração com NVD v1.2	

Importação inicial de dados de vulnerabilidade com as integrações de NVD e CWE

1. Execute uma importação inicial de dados do CWE com a Integração CWE Comprehense 2000.

   Consulte Configure e execute o trabalho agendado para atualizar registros de CWE. Por padrão, você executa atualizações de CWE **sob demanda** a partir do registro de integração e deve configurá-lo.

   Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanal** na segunda- **feira**.

2. Verifique se a integração Resposta a vulnerabilidades com a aplicação NVD está instalada e se uma importação de dados inicial da integração de banco de dados nacional de vulnerabilidades do NIST - API (somente CVE) ou da integração de banco de dados nacional de vulnerabilidades do NIST - API (CVE e CPE) foi bem-sucedida.

   Para CPEs, verifique se uma importação de dados inicial da Integração de banco de dados de vulnerabilidades do NIST - API (somente CPE) foi bem-sucedida.

   A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Depois que o plug-in é instalado, a API NIST National Vulnerability Database Integration - API (somente CVE) é ativada por padrão. Ele é executado diariamente. Para obter mais informações, consulte Instalar a integração Resposta a vulnerabilidades com o banco de dados nacional de vulnerabilidades do NIST.

3. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações do Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Noções básicas sobre dados de vulnerabilidade importados e itens vulneráveis

Na instância Now Platform, cada vulnerabilidade importada é representada por uma entrada de vulnerabilidade nas bibliotecas de origem de produtos de scanner de terceiros, como Qualys, por exemplo. Os itens vulneráveis (VI) que são importados e atualizados em sua instância são referências a bibliotecas de terceiros, como a biblioteca Qualys. Uma biblioteca de terceiros pode, por sua vez, fazer referência ao NVD.

Por exemplo, ao ingerir dados de vulnerabilidade de terceiros de um produto como Qualys, você está ingerindo IVs que fazem referência a um QID (Qualys Identificador). No caso de Qualys, esse QID, por sua vez, faz referência a um CVE da biblioteca do NVD. Ao clicar nesse QID em uma tarefa de correção ou registro de item vulnerável na aplicação Resposta a vulnerabilidades e executar as integrações de NVD e CWE para ingerir dados,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

você está exibindo dados de vulnerabilidade atuais e aprimorados que permitem ver os relacionamentos existentes entre seus VIs e CVEs, CWEs e CPEs.

Antes de executar um produto de scanner de terceiros como Qualys que tem sua própria biblioteca, você deve primeiro instalar e executar, no mínimo, a Integração do banco de dados nacional de vulnerabilidades do NIST - API (somente CVE) (também inclui detalhes relacionados ao CISA) , integração do CWE para ingerir dados de vulnerabilidade. Essas importações de dados do NVD e CWE aprimoram seus dados Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações antes de importar dados com um produto de terceiros.

Para obter mais informações sobre como gerenciar o NVD, o CWE e as bibliotecas de terceiros e exibi-las, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros e Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades.

Depois de verificar a importação bem-sucedida do NVD, para aprimorar ainda mais os dados de vulnerabilidade, Configure e execute o trabalho agendado para atualizar registros de CWE.

Execute as importações de NVD e CWE antes de importar dados de vulnerabilidade com um produto de terceiros. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações do Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Localizando as integrações do NVD

Para exibir as integrações do NVD, navegue até **Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.

As seguintes integrações estão incluídas no sistema de base.

Nota: Somente a Integração do banco de dados nacional de vulnerabilidades do NIST – API (somente CVE) está ativa, por padrão.

Integrações do NVD

Integração	Descrição
NIST National Vulnerability Database Integration - API (somente CVE)	Recupera somente dados de vulnerabilidade do NIST NVD (CVE). Por padrão, esta integração é definida automaticamente para ser executada diariamente.
NIST National Vulnerability Database Integration- API (somente CPE)	Recupera dados de CPE do NIST NVD. Esta integração está inativa por padrão. Ative esta integração se quiser capturar dados de CPE que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em Software vulnerável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do NVD

Integração	Descrição
	Esta integração está definida para ser executada diariamente e está inativa por padrão. Para ativar essa integração, consulte Ativar a API do banco de dados nacional de vulnerabilidades do NIST (somente CPE).
NIST National Vulnerability Database Integration-API (CPE não mapeado)	Recupera dados de CPE associados ao CVE obtido do NIST NVD. Esta integração está inativa por padrão. Ative esta integração se quiser capturar dados de CPE que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em uma lista relacionada ao registro de entrada de vulnerabilidade do NVD. Esta integração está definida para ser executada sob demanda e está inativa por padrão. Para ativar essa integração, consulte Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Importante: A integração "NIST National Vulnerability Database Integration-API (CVE and CPE)" está obsoleta.

Para status de execução de integração, consulte Exibir o status de execução da importação da integração do NVD (National Vulnerability Database).

Preparando para as integrações do NVD

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. As integrações do NVD presumem que você esteja familiarizado com o NIST National Vulnerability Database (NVD).

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar as integrações do NVD, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Configure e execute o trabalho agendado para atualizar registros de CWE

Dimportações de dados do CWE enriquecem ainda mais os dados de vulnerabilidade em sua instância. Use os registros de CWE (Common Weakness Enumeration, Enumeração de pontos fracos comuns) baixados do banco de dados do CWE como referência ao decidir se uma vulnerabilidade deve ser escalonada. Execute esta integração como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanal** na segunda- **feira**.

Atualize os registros de fraquezas comuns do banco de dados de enumeração de fraquezas comuns em uma base programada regularmente. Você também pode atualizar o script padrão ou escrever seus próprios scripts, conforme necessário.

Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na página Enumerações de Pontos Fracos Comuns.

- Se você tiver a função de administrador, poderá adicionar repositórios ao trabalho agendado.
- Se você tiver sn_vul.vulnerability_read, poderá executar o trabalho agendado.
- Se você tiver sn_vul.vulnerability_write, poderá editar os detalhes do trabalho agendado.

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.
2. Selecione o trabalho agendado **Integração abrangente do CWE 2000**.
3. Modifique os campos, conforme necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Integração de vulnerabilidade

Campo	Descrição
Nome	Nome do trabalho agendado.
Ativo	Se o trabalho agendado está ativo. Se você não quiser que o trabalho seja executado por um período específico, poderá configurar os parâmetros que deseja usar e desativar o trabalho.
Executar	Frequência em que o trabalho deve ser executado. Os campos subsequentes são exibidos ou ocultos com base na sua configuração neste campo. **Nota:** A atualização do CWE é **sob demanda** por padrão. Defina como um período programado anterior às atualizações do NVD. As opções incluem: ◦ Diariamente: escolha um **horário** ◦ Semanal: (opção mais comum) escolha um **dia** e**hora** ◦ Mensal: escolha **dia** e **hora** ◦ Periodicamente: escolha um **intervalo de repetição**, data e hora de **início** ◦ Uma vez: escolha uma data e hora de **início**
Dia	O dia em que você deseja que o trabalho agendado seja executado. Se você selecionou **Semanalmente** no campo **Executar**, este campo exibirá os dias da semana. Se você selecionou **Mensal** no campo **Executar**, este campo exibirá os dias do mês. **Nota:** Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanal** na segunda- **feira**.
Hora	A hora em que você deseja que o trabalho agendado seja iniciado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O tempo padrão para a atualização do NVD é 01:00:00
Script de integração	O script para extrair dados das fontes de dados especificadas na lista relacionada **Fontes de dados**.
Integração de origem	[Somente leitura]
Instância de origem	[Somente leitura]
Aplicação	[Somente leitura] O nome da aplicação para a qual você está executando o trabalho agendado.
Intervalo de repetição	O número de dias e horas antes que o trabalho agendado seja executado novamente. Este campo aparece quando **Periodicamente** é selecionado na lista **Executar**.
Início	A data e hora para iniciar as atualizações periódicas. Este campo aparece quando **Periodicamente** é selecionado na lista **Executar**.
Condicional	A caixa de seleção para adicionar parâmetros condicionais.
Condição	As condições para executar o trabalho agendado. Este campo aparece quando a caixa de seleção **Condicional** está marcada.
Estratégia do processador de relatórios	A estratégia para extrair dados e processar o trabalho agendado. ◦ Para extrair dados das fontes de dados na lista relacionada **Fontes** de dados usando o script no campo Script de **integração**, selecione **Anexo de fonte de dados**. ◦ Para selecionar um processador personalizado no campo de **script Processador de relatório**, selecione o **Processador de relatório personalizado**.
Processador de relatórios	O script a ser executado quando o trabalho agendado for executado. Este campo aparece quando o **Processador de relatório personalizado** é selecionado na lista **Estratégia do processador de relatório**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Script de fábrica do processador	O script para criar o processador de relatório. Este campo aparece quando o **Processador de relatório personalizado** é selecionado na lista **Estratégia do processador de relatório**.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar** suas mudanças.
5. Para executar o trabalho agendado imediatamente, clique em **Executar agora**. Você retornará à exibição Integrações de vulnerabilidade.
6. Para observar o andamento da importação, selecione o trabalho agendado **Integração abrangente do CWE 2000** novamente e selecione a guia **Execuções de integração de vulnerabilidade**.

   Consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades para ver as entradas importadas.

Instalar a integração Resposta a vulnerabilidades com o banco de dados nacional de vulnerabilidades do NIST

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto NIST National Vulnerability Database (NVD) se integre corretamente com Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao Gerenciador de vulnerabilidades em Resposta a vulnerabilidades ou ao grupo de gerentes de App-Sec

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	em Resposta a vulnerabilidades de aplicações. Para obter informações sobre funções de grupo em Resposta a vulnerabilidades, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades. Para obter informações sobre funções de grupo em Resposta a vulnerabilidades de aplicações, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O Gerenciador de vulnerabilidades ou o Gerenciador de App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Nota: Antes de executar as integrações do NVD, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Procedimento

1. Faça login na instância em que você deseja instalar as integrações do NVD.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a integração da Resposta a vulnerabilidades com a aplicação NVD.
4. Selecione o bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome** e **o motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Todos** > **Aplicações do sistema** > **Aplicações** > **Todos**.
10. Localize a aplicação, selecione-a e escolha **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Após a instalação inicial, para modificações, consulte Modificação e atividades opcionais de integração do NVD.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado)

Para ingerir dados de Enumeração de plataforma comum (CPE) para dados de CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) obtidos, você pode executar uma importação de dados completa com um trabalho agendado sob demanda.

Antes de Iniciar

A integração do National Vulnerability Database Integration (NVD)–API (Unmapped CPE) captura dados (CPE) do National Institute of Standards and Technology (NIST) que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vinculando texto e testes a um nome. Essas informações são armazenadas em uma lista relacionada ao registro de entrada de vulnerabilidade do NVD.

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações** > **NVD** > **Integrações**.
2. Selecione a integração NIST National Vulnerability Database Integration–API (CPE não mapeada).
3. Marque a caixa de seleção **Ativo**.

   Nota: A integração é pré-configurada para ser executada sob demanda. Ao ativar a integração, ela será executada automaticamente após a integração do NIST NVD Integration-API (somente CVE). Alterar qualquer outro parâmetro de integração requer ServiceNow e Resposta a vulnerabilidades e experiência e pode resultar em dados incompletos.

   a. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.

   b. Selecione Integração do banco de dados nacional de vulnerabilidades do NIST – Integração de API (CPE não mapeada).

   c. Selecione a guia **Detalhes da integração**.
   Independentemente do valor do campo **Importar desde**, os CPEs de todos os CVEs recuperados são recuperados.
4. Selecione **Executar agora** para executar uma execução inicial de integração de suporte completo.
   Depois que a importação inicial for concluída, as importações programadas de dados delta serão retomadas. Para status de execução de integração, consulte Exibir o status de execução da importação da integração do NVD (National Vulnerability Database).

Ativar a API do banco de dados nacional de vulnerabilidades do NIST (somente CPE)

Para ingerir dados de Enumeração de plataforma comum (CPE), você pode executar uma importação de dados completa com um trabalho agendado diário.

Antes de Iniciar

A integração do National Vulnerability Database Integration (NVD) – API (somente CPE) do Instituto Nacional de Padrões e Tecnologia (NIST) captura dados (CPE) que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vinculando texto e testes a um nome. Essas informações são armazenadas em uma tabela de software vulnerável.

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações** > **NVD** > **Integrações**.
2. Selecione a integração NIST National Vulnerability Database Integration–API (somente CPE).
3. Marque a caixa de seleção **Ativo**.

   - A integração é pré-configurada para ser executada diariamente. Alterar qualquer outro parâmetro de integração requer experiência ServiceNow e pode resultar em dados incompletos.
   - A ativação desta integração ativará automaticamente as integrações NIST National Vulnerability Database Integration- API (somente CVE) e NIST National Vulnerability Database Integration- API (CPE não mapeado) e definirá seu campo de execução como sob demanda.
   - Além disso, uma execução de integração bem-sucedida da API NIST National Vulnerability Database Integration (somente CPE) acionará automaticamente a API NIST National Vulnerability Database Integration (somente CVE). E a conclusão bem-sucedida da API NIST National Vulnerability Database Integration (somente CVE) acionará automaticamente a API NIST National Vulnerability Database Integration (CPE não mapeada).

   Nota: O campo Importar desde a data na integração do banco de dados nacional de vulnerabilidades do NIST – API (somente CPE) está vazio por padrão. Mantenha em branco para buscar dados dos últimos 357 dias.

   Para recuperar dados históricos durante a importação inicial da verificação do NVD, defina uma data de início no registro de Integração do banco de dados nacional de vulnerabilidades do NIST - API (somente CPE).

   a. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.
   b. Selecione NIST National Vulnerability Database Integration–API (somente CPE).
   c. Selecione a guia **Detalhes da integração**.
   d. Defina o valor do campo **Importar desde** como a data mais antiga que você deseja recuperar.

   Cada importação bem-sucedida redefine esta data para a data e hora do dia selecionado.
4. Selecione **Executar agora** para executar uma execução inicial de integração de suporte completo.
   Depois que a importação inicial for concluída, as importações programadas de dados delta serão retomadas. Para status de execução de integração, consulte Exibir o status de execução da importação da integração do NVD (National Vulnerability Database).

Modificação e atividades opcionais de integração do NVD

Configure modificações opcionais especificamente para as integrações do NVD.

Nota: Alterar outras configurações de integração do NVD, além das listadas aqui, requer conhecimento avançado de ServiceNow e Resposta a vulnerabilidades e está além do escopo da documentação do produto.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar uma importação manual de integração do NVD

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho agendado diário ou semanal.

Antes de Iniciar

Nota: As integrações NIST National Vulnerability Database Integration- API (somente CPE) e NIST National Vulnerability Database Integration-API (CPE não mapeadas) estão inativas por padrão. Para obter mais informações, consulte Ativar a API do banco de dados nacional de vulnerabilidades do NIST (somente CPE) e Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Escolha e integração, por exemplo, a integração do NIST National Vulnerability Database - API (somente CVE).
3. Selecione **Executar agora**.

   Nota: Se a integração NIST National Vulnerability Database Integration-API (CPE não mapeada) estiver ativada, os dados de CPE associados serão armazenados na lista relacionada de software vulnerável da entrada de vulnerabilidade do NVD. Consulte Resposta a vulnerabilidades campos de formulário de vulnerabilidade.

4. Para status de execução de integração, consulte Exibir o status de execução da importação da integração do NVD (National Vulnerability Database).

Exibir o status de execução da importação da integração do NVD (National Vulnerability Database)

Use a lista relacionada de **execuções de integração de vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status de execução da importação de integração do NVD:

- Resposta a vulnerabilidades e a integração da Resposta a vulnerabilidades com a aplicação de integração do NVD devem ser instaladas e configuradas.
- As importações de integração do NVD devem estar em execução. A integração do NIST National Vulnerability Database Integration-API (somente CVE) é executada por padrão.

  Nota: As integrações NIST National Vulnerability Database Integration-API (somente CPE) e NIST National Vulnerability Database Integration-API (CPE não mapeadas) estão inativas por padrão. Para obter mais informações, consulte Ativar a API do banco de dados nacional de vulnerabilidades do NIST (somente CPE) e Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite.

Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. O último registro processado com mais de uma hora indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Se você não estiver usando o gráfico de status de execução de integração do NVD, Navegar até **Todos** > **Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione um **link** para uma integração.
3. Selecione a lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

Trouble?

As causas mais comuns de falha na execução incluem:

- Interrupção de rede.
- Um problema na transferência de dados que resultou em dados corrompidos durante a transformação.

Se você encontrar alguma dessas condições, selecione **Executar agora**e execute novamente a integração.

Informações relacionadas

Resposta a vulnerabilidades campos de formulário de vulnerabilidade

Adicionar CVEs a entradas de terceiros

As informações de vulnerabilidade e exposição comuns (CVE) podem ser relacionadas a uma única vulnerabilidade de terceiros. Normalmente, ele é adicionado durante uma importação de integração de terceiros. No entanto, você pode adicionar vários CVEs (vulnerabilidades) manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

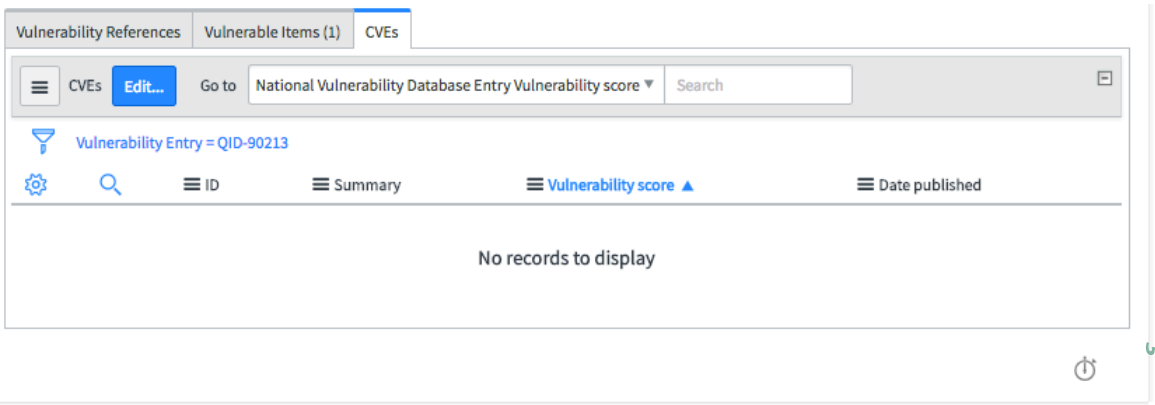
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros**.
2. Abra um registro.
3. Clique na guia da lista relacionada **CVEs**.



4. Clique em **Editar**.
5. Escolha quais CVEs serão adicionados.

   Nota: Você pode usar filtros de condição para refinar a coleção de CVE.

6. Clique em **Salvar**.

Informações relacionadas

Resposta a vulnerabilidades campos de formulário de vulnerabilidade

Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades

Você pode exibir dados de vulnerabilidade importados do Banco de dados nacional de vulnerabilidades (NVD), Enumeração de pontos fracos comuns (CWE) ou de terceiros para decidir se deve escalar uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Bibliotecas**.

   Para obter informações sobre campos específicos, consulte Resposta a vulnerabilidades campos de formulário de vulnerabilidade.

   As seguintes bibliotecas estão disponíveis:

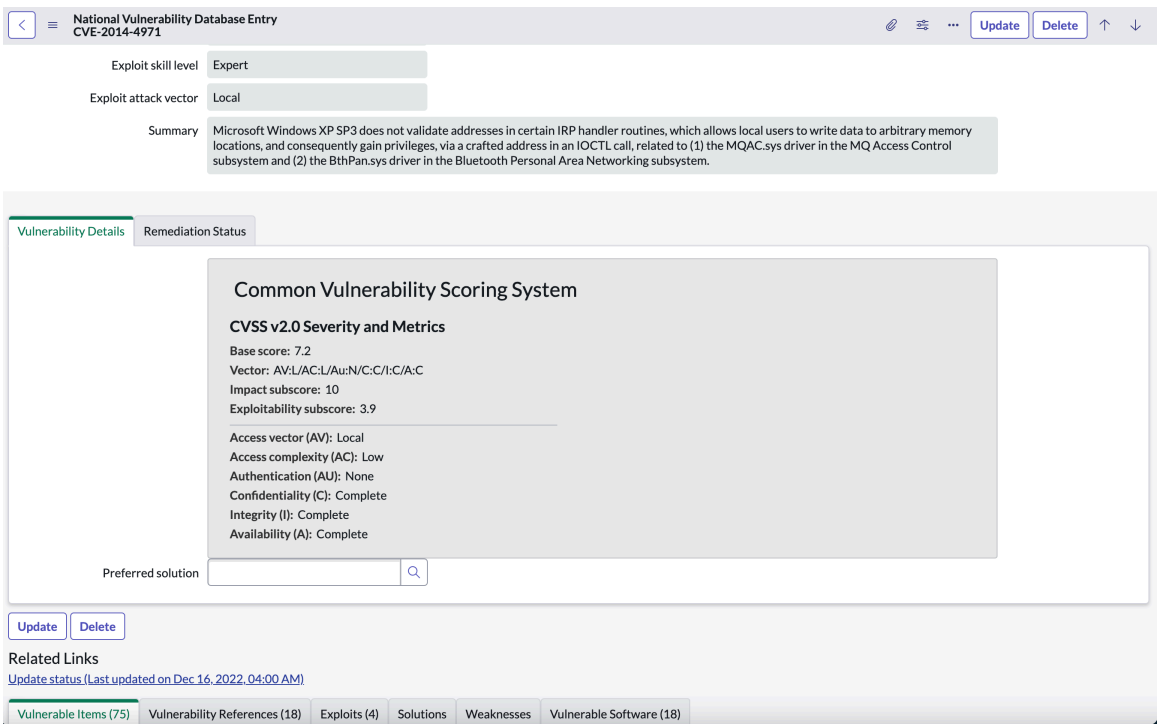
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, erros de configuração, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de pontos fracos comuns, é apenas para referência.
Terceiro	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs.

2. Escolha uma biblioteca para exibir vulnerabilidades.
3. Clique em um link na lista para abrir um registro.

   Um registro de CVE na biblioteca de entradas do banco de dados nacional de vulnerabilidades. Mais informações estão disponíveis nos **Links relacionados**. Depois de uma importação de dados, você pode escolher uma vulnerabilidade e explorar seus relacionamentos com itens vulneráveis, explorações, possíveis soluções, possíveis patches e quaisquer referências a artigos da base de conhecimento na Base de conhecimento HI. Se Solução de gestão de vulnerabilidade estiver instalado, você poderá exibir uma solução preferencial nos registros do NVD, se houver uma disponível.



CISA - Integração de vulnerabilidade de exploração conhecida (KEV)

A integração Resposta a vulnerabilidades com o catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA ingere dados para ajudar você a priorizar e corrigir essas vulnerabilidades com eficácia.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

A CISA permite a correção urgente e priorizada de vulnerabilidades ativamente exploradas para agências governamentais e empresas.

Sobre a CISA

A CISA (Cybersecurity & Infrastructure Security) é uma agência dos EUA que publica um relatório sobre as vulnerabilidades mais exploradas. Ele se integra facilmente com Resposta a vulnerabilidades para mapear vulnerabilidades de CVE (Common Vulnerability and Exposures, vulnerabilidades e exposições comuns), enriquecendo os dados em sua instância. Essas informações são acumuladas para a tabela Entradas de vulnerabilidade de terceiros. A data de vencimento mais antiga é considerada para o acúmulo dos itens vulneráveis.

Nota: A caixa de seleção **CISA existe** para CVEs recuperados pela CISA.

Valores recuperados da integração CISA:

- ID do CVE
- Prazo
- Data de inclusão
- Fornecedor/projeto
- Produto
- Ransomware conhecido (a partir da v21.0 de Resposta a vulnerabilidades, um novo campo **conhecido por ser usado em campanhas de ransomware** é ingerido do catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA. Isso é indicado pela sinalização do campo **Ransomware conhecido** na tabela do banco de dados de entrada nacional de vulnerabilidade. O sinalizador é definido no nível de Vulnerabilidades e exposições comuns (CVE) e acumulado para a entrada de terceiros (TPE).

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Trabalhos agendados

A integração CISA é invocada automaticamente como um trabalho agendado diariamente. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades v16.5, v18.0 Resposta a vulnerabilidades Integração com CISA v1.0, v1.2	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição da integração CISA

Para exibir a integração CISA, navegue até **Resposta a vulnerabilidades** > **Administração** > **Integrações** > **Integração de vulnerabilidade de exploração conhecida CISA**.

As seguintes integrações estão incluídas no sistema de base.

Nota: Somente a integração CISA está ativa, por padrão.

Integração CISA

Integração	Descrição
Integração da Agência de Segurança de Cibersegurança e Infraestrutura (CISA)	Recupera dados de vulnerabilidade CISA (CVE) e aprimora os dados de vulnerabilidade existentes. Esta integração é definida automaticamente para ser executada diariamente.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades.

Preparação para a integração CISA

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. A integração de vulnerabilidades exploradas conhecidas da CISA pressupõe que você esteja familiarizado com a Agência de segurança cibernética e de infraestrutura (CISA).

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração CISA, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Instalar a aplicação ServiceNow® Integração de resposta a vulnerabilidades com CISA

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o consultor de vulnerabilidades exploradas da Cybersecurity & Infrastructure Security (CISA) se integre com Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se a aplicação Resposta a vulnerabilidades Integration with NVD está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar a integração Resposta a vulnerabilidades com o banco de dados nacional de vulnerabilidades do NIST.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o Administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao Gerenciador de vulnerabilidades em Resposta a vulnerabilidades. Para obter

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	informações sobre funções de grupo em Resposta a vulnerabilidades, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades. • O Gerenciador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar o Integração de Resposta a vulnerabilidades com CISA.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a aplicação Integração de Resposta a vulnerabilidades com CISA.
4. Selecione o bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome** e **o motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e escolha **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Nota: Nenhuma configuração é necessária para a integração CISA.

Noções básicas sobre a integração do Sistema de pontuação de previsão de exploração (EPSS)

Visão geral da integração de EPSS com Resposta a vulnerabilidades.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

A integração do Exploit Prediction Scoring System (EPSS) importa dados EPSS relacionados a vulnerabilidades e exposições comuns (CVEs) do First.org para priorizar e corrigir vulnerabilidades. Para obter mais informações, consulte https://www.first.org . O Sistema de Pontuação de Previsão de Exploração (EPSS) é um esforço orientado por dados para estimar a probabilidade (probabilidade) de que uma vulnerabilidade de software será explorada na natureza. O modelo EPSS produz uma pontuação de probabilidade entre 0 e 1 (0 e 100%). Quanto maior a pontuação, maior a probabilidade de uma vulnerabilidade ser explorada.

As importações de dados da integração EPSS enriquecem ainda mais os dados do NVD em sua instância. Se os registros do NVD não estiverem presentes, ele criará um espaço reservado na tabela CVE e adicionará detalhes de EPSS na mesma tabela. Execute esta integração como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros.

Importante: Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é VR.System. Não altere este valor.

Importação inicial de dados com a integração de EPSS

1. Execute uma importação inicial de dados de EPSS com a Integração de EPSS com First.org. Para obter mais informações, consulte Configure e execute um trabalho agendado para atualizar registros de CVE com dados de EPSS.

   Importante: Por padrão, você executa atualizações de EPSS **diariamente** a partir do registro de integração e deve configurá-lo se quiser que ele seja executado como um trabalho agendado.

2. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Para obter mais informações, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

   Importante: É recomendável executar as integrações do NIST National Vulnerability Database Integration - API (somente CVE) antes do EPSS.

Execute as importações de EPSS antes de importar dados de vulnerabilidade com um produto de terceiros. Bibliotecas de terceiros são atualizadas como trabalhos agendados. Consulte a documentação de integração em Integrações da Resposta a vulnerabilidades para obter mais informações sobre integrações de terceiros.

Importante: A integração a seguir está incluída no sistema de base. A integração está ativa por padrão.

Após a execução inicial, os trabalhos agendados do sistema de base executam as integrações automaticamente na ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Na ativação da integração de EPSS, os campos Pontuação de EPSS, Percentil de EPSS e Última modificação de EPSS são adicionados à tabela Entradas de vulnerabilidade. Para CVEs existentes, esses campos são atualizados automaticamente na conclusão bem-sucedida do trabalho de importação inicial. Se houver novos CVEs adicionados à tabela Entradas de vulnerabilidade após a conclusão do trabalho agendado de EPSS, os CVEs

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

recém-adicionados indicarão sua origem como EPSS. As pontuações são acumuladas para TPEs existentes a partir de CVEs da tabela NVD, usando o sistema de base *`Rollup EPSS score from NVD to TPEs calculator`*. Você também pode modificar a calculadora. Para obter mais informações, consulte Resposta a vulnerabilidades Calculadoras de Acúmulo.

Informações relacionadas

Criar uma calculadora Resposta a vulnerabilidades

Configure e execute um trabalho agendado para atualizar registros de CVE com dados de EPSS

Personalize o trabalho agendado do sistema de base para atualizar registros de CVE com dados de EPSS.

Antes de Iniciar

Importante: Você precisa baixar e ativar o plug-in Integração de Resposta a vulnerabilidades com CISA (com.snc.vulnerability.cisa) para habilitar a integração de EPSS.

A seguir está a lista de novos campos adicionados à tabela do NVD para armazenar dados de EPSS.

- Pontuação de EPSS
- Percentual de EPSS
- Última modificação de EPSS

Nota: Configure a exibição de lista ou de formulário de acordo com o requisito para exibir os campos adicionados recentemente.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

As importações de dados da integração EPSS aprimoram ainda mais os dados do NVD em sua instância. Se os registros do NVD não estiverem presentes, ele criará um espaço reservado na tabela CVE e adicionará detalhes de EPSS na mesma tabela. Execute esta integração como parte da configuração inicial da Resposta a vulnerabilidades e publique para importar dados de vulnerabilidade para sua instância.

Nota: Por padrão, a integração do First.org EPSS está no estado **Ativo**. O trabalho agendado do sistema de base é configurado, por padrão, para ser executado diariamente.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Integrações**.
2. Localize e selecione Integração com First.org EPSS.
3. Modifique os campos, conforme necessário.
4. Clique com o botão direito do mouse no cabeçalho para **Salvar** suas mudanças.
5. Selecione **Executar agora**para executar o trabalho agendado imediatamente.
   Você retornará à exibição Integrações de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecionar **EPSS do First.org** > **Guia Execuções de integração de vulnerabilidade** para exibir o andamento da importação.
   Na conclusão bem-sucedida do trabalho agendado, as pontuações do EPSS, o percentil e os carimbos de data/hora da última modificação do EPSS são atualizados nos CVEs.

O que Fazer Depois

- Consulte Adicionar condição de pontuação de EPSS na regra de negócio da calculadora de risco.
- Consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades para ver as entradas importadas.

Adicionar condição de pontuação de EPSS na regra de negócio da calculadora de risco

Modifique a regra de negócio para adicionar a condição de pontuação de EPSS à calculadora de risco.

Antes de Iniciar

Nota: O procedimento a seguir é necessário para que as atualizações de EPSS sobre vulnerabilidades sejam distribuídas para os itens vulneráveis.

Função necessária: sn_vul.manage_risk_score_configuration

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Regra de negócio**.
2. Pesquise **Definir sinalizador de recálculo**.

   Nota: Há duas *`Set recalculate flag`* regras de negócio. Você pode usar qualquer um deles.

3. Navegue até a guia **Quando executar**.
4. Selecione **Adicionar cláusula "OR"** e selecione `Pontuação EPSS` em **Escolher campo** e `mudanças` em **Escolher campo de operador**.
5. Selecione **Atualizar**.

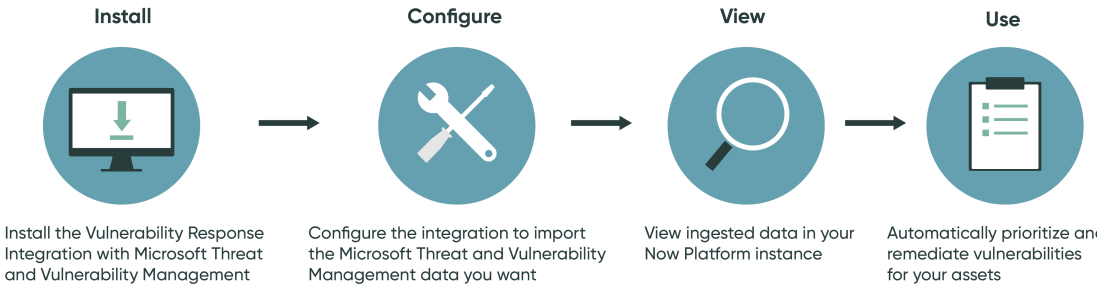
Noções básicas sobre a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft

A integração Resposta a vulnerabilidades com a aplicação Gestão de ameaças e vulnerabilidades da Microsoft (MS TVM) usa dados importados do MS TVM para ajudá-lo a priorizar e corrigir vulnerabilidades de seus ativos. A aplicação está disponível com uma assinatura separada do ServiceNow Store.

Você pode usar a integração de vulnerabilidade do MS TVM para importar dados de scanner de terceiros sobre seus ativos e vulnerabilidades. Você pode exibir relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Versões disponíveis

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades Integração com MS TVM v2.2	Para obter mais informações sobre as versões lançadas da aplicação Resposta a vulnerabilidades, compatibilidade e mudanças de esquema, consulte o artigo Matriz de compatibilidade da Resposta a vulnerabilidades e mudanças de esquema de versão [KB0856498] na Base de conhecimento HI .

Separação de domínios e MS TVM

Importe dados de integração de vulnerabilidade para um domínio especificado atribuindo um usuário nesse domínio para executar as integrações. Para criar importações separadas por domínio para a integração de vulnerabilidade do MS TVM, consulte Criar importações separadas por domínio para uma integração.

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado em sua instância Now Platform quando:

- Uma vulnerabilidade importada de um scanner de terceiros é correspondida com um ativo existente (item de configuração) em seu CMDB). O produto MS TVM se refere a essas correspondências como vulnerabilidades.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente em seu CMDB. Nesse caso, um item de configuração (IC) incompatível também é criado com um item vulnerável.

  Use o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido com um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatível. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação.

Entradas de vulnerabilidade de terceiros

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros, como o MS TVM, e são listadas na tabela Entradas de vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de terceiros na instância Now Platform. Além disso, as entradas do banco de dados nacional de vulnerabilidades (CVEs) são importadas do MS TVM. As informações de exploração associadas a esses dois tipos de entradas vêm do MS TVM. Essas informações de exploração podem ser usadas para cálculo de risco.

Nota: Uma vulnerabilidade de terceiros é recuperada somente para vulnerabilidades que não têm um CVE atribuído a elas. O MS TVM pode adicionar um nome temporário para a vulnerabilidade, por exemplo, `TVM-XXXX-XXXX`. Este nome é atualizado depois que um ID de CVE é atribuído.

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em seu CMDB.

Item descoberto

Itens descobertos são os ativos ingeridos da importação da máquina MS TVM que correspondem aos ICs existentes em seu CMDB.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Habilite o plug-in Modelos de classe de IC do CMDB para que o Mecanismo de Identificação e Reconciliação (IRE) crie ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação. Se o IC original incompatível for reclassificado, os registros de itens descobertos serão atualizados para refletir esse estado. Os itens descobertos dão visibilidade sobre como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados do MS TVM, Resposta a vulnerabilidades usa automaticamente os dados da máquina (ativo) para pesquisar correspondências no CMDB. Regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os IVs são criados.

Instância

Uma instância se refere a várias contas do MS TVM. Cada conta pode ser uma instância na aplicação MS TVM.

Integração

Uma integração é um trabalho agendado que recupera informações de uma fonte de terceiros, como a integração das máquinas MS TVM.

Implantação

Quando uma integração oferece suporte a várias origens, uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações do MS TVM em seu ambiente.

A integração do MS TVM também inclui os seguintes recursos principais:

- Você pode identificar os ativos em seu ambiente e atualizar os ICs em seus itens descobertos existentes, itens vulneráveis e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações do MS TVM. Você também pode executar trabalhos agendados sob demanda.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode agrupar itens vulneráveis.
- Você pode configurar regras de pesquisa de IC para definir como os dados de ativos de fontes de terceiros são usados para identificar ICs em seu CMDB.

Funções necessárias de Now Platform

As tarefas de integração exigem as funções a seguir em sua instância Now Platform.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

administrador

O administrador do sistema usa o Assistente de configuração para instalar a aplicação MS TVM. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das integrações do MS TVM no Assistente de configuração. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades e seus registros. O administrador de vulnerabilidades configura todas as Resposta a vulnerabilidades aplicações e regras para integrações de terceiros instaladas.

sn_vul_msft_tvm.configure_integration

Esta função contém a função granular `sn_vul_msft_tvm.read_integration`. Usuários com esta função podem configurar a Integração da Resposta a vulnerabilidades com a aplicação Gestão de ameaças e vulnerabilidades da Microsoft.

sn_vul_msft_tvm.read_integration

Usuários com esta função só podem exibir a Integração da Resposta a vulnerabilidades com os registros da aplicação Gestão de ameaças e vulnerabilidades da Microsoft.

Grupo de Resposta a vulnerabilidades

Por padrão, o grupo de Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Integrações do MS TVM

Várias origens são compatíveis com todas as integrações do MS TVM. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente a partir do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura a integração Resposta a vulnerabilidades com a aplicação MS TVM no Assistente de configuração.

Para exibir as integrações do MS TVM, navegue até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integrações**. Resposta a vulnerabilidades fornece integrações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

com endpoints do MS TVM para importar os dados de acordo com os intervalos de tempo programados. As seguintes integrações estão incluídas no sistema de base.

Integrações do MS TVM

Sequência de execução	Programação	Integração	Descrição
1	Diariamente	Integração de recomendações do Microsoft TVM	Recupera uma lista de todas as recomendações de segurança acionáveis para corrigir as vulnerabilidades.
2	Diariamente	Integração de vulnerabilidade do Microsoft TVM (CVE)	Recupera uma lista das entradas do banco de dados nacional de vulnerabilidades e entradas de vulnerabilidades de terceiros, bem como suas informações de exploração.
3	Diariamente	Integração de máquinas com Microsoft TVM	Recupera todos os dados de ativos (máquina), incluindo marcadores de máquina, do Microsoft TVM e os processa em sua instância.
4	Semanalmente **Nota:** Após a instalação, esta integração é executada automaticamente após a importação das máquinas.	Integração de vulnerabilidades de máquinas com Microsoft TVM (importação completa)	Recupera todas as vulnerabilidades em aberto em todos os ativos.
5	Diariamente	Integração de vulnerabilidades de máquinas com Microsoft TVM (importação delta)	Recupera todas as informações que mudaram na importação de vulnerabilidade completa da organização, incluindo as vulnerabilidades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do MS TVM

Sequência de execução	Programação	Integração	Descrição
			novas, corrigidas e atualizadas.

Itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de grupo que você define e são atribuídos para correção com base em suas regras de atribuição. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral e Resposta a vulnerabilidades visão geral das regras de atribuição.

Regras de pesquisa de IC

Quando os dados são importados do MS TVM, Resposta a vulnerabilidades usa automaticamente os dados da máquina (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). Regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os IVs são criados. Para obter mais informações sobre como as regras de pesquisa de IC funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.

Nota: Depois de remover uma regra, você não poderá recuperá-la. Em vez de remover uma regra existente, você deve desativá-la.

As seguintes regras de pesquisa do MS TVM são enviadas com o sistema base:

- MAC_ADDRESS
- FQDN
- IP

Nota: Você pode usar vários valores para o IP_ADDRESS e o MAC_ADDRESS de um ativo. Uma regra de pesquisa de IC considera todos os valores para correspondência.

Itens descobertos

Você pode ver os ICs que foram detectados durante uma importação da integração de máquinas com MS TVM.

Nota: O filtro padrão para esta lista está definido como `Incompatível`. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter mais informações, consulte Itens Descobertos.

Marcadores de máquina

Os marcadores de máquina, também conhecidos como marcadores de host, são usados para organizar e rastrear os ativos em sua organização. Você atribui marcadores às suas máquinas.

Todos os marcadores de máquina são importados como parte da integração de máquinas com MS TVM. Os marcadores de máquina geralmente são usados para filtrar em Resposta a vulnerabilidades regras de atribuição e regras de grupo de vulnerabilidade. Os marcadores são exibidos no formulário Item descoberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Execute a integração da máquina MS TVM antes de criar Resposta a vulnerabilidades regras de atribuição ou de tarefa de correção na aplicação Resposta a vulnerabilidades para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Se um marcador Paris for criado, um marcador PARIS não poderá ser armazenado na tabela de marcadores de máquina. `Paris` e `PARIS` são considerados o mesmo marcador de máquina pelo sistema. O marcador que for importado primeiro será o marcador armazenado e reconhecido.
- Usar marcadores de máquina como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As chaves de grupo são colunas na tabela de tarefas de correção, enquanto os marcadores de máquina devem ser usados somente no Construtor de condições.
- Os marcadores de máquina são controlados pela propriedade do sistema global sn_vul.import_host_tags. Esta propriedade é definida como `verdadeira` por padrão. Desabilitar os marcadores os desabilita em todas as Now Platform® instâncias.

O que fazer a seguir

Depois de baixar a integração Resposta a vulnerabilidades com a Gestão de ameaças e vulnerabilidades da Microsoft ServiceNow® Store, a instalação e a configuração são compatíveis com o Assistente de configuração em Resposta a vulnerabilidades. Para obter mais informações, consulte Instalar e configurar a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.

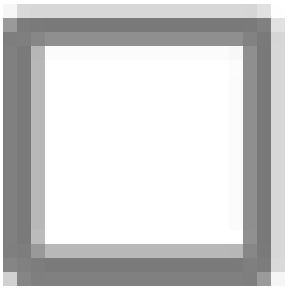
Preparação para a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft

Você pode se preparar para a integração de vulnerabilidade do ServiceNow® Gestão de ameaças e vulnerabilidades da Microsoft (MS TVM) executando tarefas de configuração.

Antes de começar a usar uma check-list

Para instalar e configurar a integração Resposta a vulnerabilidades com a aplicação MS TVM, você pode imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para sua instância Now Platform®.

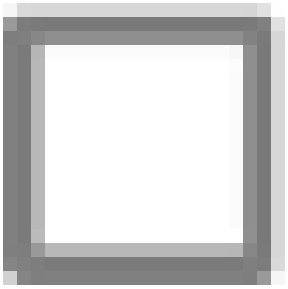
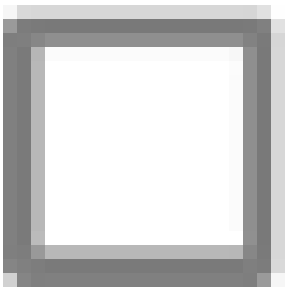
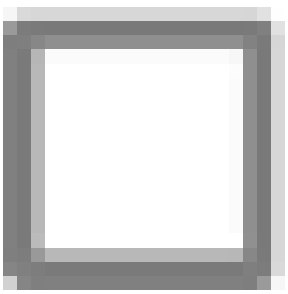
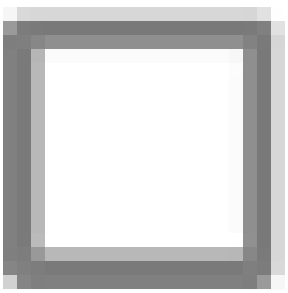
Check-list de preparação da integração

Tarefa	Descrição
	Verifique se você tem um dos seguintes conjuntos de informações: • ClientSecret, ClientId e TenantId para sua conta do MS TVM • Nome de usuário, senha, ClientId e TenantId da sua conta do MS TVM. Para obter essas informações, consulte Configurar o Microsoft Azure para a integração do MS TVM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

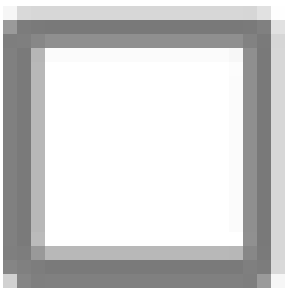
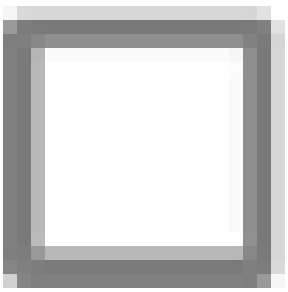
Check-list de preparação da integração

Tarefa	Descrição
	Se ainda não estiver instalado e ativado, instale a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 14.0 de Resposta a vulnerabilidades ou posterior.
	Se você ainda não tiver a aplicação em sua instância, obtenha direitos e baixe a integração Resposta a vulnerabilidades com a aplicação MS TVM para sua instância Now Platform®. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow® Suporte técnico.
	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis: administrador Usa o Assistente de configuração para instalar a integração da Resposta a vulnerabilidades com a aplicação MS TVM. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. sn_vul.vulnerability_admin Conclui a configuração da integração do MS TVM. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Este administrador configura todas as aplicações e regras de VR e configura integrações de terceiros. sn_vul_msft_tvm.configure_integration Configura a integração de vulnerabilidade do MS TVM. Esta função contém a função granular sn_vul_msft_tvm.read_integration. sn_vul_msft_tvm.read_integration

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
	Exibe (lê) registros da integração de vulnerabilidade do MS TVM. Grupo de Resposta a vulnerabilidades Por padrão, o grupo de Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Para obter mais informações, consulte Criar um grupo de usuários . Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.
	Instale a integração Resposta a vulnerabilidades com o NVD e execute a API NIST National Vulnerability Database Integration (somente CVE).
	Para promover um desempenho aprimorado para sua primeira importação, você pode desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não as usar. Essas calculadoras, além de qualquer outra que você tenha definido, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Para obter mais informações, consulte Desabilitação da calculadora de vulnerabilidade padrão se não for usada. • Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem fazer com que muitas notificações sejam geradas, o que pode afetar o desempenho da ingestão.

Você está pronto para Instalar e configurar a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o Microsoft Azure para a integração do MS TVM

Configure sua conta no portal Microsoft do Azure para acessar remotamente a API do Microsoft Threat and Vulnerability Management (MS TVM). Você precisa desta conta para que possa acessar o locatário do MS TVM para coletar informações sobre máquinas, vulnerabilidades e recomendações de segurança.

Antes de Iniciar

Função necessária: Microsoft Administrador do portal do Azure.

Por Que e Quando Desempenhar Esta Tarefa

Conclua as seguintes tarefas de configuração no portal do Azure Microsoft antes de instalar a aplicação ServiceNow® para esta integração.

Para verificar se você tem acesso ao conteúdo mais atual, consulte o site de documentos da Microsoft . Se você não criou uma ID de aplicação para autenticação OAuth 2.0 no Microsoft portal do Azure, siga as etapas deste procedimento.

Procedimento

1. Faça login no Microsoft portal do Azure usando suas credenciais de administrador do portal do Azure.
2. No painel de navegação esquerdo do painel inicial, clique em **Azure Active Directory**.
3. No painel Visão geral, clique em **Registros de apps (Visualização)**.
4. No painel Registros de aplicações (Visualização), clique em **Novo registro**.
   O formulário Registrar uma aplicação é exibido.
5. No formulário, preencha os campos.

Registrar um formulário de aplicação

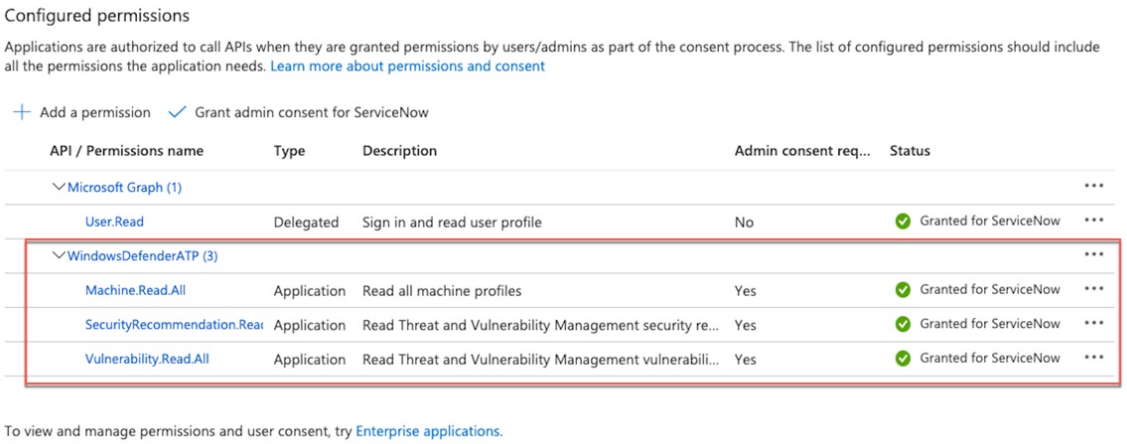
Campo	Descrição
Nome	Nome da aplicação. Neste exemplo, `a integração do MS TVM da ServiceNow` foi inserida.
Tipos de conta compatíveis	Para esta conta, em Tipos de conta compatíveis, clique **em Contas somente neste diretório organizacional (somente ServiceNow - locatário único)**.
Redirecionar URL (opcional)	Se você inserir um valor para este campo, ele não será usado pela integração.

6. Clique em **Registrar**.
   O ID da aplicação (cliente) e o ID do diretório (locatário) são criados. Insira esses valores na página de configuração nos campos ID do **cliente e ID** do **locatário** durante a etapa de configuração no ServiceNow Assistente de configuração da integração VR-TVM. Esta etapa foi descrita em Instalar e configurar a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.
7. Quando você vir o ID da aplicação (cliente) exibido no ServiceNow painel de integração do MS TVM, clique em **Exibir permissões de API**.
8. Navegar até **Solicitar permissões de API** > **APIs que minha organização usa**e clique em **Windows Defender ATP**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. No painel Integração MS TVM da ServiceNow - Permissões de API, clique em **Adicionar uma permissão**.
10. Forneça acesso de leitura a máquinas, vulnerabilidades e recomendações de



segurança.

11. Clique **em Conceder consentimento de administrador para**<your organization name> .

Nota: Para autenticar como uma aplicação de uma instância ServiceNow, execute as seguintes ações:

a. Navegar até **Servicenow MS TVM Integration** > **Certificados e segredos**e clique em **Novo segredo do cliente**.

b. No formulário, preencha os campos.

Formulário de segredos do cliente

Campo	Descrição
Descrição	Nome da aplicação.
Expira	Data de vencimento.

c. Clique em **Adicionar**.

O campo **Valor** é preenchido com o novo segredo do cliente, que é sua nova senha.

Nota: Você precisará desta senha ao configurar a integração em sua instância Now Platform. Para obter mais informações, consulte Instalar e configurar a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração.

d. Salve esta senha em um local seguro. Depois de sair desta página, esta senha não estará disponível.

Você criou com sucesso uma ID de aplicação para autenticação no portal do Azure Microsoft.

O que Fazer Depois

Você está pronto para configurar sua instância Now Platform® para a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar a Integração de resposta a vulnerabilidades com a aplicação MS TVM usando o Assistente de configuração

Instale e configure a integração Resposta a vulnerabilidades com a aplicação Gestão de ameaças e vulnerabilidades da Microsoft (MS TVM) para que você possa usar os dados importados do MS TVM para priorizar e corrigir vulnerabilidades de seus ativos.

Antes de Iniciar

Antes de executar a ServiceNow® Integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft, você deve baixar a aplicação Integração de resposta a vulnerabilidades com Gestão de ameaças e vulnerabilidades da Microsoft na aplicação ServiceNow Store, instalá-la e configurá-la usando o Assistente de configuração na aplicação Resposta a vulnerabilidades.

Antes de instalar a aplicação MS TVM, verifique se você concluiu todos os itens na check-list Preparação para a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft. Para obter informações sobre como configurar sua Microsoft conta do Azure, consulte Configurar o Microsoft Azure para a integração do MS TVM.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Gestão de ameaças e vulnerabilidades da Microsoft no Assistente de configuração. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) para configurar a aplicação no Assistente de configuração após sua instalação.

Por Que e Quando Desempenhar Esta Tarefa

Execute o procedimento a seguir antes de instalar e configurar a integração do MS TVM.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Depois de alguns momentos, as aplicações que estão disponíveis para instalação em sua instância são exibidas.

2. Localize o bloco **Gestão de ameaças e vulnerabilidades da Microsoft** e clique em **Instalar**.

   A integração Resposta a vulnerabilidades com a aplicação Gestão de ameaças e vulnerabilidades da Microsoft que você baixou de ServiceNow Store está instalada.

3. Siga os avisos no Assistente de configuração para continuar com a instalação.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de Integração** > **Integrações do Scanner** no Assistente de configuração para continuar com a configuração. Para obter mais informações para complementar os avisos fornecidos no Assistente de configuração, consulte Configurar a integração de vulnerabilidade do MS TVM usando o Assistente de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de recuperação de dados para a integração da Gestão de ameaças e vulnerabilidades da Microsoft

Você pode usar as configurações de recuperação de dados para ajudá-lo a determinar o tipo e o escopo dos dados que deseja importar da integração de vulnerabilidade ServiceNow® do Microsoft Threat and Vulnerability Management (MS TVM) para sua instância Now Platform®.

As configurações de recuperação de dados ajudam a controlar os dados que você deseja importar. Você pode definir os valores desses filtros em instâncias de integração. Para exibir as instâncias de integração, navegue até **Integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft** > **Instâncias de Integração** e clique na integração do MS TVM.

Na página Instância de integração, clique em **Parâmetros** de instância de integração para exibir uma lista de parâmetros ou clique na guia **Integrações de vulnerabilidade** para obter uma programação, detalhes de REST, detalhes de integração, fontes de dados e informações de execução de integração.

Configurações e filtros de recuperação de dados para as integrações do MS TVM em sua instância Now Platform

As configurações a seguir estão disponíveis para as integrações do MS TVM em sua instância Now Platform. Essas e outras definições de configuração são exibidas na página Instância de integração da sua instância Now Platform. Você pode preferir deixar essas configurações em suas configurações padrão para as primeiras execuções de integração.

MS TVM.

vi_size_limit

Define o número de registros de item vulnerável a serem incluídos no conjunto de resultados da integração de vulnerabilidades da máquina com MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2.000.

vulnerabilidades_size_limit

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração do MS TVM Vulnerability (CVE). Esta configuração deve estar no formato int32. O valor padrão é 2.000.

recomendações_tamanho_limite

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração de recomendações do MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2.000.

ativo_tamanho_limite

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração de máquinas com MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2.000.

filtro_máquina

Filtra as máquinas provenientes do MS TVM. Este filtro é aplicado à integração de máquinas com MS TVM. O valor padrão é trazer máquinas em que onBoardingStatus é onBoarded.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagens de REST para a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft

Você pode usar as mensagens de REST da ServiceNow® Integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft (MS TVM) para fazer chamadas para a API do MS TVM.

Token de acesso do MS TVM

Você também pode usar as mensagens de REST do token de acesso do MS TVM para recuperar o token de acesso da API do MS TVM para que possa autenticar as solicitações de API de REST. As mudanças no método de registro da mensagem REST afetam as solicitações de autenticação feitas ao MS TVM.

Integração com MS TVM

Você pode usar a mensagem REST para a integração do MS TVM para recuperar informações do MS TVM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao MS TVM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Métodos REST

Método REST	Descrição do método
GET vulnerabilidades	Recupera informações de vulnerabilidade e exploração do MS TVM.
GET vulnerabilidades de software por máquina	Recupera todas as vulnerabilidades em aberto.
GET recomendações	Recupera a lista de todas as recomendações de segurança acionáveis que afetam a organização.
GET máquinas	Recupera a coleção de ativos.
GET mudanças de vulnerabilidades de software por máquina	Recupera todas as informações que mudaram na importação de vulnerabilidade completa da organização, incluindo vulnerabilidades novas, corrigidas e atualizadas.

Transformação de dados para a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft

Depois de identificar os dados que deseja importar, os dados são recuperados da aplicação ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM), processados por meio de um conjunto de fontes de dados e transformados em sua instância.

Durante a instalação, os mapas de severidade normalizada são instalados no módulo Mapeamento de severidade normalizada. Esses mapas transformam níveis de severidade de vulnerabilidade de terceiros importados Microsoft em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de severidade, consulte Criar um Resposta a vulnerabilidades mapa de severidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de máquinas com MS TVM

Os dados das máquinas importadas são carregados primeiro na tabela Importação de máquinas do MS TVM [sn_vul_msft_tvm_machines_import].

A transformação de máquinas do MS TVM é usada para transformar as informações das máquinas importadas.

Nota: As mudanças neste mapa de transformação alteram a forma como os dados da importação de máquinas MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise **Transformação de máquinas com Microsoft TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de máquinas MS TVM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo para ativos. Este ID é mapeado para o source_id do registro do item descoberto.
u_ipaddresses.macAddress	mac_address	Endereço MAC que é mapeado da API para o campo de endereço MAC do host do registro cmdb_ci.
u_ipaddresses.ipAddress	ip_address	Campo de endereço IP que é mapeado para o campo de endereço IP do registro cmdb_ci.
u_lastseen	última_scan_data	Campo que é mapeado para o campo last_scan_date no registro do item descoberto.
u_machinetags		Marcadores que são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.
u_osplatform	os	Campo que é mapeado para o campo do sistema operacional no registro cmdb_ci.
u_computerdnsname	fqdn	Campo que mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo e finalidade do script do mapa de transformação das máquinas MS TVM

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para atualizar valores no host e verificar se o host existe. Com base nos resultados, este script modifica os valores na variável de escopo (sn_vul_msft_tvm). Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

A inclusão de script MicrosoftTVMMachinesProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração das máquinas do Microsoft TVM e a transforma em um IC. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados das máquinas do Microsoft TVM no IC e na tabela de itens descobertos.

Integração de vulnerabilidades do MS TVM

Os dados de vulnerabilidades importados são carregados primeiro na tabela de importação de CVE (vulnerabilidades) do Microsoft TVM [sn_vul_msft_tvm_vulnerability_import].

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades do MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise a **Transformação de vulnerabilidades do Microsoft TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de vulnerabilidades do Microsoft TVM

Campo de origem	Campo de destino	Descrição
u_id	ID	Mapas para a coluna ID do registro sn_vul_entry.
gravidade_u	gravidade_origem	Mapeia o campo Gravidade para a gravidade. O valor padrão é 5.
u_publishedon	date_published	Mapeia o campo u_publishedon para a data de publicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de vulnerabilidades do Microsoft TVM

Campo de origem	Campo de destino	Descrição
u_publicexploit	exploração_publica	Mapeia o u_publicexploit fornecido pelo scanner para a coluna de exploração pública na tabela de entrada de vulnerabilidade.
u_cvssv3	v3_base_score	Mapeia a pontuação cvssv3 para a pontuação base v3 no registro de entrada de vulnerabilidade.
u_description	resumo	Mapeia a descrição para o campo de resumo no registro de entrada de vulnerabilidade.
u_exploitinKit	malware_kit	Mapeia o campo u_exploitinkit para o kit de malware na tabela de exploração.
u_exploittypes	tipo	Mapeia o tipo de exploração para o tipo na tabela de exploração.
u_exploitverified	is_exploit_verified	Mapeia o campo u_exploitverified para a exploração verificada na tabela Exploit.
u_exploituris	exploit_links	Mapeia o campo u_exploituris para os links de exploração na tabela Exploração.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para criar ou atualizar os valores no NVD ou na tabela de entrada de terceiros. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir os valores dos novos itens que foram criados e os itens que foram atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de recomendações do MS TVM

Os dados de recomendação importados são carregados primeiro na tabela Importação de recomendações do MS TVM [sn_vul_msft_tvm_recom_import].

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de recomendações do MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise por **Transformação de recomendação do MS TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
u_recommendedvendor	recomendado_fornecedor	Mapeia o campo u_recommendedvendor para a coluna Fornecedor.
u_fraquezas	pontos fracos	Mapeia o campo u_weaknesses para a coluna Pontos fracos.
u_exposedmachinescount	src_exposed_machines_cnt	Mapeia o campo u_exposedmachinescount para a coluna Contagem de máquinas expostas.
u_status	status	Mapeia o status para o campo Status no registro de recomendação.
u_productname	product_name	Mapeia o campo u_productname para o nome do produto no registro de recomendação.
u_nonproductiv_impactedassets	non_prod_impacted_assets	Mapeia o campo u_nonproductiv_impactedassets para a coluna Ativos afetados no registro de recomendação.
alerta_ativo_u	alerta_ativo	Mapeia o campo u_activealert para a coluna Alerta ativo no registro de recomendação.
u_recommendedversion	recomendado_versão	Mapeia o campo u_recommendedversion para a coluna Versão recomendada no registro de recomendação.
u_totalmachinecount	total_machine_count	Mapeia o campo u_totalmachinecount para a coluna Contagem total

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
		de máquinas no registro de recomendação.
u_exposureimpact	exposição_impacto	Mapeia o campo u_exposureimpact para a coluna Impacto da exposição no registro de recomendação.
u_recommendationname	recomendação_nome	Mapeia o campo u_recommendationname para a coluna Nome da recomendação no registro de recomendação.
u_subcategoria	subcategoria	Mapeia o campo u_subcategory para a coluna Subcategoria no registro de recomendação.
u_id	source_id	Mapeia o ID de recomendação do MS TVM para a coluna ID de origem.
u_remediationtype	correção_tipo	Mapeia o campo u_remediationtype para a coluna Tipo de correção no registro de recomendação.
u_relatedcomponent	related_component	Mapeia o campo u_relatedcomponent para a coluna Componente relacionado no registro de recomendação.
u_recommendedprogram	programa_recomendado	Mapeia o campo u_recommendedprogram para a coluna Programa recomendado no registro de recomendação.
u_recommendationcategory	recomendação_categoria	Mapeia o campo u_recommendationcategory para a coluna Categoria de recomendação no registro de recomendação.
u_publicexploit	exploração_publica	Mapeia o campo u_publicexploit para a coluna Exploração pública no registro de recomendação.
u_vendor	fornecedor	Mapeia o campo u_vendor para a coluna Fornecedor no registro de recomendação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
[Script]	integração_instance	Nome da instância da qual a recomendação é importada.
[Script]	sys_domain	Domínio no qual este registro é importado.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Script do mapa de transformação de recomendação do MS TVM

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para atualizar valores nas recomendações e verificar se as recomendações existem. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir os valores de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de vulnerabilidades da máquina do MS TVM

O mapa de transformação de vulnerabilidades da máquina do MS TVM é usado para transformar informações de vulnerabilidades abertas e fixas que são importadas do MS TVM.

Nota: As mudanças neste mapa de transformação alteram o modo como os dados da Importação de vulnerabilidades de máquina do MS TVM são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e corrigidas do MS TVM, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise a **Transformação de vulnerabilidades da máquina do MS TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação das vulnerabilidades da máquina do MS TVM

Campo de origem	Campo de destino	Descrição
u_id	detecção_chave	Mapeia o campo u_id para a coluna Chave de detecção na tabela de detecção.
u_diskpaths	prova	Mapeia o campo u_diskpaths para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação das vulnerabilidades da máquina do MS TVM

Campo de origem	Campo de destino	Descrição
		a coluna Prova na tabela de detecção.
u_registrypaths	prova	Mapeia o campo u_registrypaths para a coluna Prova na tabela de detecção.
u_recommendedsecurityupdateid	solução_preferida	Mapeia o campo u_recommendedsecurityupdateid para a coluna Solução preferencial na tabela de itens vulneráveis, se a solução existir com o mesmo ID na tabela sn_vul_solution.
u_recommendationreference	recomendação	Mapeia o campo u_recommendationreference para a coluna Recomendação na tabela de itens vulneráveis.
u_cveid	vulnerabilidade	Mapeia o campo u_cveid para a coluna Vulnerabilidade na tabela de itens vulneráveis.
u_status	status_origem	Mapeia o campo u_status para a coluna Status de origem na tabela de detecção.
u_eventtimestamp	pontuação_ temporal	Mapeia o campo u_eventtimestamp para a coluna Último encontrado na tabela de itens vulneráveis.
u_lastseentimestamp	last_seen	Mapeia o campo u_lastseentimestamp para a coluna Visto pela última vez na tabela de itens vulneráveis.
u_firstseentimestamp	first_seen	Mapeia o campo u_firstseentimestamp para a coluna Visto pela primeira vez na tabela de itens vulneráveis.
u_recommendedsecurityupdate	solution_summary	Mapeia o campo u_recommendedsecurityupdate

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação das vulnerabilidades da máquina do MS TVM

Campo de origem	Campo de destino	Descrição
		para a coluna Resumo da solução na tabela de itens vulneráveis.
u_recommendedsecurityupdateurl	solution_summary	Mapeia o campo u_recommendedsecurityupdateurl para a coluna Resumo da solução na tabela de itens vulneráveis.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para verificar se a entrada de vulnerabilidade e as detecções existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para atualizar a contagem de IVs e Detecções importadas do MS TVM. Este script é para uso interno e não deve ser modificado ou excluído.

Gráfico de status de execução da integração para a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft

Você pode usar o módulo de status de execução de integração da Gestão de ameaças e vulnerabilidades da Microsoft (MS TVM) para fornecer uma exibição gráfica do status das execuções de integração do MS TVM.

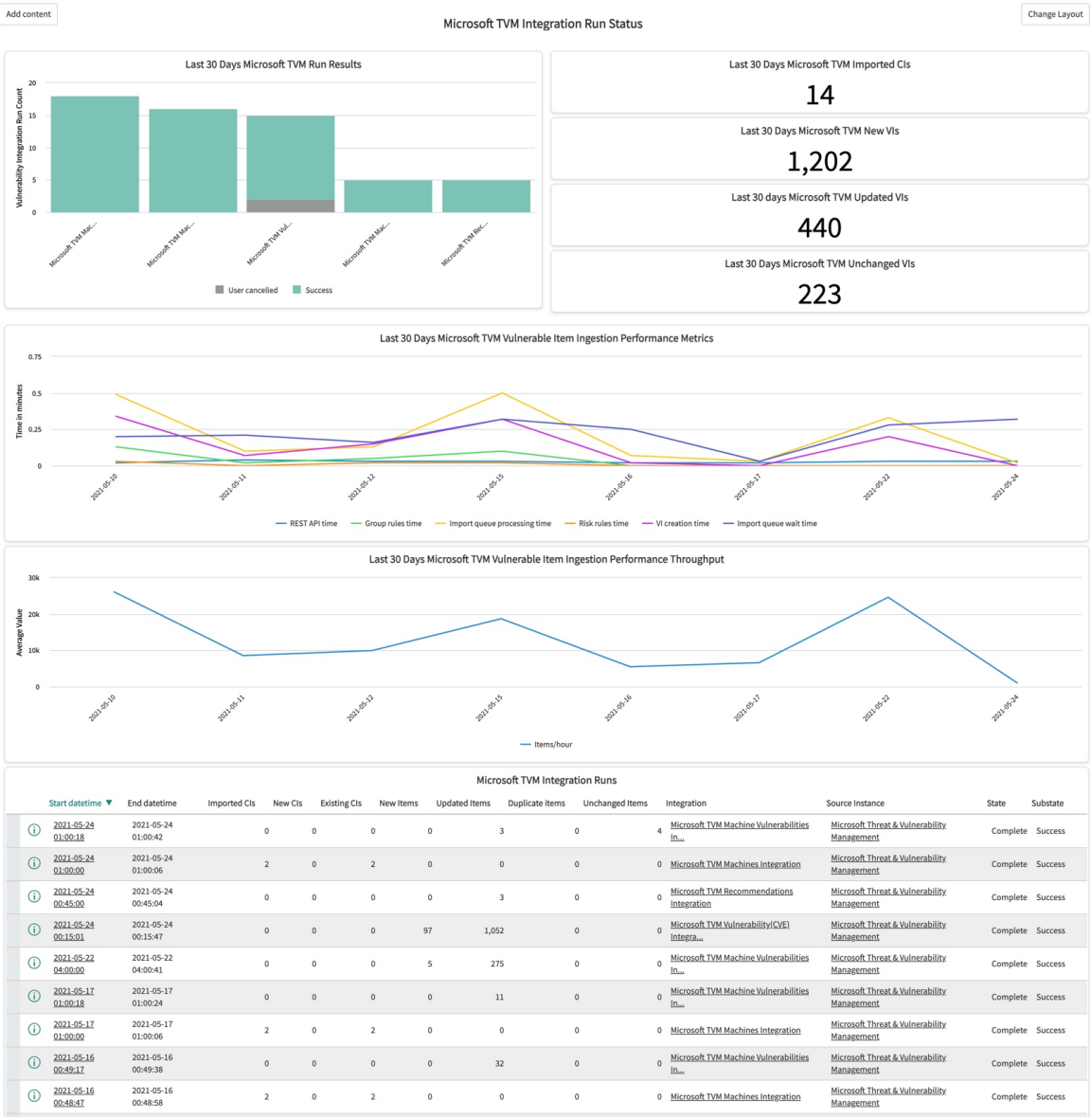
A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, você pode apontar para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer parte do gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Relatórios do gráfico de status de execução da integração do MS TVM

Nome	Descrição
Resultados dos últimos 30 dias do Microsoft TVM	Número de execuções de integração que foram concluídas para cada integração. Este relatório mostra as execuções bem-sucedidas e com falha. Cada execução é exibida como uma barra no gráfico.
VIs novos do Microsoft TVM nos últimos 30 dias	Número de novos itens vulneráveis que foram importados nos últimos 30 dias.
VIs atualizados do Microsoft TVM nos últimos 30 dias	Número de itens vulneráveis atualizados que foram importados nos últimos 30 dias.
VIs inalterados do Microsoft TVM nos últimos 30 dias	Número de itens vulneráveis duplicados que foram importados nos últimos 30 dias.
Execuções de integração do MS TVM	Registros de execução de integração em uma lista.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: V16.1: para verificar as detecções desta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow[*sn_vul_detection*] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na contagem de detecção ou descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem de data até" na instância, após a conclusão da execução da integração.
Métricas de desempenho de ingestão de item vulnerável do Microsoft TVM nos últimos 30 dias	Métricas de desempenho diárias para itens vulneráveis comparados nos últimos 30 dias.
Taxa de transferência de desempenho de ingestão de item vulnerável do Microsoft TVM nos últimos 30 dias	Taxa de transferência de ingestão de item vulnerável diária que foi medida para a integração de detecção de host do Microsoft TVM nos últimos 30 dias.
ICs importados do Microsoft TVM nos últimos 30 dias	Número de novos itens de configuração que foram importados nos últimos 30 dias.

Verificar o status de execução da importação da integração da Gestão de ameaças e vulnerabilidades da Microsoft

Use o status de execução de importação da Gestão de ameaças e vulnerabilidades da Microsoft (MS TVM) para verificar o sucesso das execuções de integração e localizar quaisquer problemas.

Antes de Iniciar

Este procedimento faz as seguintes suposições:

- Você tem Resposta a vulnerabilidades e a Integração de vulnerabilidade do MS TVM instalados e configurados.
- As importações de integração de vulnerabilidade do MS TVM estão programadas e em execução.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Gestão de ameaças e vulnerabilidades da Microsoft** > **Integrações**.
   a. Escolha uma integração.
   b. Clique na lista relacionada Execuções de integração de vulnerabilidade.
2. Verifique se o estado das importações é Concluído, com o Subestado como Êxito. As causas mais comuns de falha na execução são as seguintes:
   - Interrupção de rede.
   - Declínio de bits na transferência de dados, resultando em dados corrompidos durante a transformação.
3. Opcional: Se você vir uma dessas condições que causaram uma falha na execução, clique em **Executar agora** e execute novamente a integração.

Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades

Você pode gerenciar patches e implantações de patches para vulnerabilidades críticas de grandes grupos de ativos com a integração de orquestração de patches Resposta a vulnerabilidades com o produto HCL BigFix.

Orquestração de patches com Resposta a vulnerabilidades

A orquestração de patches com Resposta a vulnerabilidades usa importações agendadas de integrações de soluções de terceiros, fornecedores de patch e scanners de vulnerabilidade. Os dados de detecção do scanner correspondem aos ativos em seu ambiente com as vulnerabilidades e com as atualizações de patch que podem corrigi-las. Envie solicitações de patch para aprovação, programe atualizações de patch para resolver itens vulneráveis e monitore o andamento da correção, tudo a partir de registros na aplicação Resposta a vulnerabilidades em seu Now Platform®.

Vulnerability Response Patch Orchestration with HCL BigFix

Quando a Orquestração de patches de resposta a vulnerabilidades com integração do HCL BigFix é usada com as aplicações ServiceNow® Solução de gestão de vulnerabilidade, Orquestração de patches e Resposta a vulnerabilidades, os gerentes e analistas de vulnerabilidade podem executar as seguintes tarefas:

- Veja mais contexto e informações sobre os tipos de patches e soluções de fornecedores (patches).
- Exiba e monitore dados de vulnerabilidade e solução, bem como o andamento da correção de vulnerabilidades de registros nos espaços Resposta a vulnerabilidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os especialistas em TI e os proprietários de correção podem executar as seguintes tarefas:

- Implante patches compatíveis com o produto BigFix para seus Windows, CentOS, MAC, Oracle e outros ativos em intervalos regulares e programados fora do horário comercial para evitar conflitos de trabalho.
- Identifique ativos sem patch com vulnerabilidades ou ativos que não foram atualizados com sucesso por patches programados a partir de dados de detecção importados de scanners de terceiros.
- Programe os patches disponíveis do Espaço de correção de TI ou do ambiente clássico para ativos vulneráveis e sem patch da atualização de patch, tarefa de correção e registros de itens descobertos.

Termos-chave nas aplicações Resposta a vulnerabilidades e BigFix

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em seu Configuration Management Database (CMDB). BigFix chama ICs, computadores.

Grupos de computadores

Terminologia usada no produto BigFix que se refere a um grupo de ativos.

Item vulnerável

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB.

Instância

Uma conta distinta da aplicação BigFix. Cada conta de usuário pode ser uma instância na aplicação BigFix. Este termo também se refere a um endereço da Web exclusivo e seguro para uma instância Now Platform.

Integração

Uma integração é um trabalho agendado no Now Platform que recupera informações de uma fonte de terceiros, como a integração com as máquinas do BigFix.

Solução

Existem dois tipos de soluções no contexto desta integração, potenciais e preferenciais. Uma possível solução é aquela que pode resolver uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis. Uma solução preferencial corresponde à solução mais eficaz para uma vulnerabilidade específica detectada.

Patch

Atualizações de software que corrigem vulnerabilidades. Na aplicação BigFix, os patches são chamados de Fixlets. Por exemplo, o BigFix tem Fixlets para Windows, CentOS, MAC, Oracle e outros produtos.

Patch preferencial

Patches preferenciais são atualizações de software que têm como objetivo corrigir vulnerabilidades específicas. Os patches, uma vez implantados, são mapeados para os itens vulneráveis que estão relacionados a vulnerabilidades específicas e os corrigem.

Tarefa de correção

Listas de itens vulneráveis na aplicação Resposta a vulnerabilidades de ações que são necessárias para corrigir vulnerabilidades.

Implantação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para fins desta integração, a implantação se refere a quando você aplica, inicia ou programa um patch em uma máquina. O BigFix chama essas implantações de ações. Você pode implantar (criar ações) para os patches baixados do BigFix em seu Now Platform. Navegue até itens descobertos, patches ou tarefas de correção de registros individuais em Resposta a vulnerabilidades. Você pode implantar patches com trabalhos agendados em máquinas individuais ou em grupos de computadores.

A implantação no Now Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações da integração do BigFix Vulnerability em seu ambiente.

Gestão de soluções de vulnerabilidade e Orquestração de patches de resposta a vulnerabilidades com HCL BigFix Integration

A gestão de soluções é fornecida pela aplicação Solução de gestão de vulnerabilidade, uma aplicação Now Platform que correlaciona suas descobertas de vulnerabilidade com o detalhamento das soluções (patches) que as corrige. Identifique os patches de software de terceiros para produtos e serviços, atualizações de configuração e outros controles que têm o maior impacto para sua organização. Junto com as informações do scanner de terceiros, as aplicações Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidadese a Orquestração de patches de resposta a vulnerabilidades com HCL BigFix trabalham juntos para distribuir os patches preferenciais da solução, para a vulnerabilidade, para o item vulnerável para ajudá-lo a corrigir e fechar vulnerabilidades ao seu ambiente.

O Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidadese a Orquestração de patches de resposta a vulnerabilidades com HCL BigFix Integration estão todos disponíveis no ServiceNow® Store.

Funções necessárias de Now Platform

As tarefas de instalação, configuração e correção de integração exigem as funções a seguir em sua instância Now Platform.

administrador

Usuários com esta função obtêm direitos para aplicações nas instâncias ServiceNow Store e as baixam para instâncias Now Platform.

sn_vul.vulnerability_admin

Usuários com esta função ativam aplicações na instância Now Platform e concluem a configuração da aplicação Resposta a vulnerabilidades. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Este usuário administrador configura todas as aplicações de VR, regras e integrações de terceiros.

sn_vul_bigfix.configure_integration

Usuários com esta função configuram a aplicação BigFix Patch Orchestration Integration. Esta função contém a função granular sn_vul_bigfix.read_integration.

sn_vul_bigfix.read_integration

Usuários com esta função podem visualizar (somente leitura) os registros da Resposta a vulnerabilidades e da aplicação Integração de orquestração de patches do BigFix e os dados de orquestração de patches.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sn_vul_patch_orch.configure_patch

Usuários com esta função podem configurar e aplicar patches.

sn_vul_patch_orch.read_patch

Usuários com esta função podem exibir (somente leitura) informações de patch.

Aprovadores

Atribua usos aos grupos de aprovadores de nível 1 e aprovador de nível 2 se quiser que as solicitações de patch enviadas sejam aprovadas antes da implantação.

Para obter mais informações sobre como atribuir essas funções usando o Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre as funções Resposta a vulnerabilidades em seu Now Platform, consulte Resposta a vulnerabilidades personas e funções granulares.

Regras de pesquisa de IC

Quando os dados são importados da aplicação BigFix, a aplicação Resposta a vulnerabilidades pesquisa automaticamente correspondências em Configuration Management Database (CMDB) usando dados da máquina (ativo). Regras de pesquisa de IC são usadas para identificar ICs (ativos) e adicioná-los automaticamente aos registros de item vulnerável (VI) quando os IVs são criados.

As seguintes regras de pesquisa de IC são enviadas com o sistema de base e são usadas para identificar ICs (ativos) e adicioná-los à aplicação Resposta a vulnerabilidades :

- MAC_ADDRESS
- ENDEREÇO_IP
- DNS_NAME

Você pode usar vários valores para o IP_ADDRESS de um ativo. Uma regra de pesquisa de IC considera todos os valores para correspondência. Para obter mais informações sobre como as regras de pesquisa de IC e como elas funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.

MID Server

A Resposta a vulnerabilidades Orquestração de patches com integração HCL BigFix é uma integração no local. Ele requer um MID Server autônomo que não faz parte de um cluster de MID Server. O MID Server é necessário para executar scripts em máquinas remotas da sua instância para importar dados do servidor BigFix. As APIs para esta integração são chamadas usando MID Servers que você configura em sua instância Now Platform. Para obter mais informações, consulte Preparação para a Resposta a vulnerabilidades Integração de Orquestração de patches com HCL BigFix.

Integrações e dependências da Resposta a vulnerabilidades Integração de Orquestração de patches com HCL BigFix

As aplicações de produto e dependência a seguir são necessárias para a Orquestração de patches de resposta a vulnerabilidades com HCL BigFix Integration. Essas aplicações estão disponíveis no ServiceNow® Store.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

Para exibir dados de orquestração de patches e atualizações disponíveis (patches) nos espaços em Resposta a vulnerabilidades, as seguintes aplicações são necessárias. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas.

Para obter mais informações sobre a compatibilidade de versões com as aplicações e versões da família necessárias, consulte o artigo KB0856498 Matriz de compatibilidade da Resposta a vulnerabilidades e mudanças no esquema de versão na Base de conhecimento HI.

Aplicação e versão de lançamento
Resposta a vulnerabilidades
Solução de gestão de vulnerabilidade
Aplicação Vulnerability Response Patch Orchestration
Resposta a vulnerabilidades Orquestração de patches com aplicação HCL BigFix
Security Support Common
Orquestração de suporte de segurança
Uma aplicação de scanner de vulnerabilidade de terceiros compatível

Resposta a vulnerabilidades Tabelas da aplicação Orquestração de patches

A aplicação Orquestração de patches Resposta a vulnerabilidades contém as seguintes tabelas:

Tabela	Descrição
Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Atualização de dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de itens descobertos.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre Coleções e ICs.
Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de orquestração de patches da Resposta a vulnerabilidades com HCL BigFix

As integrações desenvolvidas pela engenharia ServiceNow® compõem a implantação da solução orquestrada com o produto BigFix. As seguintes integrações estão incluídas com a aplicação Resposta a vulnerabilidades Patch Orchestration Integration with HCL BigFix que você baixa do ServiceNow® Store.

Depois de instalar a aplicação de integração em sua instância Now Platform, para exibir essas integrações, navegue até **Integrações** > **Integração da Orquestração de patches do BigFix** > **Integrações**. A aplicação Resposta a vulnerabilidades processa dados em intervalos de tempo programados importados por essas integrações com endpoints do BigFix.

Integração	Descrição
Integração do BigFix Collection	• Esta integração está programada para ser executada diariamente e é executada primeiro na execução de integração encadeada. • Recupera os computadores e grupos de computadores que compõem os grupos de computadores (itens de configuração) da aplicação BigFix.
Integração de Fixlet do BigFix	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Collection. Você também pode executá-lo sob demanda. • Recupera informações sobre todos os fixlets (patches) disponíveis do servidor BigFix.
BigFix Device Fixlet Integration	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Fixlet. Você também pode executá-lo sob demanda. • Recupera informações sobre os fixlets que estão atualmente em computadores (ativos) do servidor BigFix.
Integração de ações do BigFix	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Device Fixlet. Você também pode executá-lo sob demanda. • Recupera informações sobre os patches programados pela equipe de TI no servidor BigFix.

Preparação para a Resposta a vulnerabilidades Integração de Orquestração de patches com HCL BigFix

Prepare-se para a integração executando as seguintes tarefas de configuração.

Antes de Iniciar

Funções necessárias: administrador para instalar as aplicações e atribuir funções. Outras funções estão listadas na tabela a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

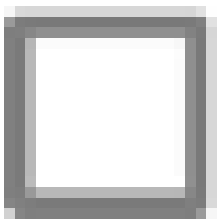
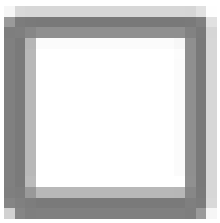
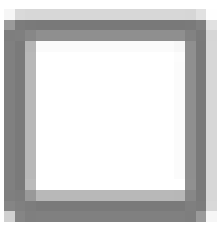
Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração.

Você está pronto para Instalar a aplicação Resposta a vulnerabilidades Patch Orchestration with HCL BigFix.

Procedimento

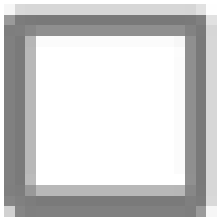
1. Para uma instalação e configuração tranquilas da aplicação Resposta a vulnerabilidades Patch Orchestration with HCL BigFix, siga a check-list fornecida.
2. Você pode preferir imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação.

   Após a instalação e a configuração, importe as informações relacionadas a patches e vulnerabilidades para sua instância Now Platform®.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte, Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 16.0 de Resposta a vulnerabilidades ou posterior.
	Se ainda não estiver instalado, obtenha direitos e instale um aplicativo de scanner de terceiros para importar dados de vulnerabilidade. Consulte Integrações do Resposta a vulnerabilidades para obter mais informações sobre scanners de terceiros compatíveis com Resposta a vulnerabilidades. Consulte .
	Se ainda não estiver instalado, obtenha direitos e baixe a Orquestração de patches de resposta a vulnerabilidades com a aplicação HCL BigFix para sua instância Now Platform®. Consulte .
	Obter credenciais do BigFix. Verifique se você tem nomes de contas, senhas e outras informações de serviço exigidas por seus produtos BigFix para que você tenha acesso a eles.

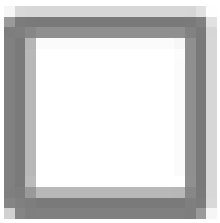
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. administrador O administrador do sistema obtém direitos, baixa e instala a aplicação BigFix Patch Orchestration e as outras aplicações necessárias para a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração em Resposta a vulnerabilidades ou no módulo Administração de usuários. sn_vul.vulnerability_admin Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das integrações do BigFix e de outras aplicações de terceiros. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Esta função configura todas as aplicações de VR, regras, integrações de terceiros, Orquestração de patches de resposta a vulnerabilidades e aplicações de Gestão de soluções de vulnerabilidade. sn_vul_bigfix.configure_integration Usuários com esta função configuram a aplicação BigFix Patch Orchestration Integration. Esta função contém as funções granulares sn_vul_bigfix.read_integration e connection_admin que permitem ao usuário se conectar ao console do BigFix e configurar as instâncias de integração em seu Now Platform. sn_vul_bigfix.read_integration Usuários com esta função podem visualizar (somente leitura) os registros da Resposta a vulnerabilidades e da aplicação Integração de orquestração de patches do BigFix e os dados de orquestração de patches. sn_vul_patch_orch.configure_patch Usuários com esta função podem configurar e aplicar patches. Os patches solicitados por este usuário do item vulnerável e os registros de atualização de patch serão enviados para aprovação se a gestão de mudanças estiver ativa e os aprovadores estiverem atribuídos. sn_vul_patch_orch.read_patch

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Usuários com esta função podem exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os Espaços de correção e vulnerabilidade de TI. Aprovadores Usuários atribuídos ao Aprovador nível 1 e, opcionalmente, ao Aprovador nível 2, grupos de aprovadores aprovam as solicitações de patch enviadas. Por padrão, os patches são enviados ao grupo de aprovadores de nível 1 para aprovação antes da implantação. Para obter mais informações sobre o processo de aprovação, consulte Orquestração de patches com Resposta a vulnerabilidades. Para obter mais informações sobre como configurar aprovadores e grupos, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos para a integração. Por padrão, o grupo de Resposta a vulnerabilidades está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais para funções de especialista em correção e analista de vulnerabilidade e adicionar usuários com o módulo Administração de usuário em sua instância. Consulte Criação de um grupo de usuários .
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. ◦ A Orquestração de patches de resposta a vulnerabilidades com HCL BigFix é uma integração no local que requer o uso de um MID Server autônomo. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . ◦ Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

O que Fazer Depois

Agora você está pronto para Instalar a aplicação Resposta a vulnerabilidades Patch Orchestration with HCL BigFix.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar a aplicação Resposta a vulnerabilidades Patch Orchestration with HCL BigFix

Baixe a Orquestração de patches de resposta a vulnerabilidades com a aplicação HCL BigFix em ServiceNow® Store.

Antes de Iniciar

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)) para configurar a Orquestração de patches de resposta a vulnerabilidades com HCL BigFix e outras aplicações depois que elas forem instaladas.

Por Que e Quando Desempenhar Esta Tarefa

Antes de instalar a aplicação, verifique se você concluiu todos os itens da check-list em Preparação para a Resposta a vulnerabilidades Integração de Orquestração de patches com HCL BigFix.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Procedimento

1. Navegar até **Todos** > **Aplicações do sistema** > **todas as aplicações disponíveis** > **Todos**.
2. Localize a aplicação **Vulnerability Response Patch Orchestration with HCL BigFix** e clique em **Instalar**.

   Esta ação instala a aplicação que você baixou de ServiceNow Store.
3. Como alternativa, você pode instalar aplicações do Assistente de configuração. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Todos** > **Integração da Orquestração de patches do BigFix** > **Configuração** para continuar com a configuração.

Configurar a integração de orquestração de patches Resposta a vulnerabilidades com HCL BigFix

Depois de instalar a aplicação, configure-a com as informações da sua conta do BigFix e valide suas credenciais.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin e sn_vul_bigfix.configure_integration

Procedimento

1. Navegar até **Integração da Orquestração de patches do BigFix** > **Configuração**.
2. Preencha os campos com suas informações e credenciais do BigFix.

Campo	Descrição
Instância de integração	O nome da conta da instância do BigFix que você deseja usar, por exemplo, `BigFix Patch Management integration`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome do host	Insira o URL do host do BigFix.
Nome de usuário	Insira o nome de usuário da sua conta do BigFix.
Senha	Insira a senha da sua conta do BigFix.
MID Server	Insira o nome do MID Server autônomo na lista que você deseja usar. Consulte Preparação para a Resposta a vulnerabilidades Integração de Orquestração de patches com HCL BigFix para obter mais informações sobre MID Servers e configurar tarefas em seu Now Platform®.

3. Clique em Salvar e testar credenciais.
   O status da sua conexão entre o BigFix e sua instância Now Platform® é exibido no campo Status de validação. Se você não vir um teste bem-sucedido, siga os avisos.
4. Opcional: A separação de domínios é compatível com esta integração.
   Você pode adicionar várias configurações de à sua instância. Para adicionar configurações adicionais:

   a. Navegar até **Integração da Orquestração de patches do BigFix Instâncias de integração**.

   b. Verifique se o escopo da aplicação, `Orquestração de patches de resposta a vulnerabilidades com HCL BigFix`, é exibido no campo Escopo da aplicação.

   c. Clique em **Nova**.

   d. Preencha o formulário.

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Vulnerability Response Patch Orchestration with HCL BigFix
Integração	[Somente leitura] A gestão de patches do BigFix é o padrão.
Ativo	O padrão é ativado (selecionado). Se desmarcada, a instância não está ativa.

   e. Clique em **Enviar**.
   Sua nova instância de integração é exibida na lista Instâncias de integração.

   f. Repita as etapas 1 a 3 para configurar sua instância de integração e testar suas credenciais.

5. Configure aprovações para solicitações de patch.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, uma propriedade do sistema [**sn_vul_patch_orch.patch_approval_required**] é ativada para que, quando as implantações de patch forem programadas, elas sejam enviadas para revisão e aprovação para usuários atribuídos ao Nível 1 - Grupo de aprovação de atualizações de patch.

Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, poderá desativar a propriedade [**sn_vul_patch_orch.patch_approval_required**]. Você pode preferir deixar as aprovações ativadas para que os patches programados não entrem em conflito com o horário comercial normal.

Nota: Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema:

a. Navegar até **sys.properties.list**.

b. Localize **sn_vul_patch_orch.patch_approval_required** e clique nele para abrir o registro.

c. No campo Valor, digite `falso`.

d. Clique em **Atualizar**.

6. Se você não desativar esta propriedade, deverá atribuir aprovadores para solicitações de patch.
Como um usuário com a função sn_vul.vulnerability_admin, siga estas etapas.

a. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.

b. Se a Regra de **aprovação Implantar aprovação de atualização de patch** não for exibida na lista, clique em **Todos** à direita do ícone de filtro verde no canto superior esquerdo da tela para exibir a lista inteira.

c. Na lista, clique em **Implantar aprovação de atualização de patch**.

d. No registro, com a guia Configuração de aprovação selecionada, clique em **Configuração padrão Aprovação de atualização de patch**.

e. No registro, clique em **Nível 1 - Aprovação de atualização de patch**.

f. Adicione usuários a este grupo.

Os usuários atribuídos a este grupo aprovam as solicitações de patch enviadas por usuários com a função sn_vul_patch_orch.configure_patch. Navegue até **Minhas aprovações** para exibir e processar as solicitações.

7. Clique em**Atualizar** para salvar suas mudanças.

8. Opcional: Você pode configurar aprovações de vários níveis para que mais de uma aprovação seja necessária antes da implantação de solicitações de patch programadas.

a. Com o registro de aprovação da Atualização de patch de configuração padrão exibido, clique em **Novo**.

b. Preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome do nível de aprovação, por exemplo, **Nível 2 - Aprovação de atualização de patch**.
Ativo	Ativado por padrão, o que significa que o nível de aprovação está em uso.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ▪ Um aprovador necessário ▪ Todos os usuários devem aprovar
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Função	Selecione uma função para o grupo na lista.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção: ▪ Usuário e grupo de usuários ▪ Campo da tabela de aprovação ▪ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções especificadas por você.
Usuários	Edite os usuários listados nos grupos.

Tradução automática

c. Clique em **Enviar** para salvar suas edições.

Exibição de dados de patch para a integração de orquestração de patches Resposta a vulnerabilidades com HCL BigFix

Os dados de patch e os dados de rollup de patch, bem como as informações de vulnerabilidade e o status de correção de suas vulnerabilidades, são exibidos em registros em sua instância.

Exibição de dados de patch nos espaços Resposta a vulnerabilidades

Funções necessárias:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços do gerente de correção e vulnerabilidade de TI

No Espaço de correção de TI, você pode exibir os patches:

- Na exibição inicial, é possível clicar em cartões de pontuação para exibir registros de soluções preferenciais em IVs, ICs vulneráveis e patches preferenciais em VIs.
- Na exibição de lista, é possível exibir todos os registros de atualização de patch (VPUs) nos links de patches e os itens vulneráveis (VITs) atribuídos a você que têm patches.

Você pode programar patches dos seguintes registros:

- Da atualização do patch (VPU)
- Tarefa de correção (RT)
- Registros de item descoberto (SDI)

No Espaço do gerenciador de vulnerabilidades, você pode exibir os patches:

- Na exibição inicial em tópicos de observação, onde você pode exibir patches preferenciais e potenciais, datas programadas de patches e, se o patch foi baixado, tudo na guia **Itens vulneráveis**.
- Na exibição de lista sobre esforços de correção, é possível exibir dados de patch em registros de VI na guia**Itens vulneráveis**.

Na exibição do ambiente clássico, navegue até **Todos** > **Resposta a vulnerabilidades** > **Patches**.

Registros de atualização de patch nos espaços de VR e na exibição clássica do ambiente

Os dados de patch e os dados e status de rollup de patch são exibidos em registros em sua instância. Os registros de patch são incluídos como parte do recurso de orquestração de patches desta integração com Resposta a vulnerabilidades. Exibir registros de patch (VPU) em espaços Resposta a vulnerabilidades na exibição de lista no espaço de correção de TI. Os registros de atualização de patch na exibição clássica e nos espaços Resposta a vulnerabilidades incluem os seguintes dados:

- Dados de solução de vulnerabilidade e informações de fornecedores de patch importados pela aplicação Gestão de soluções de vulnerabilidade.
- Status de correção de origem que inclui o número total de dispositivos que têm uma determinada vulnerabilidade que pode ser corrigida por um patch e todos os dispositivos com atualizações ausentes.
- Status de correção que inclui % de IVs corrigidos e o total de VIs que têm um patch como preferencial.
- Dispositivos associados, itens vulneráveis, implantações de patch e solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos espaços Resposta a vulnerabilidades.
- Solicitações de patch que os proprietários de correção enviaram para aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acúmulo de estado em registros de itens vulneráveis

Para obter mais informações sobre acúmulo de estado para registros, consulte Dados de patch e rollup de estado para orquestração de patches no Resposta a vulnerabilidades.

Registros que acumulam contagens de VI ativo

Para evitar o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho agendado seleciona apenas as mudanças na contagem de VI ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros em Resposta a vulnerabilidades:

- VIT
- RT
- Solução de vulnerabilidade
- Atualização de patch

Exibição de dados de patches sem soluções

Para obter mais informações sobre como exibir patches sem soluções, consulte Exibir patches sem soluções em Resposta a vulnerabilidades.

Dados de patch no Resposta a vulnerabilidades

Os painéis da Gestão de vulnerabilidades (PA) e do CISO estão incluídos com uma assinatura com o Performance Analytics para a aplicação Resposta a vulnerabilidades. Se você tiver uma assinatura do Performance Analytics, mas não tiver uma integração de orquestração de patches instalada, a guia de correção será exibida no painel do CISO, mas não será preenchida com dados.

No painel Gestão de vulnerabilidades (PA), navegue até **Todos** > **Resposta a vulnerabilidades** > **Visão geral**. Clique na guia **Correção** e role até a parte inferior da página para exibir os dados de atualizações de patch: patches programados e não programados, patches sem datas de destino e contagens semanais.

No Painel do CISO, navegue até **Todos** > **Resposta a vulnerabilidades** > **Painel do CISO**. Com a guia Visão geral selecionada, role até a parte inferior da página para exibir os dados de cobertura de patch: criticidade, patches programados e não programados e patches sem datas de destino.

Para obter mais informações sobre os painéis Resposta a vulnerabilidades, consulte Usando os painéis padrão Resposta a vulnerabilidades, Orquestração de patches com os espaços Resposta a vulnerabilidadese Exibição de dados de orquestração de patches nos painéis Resposta a vulnerabilidades.

Programar patches com o HCL BigFix de integração de orquestração de patches Resposta a vulnerabilidades

Programe patches a partir dos registros de Atualização de patch e Tarefa de correção na aplicação Resposta a vulnerabilidades em sua instância Now Platform.

Antes de Iniciar

A partir da versão 16.1, você pode programar patches nos espaços Resposta a vulnerabilidades ou no ambiente clássico.

Funções necessárias:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços do gerente de correção e vulnerabilidade de TI

Procedimento

1. Nos Espaços de vulnerabilidade Resposta a vulnerabilidades, como um usuário com a função sn_vul.remediation_owner, navegue até **Todos** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Na página inicial, clique **em Patch preferencial em IVs**.
   A lista de registros de atualização de patch para os IVs com patches preferenciais atribuídos a você é exibida.
3. Localize um registro que você deseja abrir e clique para abri-lo.
4. Como alternativa, na exibição de lista no espaço, clique em **Patches** > **Todos** e localize um registro de atualização de patch.
   O registro de atualização de patch é exibido. Talvez você prefira revisar os dados antes de programar um patch, pois pode haver outros patches já programados.
5. Consulte a tabela a seguir sobre os dados exibidos e o que você pode fazer.

Tarefa	Descrição
Clique em um link de Itens relacionados	◦ Visão geral - Exibir detalhes como o número do registro de atualização do patch, os IDs do artigo e do boletim, a data de lançamento e a categoria da atualização, o nome do site do patch, a classificação de risco, a pontuação de risco, a descrição, a solução (se fornecida) e a correção status. ◦ Dispositivos associados - A lista de itens de configuração afetados pelo patch e pelo status. ◦ Itens vulneráveis - A lista de itens vulneráveis associados à vulnerabilidade e ao patch. ◦ Implantações de patch - Os nomes e informações relacionados às implantações deste patch em ativos ou grupos de ativos para este patch. ◦ Solicitações de patch — Uma lista de solicitações de patch já enviadas para este patch. Isso é exibido.
Clique em um link para abrir um registro	Nas listas exibidas em registros abertos dos links de itens relacionados, exiba mais detalhes, incluindo mensagens sobre metas perdidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Depois de abertos, os registros permanecem abertos como guias até que você os feche.
Programar patch	Quando você estiver pronto para programar um patch ou enviar uma solicitação, clique em **Programar patch**. Na caixa de diálogo exibida, preencha os campos. Consulte as etapas abaixo para obter mais detalhes.
Adicionar uma anotação de trabalho ou anexar um arquivo	Na extrema direita da tela, clique no ícone **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.

6. Clique **em Programar patch**.
7. Na caixa de diálogo, preencha os campos.

Campo	Descrição
Selecionar destino	
Ativos	Escolha um na lista para continuar. `O grupo de computadores` é exibido por padrão. ◦ Grupo de computadores: selecione esta opção se quiser escolher uma coleção (um grupo de ativos) para este patch. Os grupos são compostos pelos itens de configuração que são importados da aplicação BigFix. ◦ Lista de computadores: selecione esta opção se quiser escolher computadores individuais (ativos) para este patch. Você pode ver dados sobre o fabricante, local, classe, quando foi atualizado pela última vez e o cronograma de manutenção na caixa de diálogo exibida. Clique em **Avançar** para continuar.
Grupo de computadores ou lista de computadores	Dependendo da sua seleção para Ativos, um dos campos será exibido. Escolha nas listas.
Programação	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda a rastrear suas atualizações.
Tipo de implantação	Escolha uma opção da lista.
Hora do vencimento	Defina o valor da hora do prazo. Este valor é a hora em que o patch está disponível pela última vez para implantação.
Horário disponível	Defina o valor para o tempo em que o patch se torna disponível.
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Permitir reinicialização	O padrão é desativado. Ative (selecione) esta opção para instruir as máquinas do grupo a reiniciar automaticamente após a conclusão bem-sucedida do patch.
Descrição	Adicione mais texto para sobre o patch. Essas informações são exibidas no campo Descrição dos registros de atualização de patch.

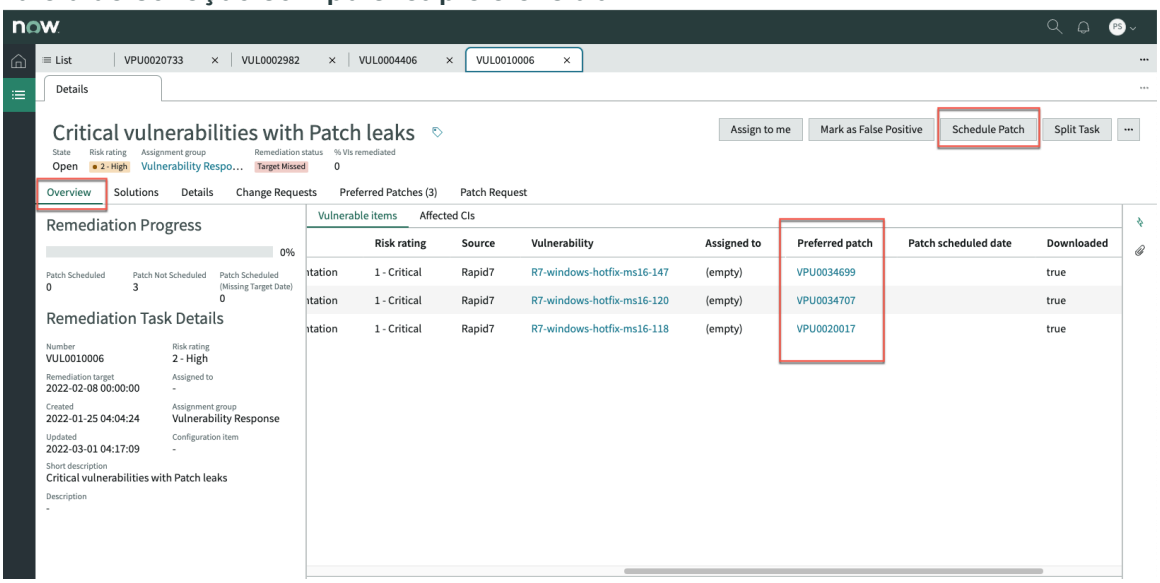
8. Clique em **Implantar**.
   A solicitação de patch é enviada para para revisão. Você pode exibir o status de todas as solicitações enviadas em **Solicitações de exceção** > **Minhas solicitações** na exibição de lista.
9. Como alternativa, você pode programar patches a partir de tarefas de correção (RT) atribuídas a você ou ao seu grupo.

   Nota: A opção de programar um patch a partir de um registro de tarefa de correção estará disponível somente se houver patches mapeados para (associados aos) IVs na tarefa. Esses patches serão exibidos na coluna Patch preferencial se você rolar para a direita de registros de tarefa de correção com a guia Visão geral selecionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção com patches preferenciais



10. Clique em **Programar patch** no registro RT e siga as etapas listadas acima para programá-lo na caixa de diálogo.
11. Você pode programar patches para as etapas listadas anteriormente no ambiente clássico.
    Para localizar esses registros, siga estas etapas.

    a. No ambiente clássico, navegue até **Resposta a vulnerabilidades** > **Patches** > **Todos**.

    b. Na lista exibida, localize um registro de atualização de patch.

    c. Para tarefas de correção, navegue até **Resposta a vulnerabilidades** > **Tarefas de correção** e localize um registro.
    O rastreia o status da correção na guia Status da correção. Na parte inferior do registro, os dados do patch são exibidos nos Links relacionados.

    d. Clique em Programar patch e preencha os campos.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda a rastrear suas atualizações.
Atualização de patch	Escolha um dos patches disponíveis na lista.
Ativos	Selecione um: ▪ Grupo de computadores: selecione esta opção se quiser escolher uma coleção (um grupo de ativos) para este patch. Os grupos são compostos pelos itens de configuração que são importados da aplicação BigFix.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	▪ Lista de computadores: selecione esta opção se quiser escolher computadores individuais (ativos) para este patch. Você pode ver dados sobre o fabricante, local, classe, quando foi atualizado pela última vez e o cronograma de manutenção na caixa de diálogo exibida.
Hora de início e hora de término	Insira as horas de início e de término da janela de tempo. Insira quando quiser que o patch inicie sua implantação e último dia em que o patch pode ser instalado.

Mensagens de REST para a integração de orquestração de patches da Resposta a vulnerabilidades com HCL BigFix

A integração de orquestração de patches Resposta a vulnerabilidades com mensagens HCL BigFix REST é usada para fazer chamadas para a API do BigFix.

Login do BigFix

Você também pode usar as mensagens de REST para o login do BigFix para que possa autenticar as solicitações de REST API. As mudanças no método de registro da mensagem REST afetam as solicitações de autenticação feitas para o BigFix.

Nome do parâmetro	Valor	Descrição
sourceType	cumulativo	Indica de onde a integração de origem extrai dados. Usado pelo código. Mudanças não são recomendadas.
classificaçãoDIR	desc	Indica a direção de classificação dos dados extraídos da integração. Mudanças não são recomendadas.
campo_classificação	severidade	Indica o campo no qual a classificação de dados se baseia. Mudanças não são recomendadas.
tipo	vulnerabilidade	Indica o tipo de dados a serem obtidos da integração para a integração de ativos. Mudanças não são recomendadas.

Integração do BigFix

Você pode usar a mensagem REST para a integração do BigFix para recuperar informações do BigFix. As mudanças no método de registro da mensagem REST afetam as solicitações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

feitas ao BigFix para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Métodos REST

Método REST	Descrição
Obter dados de busca	Recupera as informações do BigFix sobre um dos itens a seguir com base na consulta fornecida: • Computador/Grupos de computadores • Fixlets • Fixlets relevantes em computadores • Ações

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos com base no usuário	Indica o endpoint do console do BigFix

Patch de implantação do BigFix

Você pode usar a mensagem REST da integração do BigFix para programar patches do seu Now Platform® para o BigFix. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao BigFix para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Método REST	Descrição
Patch de implantação POST	Programa o patch para o console do BigFix em um ou vários computadores.

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos com base no usuário	Indica o endpoint do Console do BigFix.
título	Valores dinâmicos com base no usuário	Título da implantação.
configurações_marcador	Configurações nomeadas por marcador XML com valores	Indica configurações que têm parâmetros diferentes e são enviadas para o BigFix ao programar o patch.
computer_tag	Computadores nomeados com marcador XML com valores	Indica a lista de computadores nos quais o patch será programado.
site_name	Valor da atualização do patch	Nome do site onde o Fixlet está presente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do parâmetro	Valor	Descrição
fixlet_id	Valor da atualização do patch	ID do Fixlet.

Transformação de dados para a integração de orquestração de patches com HCL BigFix

Os dados são recuperados da orquestração de patches Resposta a vulnerabilidades com integração HCL BigFix, processados por meio de um conjunto de fontes de dados e transformados em sua instância Now Platform®.

Importação de coleção do BigFix

Os dados dos ativos importados (computadores e grupos de computadores) são carregados na tabela Importação de coleção do BigFix [sn_vul_bigfix_collection_import]. O BigFix Computer and Computer Groups Import TM (mapa de transformação?) é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram a forma como os dados da importação da coleção BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e localize o BigFix Computer e o Computer Groups Import TM. A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo de script do mapa de transformação da importação do computador BigFix e grupos de computadores

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para criar e atualizar ICs com base em regras de pesquisa de IC e coleções, bem como na relação entre elas. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de fixlet do BigFix

Os dados dos fixlets importados são carregados na tabela BigFix Fixlet Import [sn_vul_bigfix_patch_update_import].

O BigFix Fixlet Import TM é usado para transformar as informações importadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação do BigFix Fixlet são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e localize o BigFix Fixlet Import TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de importação de Fixlet do BigFix

Campo de origem	Campo de destino	Descrição
u_id	article_id	ID exclusivo de um fixlet em um site.
u_id	source_id	ID exclusivo de um fixlet em um site.
U_site_name	Sn_vul_bigfix_site_name	Nome do site no BigFix em que o Fixlet se baseia.
U_display_name	Título	Título do Fixlet.
[Script]	ID do boletim	ID de origem da solução.
[Script]	Sn_vul_solution	Solução com base no ID de origem.
U_origem	boletim_origem	Fornecedor de origem da solução.
[Script]	Data_versão	Data da versão do fixlet.
U_category	Atualizar_categoria	Categoria do fixlet.
[Script]	Is_highest_supersedence	Booliano para se o fixlet for a substituição mais alta ou não.
[Script]	Foi_baixado	Booliano de se o fixlet foi baixado ou não.
[Script]	Integration_instance	Nome da instância da qual o fixlet é importado.
U_source_severity	Source_severity	Severidade do fixlet.
U_conta_aplicável	Num_total	Número total de dispositivos com fixlets ausentes.
[Script]	Última_modificação	Data da última modificação do fixlet.

Tempo de script do mapa de transformação de importação de Fixlet do BigFix

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo de script do mapa de transformação de importação de Fixlet do BigFix

Script	Descrição
onBefore (antes de um conjunto para importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de fixlets criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de fixlet de dispositivo do BigFix

Os dados dos fixlets relevantes importados nos computadores são carregados na tabela Importação de fixlet de dispositivo do BigFix [sn_vul_bigfix_device_patch_import].

O BigFix Device Fixlet TM é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de Fixlet de dispositivo do BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e localize o BigFix Device Fixlet TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação do Fixlet do dispositivo do BigFix

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para criar e atualizar ICs com base em regras de pesquisa de IC e coleções, bem como na relação entre elas. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de ações do BigFix

Os dados das ações importadas são carregados na tabela Importação de ações do BigFix [sn_vul_bigfix_deployment_import].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O BigFix Actions Import TM é usado para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram a forma como os dados da importação de ações do BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e localize o BigFix Fixlet Import TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de importação de ações do BigFix

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma ação.
U_name	nome	Nome da ação
[Script]	Sn_vul_bigfix_discovered_item	Referência do item descoberto no qual o patch está implantado
U_status	status	Status da ação
[Script]	sn_vul_patch_orch_update	Referência do patch
U_apply_count	Contagem_sucesso	Contagem de sucesso da ação.
U_retry_count	tentar novamente	Contagem de novas tentativas da ação.
[Script]	Tempo_de_implantação	Hora de início da ação.
[Script]	prazo	Hora de término da ação.
[Script]	Origem_criada	Hora de criação da ação.
[Script]	Integration_instance	Nome da instância da qual a ação é importada.

Tempo de script do mapa de transformação de importação de ações do BigFix

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ações criadas, atualizadas e ignoradas. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de fluxo de trabalho para a integração de orquestração de patches da Resposta a vulnerabilidades com HCL BigFix

Um exemplo de como a orquestração de patches funciona com o produto HCL BigFix.

Antes de Iniciar

Digamos que, por exemplo, todo o seu ambiente seja corrigido uma vez a cada três semanas. A janela de patch mais recente foi concluída há uma semana, mas você deseja aplicar um patch para corrigir uma vulnerabilidade crítica que se tornou conhecida recentemente. Devido à natureza crítica desta vulnerabilidade, você não pode esperar mais duas semanas pelo próximo patch programado.

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para o Espaço do gerenciador de vulnerabilidades.
- sn_vul.remediation_owner para exibir o espaço do responsável pela correção de TI.
- Função sn_vul_patch_orch.configure_patch para configurar e programar patches.
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os Espaços de correção e vulnerabilidade de TI.

Por Que e Quando Desempenhar Esta Tarefa

Como gerente de vulnerabilidades ou analista que trabalha no Espaço do gerenciador de vulnerabilidades, considere criar tópicos de observação ou editar tópicos de observação existentes para ajudá-lo a capturar IVs importados com vulnerabilidades críticas. Com a integração de orquestração de patches, você também pode ver os patches que deseja usar para corrigir e rastrear essas vulnerabilidades. A tabela a seguir lista alguns exemplos com as condições que você pode definir para tópicos de observação para orquestração de patches. Use estes exemplos para ajudá-lo a determinar as configurações que funcionam melhor para o seu ambiente. Consulte Criar um tópico de observação no Espaço do gerenciador de vulnerabilidades para obter mais informações sobre como configurar o tópico de observação.

Amostra de tópicos de observação para orquestração de patches no Espaço do gerenciador de vulnerabilidades

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com vazamentos de patch	`A classificação de risco é 1 - crítico` E `O motivo é patch não programado`
Vulnerabilidades críticas com patches programados (ANS ausente)	`O motivo é patch programado (data de destino ausente)`
Vulnerabilidades críticas com patches programados	`A classificação de risco é 1 - crítico` E `A data programada do patch não está vazia` E

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Amostra de tópicos de observação para orquestração de patches no Espaço do gerenciador de vulnerabilidades

Nome do tópico de observação	Descrição
	`O motivo é patch programado`

- Como gerente ou analista de vulnerabilidades, depois de criar os tópicos de observação e os esforços de correção, você gera tarefas de correção. Em registros de VI e tarefas de correção, você pode fazer uma busca detalhada na guia Detecções e localizar registros de itens descobertos que têm a vulnerabilidade que você está rastreando, junto com os ativos importados pelo produto BigFix.
- Como analista de vulnerabilidade ou administrador, você pode monitorar os dados de patch associados à vulnerabilidade. Você também pode implantar um patch ou vários patches em um ativo específico (item de configuração) a partir de um registro de item descoberto.

Como especialista em correção de TI, você tem opções de como lidar com a vulnerabilidade com uma implantação de patch.

- Você pode programar o patch a partir de um registro de atualização de patch (VPU#).
- Se os itens vulneráveis (VI) tiverem soluções preferenciais mapeadas para eles e forem atribuídos a você ou aos seus grupos, você poderá programar os patches de uma tarefa de correção que tenha esses itens vulneráveis.

Procedimento

1. Como Especialista em correção de TI, no Espaço de correção de TI, clique na exibição inicial.
2. Na exibição inicial, clique no cartão de pontuação **Tarefas de correção atribuídas** para exibir os registros.

   Para fins deste exemplo, você pode verificar o campo Descrição resumida na tarefa de correção (VUL#) em busca de qualquer texto relacionado à sua vulnerabilidade crítica. Digamos, por exemplo, que você saiba que seu gerenciador de vulnerabilidades criou um tópico de observação chamado Vulnerabilidades críticas com vazamentos de patch para detectar IVs (VIT#) com esta vulnerabilidade crítica.

   Com o registro aberto, você também pode revisar os IVs, os patches preferenciais e ver se você ou alguém do seu grupo já enviou solicitações de patch para aprovação.
3. Se você tiver informações suficientes, talvez prefira enviar uma solicitação de patch agora a partir desta tarefa de correção.

   Nota: Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.
4. Clique em **Programar patch** e preencha os campos na caixa de diálogo.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com o HCL BigFix de integração de orquestração de patches Resposta a vulnerabilidades.
5. Como alternativa, na exibição de lista no Espaço de correção de TI, você pode clicar nos links Tarefas de correção, Itens vulneráveis, Soluções e Patches para exibir esses registros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No caso deste exemplo, em vez de um nome de tópico de observação, você pode saber o ID do artigo ou o ID do boletim e o título do patch. Em caso afirmativo, convém verificar se algum dos IVs com esta vulnerabilidade está atribuído a você ou aos seus grupos. Em registros de atualização de patch, você pode enviar solicitações de patch. Em registros de VI, você pode verificar possíveis patches e abrir a tarefa de correção associada se quiser enviar uma solicitação de patch.

6. Se você não tiver acesso aos espaços ou preferir exibir dados e programar patches no ambiente clássico, siga estas etapas.

   a. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Patches** > **Todos**.

   b. Localize o registro de atualização de patch desejado.
   Você pode preferir filtrar os registros com pontuações de risco `crítico`.

   c. Revise os campos de VIs associados e % de VIs corrigidos na guia Status de correção.
   Se os IVs tiverem patches disponíveis, o botão **Programar patch** será exibido no canto superior direito do registro.

   d. Se você decidir enviar uma solicitação, clique em **Programar patch**.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com o HCL BigFix de integração de orquestração de patches Resposta a vulnerabilidades.

   e. Como alternativa, diga que você não tem as informações de ID do patch, mas pode verificar o campo Descrição resumida nas tarefas de correção atribuídas ao seu grupo para qualquer texto relacionado à sua vulnerabilidade crítica.

   f. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuído aos Meus grupos**.

   g. Localize o registro desejado e clique nele para abri-lo.
   No registro aberto, revise a guia Status de correção para VIs e % de VIs corrigidos. Clique nos Links relacionados para registros IV, Soluções preferenciais, Patches preferenciais e Solicitações de patch.

      Nota: Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.

   h. Clique em **Programar patch** no registro se quiser enviar uma solicitação de patch.

Noções básicas sobre a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM

Gerencie patches e implantações de patches para as vulnerabilidades críticas em seus ativos com a integração Resposta a vulnerabilidades com o produto Microsoft System Center Configuration Manager (SCCM).

Orquestração de patches com Resposta a vulnerabilidades

A orquestração de patches com Resposta a vulnerabilidades usa importações agendadas de integrações de soluções de terceiros, fornecedores de patch e scanners de vulnerabilidade. Os dados de detecção do scanner correspondem aos ativos em seu ambiente com as vulnerabilidades e com as atualizações de patch que podem corrigi-las.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você envia solicitações de patch para aprovação, programa atualizações de patch para resolver itens vulneráveis e monitora o andamento da correção a partir da sua instância Now Platform®.

Resposta a vulnerabilidades orquestração de patches com Microsoft SCCM

Quando a Orquestração de patches de resposta a vulnerabilidades com a aplicação Microsoft SCCM é usada com as aplicações ServiceNow® Solução de gestão de vulnerabilidade, Orquestração de patches e Resposta a vulnerabilidades, os gerentes e analistas de vulnerabilidade podem executar as seguintes tarefas:

- Veja mais contexto e informações sobre os tipos de patches e soluções de fornecedores (patches).
- Exiba e monitore dados de vulnerabilidade e solução, bem como o andamento da correção de vulnerabilidades de registros nos espaços Resposta a vulnerabilidades.

Os especialistas em TI e os proprietários de correção podem executar as seguintes tarefas:

- Implante patches compatíveis com o produto Microsoft SCCM para seus Windows, CentOS, macOS, Oraclee outros ativos em intervalos regulares e programados fora do horário comercial para evitar conflitos com o trabalho.
- Identifique ativos sem patch com vulnerabilidades ou ativos que não foram atualizados com sucesso por patches programados a partir de dados de detecção importados de scanners de terceiros.
- Programe os patches disponíveis do Espaço de correção de TI ou da IU clássica para ativos vulneráveis e sem patch da atualização de patch, tarefa de correção e registros de itens descobertos.

Termos-chave nas aplicações SCCM Resposta a vulnerabilidades e Microsoft

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em seu Configuration Management Database (CMDB). Microsoft O SCCM chama ICs, dispositivos.

Coleções e coleções de dispositivos

Terminologia usada no Microsoft produto SCCM que se refere a um grupo de ativos.

Item vulnerável

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB.

Instância

Uma conta distinta da aplicação Microsoft SCCM. Cada conta de usuário pode ser uma instância na aplicação Microsoft SCCM. Este termo também se refere a um endereço da Web exclusivo e seguro para uma instância Now Platform.

Integração

Uma integração é um trabalho agendado no Now Platform que recupera informações de uma fonte de terceiros, como a integração com as Microsoft máquinas SCCM.

Solução

Existem dois tipos de soluções no contexto desta integração, potenciais e preferenciais. Uma possível solução é aquela que pode resolver uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma solução preferencial corresponde à solução mais eficaz para uma vulnerabilidade específica detectada.

Patches

Atualizações de software que corrigem vulnerabilidades. Na aplicação Microsoft SCCM, os patches são chamados de Patches. Por exemplo, Microsoft SCCM tem patches para Windows, CentOS, MAC, Oracle e outros produtos.

Patch preferencial

Patches preferenciais são atualizações de software que têm como objetivo corrigir vulnerabilidades específicas. Os patches, uma vez implantados, são mapeados para os itens vulneráveis que estão relacionados a vulnerabilidades específicas e os corrigem.

Tarefa de correção ou, antes da v15.0 de Resposta a vulnerabilidades, grupos de vulnerabilidades

Listas de itens vulneráveis na aplicação Resposta a vulnerabilidades de ações que são necessárias para corrigir vulnerabilidades.

Implantação

Para fins desta integração, a implantação se refere a quando você aplica, inicia ou programa um patch em uma máquina. Você pode implantar os patches baixados do Microsoft SCCM no seu Now Platform navegando até itens descobertos, patches ou tarefas de correção de registros individuais em Resposta a vulnerabilidades. Você pode implantar patches com trabalhos agendados em máquinas individuais ou em grupos de computadores.

A implantação no Now Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações da integração de vulnerabilidade Microsoft do SCCM em seu ambiente.

Solução de gestão de vulnerabilidade e a Resposta a vulnerabilidades integração de orquestração de patches com Microsoft SCCM

A aplicação Solução de gestão de vulnerabilidade é uma aplicação Now Platform que correlaciona suas descobertas de vulnerabilidade com o detalhamento das soluções (patches) que as corrigem. Identifique os patches de software de terceiros para produtos e serviços, atualizações de configuração e outros controles que têm o maior impacto para sua organização. Junto com as informações do scanner de terceiros, as aplicações Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidadese a Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM trabalham juntas para distribuir patches preferenciais da solução, para a vulnerabilidade, para o item vulnerável para ajudá-lo a corrigir e feche vulnerabilidades do seu ambiente. As aplicações de integração Solução de gestão de Resposta a vulnerabilidades, Resposta a vulnerabilidadese Resposta a vulnerabilidades Patch Orquestração Microsoft SCCM estão disponíveis no ServiceNow® Store.

Funções necessárias de Now Platform

As tarefas de instalação, configuração e correção de integração exigem as funções a seguir em sua instância Now Platform.

administrador

Usuários com esta função obtêm direitos para aplicações nas instâncias ServiceNow Store e as baixam para instâncias Now Platform.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sn_vul.vulnerability_admin

Usuários com esta função ativam aplicações na instância Now Platform e concluem a configuração da aplicação Resposta a vulnerabilidades. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Este usuário administrador configura todas as aplicações de VR, regras e integrações de terceiros.

sn_vul_sccm.configure_integration

Usuários com esta função configuram a aplicação Microsoft Integração de Orquestração de Patches do SCCM. Esta função contém a função granular sn_vul_sccm.read_integration.

sn_vul_sccm.read_integration

Usuários com esta função podem exibir (somente leitura) os registros da aplicação Resposta a vulnerabilidades e Microsoft da Integração de Orquestração de Patches do SCCM e os dados de orquestração de patches.

sn_vul_patch_orch.configure_patch

Usuários com esta função podem configurar e aplicar patches.

sn_vul_patch_orch.read_patch

Usuários com esta função podem exibir (somente leitura) informações de patch.

Aprovadores

Atribua usos aos grupos de aprovadores de nível 1 e aprovador de nível 2 se quiser que as solicitações de patch enviadas sejam aprovadas antes da implantação.

Para obter mais informações sobre como atribuir essas funções usando o Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Regras de pesquisa de IC

Quando os dados são importados da aplicação Microsoft SCCM, a aplicação Resposta a vulnerabilidades pesquisa automaticamente correspondências em Configuration Management Database (CMDB) usando dados de ID de recurso. Regras de pesquisa de IC são usadas para identificar ICs (ativos) e adicioná-los automaticamente aos registros de item vulnerável (VI) quando os IVs são criados. As regras de pesquisa de IC a seguir são enviadas com o sistema base e são usadas para identificar ICs (ativos) e adicioná-los aos itens descobertos.

Esta regra de pesquisa se baseia nos dados trazidos pelo Conector do Service Graph com SCCM. Você deve instalar e executar a integração do CMDB antes de executar as integrações do SCCM. Se você tiver várias instalações do servidor SCCM, poderá configurar o alias de conexão do Conector do Service Graph na página de configuração da Orquestração de patches do SCCM.

MID Server

A Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM é uma integração no local. Ele requer um Windows MID Server autônomo que não faz parte de um cluster de MID Server. O MID Server é necessário para executar scripts em máquinas remotas da sua instância para importar dados do servidor SCCM. As APIs para esta integração são chamadas usando MID Servers que você configura em sua instância Now Platform. Preparação para a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações e dependências da Orquestração de patches de resposta a vulnerabilidades com a aplicação Microsoft SCCM

As aplicações de produto e dependência a seguir são necessárias para a Orquestração de patches de resposta a vulnerabilidades com Microsoft integração do System Center Configuration Manager (SCCM). Essas aplicações estão disponíveis no ServiceNow® Store

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

Para exibir dados de orquestração de patches e atualizações disponíveis (patches) nos espaços e na IU clássica em Resposta a vulnerabilidades, as aplicações a seguir são necessárias. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas.

Para obter mais informações sobre a compatibilidade de versões com as aplicações e versões da família necessárias, consulte o artigo KB0856498 Matriz de compatibilidade da Resposta a vulnerabilidades e mudanças no esquema de versão na Base de conhecimento HI.

Aplicação e versão de lançamento
Resposta a vulnerabilidades
Solução de gestão de vulnerabilidade
Aplicação Vulnerability Response Patch Orchestration
Aplicação de Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM
Security Support Common
Orquestração de suporte de segurança
Conector do Service Graph com SCCM

Resposta a vulnerabilidades tabelas da aplicação de orquestração de patches

A aplicação Orquestração de patches Resposta a vulnerabilidades contém as seguintes tabelas:

Tabela	Descrição
Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Atualização de dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de itens descobertos.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre Coleções e ICs.
Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.

Orquestração de patches de resposta a vulnerabilidades com Microsoft integrações de SCCM

As integrações desenvolvidas pela engenharia ServiceNow® compõem a implantação da solução orquestrada com o produto Microsoft SCCM. As seguintes integrações estão incluídas com a aplicação Integração de Orquestração de Patches do Microsoft SCCM que você baixa do ServiceNow® Store.

Depois de instalar a aplicação de integração em sua instância Now Platform, para exibir essas integrações, navegue até **Integrações** > **SCCM Patch Orchestration Integration** > **Integrações**. A aplicação Resposta a vulnerabilidades processa dados em intervalos de tempo programados importados por essas integrações com Microsoft endpoints do SCCM.

Integração	Descrição
Microsoft Integração de coleta do SCCM	• Esta integração está programada para ser executada diariamente e é executada primeiro na execução de integração encadeada. • Recupera as coleções de dispositivos das Coleções do SCCM.
Microsoft SCCM Device Collection Integration	• Quando programada, essa integração é acionada pela conclusão da integração de coleta do SCCM. Você também pode executá-lo sob demanda. • Esta integração busca os dispositivos em cada coleção. Esta integração cria registros na tabela de itens descobertos e na tabela de coleção de dispositivos.
Microsoft Integração de atualização de patch do SCCM	• Quando programada, esta integração é acionada pela conclusão da Integração de Coleção de Dispositivos SCCM. Você também pode executá-lo sob demanda. • Recupera informações do servidor SCCM sobre os patches que estão instalados ou ausentes nos dispositivos (ativos).
Microsoft Integração de implantações do SCCM	• Quando programada, essa integração é acionada pela conclusão da integração de atualização de patch. Você também pode executá-lo sob demanda. • Recupera informações sobre os patches programados pela equipe de TI no servidor SCCM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparação para a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM

Prepare-se para a integração executando as seguintes tarefas de configuração.

Antes de Iniciar

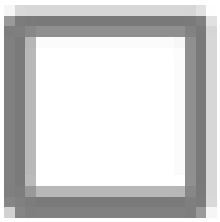
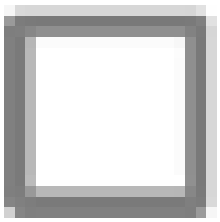
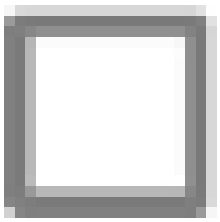
Funções necessárias: administrador para instalar as aplicações e atribuir funções. Outras funções estão listadas na tabela a seguir.

Por Que e Quando Desempenhar Esta Tarefa

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração.

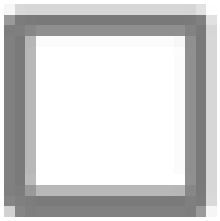
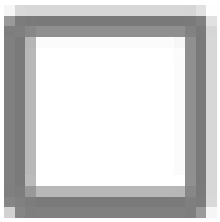
Procedimento

1. Para uma instalação e configuração tranquilas da Orquestração de patches de resposta a vulnerabilidades com a aplicação Microsoft SCCM, siga a check-list fornecida abaixo.
2. Você pode preferir imprimir a check-list a seguir e verificar se os itens listados estão concluídos antes de instalar a aplicação e importar informações relacionadas a patches e vulnerabilidades para sua instância Now Platform®.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte, Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 16.1 de Resposta a vulnerabilidades ou posterior.
	Se ainda não estiver instalado, obtenha direitos e instale um aplicativo de scanner de terceiros para importar dados de vulnerabilidade. Consulte Integrações do Resposta a vulnerabilidades para obter mais informações sobre scanners de terceiros compatíveis com Resposta a vulnerabilidades. Consulte .
	Se ainda não estiver instalado, obtenha direitos e baixe a Orquestração de patches de resposta a vulnerabilidades com a aplicação Microsoft SCCM para sua instância Now Platform®. Consulte .

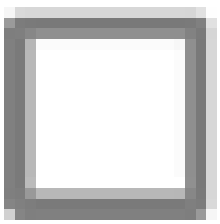
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Obtenha Microsoft credenciais do SCCM. Verifique se você tem nomes de contas, senhas e outras informações de serviço exigidas por seus produtos Microsoft para que você tenha acesso a eles.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. administrador O administrador do sistema obtém direitos, baixa e instala a aplicação Microsoft Orquestração de patches do SCCM e as outras aplicações necessárias para a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração em Resposta a vulnerabilidades ou no módulo Administração de usuários. sn_vul.vulnerability_admin Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das Microsoft integrações do SCCM e de outras aplicações de terceiros. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Esta função configura todas as aplicações de VR, regras, integrações de terceiros, Resposta a vulnerabilidades aplicações de Orquestração de patches e Gestão de soluções de vulnerabilidade. sn_vul_sccm.configure_integration Usuários com esta função configuram a aplicação Microsoft Integração de Orquestração de Patches do SCCM. Esta função contém as funções granulares sn_vul_sccm.read_integration e connection_admin que permitem ao usuário se conectar ao console do SCCM e configurar as instâncias de integração em seu Now Platform. sn_vul_sccm.read_integration Usuários com esta função podem exibir (somente leitura) os registros da aplicação Resposta a vulnerabilidades e Microsoft da Integração de Orquestração de Patches do SCCM e os dados de orquestração de patches.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	sn_vul_patch_orch.configure_patch Usuários com esta função podem configurar e aplicar patches. Os patches solicitados por este usuário do item vulnerável e os registros de atualização de patch serão enviados para aprovação se a gestão de mudanças estiver ativa e os aprovadores estiverem atribuídos. sn_vul_patch_orch.read_patch Usuários com esta função podem exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os Espaços de correção e vulnerabilidade de TI. Aprovadores Usuários atribuídos ao Aprovador nível 1 e, opcionalmente, ao Aprovador nível 2, grupos de aprovadores aprovam as solicitações de patch enviadas. Por padrão, os patches são enviados ao grupo de aprovadores de nível 1 para aprovação antes da implantação. Para obter mais informações sobre o processo de aprovação, consulte Configurar a Orquestração de patches de resposta a vulnerabilidades com integração de Microsoft SCCM. Para obter mais informações sobre como configurar aprovadores e grupos, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos para a integração. Por padrão, o grupo Resposta a vulnerabilidades está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais para funções de especialista em correção e analista de vulnerabilidade e adicionar usuários com o módulo Administração de usuário em sua instância. Consulte Criação de um grupo de usuários .
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. ◦ A Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM é uma integração no local que requer que você use um Windows MID Server autônomo. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	◦ Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

Instalar a aplicação Resposta a vulnerabilidades Patch Orquestração com Microsoft SCCM

Baixe a aplicação do ServiceNow Store.

Antes de Iniciar

Antes de instalar a aplicação, verifique se você concluiu todos os itens da check-list em Preparação para a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) para configurar a Resposta a vulnerabilidades Orquestração de patches Microsoft SCCM e outras aplicações após a instalação.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter o direito de prosseguir para .

Procedimento

1. Navegar até **Todos** > **Aplicações do sistema** > **todas as aplicações disponíveis** > **Todos**.
2. Localize a aplicação **Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM** e clique em **Instalar**.

   Esta ação instala a aplicação que você baixou de ServiceNow Store.
3. Como alternativa, você pode instalar aplicações do Assistente de configuração. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Todos** > **Microsoft SCCM Patch Orchestration Integration** > **Configuração** para continuar com a configuração.

Configurar a Orquestração de patches de resposta a vulnerabilidades com integração de Microsoft SCCM

Depois de instalar a aplicação, configure-a com as informações da sua conta e valide suas credenciais.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin e sn_vul_sccm.configure_integration

Procedimento

1. Navegar até **Todos** > **Microsoft SCCM Patch Orchestration Integration** > **Configuração**.
2. Preencha os campos com suas Microsoft informações e credenciais do SCCM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Instância de integração	O nome da Microsoft conta de instância do SCCM que você deseja usar, por exemplo, `Microsoft SCCM Patch Management integration`.
Nome do host	Insira o URL do Microsoft host SCCM.
Nome de usuário	Insira o Microsoft nome de usuário da conta do SCCM.
Senha	Insira a senha da sua Microsoft conta do SCCM.
MID Server	Insira o nome do MID Server autônomo na lista que você deseja usar. Consulte Preparação para a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM para obter mais informações sobre MID Servers e configurar tarefas em seu Now Platform®.

3. Clique em Salvar e testar credenciais.
   O status da sua conexão entre o Microsoft SCCM e sua instância Now Platform® é exibido no campo Status de validação. Se você não vir um teste bem-sucedido, siga os avisos.
4. Opcional: A separação de domínios é compatível com esta integração.
   Você pode adicionar várias configurações de à sua instância. Para adicionar configurações adicionais:

   a. Navegar até **Todos** > **Microsoft SCCM Patch Orchestration Integration Instâncias de integração**.

   b. Verifique se o escopo da aplicação, `Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM`, é exibido no campo Escopo da aplicação.

   c. Clique em **Nova**.

   d. Preencha o formulário.

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM
Integração	[Somente leitura] Microsoft O gerenciamento de patches do SCCM é o padrão.
Ativo	O padrão é ativado. Se desmarcada, a instância não está ativa.

   e. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sua nova instância de integração é exibida na lista Instâncias de integração.

f. Repita as etapas 1 a 3 para configurar sua instância de integração e testar suas credenciais.

5. Configure aprovações para solicitações de patch.
Por padrão, uma propriedade do sistema [**sn_vul_patch_orch.patch_approval_required**] é ativada para que, quando as implantações de patch forem programadas, elas sejam enviadas para revisão e aprovação para usuários atribuídos ao Nível 1 - Grupo de aprovação de atualizações de patch.

Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, poderá desativar a propriedade [**sn_vul_patch_orch.patch_approval_required**]. Você pode preferir deixar as aprovações ativadas para que os patches programados não entrem em conflito com o horário comercial normal.

Nota: Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema:

a. Navegar até **Todos** > **sys.properties.list**.

b. Localize **sn_vul_patch_orch.patch_approval_required** e clique nele para abrir o registro.

c. No campo Valor, digite `falso`.

d. Clique em **Atualizar**.

6. Se você não desativar esta propriedade, precisará atribuir aprovadores para solicitações de patch.
Como um usuário com a função sn_vul.vulnerability_admin, siga estas etapas.

a. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de aprovação**.

b. Se a Regra de **aprovação Implantar aprovação de atualização de patch** não for exibida na lista, clique em **Todos** à direita do ícone de filtro verde no canto superior esquerdo da tela para exibir a lista inteira.

c. Na lista, clique em **Implantar aprovação de atualização de patch**.

d. No registro, com a guia Configuração de aprovação selecionada, clique em **Configuração padrão Aprovação de atualização de patch**.

e. No registro, clique em **Nível 1 - Aprovação de atualização de patch**.

f. Adicione usuários a este grupo.

Os usuários atribuídos a este grupo aprovam as solicitações de patch enviadas por usuários com a função sn_vul_patch_orch.configure_patch. Navegue até **Minhas aprovações** para exibir e processar as solicitações.

7. Clique em**Atualizar** para salvar suas mudanças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Opcional: Você pode configurar aprovações de vários níveis para que mais de uma aprovação seja necessária antes da implantação de solicitações de patch programadas.

   a. Com o registro de aprovação da Atualização de patch de configuração padrão exibido, clique em **Novo**.

   b. Preencha os campos.

Campo	Descrição
Nome	Nome do nível de aprovação, por exemplo, **Nível 2 - Aprovação de atualização de patch**.
Ativo	Ativado por padrão, o que significa que o nível de aprovação está em uso.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ▪ Um aprovador necessário ▪ Todos os usuários devem aprovar
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Função	Selecione uma função para o grupo na lista.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção: ▪ Usuário e grupo de usuários ▪ Campo da tabela de aprovação ▪ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções especificadas por você.
Usuários	Edite os usuários listados nos grupos.

   c. Clique em **Enviar** para salvar suas edições.

Exibição de dados de patch e acúmulo de dados de patch para a integração da Orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM

Os dados de patch e os dados de rollup de patch, bem como as informações de vulnerabilidade e o status de correção de suas vulnerabilidades, são exibidos em registros em sua instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de dados de patch nos espaços Resposta a vulnerabilidades

Funções necessárias:

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços do gerente de correção e vulnerabilidade de TI

No Espaço de correção de TI, você pode exibir os patches:

- Na exibição inicial, é possível clicar em cartões de pontuação para exibir registros de soluções preferenciais em IVs, ICs vulneráveis e patches preferenciais em VIs.
- Na exibição de lista, é possível exibir todos os registros de atualização de patch (VPUs) nos links de patches e os itens vulneráveis (VITs) atribuídos a você que têm patches.

Você pode programar patches dos seguintes registros:

- Da atualização do patch (VPU)
- Tarefa de correção (RT)
- Registros de item descoberto (SDI)

No Espaço do gerenciador de vulnerabilidades, você pode exibir os patches:

- Na exibição inicial em tópicos de observação, onde você pode exibir patches preferenciais e potenciais, datas programadas de patches e, se o patch foi baixado, tudo na guia **Itens vulneráveis**.
- Na exibição de lista sobre esforços de correção, é possível exibir dados de patch em registros de VI na guia**Itens vulneráveis**.

Na exibição do ambiente clássico, navegue até **Todos** > **Resposta a vulnerabilidades** > **Patches**.

Registros de atualização de patch nos espaços de VR e na exibição clássica do ambiente

Os dados de patch e os dados e status de rollup de patch são exibidos em registros em sua instância. Os registros de patch são incluídos como parte do recurso de orquestração de patches desta integração com Resposta a vulnerabilidades. Exibir registros de patch (VPU) em espaços Resposta a vulnerabilidades na exibição de lista no espaço de correção de TI. Os registros de atualização de patch no ambiente clássico e nos espaços Resposta a vulnerabilidades incluem os seguintes dados:

- Dados de solução de vulnerabilidade e informações de fornecedores de patch importados pela aplicação Gestão de soluções de vulnerabilidade.
- Status de correção de origem que inclui o número total de dispositivos que têm uma determinada vulnerabilidade que pode ser corrigida por um patch. Além disso, ele também inclui e todos os dispositivos com atualizações ausentes.
- Status de correção que inclui % de IVs corrigidos e o total de VIs que têm um patch como preferencial.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Dispositivos associados, itens vulneráveis, implantações de patch e solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos espaços Resposta a vulnerabilidades.
- Solicitações de patch que os proprietários de correção enviaram para aprovação.

Acúmulo de estado em registros de itens vulneráveis

Para obter mais informações sobre acúmulo de estado para registros, consulte Dados de patch e rollup de estado para orquestração de patches no Resposta a vulnerabilidades.

Registros que acumulam contagens de VI ativo

Para evitar o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho agendado seleciona apenas as mudanças na contagem de VI ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros em Resposta a vulnerabilidades:

- VIT
- RT
- Solução de vulnerabilidade
- Atualização de patch

Exibição de dados de patches sem soluções

Para obter mais informações sobre como exibir patches sem soluções, consulte Exibir patches sem soluções em Resposta a vulnerabilidades.

Dados de patch no Resposta a vulnerabilidades

Os painéis da Gestão de vulnerabilidades (PA) e do CISO estão incluídos com uma assinatura com o Performance Analytics para a aplicação Resposta a vulnerabilidades. Se você tiver uma assinatura do Performance Analytics, mas não tiver uma integração de orquestração de patches instalada, a guia de correção será exibida no painel do CISO, mas não será preenchida com dados.

No painel Gestão de vulnerabilidades (PA), navegue até **Todos** > **Resposta a vulnerabilidades** > **Visão geral**. Clique na guia **Correção** e role até a parte inferior da página para exibir os dados de atualizações de patch: patches programados e não programados, patches sem datas de destino e contagens semanais.

No Painel do CISO, navegue até **Todos** > **Resposta a vulnerabilidades** > **Painel do CISO**. Com a guia Visão geral selecionada, role até a parte inferior da página para exibir os dados de cobertura de patch: criticidade, patches programados e não programados e patches sem datas de destino.

Para obter mais informações sobre os painéis Resposta a vulnerabilidades, consulte Usando os painéis padrão Resposta a vulnerabilidades, Orquestração de patches com os espaços Resposta a vulnerabilidadese Exibição de dados de orquestração de patches nos painéis Resposta a vulnerabilidades.

Programar patches com a integração Microsoft do SCCM com Resposta a vulnerabilidades

Programe patches a partir dos registros de Atualização de patch e Tarefa de correção na aplicação Resposta a vulnerabilidades em sua instância Now Platform.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

A partir da versão 16.1, você pode programar patches nos espaços Resposta a vulnerabilidades ou no ambiente clássico.

Funções necessárias:

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os espaços do gerente de correção e vulnerabilidade de TI

Procedimento

1. Nos Espaços de vulnerabilidade Resposta a vulnerabilidades, como um usuário com a função sn_vul.remediation_owner, navegue até **Todos** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Na página inicial, clique **em Patch preferencial em IVs**.
   A lista de registros de atualização de patch para os IVs com patches preferenciais atribuídos a você é exibida.
3. Localize um registro que você deseja abrir e clique para abri-lo.
4. Como alternativa, na exibição de lista no espaço, clique em **Patches** > **Todos** e localize um registro de atualização de patch.
   O registro de atualização de patch é exibido. Talvez você prefira revisar os dados antes de programar um patch, pois pode haver outros patches já programados.
5. Consulte a tabela a seguir sobre os dados exibidos no Espaço de correção de TI e o que você pode fazer.

Tarefa	Descrição
Clique em um link de Itens relacionados	◦ Visão geral - Exibir detalhes como o número do registro de atualização do patch, os IDs do artigo e do boletim, a data de lançamento e a categoria da atualização, o nome do site do patch, a classificação de risco, a pontuação de risco, a descrição, a solução (se fornecida) e a correção status. ◦ Dispositivos associados - A lista de itens de configuração afetados pelo patch e pelo status. ◦ Itens vulneráveis - A lista de itens vulneráveis associados à vulnerabilidade e ao patch. ◦ Implantações de patch - Os nomes e informações relacionados às implantações deste patch em ativos ou grupos de ativos para este patch. ◦ Solicitações de patch — Uma lista de solicitações de patch já enviadas para este patch.
Clique em um link para abrir um registro	Nas listas exibidas em registros abertos dos links de itens relacionados, exiba mais deta-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	lhes, incluindo mensagens sobre metas perdidas. Depois de abertos, os registros permanecem abertos como guias até que você os feche.
Programar patch	Quando você estiver pronto para programar um patch ou enviar uma solicitação, clique em **Programar patch**. Na caixa de diálogo exibida, preencha os campos. Consulte as etapas abaixo para obter mais detalhes.
Adicionar uma anotação de trabalho ou anexar um arquivo	Na extrema direita da tela, clique no ícone **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.

6. Clique **em Programar patch**.
7. Na caixa de diálogo, preencha os campos.

Campo	Descrição
Etapa 1 Selecionar destino	
Coleção	Escolha uma coleção (grupo de ativos) na lista para continuar. Estas são as coleções importadas do SCCM.
Programação da Etapa 2	
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda a rastrear suas atualizações.
Tipo de implantação	Escolha uma opção da lista. ◦ Obrigatório - este patch é uma atualização necessária. ◦ Disponível - este patch não é necessário, mas está disponível para implantação.
Hora do vencimento	Defina o prazo. Este valor indica o último dia em que o patch pode ser instalado.
Horário disponível	Defina o valor para a hora em que o patch se torna disponível pela primeira vez para implantação.
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Permitir reinicialização	O padrão é desativado. Ative (selecione) esta opção para instruir as máquinas do

Tradução automática

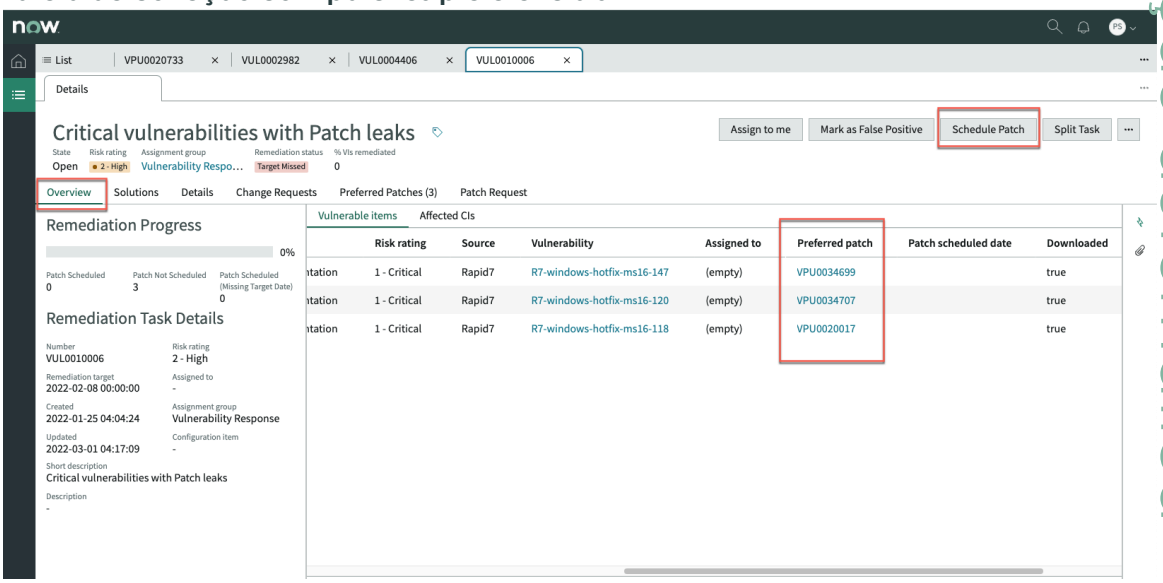
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	grupo a reiniciar automaticamente após a conclusão bem-sucedida do patch.
Descrição	Adicione mais texto para sobre o patch. Essas informações são exibidas no campo Descrição do registro de atualização de patch.

8. Clique em **Implantar**.
   A solicitação de patch é enviada para para revisão. Você pode exibir o status de todas as solicitações enviadas em **Solicitações de exceção** > **Minhas solicitações** na exibição de lista.
9. Como alternativa, você pode programar patches a partir de tarefas de correção (RT) atribuídas a você ou ao seu grupo.

   Nota: A opção de programar um patch a partir de um registro de tarefa de correção estará disponível somente se houver patches mapeados para (associados aos) IVs na tarefa. Esses patches serão exibidos na coluna Patch preferencial se você rolar para a direita de registros de tarefa de correção com a guia Visão geral selecionada.

Tarefa de correção com patches preferenciais



10. Clique em **Programar patch** no registro RT e siga as etapas listadas acima para programá-lo na caixa de diálogo.
11. Opcional: Você pode programar patches para as etapas anteriores no ambiente clássico.
    Para localizar esses registros, siga estas etapas.

    a. No ambiente clássico, navegue até **Todos** > **Resposta a vulnerabilidades** > **Patches** > **Todos**.

    b. Na lista exibida, localize um registro de atualização de patch.

    c. Para tarefas de correção, navegue até **Resposta a vulnerabilidades** > **Tarefas de correção** e localize um registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O rastreia o status da correção na guia Status da correção. Na parte inferior do registro, os dados do patch são exibidos nos Links relacionados.

d. Clique em **Programar patch** e preencha os campos.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda a rastrear suas atualizações.
Descrição	Adicione mais texto para sobre o patch. Essas informações são exibidas no campo Descrição do registro de atualização de patch.
Tipo de implantação	Escolha uma opção da lista. ▪ Obrigatório - este patch é uma atualização necessária. ▪ Disponível - este patch não é necessário, mas está disponível para implantação.
Coleção	Escolha uma coleção (grupo de ativos) na lista para continuar. Esses grupos são as coleções de ativos importadas do SCCM.
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Tempo disponível	Defina o valor para a hora em que o patch se torna disponível pela primeira vez para implantação.
Vencimento	Defina o prazo. Este valor indica o último dia em que o patch pode ser instalado.

e. Clique em **Implantar**.

Tradução automática

Mensagens de REST para a Resposta a vulnerabilidades Orquestração de patches com Microsoft SCCM

A Orquestração de patches de resposta a vulnerabilidades com Microsoft SCCM usa as classes do SCCM Windows Management Instrumentation (WMI) para fazer chamadas para a API do servidor SCCM.

Visão geral

O Provedor de SMS fornece à API um acesso de interoperabilidade sobre HTTPS, chamado de serviço de administração. O serviço de administração é uma API de transferência de estado representacional (REST) baseada no protocolo Open Data (OData) v4.

Consulte O que é o serviço de administração no Configuration Manager para obter mais informações sobre o uso do serviço de administração com esta integração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como a autenticação necessária usa o protocolo NTLM do Windows New Technology LAN Manager, as chamadas para as APIs são feitas por meio do MID Server usando scripts do PowerShell.

Microsoft Integração do SCCM

Você pode usar a mensagem REST para a integração do Microsoft SCCM para recuperar informações do Microsoft SCCM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao Microsoft SCCM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Nomes das classes WMI:

- Coleção_SMS
- SMS_ResumoDeImplantação

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos com base no usuário	Indica o endpoint do Console do SCCM

Microsoft Patch de implantação do SCCM

Você pode usar a mensagem REST para a integração do Microsoft SCCM para programar patches do Now Platform® para o Microsoft SCCM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao SCCM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Método REST	Descrição
Patch de implantação POST	Programa o patch para o console do SCCM em um ou vários computadores.

Nome do parâmetro	Valor	Descrição
URL	Valores dinâmicos com base no usuário	Indica o endpoint do Console do SCCM.
título	Valores dinâmicos com base no usuário	Título da implantação.
configurações_marcador	Configurações nomeadas por marcador XML com valores	Indica configurações que têm parâmetros diferentes e são enviadas para o SCCM durante a programação do patch.
computer_tag	Computadores nomeados com marcador XML com valores	Indica a lista de computadores nos quais o patch será programado.
site_name	Valor da atualização do patch	Nome do site onde o Patch está presente.
Patch_id	Valor da atualização do patch	ID do patch.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transformação de dados para a Orquestração de patches com integração de Microsoft SCCM

Os dados são recuperados da Orquestração de patches com a integração Microsoft do SCCM, processados por meio de um conjunto de fontes de dados e transformados em sua instância Now Platform®.

Importação de coleção do SCCM

Os dados das coleções importadas são carregados na tabela Importação de coleção do SCCM [sn_vul_sccm_collection_import]. As Coleções do SCCM (mapa de transformação) são usadas para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação da Coleção SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos para importação do sistema** > **Mapas de transformação** e localize a Transformação da coleção do SCCM. A tabela a seguir lista os campos do mapa de transformação por integração.

Campo de origem	Campo de destino	Descrição
u_collectionid	source_id	ID exclusiva da coleção.
u_name	nome	Nome da coleção.
u_membercount	device_count	Número de dispositivos nesta coleção.
[script]	integração_instance	Nome da instância da qual o patch é importado.

Tempo do script do mapa de transformação de importação da coleção SCCM

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de atualização de patch do SCCM

Os dados dos patches importados são carregados na tabela Importação de atualização de patch do SCCM [sn_vul_sccm_patch_update_import].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A transformação de atualização do patch do SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de atualização de patch do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos para importação do sistema** > **Mapas de transformação** e localize a transformação de atualização do Patch do SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de importação e atualização de patch do SCCM

Campo de origem	Campo de destino	Descrição
[Script]	urls	URLs do patch.
u_nummisso	num_missing	Número de dispositivos sem este patch.
[Script]	data_versão	Data de versão do patch.
u_bulletinid	ID_do_boletim	ID do boletim para o patch.
u_numtotal	num_total	Número total de dispositivos.
u_localizeddescription	descrição	Descrição do patch.
[Script]	is_highest_supersedence	É o Patch com a maior substituição.
u_numnãoaplicável	num_não_aplicável	Número de dispositivos não aplicável a este patch.
u_iscontentprovisioned	está_baixado	Se o Patch for baixado para o Servidor SCCM.
u_num desconhecido	num_unknown	Número total de dispositivos desconhecidos.
u_articleid	article_id	ID do artigo do patch.
u_localizeddisplayname	título	Título do patch.
u_ci_id	source_id	ID exclusivo do patch no SCCM.
u_numpresente	num_presente	Número de dispositivos em que o patch está instalado.
[Script]	integração_instance	Nome da instância da qual o patch é importado.
[Script]	sn_vul_solution	Solução com base no ID de origem.
[Script]	last_modified	Data da última modificação do patch.
gravidade_u	gravidade_origem	Gravidade do patch.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo de script do mapa de transformação de importação de atualização de patch do SCCM

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de atualização de patch do dispositivo SCCM

Os dados dos patches relevantes importados nos dispositivos são carregados na tabela Importação de atualização de patch do dispositivo SCCM [sn_vul_sccm_device_patch_import].

A transformação de atualização de patch do dispositivo SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de atualização de patch do dispositivo SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos para importação do sistema** > **Mapas de transformação** e localize a transformação de atualização de patch do dispositivo SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação da atualização do patch do dispositivo SCCM

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	Script usado para criar e atualizar ICs com base em regras de pesquisa de IC e patches, bem como no relacionamento entre eles. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_sccm]. Este script é para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo do script do mapa de transformação da atualização do patch do dispositivo SCCM

Script	Descrição
	uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de coleção de dispositivos do SCCM

Os dados das coleções de dispositivos importados são carregados na tabela Importação de coleção de dispositivos SCCM [sn_vul_sccm_device_collection_import].

A transformação de importação de coleção de dispositivos SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de coleção de dispositivos SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos para importação do sistema** > **Mapas de transformação** e localize a transformação da coleção de dispositivos SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação de importação da coleção de dispositivos

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	O script usado para criar e atualizar ICs com base nas regras de pesquisa de IC e nas coleções, bem como no relacionamento entre elas. Com base nos resultados, este script modifica valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de importação da coleção de dispositivos SCCM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma ação.
U_name	nome	Nome da ação
[Script]	Sn_vul_sccm_discovered_item	Referência do item descoberto no qual o patch está implantado
U_status	status	Status da ação
[Script]	sn_vul_patch_orch_update	Referência do patch
U_apply_count	Contagem_sucesso	Contagem de sucesso da ação.
U_retry_count	tentar novamente	Contagem de novas tentativas da ação.
[Script]	Tempo_de_implantação	Hora de início da ação.
[Script]	prazo	Hora de término da ação.
[Script]	Origem_criada	Hora de criação da ação.
[Script]	Integration_instance	Nome da instância da qual a ação é importada.

Importação de implantação do SCCM

Os dados de implantações importadas são carregados na tabela Importação de implantação do SCCM [sn_vul_sccm_deployment_import].

A transformação de importação de implantação do SCCM é usada para transformar as informações importadas.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de implantação do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos para importação do sistema** > **Mapas de transformação** e localize a transformação de implantação do SCCM.

Campos do mapa de transformação de implantação do SCCM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma implantação.
u_name	nome	Nome da implantação.
[Script]	prazo	Prazo para a implantação.
u_numberinprogress	contagem_progresso	Contagem de dispositivos em andamento para a implantação.
[Script]	implant_time	Hora de início da implantação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de implantação do SCCM

Campo de origem	Campo de destino	Descrição
[Script]	integração_instance	Nome da instância da qual a implantação é importada.
[Script]	source_created	Hora de criação da implantação.
[Script]	sn_vul_patch_orch_update	Referência do patch
[Script]	sn_vul_patch_orch_collection	Referência do item descoberto em que o patch está implantado.
u_softwarename	nome	Nome da implantação.
u_numberoutro	count_outros	Outra contagem de dispositivos para a implantação.
u_numberunknown	contagem_desconhecida	Contagem de estados desconhecidos de dispositivos para a implantação.
u_deploymentid	source_id	Identificador exclusivo da implantação.
u_numbersucesso	contagem_sucesso	Contagem de sucesso de dispositivos para a implantação.
u_numbererrors	erro_contagem	Contagem de erros de dispositivos para a implantação.
u_numbertargeted	count_total	Contagem total de dispositivos para a implantação.

Tempo de script do mapa de transformação de importação de implantação do SCCM

Script	Descrição
OnStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo de script do mapa de transformação de importação de implantação do SCCM

Script	Descrição
	script é para uso interno e não deve ser modificado ou excluído.

Exemplo de fluxo de trabalho para a integração da Orquestração de patches [Resposta a vulnerabilidades com o Microsoft SCCM

Um exemplo de como a orquestração de patches funciona com o Microsoft SCCM.

Antes de Iniciar

Digamos que, por exemplo, todo o seu ambiente seja corrigido uma vez a cada três semanas. A janela de patch mais recente foi concluída há uma semana, mas você deseja aplicar um patch para corrigir uma vulnerabilidade crítica que se tornou conhecida recentemente. Devido à natureza crítica desta vulnerabilidade, você não pode esperar mais duas semanas pelo próximo patch programado.

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para o Espaço do gerenciador de vulnerabilidades.
- sn_vul.remediation_owner para exibir o espaço do responsável pela correção de TI.
- Função sn_vul_patch_orch.configure_patch para configurar e programar patches.
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para os Espaços de correção e vulnerabilidade de TI.

Por Que e Quando Desempenhar Esta Tarefa

Como gerente de vulnerabilidades ou analista que trabalha no Espaço do gerenciador de vulnerabilidades, considere criar tópicos de observação ou editar tópicos de observação existentes para ajudá-lo a capturar IVs importados com vulnerabilidades críticas. Com a integração de orquestração de patches, você também pode ver os patches que deseja usar para corrigir e rastrear essas vulnerabilidades. A tabela a seguir lista alguns exemplos com as condições que você pode definir para tópicos de observação para orquestração de patches. Use estes exemplos para ajudá-lo a determinar as configurações que funcionam melhor para o seu ambiente. Consulte Criar um tópico de observação no Espaço do gerenciador de vulnerabilidades para obter mais informações sobre como configurar o tópico de observação.

Amostra de tópicos de observação para orquestração de patches no Espaço do gerenciador de vulnerabilidades

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com vazamentos de patch	`A classificação de risco é 1 - crítico` E `O motivo é patch não programado`
Vulnerabilidades críticas com patches programados (ANS ausente)	`O motivo é patch programado (data de destino ausente)`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Amostra de tópicos de observação para orquestração de patches no Espaço do gerenciador de vulnerabilidades

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com patches programados	`A classificação de risco é 1 - crítico` E `A data programada do patch não está vazia` E `O motivo é patch programado`

- Como gerente ou analista de vulnerabilidades, depois de criar os tópicos de observação e os esforços de correção, você gera tarefas de correção. Em registros de VI e tarefas de correção, você pode fazer uma busca detalhada na guia Detecções e localizar registros de itens descobertos que têm a vulnerabilidade que você está rastreando, junto com os ativos importados pelo produto SCCM.
- Como analista de vulnerabilidade ou administrador, você pode monitorar os dados de patch associados à vulnerabilidade. Você também pode implantar um patch ou vários patches em um ativo específico (item de configuração) a partir de um registro de item descoberto.

Como especialista em correção de TI, você tem opções de como lidar com a vulnerabilidade com uma implantação de patch.

- Você pode programar o patch a partir de um registro de atualização de patch (VPU#).
- Se os itens vulneráveis (VI) tiverem soluções preferenciais mapeadas para eles e forem atribuídos a você ou aos seus grupos, você poderá programar os patches de uma tarefa de correção que tenha esses itens vulneráveis.

Procedimento

1. Como Especialista em correção de TI, no Espaço de correção de TI, clique na exibição inicial.
2. Na exibição inicial, clique no cartão de pontuação **Tarefas de correção atribuídas** para exibir os registros.

   Para fins deste exemplo, você pode verificar o campo Descrição resumida na tarefa de correção (VUL#) em busca de qualquer texto relacionado à sua vulnerabilidade crítica. Digamos, por exemplo, que você saiba que seu gerenciador de vulnerabilidades criou um tópico de observação chamado Vulnerabilidades críticas com vazamentos de patch para detectar IVs (VIT#) com esta vulnerabilidade crítica.

   Com o registro aberto, você também pode revisar os IVs, os patches preferenciais e ver se você ou alguém do seu grupo já enviou solicitações de patch para aprovação.

3. Se você tiver informações suficientes, talvez prefira enviar uma solicitação de patch agora a partir desta tarefa de correção.

   Nota: Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.

4. Clique em **Programar patch** e preencha os campos na caixa de diálogo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como programar um patch, consulte Programar patches com a integração Microsoft do SCCM com Resposta a vulnerabilidades.

5. Como alternativa, na exibição de lista no Espaço de correção de TI, você pode clicar nos links Tarefas de correção, Itens vulneráveis, Soluções e Patches para exibir esses registros. No caso deste exemplo, em vez de um nome de tópico de observação, você pode saber o ID do artigo ou o ID do boletim e o título do patch. Em caso afirmativo, convém verificar se algum dos IVs com esta vulnerabilidade está atribuído a você ou aos seus grupos. Em registros de atualização de patch, você pode enviar solicitações de patch. Em registros de VI, você pode verificar possíveis patches e abrir a tarefa de correção associada se quiser enviar uma solicitação de patch.
6. Se você não tiver acesso aos espaços ou preferir exibir dados e programar patches no ambiente clássico, siga estas etapas.

   a. Navegar até **Resposta a vulnerabilidades** > **Patches** > **Todos**.

   b. Localize o registro de atualização de patch desejado.
   Você pode preferir filtrar os registros com pontuações de risco `crítico`.

   c. Revise os campos de VIs associados e % de VIs corrigidos na guia Status de correção.
   Se os IVs tiverem patches disponíveis, o botão **Programar patch** será exibido no canto superior direito do registro.

   d. Se você decidir enviar uma solicitação, clique em **Programar patch**.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com a integração Microsoft do SCCM com Resposta a vulnerabilidades.

   e. Como alternativa, diga que você não tem as informações de ID do patch, mas pode verificar o campo Descrição resumida nas tarefas de correção atribuídas ao seu grupo para qualquer texto relacionado à sua vulnerabilidade crítica.

   f. Navegar até **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuído aos Meus grupos**.

   g. Localize o registro desejado e clique nele para abri-lo.
   No registro aberto, revise a guia Status de correção para VIs e % de VIs corrigidos. Clique nos Links relacionados para registros IV, Soluções preferenciais, Patches preferenciais e Solicitações de patch.

      Nota: Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.

   h. Clique em **Programar patch** no registro se quiser enviar uma solicitação de patch.

Noções básicas sobre Qualys Vulnerability Integration

Os sensores do produto Qualys coletam os dados e os enviam automaticamente para a aplicação Qualys, que analisa e correlaciona continuamente as informações. Ele se integra facilmente com Resposta a vulnerabilidades como o Qualys Vulnerability Integration para mapear vulnerabilidades para ICs e serviços de negócio para determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas.

Configure seu Qualys Vulnerability Integration usando **Vulnerabilidade** > **Administração** > **Assistente de configuração** para tornar a recuperação de dados mais flexível e escalonável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você tiver várias implantações da aplicação Qualys Cloud Platform, poderá adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com o seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados obtidos de cada implantação são identificados e estão disponíveis em uma única instância de Resposta a vulnerabilidades. Qualys Vulnerability Integration Os registros da base de conhecimento são normalizados em implantações, garantindo que as instâncias da mesma vulnerabilidade em implantações sejam tratadas como a mesma vulnerabilidade.

Nota: Você não pode excluir a integração de vulnerabilidade original, mas pode desativá-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Nota: Embora o Qualys Vulnerability Integration crie integrações para lista de dispositivos, grupo de ativos, lista de pesquisa dinâmica e lista de pesquisa estática, eles não são necessários para a operação normal.

Versões disponíveis

Versão de lançamento para Xanadu	**Notas de versão**
Qualys Vulnerability Integration v12.7, v12.8	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Componentes instalados

Para obter uma lista atual das funções, trabalhos de integração e tabelas instaladas com a integração, bem como um link para instruções de como exibir o que está instalado no momento em sua instância, consulte Componentes instalados com o Qualys Vulnerability Integration.

Integrações primárias e de suporte

Qualys As integrações primárias e de suporte aprimoram os dados de vulnerabilidade em sua instância recuperando dados da integração de vulnerabilidade da Qualys. Uma série de trabalhos agendados invoca as integrações automaticamente. Você também pode executá-los manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. As integrações primárias e de suporte podem ser modificadas.

As Qualys integrações são executadas como trabalhos agendados. Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Este valor não deve ser alterado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A falha ao definir um usuário run-as válido resulta em vários anexos de recuperação de dados, geralmente duplicados, nos registros de fonte de dados, sempre que a integração é executada. Vários anexos na fonte de dados aumentam o tempo de processamento, resultando em resultados de transformação inconsistentes.

Durante a importação, os registros CVE, que ainda não estão presentes, são criados como registros NVD e referenciados em entradas de terceiros para Qualys por padrão.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Integrações primárias

Uma integração primária é um ponto de entrada para a Qualys Cloud Platform que interage com a Qualys API invocada em uma programação.

Exiba as integrações primárias navegando até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.

Integrações de suporte

Uma integração de suporte é um processo que não deve ser executado em uma programação nem sem invocação por uma integração primária.

Exiba as integrações de suporte navegando até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações de Suporte**.

Conector do Service Graph para Qualys

A partir da versão 2.2, o Conector do Service Graph para Qualys está disponível no ServiceNow® Store. Para obter mais informações, consulte Conector do Service Graph para Qualys (2.0.0) .

Os dados dos campos de fonte de dados da Qualys são importados com a API Ativo global e a Gestão de ativos e a API Marcação.

API Ativo global:

- É necessária uma licença de CSAM.
- As informações de ativos incluem detalhes como Categoria de hardware e Categoria de SO.

API Asset Management and Tagging:

- Não requer uma licença do CSAM
- As informações de ativos não incluem detalhes sobre Categoria de hardware e Categoria de SO.

Para obter mais informações, consulte Conector do Service Graph para Qualys APIs .

.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ICs usando o Mecanismo de Identificação e Reconciliação (IRE)

Você pode usar o Mecanismo de Identificação e Reconciliação para criar novos ICs quando um IC existente não puder ser correspondido com um host importado de um scanner de terceiros. Habilite o plug-in Modelos de classe de IC do CMDB para criar ICs usando as novas classes, caso contrário, ICs incompatíveis serão criados nas classes de IC incompatível. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos em nuvem incompatíveis.

Listas de pesquisa

As listas de pesquisa são usadas em Qualys para criar grupos personalizados de vulnerabilidades. Você pode salvá-los e usá-los para a criação de tíquetes e para personalizar verificações e relatórios de vulnerabilidades. O módulo Listas de pesquisa permite que você baixe os dados da lista de pesquisa da Qualys para sua instância de forma programada.

As listas de pesquisa são extraídas de Qualys usando os mapas de transformação de dados Importação de lista de pesquisa dinâmica e/ou Importação de lista de pesquisa estática. Em cada uma dessas transformações, você pode definir cronogramas para executar a importação.

Perfis de opção

Os perfis de opção estão disponíveis com Qualys configurações de verificação. Um perfil de opção é necessário quando você inicia uma verificação a partir do seu Now Platform.

Os perfis de opção são importados do produto Qualys pela integração da lista de perfis de opção. Você pode preferir executar a integração da lista de perfil de opção após uma importação das integrações de listas de pesquisa, Qualys lista de pesquisa dinâmica e Qualys integrações de lista de pesquisa estática para que você possa ver quais listas de pesquisa estão associadas a perfis de opção.

Grupos de ativos

Os grupos de ativos são configurados na plataforma Qualys. Os grupos de ativos identificam quais dispositivos scanner são usados para verificar endereços IP correspondentes quando uma verificação é iniciada a partir do Now Platform.

Os grupos de ativos que têm dispositivos associados são extraídos de Qualys pela integração da lista de grupos de ativos.

Inicie a integração da lista de dispositivos depois de importar grupos de ativos para preencher os campos Nome do dispositivo e Status do dispositivo nos registros de Aplicações padrão Qualys na Now Platform.

Marcadores de host

Todos os marcadores de host são importados como parte da integração Qualys de lista de hosts. Os marcadores de host são usados principalmente para filtragem em Resposta a vulnerabilidades Regras de grupo de atribuição e vulnerabilidade. Eles são exibidos no formulário Item descoberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A integração Qualys da lista de hosts deve ser executada antes da criação de regras de atribuição ou de tarefa de correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Se um marcador **San Diego** for criado, um marcador **SAN DIEGO** não poderá ser armazenado na tabela de marcadores do host. 'San Diego' e 'SAN DIEGO' são considerados o mesmo marcador de host. O marcador que foi importado primeiro vence.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags**. Esta propriedade é definida como verdadeira por padrão. A desativação dos marcadores os desativa em todas as instâncias.

As etiquetas de host (também chamadas de etiquetas do ativo) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos ativos do host. Em seguida, ao iniciar verificações, você pode selecionar marcadores associados aos hosts que deseja verificar. O módulo Marcadores de host permite que você baixe dados de marcador de host de Qualys para sua instância de forma programada.

Reabrir itens vulneráveis resolvidos não encerrados por verificações

Itens vulneráveis definidos como "Resolvidos" em sua instância Now Platform, mas não transicionados para "Fechados/Corrigidos" pelas execuções de integração de terceiros, serão reabertos se forem detectados durante novas verificações.

Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como "Resolvidos", mas que não foram transicionados para "Encerrado/Corrigido" pelas verificações subsequentes, esses IVs voltarão para "Aberto" quando a última data encontrada for posterior a Data de resolução.

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados de Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa gravidade que um cliente não está disposto a corrigir usando o processo de resposta a vulnerabilidades. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection – Standard/post**. Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método post com os seguintes valores:

- Nome: gravidades
- Valor: 3-5 (ou qualquer gravidade apropriada desejada)

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Mensagens REST da Qualys

Preparando para o Qualys Vulnerability Integration

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. É essencial que você se prepare para a integração executando estes procedimentos. O Qualys Vulnerability Integration pressupõe que você esteja familiarizado e execute verificações da Qualys Cloud Platform em seu ambiente.

Nota: Faça as mudanças de configuração necessárias com base em seus requisitos antes de executar as integrações.

Pré-requisitos importantes

Valide o dimensionamento da instância com base no número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

Use a filtragem para limitar o número de itens para importação inicial e fasear sua implantação ajustando os filtros nas importações subsequentes.

Os scanners Qualys são desativados por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Ações a serem tomadas

- Determine uma data de início inicial para integrações de **importação de lista de detecção de host**.

  Considere definir o campo **Hora** de início para algumas horas ou dias no passado. O ideal é escolher a data da última verificação da Qualys. A data de início pode incluir vulnerabilidades descobertas antes de usar a solução de gestão de vulnerabilidades. Defina a hora de início mais antiga usada para o início do ciclo de verificação. Portanto, se demorar uma semana antes que todos os hosts sejam verificados, defina este valor como uma semana antes dessa hora.

- Adicione usuários às funções de administrador, sn_vuln.admin e sn_vul_qualys.admin. Para obter mais informações, consulte Atribuir uma função a um usuário .

- Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

- Se você não usar calculadoras de vulnerabilidade, Desabilitar a calculadora de vulnerabilidade padrão se não for usada, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.
- Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, desabilite as regras de negócio.
- Se você quiser usar um scanner diferente do padrão da Qualys, consulte configuração de dispositivos scanner.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tenha a URL do servidor Qualys e as credenciais de autenticação prontas. As credenciais devem fornecer permissões adequadas para recuperar informações de conhecimento, verificação e detecção para uma assinatura da Qualys.
- Se você planeja usar marcadores de host em Resposta a vulnerabilidades Regras de Grupo de Atribuição ou Vulnerabilidade, certifique-se de que a integração Qualys da Lista de Hosts tenha sido executada antes de criar regras.

Instalar o Qualys Vulnerability Integration

Antes de executar Qualys Vulnerability Integration em sua instância, você deve instalar e configurar a aplicação Qualys Vulnerability Integration. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Função necessária: administrador para baixar e instalar a aplicação

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Obtenha direitos da aplicação Qualys Vulnerability Integration e baixe-os para sua instância Now Platform®.	Se a aplicação ainda não foi baixada em sua instância, consulte .
Prepare-se para a integração.	Consulte Preparando para o Qualys Vulnerability Integration.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.

   Depois de alguns momentos, as aplicações que estão disponíveis para instalação em sua instância são exibidas.

2. Localize o bloco Qualys Vulnerability Integration e clique em **Instalar**.
3. Siga os avisos no Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Navegue até **Configuração de integração>Integrações de scanner** no Assistente de configuração para continuar com a configuração.
   Para obter mais informações sobre como complementar os avisos fornecidos no Assistente de configuração, consulte Configurar o Qualys Vulnerability Integration usando o Assistente de configuração.

O que Fazer Depois
Ative os scanners, pois eles estão inativos por padrão na aplicação Resposta a vulnerabilidades. Para obter mais informações sobre como ativar os Qualys scanners, consulte Ativar os Qualys scanners.

Ativar os Qualys scanners

Você deve ativar os scanners após instalar o Qualys Vulnerability Integration porque os scanners são desativados por padrão na aplicação Resposta a vulnerabilidades.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não ficará disponível.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto scanner que você deseja ativar e selecione o registro para abri-lo.
3. Marque a caixa de seleção **Ativo**.
4. Selecione **Atualizar**.
5. O produto que você ativou é exibido no campo **Origem** em um item vulnerável e nos registros de tarefa de correção após a próxima importação, e a nova **verificação** está disponível como uma ação de IU.

Componentes instalados com o Qualys Vulnerability Integration

As seguintes funções, trabalhos de integração e tabelas são instaladas com o Qualys Vulnerability Integration.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos agendados e as tabelas instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No Construtor de condições, para adicionar um segundo filtro, selecione **AND e**, em seguida, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, Trabalho **agendado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_vul_qualys.read	Tem acesso de leitura aos registros Qualys Vulnerability Integration.	
sn_vul_qualys.usuário	Usuário para Qualys Vulnerability Integration. Pode ler e gravar registros	sn_vul_qualys.read
sn_vul_qualys.admin	Administrador paraQualys Vulnerability Integration. Por exemplo, você pode modificar as datas de início da integração e executar algumas definições de configuração avançadas.	• sn_vul_qualys.usuário • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Pode configurar o Qualys Vulnerability Integration	sn_vul_qualys.admin

Trabalhos de integração instalados

Trabalho de integração	Descrição
Qualys Integração da lista de pesquisa estática	Sincroniza Qualys listas de pesquisa para encontrar entradas vulneráveis. Recupera somente registros do tipo lista estática.
Qualys Integração abrangente de detecção de host	Recupera dados de host e vulnerabilidade de Qualys e os processa em sua instância. Ele coordena as chamadas de mensagem REST para a API de detecção de host. A saída desta integração são itens vulneráveis. Esta integração importa todos os estados da vulnerabilidade: Novo, Corrigido, Ativo e Reaberto. Por padrão, esta integração está inativa e é executada semanalmente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de integração	Descrição
	Nota: Depois que essa integração é ativada, o trabalho abrangente diário importa somente os estados Novo, Corrigido e Reaberto.
Qualys Integração da lista de hosts	Recupera dados de verificação de host autenticados e não autenticados e marcadores de host de Qualys uma vez por semana e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente.
Qualys Integração de detecção de host	Recupera dados de host e vulnerabilidade de Qualys e os processa em sua instância. Ele coordena as chamadas de mensagem REST para a API de detecção de lista de hosts. As saídas desta integração são itens vulneráveis. Qualys marcadores de host são importados nesta integração.
Qualys Integração de tíquete	Recupera Qualys tíquetes e os adiciona à sua instância. Ele coordena as chamadas de mensagem REST para a API da lista de tíquetes. Frequentemente, há menos tíquetes do que detecções de host, já que as configurações Qualys podem restringir as detecções que resultam em um tíquete.
Qualys Integração da lista de perfis de opção	Recupera perfis de opção do produto Qualys. Os perfis de opção incluem configurações de verificação que são necessárias quando você inicia verificações da sua instância Now Platform.
Qualys Integração da lista de dispositivos	Recupera informações do dispositivo scanner de Qualys.
Qualys Integração de grupo de ativos	Recupera informações do grupo de ativos de Qualys. Grupos de ativos são usados para identificar quais dispositivos scanner usar para verificar itens de configuração correspondentes.
Qualys Base de conhecimento (preenchimento)	Recupera Qualys entradas da base de conhecimento. Programado para ser executado após a Qualys Integração de detecção de host. Atualiza sua instância com todos os QIDs que foram referenciados na integração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de integração	Descrição
	de detecção de host, mas não existiam no sistema.
Qualys Base de conhecimento	Recupera Qualys entradas da base de conhecimento. Os dados recuperados são baseados na data em que as vulnerabilidades foram atualizadas por Qualys e desde a última vez em que a integração foi executada. Esses dados são úteis para preencher dados históricos em sua instância, bem como garantir que os Qualys Identificadores (QIDs) estejam atualizados.
Qualys Integração da lista de pesquisa dinâmica	Sincroniza Qualys listas de pesquisa para encontrar entradas vulneráveis e recupera registros do tipo de lista dinâmica.
Corrigindo as detecções de chave atualizada para Qualys	Uma combinação de hash de campos que fornecia uma maneira de identificar e vincular uma detecção a um Qualys item vulnerável.
Qualys Atualizar itens descobertos existentes com o identificador de partição de rede	Atualiza os itens descobertos existentes. Os ICs para seus dados de integração de vulnerabilidade Qualys existentes são criados ou atualizados para incluir a granularidade do identificador de partição de rede.

Tabelas instaladas

Tabela	Descrição
Vulnerabilidade da Lista de Pesquisa sn_vul_qualys_m2m_search_list_vul	Armazena o mapeamento entre a lista de pesquisa Qualys e uma vulnerabilidade.
Qualys Verificador de vulnerabilidade sn_vul_qualys_scanner	Tabela que estende os Verificadores de vulnerabilidade para armazenar informações do scanner para o recurso de nova verificação Qualys.
Qualys Listas de Pesquisa sn_vul_qualys_search_list	Armazena listas de pesquisa recuperadas pela integração de lista de pesquisa Qualys.
Qualys Importação de dispositivo sn_vul_qualys_appliance_imp	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Qualys IC	A tabela não é mais usada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
sn_vul_qualys_ci	
Paginação de Detecção de Host sn_vul_qualys_host_detection_pagination	A tabela não é mais usada.
Qualys Execução de integração sn_vul_qualys_integration_run	A tabela não é mais usada.
Qualys Integração sn_vul_qualys_integration	Tabela que estende a integração de vulnerabilidade e armazena todas as integrações que correspondem a Qualys.
Qualys Importação da lista de pesquisa estática sn_vul_qualys_static_search_list_imp	Tabela que estende a linha do conjunto de importação. Mapas de campo são usados para transformar dados na tabela de destino, Qualys Listas de pesquisa.
Qualys Base de conhecimento sn_vul_qualys_knowledge_base	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Qualys Lista de tíquetes sn_vul_qualys_ticket_list_imp	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Qualys Perfil de opção sn_vul_qualys_option_profile	Tabela que armazena os perfis de opção recuperados de Qualys. Esta tabela é usada com a nova verificação.
Qualys Importação da lista de pesquisa dinâmica sn_vul_qualys_dynamic_search_list_imp	Tabela que estende a linha do conjunto de importação. Mapas de campo são usados para transformar dados na tabela de destino, Qualys Listas de pesquisa.
Qualys Reexecução do conjunto de importação sn_vul_qualys_import_rerun	A tabela não é mais usada.
Qualys Importação de perfil de opção sn_vul_qualys_option_profile_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.

Atualizar itens de configuração com o identificador de partição de rede para o Qualys Vulnerability Integration

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão, na aplicação Resposta a vulnerabilidades, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC `(IC 1)` durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_ID	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	REPOSITORY_ID	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. A partir de uma nova importação de dados, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para as integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

A partir da v14.0 de Resposta a vulnerabilidades e v12.1 da Integração de vulnerabilidade Qualys Vulnerability Integration, os Modelos de classe de IC do CMDB (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

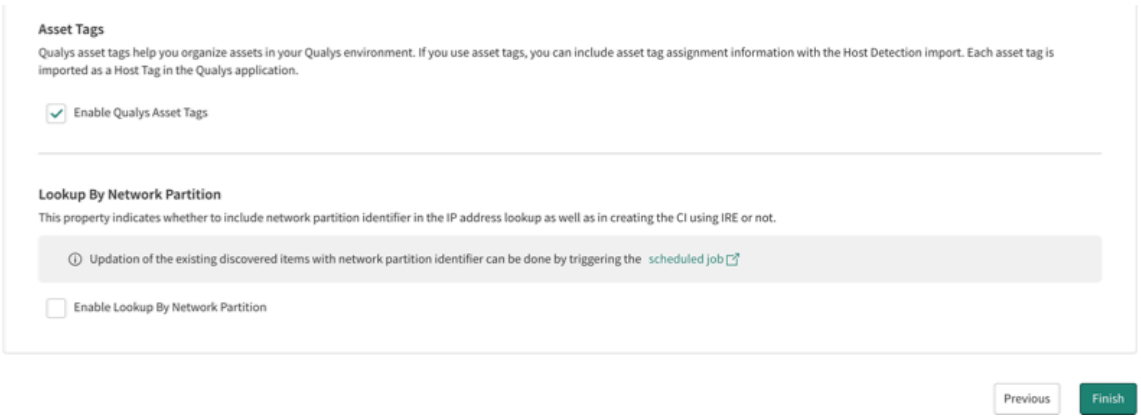
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. Os ICs dos dados Qualys Vulnerability Integration existentes são criados ou atualizados para incluir a granularidade do identificador de partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são todos atualizados com os novos ICs.
Aguarde as importações de novos dados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo trabalho agendado. IC, item vulnerável e registros de detecção são todos atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Escolha Qualys Vulnerability Integration.
3. **Edite** a integração necessária.
4. Escolher **Configuração de Detecção de Host**.
5. Escolher **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede**



seção.

6. Clique em **Concluir**.

Identificadores de partição de rede NETWORK_ID e REPOSITORY _ID incluídos na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys Vulnerability Integration: integrações de ativos e	123.12.12.141	03712	IC 1	IC 1

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
vulnerabilidades fixas e abertas				
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

As regras de pesquisa de identificação de IC de endereço IP e endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration.

Depois de ativar o trabalho agendado e salvar os registros, você pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando trabalhos agendados sob demanda. Os ICs em seu item descoberto existente, item vulnerável e registros de detecção são atualizados automaticamente.

Modificações opcionais da Qualys

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração da Qualys.

Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, ou modificar regras de negócio para desativá-las durante uma importação inicial.

Desabilitar regras de negócio relacionadas a notificações antes da importação do registro inicial

Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem gerar muitas notificações, afetando o desempenho. Essas regras de negócio devem ser modificadas para desativá-las durante a importação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócio**.
2. Pesquise **notificações de IC afetado**.
3. Abra a regra de negócio e insira esta condição: `current.sys_class_name != "sn_vul_vulnerable_item"`.
4. Clique em **Atualizar**.
5. Repita este procedimento para as seguintes regras de negócio:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Notificações do centro de custos afetado
- Notificações do grupo afetado
- Notificações de locais afetados

Nota: Após a conclusão da importação do registro inicial, você tem a opção de habilitar novamente essas regras de negócio. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Modificar uma data de início inicial

Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações da Qualys. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado abaixo.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
2. Clique **em Qualys Host Detection Integration**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique **em Detalhes da integração**.
4. Defina o campo **Hora** de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde essa hora sejam detectadas.

   Se você configurou Qualys usando o Assistente de configuração, o campo **Hora** de início será preenchido previamente, inicialmente até três meses antes da data de hoje e, posteriormente, até a data de hoje.

   Nota: Considere definir o valor para um máximo de um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Qualys, bem como o acionamento de tempos limites de execução.

5. Clique em **Enviar** ou **Atualizar**.
6. Opcional: Clique **em Executar agora** para executar imediatamente.

Configurações e modificações avançadas da Qualys

Configure modificações opcionais avançadas e simplifique alguns dos dados especificamente para a integração da Qualys. A maioria dessas modificações requer codificação ou conhecimento avançado ServiceNow ou Qualys Cloud Platform.

Modifique os valores de mapeamento de estado e prioridade da Qualys para ServiceNow

Modifique os valores de mapeamento de prioridade e estado para seus requisitos.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Esta é uma opção de personalização avançada.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócio**.
2. Pesquise **Mapear valores da Qualys** e abra-o.
3. Clique na guia **Avançado**.
4. Modifique de acordo com seus requisitos.
   As modificações mais comuns incluem a adição de novos valores de estado ou a revisão da criticalidade ou prioridade.
5. Clique em **Atualizar**.

Restringir a capacidade de gravar em um registro com base em um grupo de atribuição

Você pode restringir os direitos de gravação/leitura em registros com base na associação a um grupo atribuído. Modifique as condições e o script com base em requisitos específicos.

Antes de Iniciar
Função necessária: security_admin (função elevada de administrador)

Nota: Esta ação é realizada no escopo de vulnerabilidade.

Procedimento

1. Navegar até **Todos** > **Segurança do sistema** > **Controle de Acesso (ACL)**.
2. Pesquise ACLs que começam com `sn_vul`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Escolha um registro de controle de acesso, por exemplo, `sn_vul_vulnerable_item`, **Operação** de **gravação**.
4. Marque a caixa **Avançado** no registro, se necessário, para exibir as entradas de **Função**.
5. Modifique o script de **função** para seus requisitos.
   Exemplo de script de modificação de acesso por grupo.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Clique em **Atualizar**.

Configurar dispositivos scanner

Se você estiver iniciando verificações a partir do seu Now Platform® em vez de diretamente da Qualys, poderá configurar verificações para intervalos de endereços IP.

Antes de Iniciar

Os dados vêm da integração Qualys com base em Qualys grupos de ativos e seus dispositivos padrão relacionados (scanners).

Se nenhum dispositivo estiver configurado para os intervalos de endereços IP de destino, o dispositivo definido como padrão para a instância de integração será usado para a verificação.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Dispositivos de Scanner**.
2. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome do dispositivo	Você será solicitado a preencher este campo ao criar um registro manualmente. Insira o nome do dispositivo scanner Qualys a ser usado para invocar verificações para itens de configuração correspondentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Use o valor `Externo` quando quiser que a verificação seja iniciada com um scanner externo.
ID de dispositivo	Insira o identificador do dispositivo para o dispositivo scanner Qualys a ser usado para invocar verificações para itens de configuração correspondentes. Você será solicitado a preencher este campo ao criar um registro manualmente. Use o valor `0` quando quiser que a verificação seja iniciada com um scanner externo.
Status do dispositivo	Exibe o último status do dispositivo scanner nos dados retornados pela integração Qualys. Para registros criados manualmente, o status será atualizado somente se um **ID de dispositivo** válido for especificado.
ID de grupo de ativos	Exibe o identificador do grupo de ativos Qualys que criou este registro. Este campo exibe um valor somente para registros criados pela integração Qualys.
Nome do grupo de ativos	Exibe o nome do grupo de ativos Qualys que criou este registro. Este campo exibe um valor somente para registros criados pela integração Qualys.
Ordem	Insira um valor a ser usado para determinar a prioridade de verificação. Para dispositivos com critérios conflitantes, um dispositivo com um valor de ordem mais baixo recebe uma prioridade mais alta.
Criado manualmente	Indica se este registro foi criado manualmente pelo usuário.
Usar grupo de filtros	Marque esta caixa de seleção para especificar um grupo de filtros para encontrar itens de configuração correspondentes para verificação.
Grupo de filtros	Selecione o grupo de filtros que você deseja usar para encontrar itens de configuração correspondentes para verificação. Este campo aparecerá somente se você selecionou **Usar grupo de filtros**.
IPs	Uma lista separada por vírgulas de endereços IP ou intervalos de endereços IP a serem usados por este dispositivo ao invocar verificações.
Instância de integração	A instância de integração Qualys associada a este dispositivo.
Perfil de opção	Selecione o perfil de opção que você deseja usar para verificações de itens de configuração correspondentes.

3. Clique em **Atualizar**.

Configurar e gerenciar Qualys scanners e verificações de vulnerabilidade

Qualys verificações de vulnerabilidade podem ser realizadas para encontrar vulnerabilidades de software que afetam seus ICs. Você pode iniciar verificações a partir de um registro de item vulnerável ou criando um registro de verificação diretamente para itens de configuração (ICs) e endereços IP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você verificar Qualys itens vulneráveis diretamente na tela Itens vulneráveis, também terá a opção de verificar vários itens vulneráveis ao mesmo tempo.

Se Security Incident Response estiver ativado, você também poderá iniciar uma verificação a partir do catálogo de incidentes de segurança, de um registro de incidente de segurança ou de uma solicitação de verificação de segurança.

Verificações enviadas de Qualys itens vulneráveis, Catálogo de incidentes de segurança, incidentes de segurança ou solicitações de verificação de segurança são realizadas pelo scanner Qualys padrão.

Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

- Os perfis de opção contêm Qualys configurações de verificação.
- Um perfil de opção é necessário quando você inicia uma verificação de [Qualys a partir do seu Now Platform®.

Configurar a verificação de IP Qualys iniciada pela ServiceNow

O scanner Qualys incluído com o sistema de base fornece uma integração de linha de base para iniciar verificações com base em endereços IP.

Antes de Iniciar

Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

- Os perfis de opção contêm Qualys configurações de verificação.
- Um perfil de opção é necessário quando você inicia uma verificação da Qualys a partir do seu Now Platform®.

Função necessária: sn_vul_qualys.admin

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Abra o registro Qualys.
3. Marque as caixas de seleção**Ativo** e **Padrão**.

   É necessário selecionar **Ativo** para usar o scanner Qualys para verificar Qualys VIs automaticamente. Você também não precisa selecionar **Padrão** para que ele seja executado automaticamente.

   Antes da v12.0, **o ativo** era necessário para usar o scanner. Se **Padrão** também for selecionado, o scanner será usado automaticamente sem precisar ser selecionado durante a digitalização.

4. Para o campo Integração de origem, clique no ícone de pesquisa e selecione a opção para **Qualys**, por exemplo, **Qualys Cloud Platform**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Atualizar**.
6. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
7. Abra a **integração da lista de grupos de ativos da Qualys**.
   a. Marque a caixa de seleção **Ativo**.
   b. Clique em **Executar Agora**.
8. Siga estas etapas para preencher seus dispositivos scanner.

   Nota: Você pode preferir executar a integração da lista de perfil de opção após uma importação das integrações de listas de pesquisa, da lista de pesquisa dinâmica da Qualys e das integrações da lista de pesquisa estática da Qualys, para que você possa ver quais listas de pesquisa estão associadas aos perfis de opção.

   a. Abra a **Integração da lista de perfis de opção da Qualys**.
   b. Marque a caixa de seleção **Ativo**.
   c. Clique em **Executar Agora**.
   d. Siga as etapas listadas em Configurar dispositivos scanner para configurar seus dispositivos scanner.
      Retorne aqui depois de concluir essas etapas para continuar com a configuração.
   e. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
   f. Abra a **Integração da lista de dispositivos da Qualys**.
   g. Marque a caixa de seleção **Ativo**.
   h. Clique em **Executar Agora**.
      Seus Qualys dispositivos scanner agora estão preenchidos corretamente.

Informações relacionadas

Noções básicas sobre Qualys Vulnerability Integration

Verificar várias Qualys vulnerabilidades ou itens vulneráveis

Você pode verificar simultaneamente várias Qualys vulnerabilidades ou itens vulneráveis que contenham pelo menos um item de configuração (IC) afetado ou um endereço IP preenchido no formulário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Siga um destes procedimentos:
   - Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
   - Navegar até **Todos** > **Resposta a vulnerabilidades** > **Todos os Itens vulneráveis**.
2. Marque as caixas de seleção dos registros que você deseja verificar.
3. Clique na lista **Ações nas linhas selecionadas** e clique em **Verificar novamente se há itens vulneráveis**.
   Uma mensagem aparece com um link para a verificação e as anotações de trabalho são atualizadas.
4. Clique no link para ver o andamento ou os resultados da verificação.

Configurar a verificação automática Qualys para tarefas de correção resolvidas

Você pode programar a verificação que é executada automaticamente para atualizar seus Qualys itens vulneráveis.

Antes de Iniciar

Depois que uma tarefa de correção é transicionada para **Resolvida**, uma verificação é iniciada automaticamente para atualizar o estado dos itens vulneráveis associados.

- A verificação está desabilitada por padrão.
- Habilite a verificação com o parâmetro de instância de integração **scan_on_resolved** no registro da **Qualys** localizado em **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração** > **Qualys**. Consulte as etapas a seguir para obter mais informações.
- Esta verificação é específica da instância. Se você tiver várias instâncias e quiser habilitar ou desabilitar esta verificação, deverá desabilitar o parâmetro **scan_on_resolved** nos parâmetros de instância de integração em cada instância que deseja alterar.
- Quando a verificação está habilitada, você pode iniciar a verificação sob demanda ou pode programar a verificação para ser executada somente dentro de uma janela de tempo especificada. Consulte Configure Qualys novas verificações para serem executadas somente dentro de intervalos programados para saber como definir os horários de início e término da janela de tempo.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.
2. Selecione **Qualys** para abrir o registro.
   Os parâmetros de instância de integração para Qualys são exibidos em uma guia.
3. Para habilitar a verificação automática, localize o parâmetro *scan_on_resolved*.
4. Na coluna Valor da propriedade, insira `verdadeiro`.
5. Clique em **Atualizar**.

Configure Qualys novas verificações para serem executadas somente dentro de intervalos programados

Para a integração de vulnerabilidade Qualys, defina os parâmetros de hora de início e término da verificação para que as novas verificações sejam executadas ou estejam disponíveis somente durante os horários desejados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Esta configuração se aplica a novas verificações programadas e a novas verificações que você inicia manualmente no produto Qualys da sua instância Now Platform®.

Definir os parâmetros de hora de início e término da verificação para instâncias de integração permite especificar janelas de tempo quando novas verificações no produto Qualys estão disponíveis. Por exemplo, você pode preferir especificar que as novas verificações só estão disponíveis fora do horário comercial, por exemplo, da meia-noite às 10h.

Esta configuração é específica da instância. Se você tiver várias instâncias, deverá configurar os valores scan_start_time e scan_end_time nos parâmetros de instância de integração em cada instância que deseja mudar.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração** > **Qualys**.
2. Clique em **Qualys** para abrir o registro.
   Os parâmetros de instância de integração para Qualys são exibidos.
3. Para o parâmetro scan_start_time, na coluna Valor, insira a hora no fuso horário UTC no formato de 24 horas (00:00 a 24:00) para a hora de início da janela em que você deseja novas verificações disponíveis.
4. Para scan_end_time, na coluna Valor, insira horas no mesmo formato (00:00 a 24:00) para a hora de término da janela disponível.
   Por exemplo, se você inserir uma hora de início de 00:00 para o parâmetro scan_start_time e um scan_end_time de 10:00 AM na mesma manhã, as verificações programadas ou iniciadas manualmente fora da janela de tempo da meia-noite às 10 AM serão enfileiradas e iniciadas no hora de início da janela de tempo do dia seguinte, 00:00.

   No mesmo exemplo, se um proprietário de correção iniciar manualmente uma nova verificação às 11h, a nova verificação não será iniciada imediatamente, pois está fora dos tempos de verificação configurados disponíveis. A solicitação de verificação permanece na fila até o início da janela de tempo do dia seguinte, neste exemplo, (00:00).
5. Clique em **Atualizar** para salvar suas configurações.

Qualys limites de taxa de verificação de vulnerabilidades

Você pode definir a taxa em que diferentes tipos de verificações são executadas para limitar o número de solicitações que são enviadas para um scanner externo. Depois de definir os limites de taxa, você pode aplicá-los aos Qualys scanners.

Definir Qualys limites de taxa de verificação

Você pode definir a taxa em que diferentes tipos de verificações são realizadas para equilibrar a carga na fila de verificação. As condições definidas no limite de taxa determinam se os limites de taxa são aplicados a entradas na fila.

Antes de Iniciar

Função necessária: sn_vul.admin

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Definições de Limite de Taxa**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Definição de limite de taxa

Campo	Descrição
Nome	Forneça um nome descritivo que identifique as condições que a entrada da fila deve atender. Por exemplo, verificações por minuto
Condições de fila	Insira as condições usadas para determinar se uma entrada de verificação na fila está sujeita a este limite de taxa. As condições não devem ser específicas para um scanner específico.
Script de avaliação	Grave um script com a lógica para avaliar a entrada na fila. É importante que o script retorne verdadeiro/falso para definir se a entrada é processada. Além disso, baseie o script de avaliação na entrada da fila que está sendo avaliada.

4. Clique em **Enviar**.

Aplicar limites de taxa de verificação a Qualys scanners

Depois de definir os limites de taxa de varredura usando **Definições de limite de taxa**, você pode aplicar limites de taxa a Qualys scanners específicos.

Antes de Iniciar

Função necessária: sn.vul_admin

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Limites de Taxa do Scanner**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Limite de taxa do scanner

Campo	Descrição
Scanner	Selecione o scanner ao qual você deseja aplicar um limite de taxa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Limite de taxa	Selecione o limite de taxa que você deseja aplicar a este scanner.
Limite	Insira o limite ao qual você deseja sujeitar o scanner selecionado para o limite de taxa selecionado. Por exemplo, se o scanner permitir 4 varreduras por minuto e o limite de taxa for definido como solicitações por minuto, o limite será 4.

4. Clique em **Enviar**.

Exibir a Qualys fila de verificação de vulnerabilidades

As solicitações de verificação de vulnerabilidade enviadas para a integração de verificação de vulnerabilidades Qualys são enfileiradas para não sobrecarregar os recursos do sistema. Você pode exibir o status das solicitações na fila, conforme necessário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Na lista de verificações enfileiradas, cada verificação inclui um nome de verificação gerado automaticamente que identifica o IC que foi verificado.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Fila de Verificação**.
   Todas as Qualys solicitações de verificação que foram enviadas são mostradas em uma lista. A coluna **Estado** mostra o estado atual de cada entrada na fila. Um estado **Concluído** indica que a verificação saiu da fila. Isso não indica necessariamente que a verificação concluiu o processamento. Quando as verificações forem concluídas ou houver falha, a coluna **Processamento** mostrará o texto de anotações de trabalho apropriado.

   Nota: Se um valor de hash tiver sido enviado para verificação e o scanner falhar em encontrar um resultado, o **Estado** será **Concluído** e a anotação de trabalho na coluna **Processamento** indicará **Desconhecido**.

2. Depois que uma verificação terminar de processar, clique em um registro na fila para exibir detalhes da solicitação de verificação.

Habilitar filtro do sistema de base para importações de detecção confirmadas

Habilite um filtro padrão usando parâmetros de integração para importar somente detecções confirmadas de Qualys Cloud Platform.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin, sn_vul.vr_import_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Um parâmetro de instância de integração de sistema de base "include_only_confirmed" está disponível para importar uma lista filtrada de detecções de Qualys Cloud Platform. Por padrão, este parâmetro é definido como *FALSO* e todas as detecções, sejam potenciais, confirmadas ou informativas, são importadas.

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.
2. Abra a integração da plataforma Qualys Cloud na lista Instâncias de integração.
3. Na lista Parâmetros de instância de integração, abra o parâmetro *'include_only_confirmed'*.
4. Atualize o valor padrão para *Verdadeiro*.
5. Clique em **Atualizar**.
   Você habilitou o filtro para importar detecções confirmadas da integração Qualys Cloud Platform.

Resultados

Por padrão, somente as detecções confirmadas da integração Qualys Cloud Platform são importadas quando a próxima importação de vulnerabilidade da Qualys é executada. Todas as outras detecções, como informativas e potenciais, são ignoradas e não importadas. Para obter mais informações, consulte Exibir dados de detecção de itens vulneráveis da Resposta a vulnerabilidades.

Iniciar nova verificação para Qualys Vulnerability Integration

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados, iniciando novas verificações no produto Qualys a partir do Now Platform sob demanda.

Antes de Iniciar

Você pode iniciar novas verificações nos espaços da Resposta a vulnerabilidades. Para obter mais informações, consulte Verificar novamente registros e tarefas de correção no Espaço do gerenciador de vulnerabilidades e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Para novas verificações no ambiente clássico, consulte as seções a seguir para saber como iniciar novas verificações.

Configuração necessária para novas verificações no produto Qualys iniciadas a partir do seu Now Platform:

Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Qualys da sua instância Now Platform®.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações no produto Qualys a partir de itens vulneráveis (VI), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de itens descobertos da sua instância Now Platform.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Caso de uso:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada a partir de seus Now Platform para Qualys itens vulneráveis.

Você pode iniciar novas verificações para IVs que tenham Qualys como origem em estados diferentes de encerrado. Consulte Verificar novamente registros e tarefas de correção no Espaço do gerenciador de vulnerabilidades e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Verifique se você concluiu a seguinte configuração necessária para novas verificações. Consulte as etapas que começam com Configurar e gerenciar Qualys verificações e verificações de vulnerabilidade listadas nas seções anteriores para obter mais informações.

Função necessária: sn_vul_manually_initiate_rescan

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável a partir do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Você só pode iniciar novas verificações de IVs com Qualys como origem. Verifique se Qualys é exibido na coluna **Origem** nas exibições de lista de VI ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condições para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição de lista de VI, no canto superior esquerdo da lista, clique no ícone**Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **Origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**, **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros**ou para **Itens descobertos** para a tarefa de correção, entrada de terceiros ou registros de itens descobertos, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de VI, o VI deve ser do produto Qualys e estar em qualquer estado diferente de **Closed**. Para vários registros de VI, todos os IVs devem ter Qualys como origem e em qualquer estado diferente de **Encerrado**.
   - Em um registro de RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ter Qualys como origem.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado em qualquer estado diferente de **Encerrado** com Qualys como origem.
   - Em um registro de item descoberto, o item de configuração tem pelo menos um VI associado a Qualys como origem em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro escolhido, clique em **Verificar novamente**.
   Na caixa de diálogo exibida, escolha uma para continuar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Marque a caixa de seleção **Especificar perfis de opção**.	Na lista, escolha o perfil de opção para o scanner Qualys que você deseja usar para a nova verificação. Estes são os dispositivos (scanners) que você configurou e listou em **Integração de Vulnerabilidade da Qualys** > **Dispositivos de Scanner**.
Desmarque a caixa de seleção **Especificar perfis de opção** (não selecionada).	O perfil de opção Qualys do scanner que você definiu como padrão na lista de dispositivos scanner é usado para a verificação. Para obter mais informações sobre como definir os scanners padrão que você inicia a partir do seu Now Platform, Configure os dispositivos de scanner listados na seção anterior para obter mais informações.

5. Clique **em Solicitar verificação**.

   Uma mensagem é exibida indicando que a verificação está sendo processada. O status de todas as novas verificações pode ser encontrado a qualquer momento nas listas relacionadas a Verificação nos registros de VI, RT, TPE e itens descobertos que você usou para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e outras verificações iniciadas a partir de um determinado registro.

   Sua instância rastreia o status de nova verificação até que seja concluído com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform parou de rastrear seu status de nova verificação, não quando a nova verificação real parou.

   Depois que a nova verificação for concluída com sucesso, a Qualys Integração de detecção de host será iniciada automaticamente para atualizar seus itens vulneráveis. Dependendo de quantos IVs você tiver, suas detecções, VIs e RTs serão atualizados após a conclusão da Qualys verificação de integração de detecção de host. Navegue até esses registros para exibir as atualizações após a conclusão da integração de detecção de host.

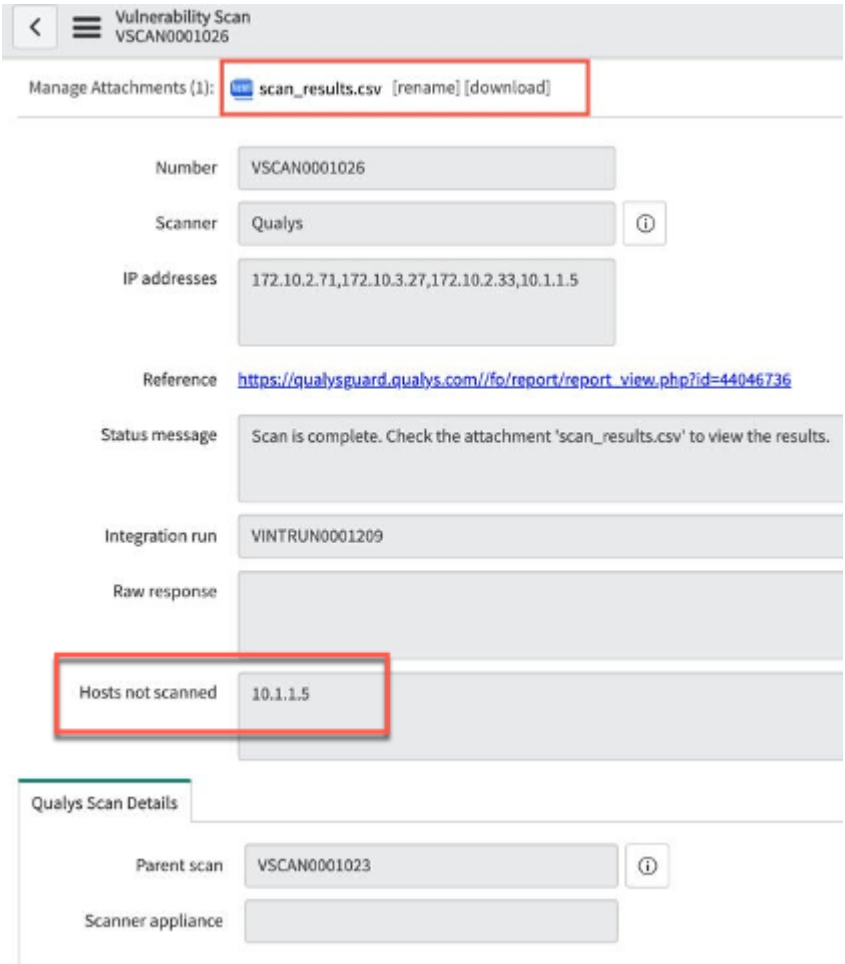
   Esta verificação é específica da instância e pode ser desabilitada. Para obter mais informações sobre as Qualys integrações e como exibir as integrações, consulte Noções básicas sobre Qualys Vulnerability Integration.

O que Fazer Depois

Você pode exibir um anexo .csv no registro de verificação para ver detalhes sobre as novas verificações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Conforme mostrado na imagem anterior, durante a nova verificação, se os hosts (itens de configuração) em seu ambiente não estiverem acessíveis, todas as detecções e IVs associados a esses ativos não serão atualizados quando a nova verificação for concluída. Para ajudar você a entender por que eles não estão incluídos, após a conclusão da nova verificação, os endereços IP do ativo desses ICs são listados em Registros de vulnerabilidade no campo Hosts não verificados.

Qualys metadados para vulnerabilidades

A integração de detecção de host Qualys foi aprimorada para incluir mais campos de Qualys. Esses campos ajudam a filtrar as vulnerabilidades Linux não exploráveis. Essa melhoria aprimora a integração no nível de detecção e no nível de item vulnerável (VI).

Importar metadados adicionais de Qualys

Importe metadados adicionais para itens de vulnerabilidade (VI) para filtrar vulnerabilidades com base no impacto em um kernel ou serviço.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.
2. Em Configuração de integração, clique em **Integrações de scanner**.
3. Em Aplicação instalada, clique em **Editar** para a aplicação Qualys.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique **em Configuração de detecção de host**.
5. Navegar até **Importar metadados adicionais para detecções**.
6. Para importar metadados adicionais de Qualys, marque manualmente qualquer uma das seguintes caixas de seleção necessárias.
   - **Metadados do Kernel**: identifica vulnerabilidades encontradas em kernels do Linux em execução ou não.

     Se o valor dos metadados retornados for **Não**, isso significa que a vulnerabilidade não é explorável devido a um kernel que não está em execução. Para obter informações sobre os valores recuperados, consulte Qualys valores de metadados para vulnerabilidades.

   - **Metadados de serviço**: identifica vulnerabilidades encontradas em portas ou serviços em execução ou não em execução.
   - **Metadados de configuração**exploráveis: identifica vulnerabilidades que podem ou não ser exploráveis devido à configuração do host atual.

   Nota: Por padrão, essas caixas de seleção não estão marcadas.

7. Execute a Qualys Integração de detecção de host com uma data anterior.
   Para obter mais informações sobre como definir a data de início, consulte Modificações opcionais da Qualys.

Resultados
Os metadados foram importados.

O que Fazer Depois
Para exibir os metadados importados, insira `sn_vul_detection.list` na Navegação de filtro. A lista de Detecções de item vulnerável é exibida. Para obter mais informações sobre os valores exibidos nas colunas recém-adicionadas, consulte Qualys valores de metadados para vulnerabilidades.

Qualys valores de metadados para vulnerabilidades

Quando os metadados do kernel, os metadados de serviço e os metadados de configuração são importados, alguns valores também são recuperados. Os valores **0**, **1** e **Não disponível** são processados no back-end e convertidos para **Não**, **Sim** e **Vazio**, respectivamente.

Esses valores são preenchidos nas seguintes colunas nas listas Detecções de item de vulnerabilidade e Itens de vulnerabilidade:

- Afeta a coluna de serviço em execução
- Afeta a coluna de configuração explorável
- Afeta as colunas do kernel em execução

Nota:

- Essas colunas não estão visíveis por padrão. Para obter mais informações sobre como configurar o layout do formulário, consulte Configurar o layout do formulário
- Para detecções mais antigas, os valores dessas colunas podem estar vazios. Para atualizar os dados, execute uma integração de detecção de host da Qualys com data anterior. Para obter mais informações sobre como definir a data de início, consulte Modificações opcionais da Qualys.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tabela a seguir mostra os valores recuperados e seu significado.

Valores de campo recuperados e seu significado

Campo	Valor	Significância
AFFECT_RUNNING_KERNEL	0	A vulnerabilidade foi encontrada em um kernel que não está em execução. A vulnerabilidade não é explorável.
AFFECT_RUNNING_KERNEL	1	A vulnerabilidade foi encontrada em um kernel em execução. A vulnerabilidade é explorável.
AFFECT_RUNNING_KERNEL	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada ao kernel.
AFFECT_RUNNING_SERVICE	1	A vulnerabilidade é encontrada em portas ou serviços que não estão em execução. A vulnerabilidade não é explorável.
AFFECT_RUNNING_SERVICE	0	A vulnerabilidade foi encontrada em portas ou serviços em execução. A vulnerabilidade é explorável.
AFFECT_RUNNING_SERVICE	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada.
AFFECT_EXPLOItable_CONFIG	1	A vulnerabilidade não é explorável devido à configuração do host.
AFFECT_EXPLOItable_CONFIG	0	A vulnerabilidade é explorável devido à configuração do host.
AFFECT_EXPLOItable_CONFIG	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada.

Definir parâmetros de filtro adicionais para Qualys importações

Personalize os parâmetros de filtragem das suas consultas programadas com Qualys Vulnerability Integration para ajudá-lo a refinar ainda mais os dados de vulnerabilidade importados com as integrações Qualys compatíveis.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para que você possa revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por IPs ou intervalos de IP específicos. Ou você deseja importar somente máquinas que estão no seu escopo, por exemplo, somente máquinas em sua rede corporativa que não sejam dispositivos externos.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros Qualys para ajudá-lo a importar os detalhes específicos da vulnerabilidade necessários.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com Qualys parâmetros em seu Now Platform. Você modifica ou adiciona esses valores ao registro do método HTTP no método REST para as integrações Qualys compatíveis do Qualys Vulnerability Integration.

Função necessária: sn_vul.vulnerability_admin

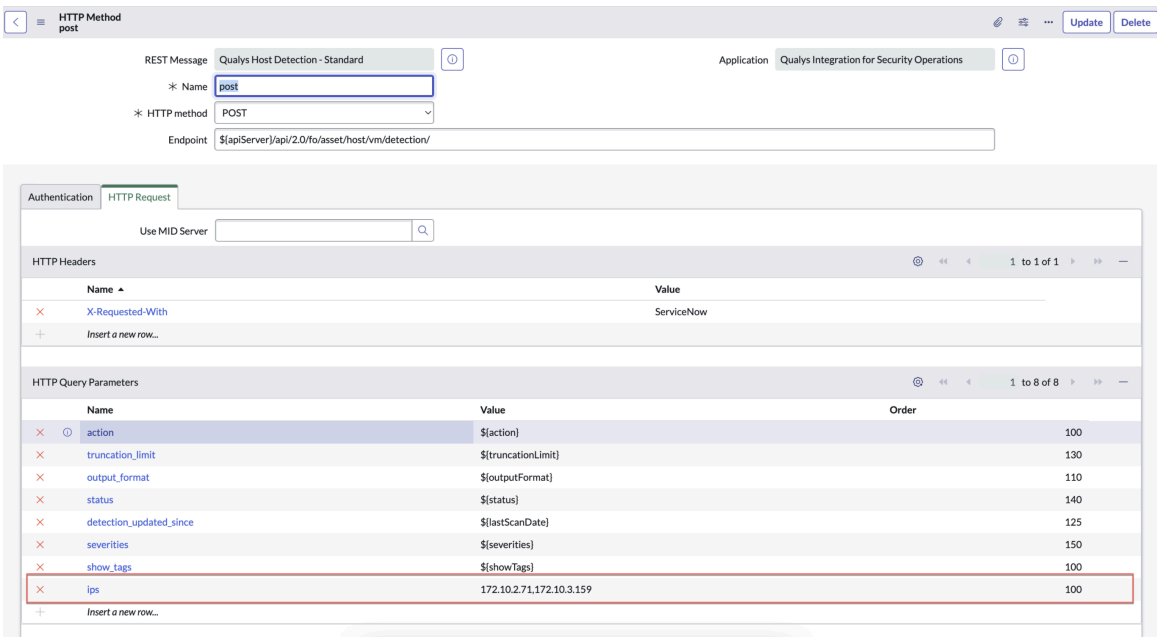
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Localize os parâmetros compatíveis com o produto Qualys no site do desenvolvedor que você deseja usar para a filtragem.
   Os parâmetros e valores inseridos no produto Qualys são compatíveis somente no nível da instância de integração em seu Now Platform. Todas as Qualys integrações oferecem suporte à filtragem usando parâmetros de consulta.
2. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
3. Na página da lista de integrações Qualys, clique no registro da integração que você deseja abrir.
4. Com a guia Qualys Detalhes de REST selecionada, localize e clique no ícone de informações (I) do método REST, seguido por **Abrir registro** para abrir o registro do método HTTP.
5. Selecione a guia **Solicitação HTTP**.
6. Em Parâmetros de consulta HTTP do corpo da solicitação, adicione os valores obtidos do site do desenvolvedor Qualys.

   Na imagem a seguir, como exemplo, o parâmetro que ingere somente determinados endereços/intervalos IP, *`ips={value}`* foi adicionado. Nesse caso, o **valor** é um ou mais IPs/intervalos especificados por você. Várias entradas são separadas por vírgulas, `172.10.2.71, 172.10.3.159`, e um intervalo é especificado com um hífen, `10.10.10.1-10.10.10.100`. Consulte o site do desenvolvedor Qualys para obter mais informações.



   Se você quiser inserir mais de um parâmetro, consulte a documentação Qualys para obter mais informações sobre como separar cada valor.

   Nota: Você deve estar ciente de seus requisitos de API. Pode ser necessário adicionar essas propriedades de API aos Parâmetros de consulta ou ao conteúdo do corpo.

   Alguns outros parâmetros que podem ser úteis no site do desenvolvedor Qualys :

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- *ag_ids* - IDs da lista do grupo de ativos a serem recuperados. Este parâmetro garante que somente máquinas no seu escopo sejam trazidas.
- *qids* - Este parâmetro limita os resultados a somente determinadas vulnerabilidades (QID na tabela Entrada de terceiros). Esta configuração evita que o sistema seja inundado com registros informativos.

7. Clique em **Atualizar**.

Resolvendo problemas de integração de vulnerabilidade da Qualys

Alguns problemas comumente encontrados, junto com as soluções alternativas, são discutidos.

Anexos não aparecem após a importação

Se os anexos não estiverem aparecendo conforme o esperado para as fontes de dados ou em um incidente de segurança após as importações de integração de terceiros, verifique as restrições de IP.

As restrições de acesso por IP podem impedir que os anexos sejam vistos, a menos que você esteja conectado a partir de um IP seguro. Como um novo anexo é adicionado a cada importação, isso pode resultar em duplicatas que você precisa remover.

Por exemplo, ao executar uma integração de importação de host de terceiros, se você não vir nenhum anexo em suas fontes de dados, verifique as restrições de IP e adicione usuários à lista segura antes da importação.

Modificar mapas de transformação

Mapas de transformação são fornecidos com configurações de base e geralmente são suficientes. Você pode modificar mapeamentos de transformação dependendo das necessidades da sua organização.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin + import_admin

Procedimento

1. Navegar até **Todos** > **Conjuntos para importação do sistema** > **Administração** > **Mapas de transformação** para exibir as mensagens de REST.
2. Filtre a lista resultante por aplicação e limite a lista à aplicação **Qualys Vulnerability Integration**.
3. Modifique os mapas de transformação de acordo com os requisitos do cliente.

   Para obter detalhes sobre os dados fornecidos pela API da Qualys, consulte a documentação da API da Qualys .

Verificar o tamanho da propriedade de anexo XML

Verifica se a propriedade de anexo XML é suficiente para arquivos grandes.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Propriedades do sistema** > **Importação/Exportação**.
2. Role para baixo até **Propriedades de importação** > **Formato XML** na parte inferior da página.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Se necessário, altere o valor para 250 e clique em **Salvar**.

Informações relacionadas

Propriedades do sistema disponíveis

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados da Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa gravidade que um cliente não está disposto a corrigir usando o processo de resposta a vulnerabilidades. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection – Standard/post**. Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método post com os seguintes valores:

- Nome: gravidades
- Valor: 3-5 (ou qualquer gravidade apropriada desejada)

Resolvendo falha na integração da base de conhecimento da Qualys

Resolva Qualys falha de integração da base de conhecimento reduzindo o tamanho do anexo de carga recebido de Qualys para o limite especificado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Certifique-se de que o tamanho do anexo de carga esteja dentro do limite especificado.
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   b. Selecione a guia **Parâmetros de instância de integração**.
   c. Selecione **max_delta_days** e modifique o valor padrão para 3.
2. Se a integração ainda falhar, execute as seguintes etapas:
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias**.
   b. Selecione **Base de conhecimento da Qualys**.
   c. Selecione a guia **Detalhes da integração**.
   d. No campo **Hora** de início, selecione a data atual para ignorar a execução da execução desse dia.
   e. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Selecione a guia **Parâmetros de instância de integração**.

g. Selecione **kb_backfill_full_import** e modifique o valor padrão para verdadeiro.

Resultados
A execução da integração de preenchimento da base de conhecimento da Qualys atualiza todas as entradas de terceiros (TPEs) no sistema. Enquanto a integração de detecção de host da Qualys cria uma entrada de espaço reservado, a integração de preenchimento da base de conhecimento da Qualys a atualiza.

Qualys Vulnerability Integration emissão de relatórios

A Qualys Cloud Platform visão geral é uma exibição executiva da atividade de vulnerabilidade. Ao fornecer tendências, relatórios e detalhamentos de dados específicos, um administrador ou analista pode identificar rapidamente as áreas de preocupação. Os gráficos são preenchidos com dados depois que os itens vulneráveis e os dados da base de conhecimento Qualys são recuperados.

Visualizações de dados nos espaços Resposta a vulnerabilidades

Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços, Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Versões anteriores de Resposta a vulnerabilidades

Os analistas de vulnerabilidade também podem usar os painéis padrão no ambiente clássico para monitorar dados de vulnerabilidade. Para obter mais informações, consulte Usando os painéis padrão Resposta a vulnerabilidades.

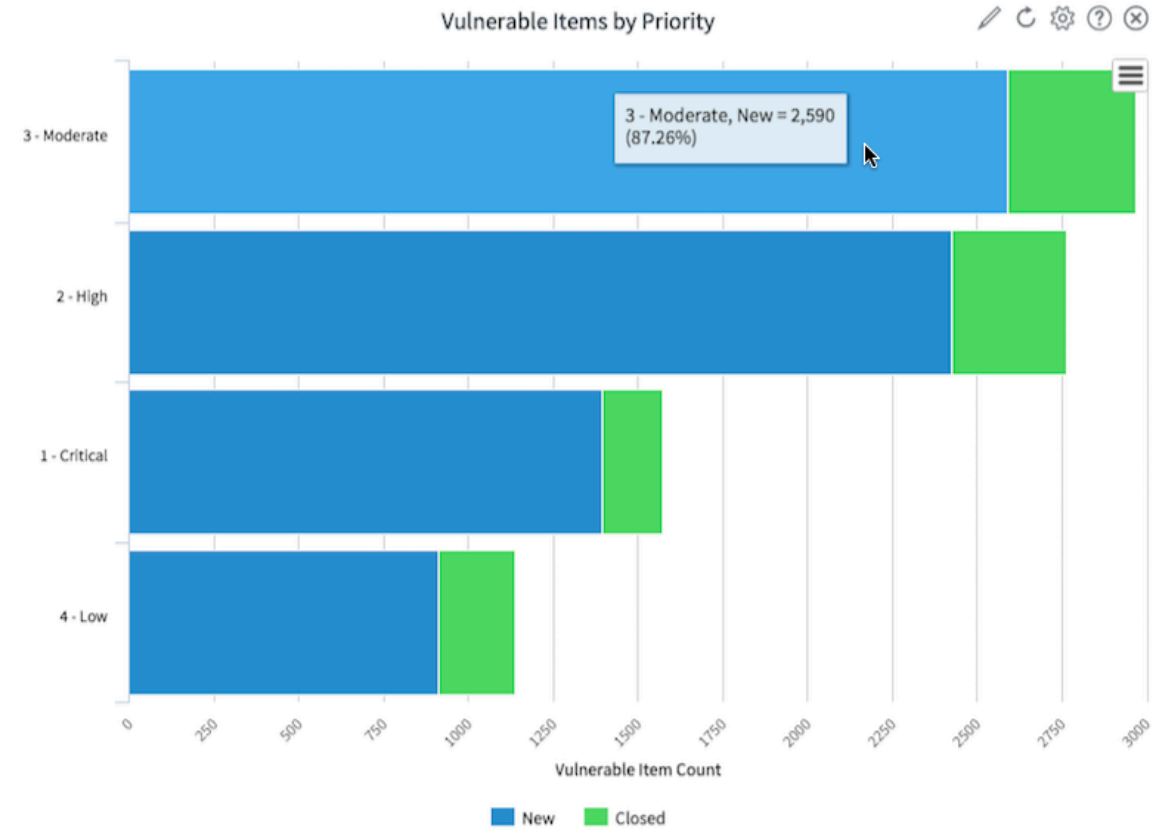
Nota: O uso da integração de vulnerabilidade Qualys Cloud Platform pressupõe que o ajuste, o teste e a implantação ocorreram em sua instância. Essas funções são áreas além do escopo da documentação do produto. Para obter assistência, entre em contato com Suporte e atendimento ao cliente.

Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gráfico de amostra Qualys Vulnerability Integration



Os relatórios a seguir estão disponíveis na página inicial Qualys Cloud Platform.

Qualys Vulnerability Integration Relatórios de visão geral

Nome	Visual	Descrição
ICs sincronizados com Qualys	Barra	Exibe o número de itens vulneráveis em aberto registrados para cada IC, do mais para o menos.
Itens vulneráveis do Qualys em aberto	Barra	Exibe o número de itens vulneráveis em aberto associados a vulnerabilidades (registros CVE), do maior para o menor.
Total de itens vulneráveis da Qualys	Barra	Exibe o número de itens vulneráveis ignorados programados para expirar em 7 dias.
Itens vulneráveis por prioridade	Tendência	Exibe o número de entradas de vulnerabilidade registradas a cada semana.
Prevalência de QID	Barra	Exibe o número de itens vulneráveis registrados para cada modelo, do mais para o menos.
Itens vulneráveis do Qualys em aberto	Lista	Exibe o número de itens vulneráveis registrados para cada fornecedor, do mais para o menos.

Qualys gráfico de status de execução de integração

O módulo Qualys Status de execução de integração é uma exibição gráfica do status de Qualys execuções de integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir o status das execuções de integração, navegue até **Integração de Vulnerabilidade da Qualys** > **Status da Execução da Integração**.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

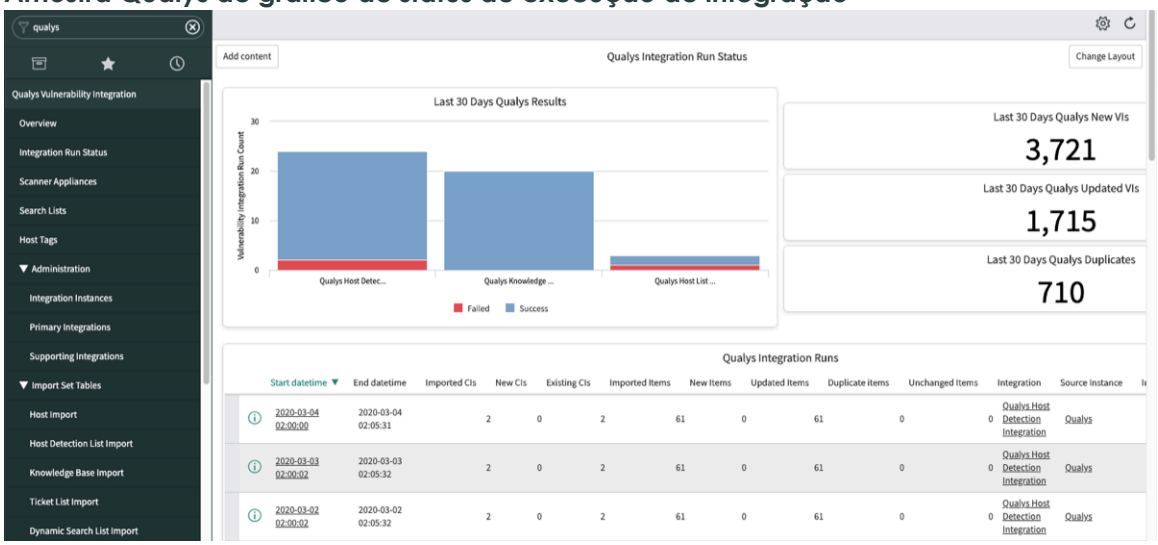
Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

O Qualys Status de execução de integração exibe o status de execução da integração de vulnerabilidades nos últimos 30 dias. A contagem de IVs atualizados da Qualys[qualys] indica a contagem de detecções exclusivas no mesmo ativo. O VI é atualizado com a nova detecção.

Nota: A contagem de execuções de integração de vulnerabilidade é exibida somente para as integrações, que estão definidas para o estado ativo. Navegar até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias** e defina o estado como ativo.

Amostra Qualys de gráfico de status de execução de integração



- Os valores na coluna Itens importados representam o número total de registros que são criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de registros que são criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que os registros são atualizados durante uma execução de integração. Este valor não é o número de registros exclusivos que são atualizados. Se, por exemplo, um registro for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
- A coluna Itens inalterados exibe registros encontrados durante a execução de integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campos relevantes foi alterado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A integração é executada sem resultados para todos os quatro dos seguintes valores: **Novos ICs**, **ICs existentes**, **Novos itens**e **Itens atualizados** são filtrados da lista de execuções de **integração da Qualys**.

Qualys relatórios de gráfico de status de execução de integração

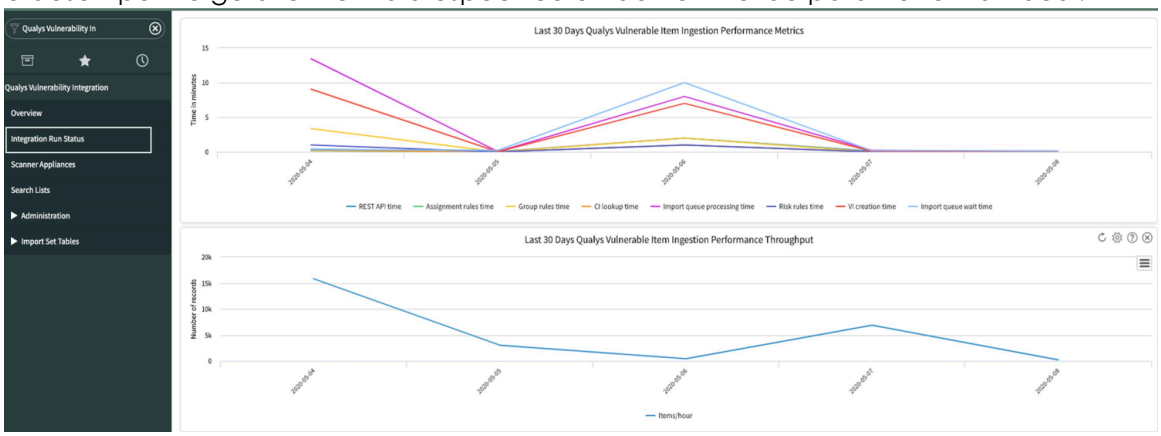
Nome	Descrição
Resultados dos últimos 30 dias Qualys	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Qualys Novos IVs	O número de novos registros importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys VIs atualizados	O número de registros atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys duplicados	O número de registros duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Qualys Execuções de integração	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções desta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na contagem de detecção ou descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem de data até" na instância, após a conclusão da execução da integração.
Últimos 30 dias Qualys Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparados nos últimos 30 dias.
Últimos 30 dias Qualys Taxa de transferência de desempenho de ingestão de item vulnerável	Taxa de transferência de ingestão de item vulnerável diária medida para a integração de detecção de host Qualys nos últimos 30 dias.

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois gráficos comparam as métricas de desempenho:

- Qualys Métricas de desempenho de ingestão de itens vulneráveis: compare as métricas diárias de desempenho para regras de atribuição, regras de grupo, regras de risco, tempo de espera na fila, tempo de processamento da fila e outras estatísticas de itens vulneráveis nos últimos 30 dias para identificar a causa de quaisquer desvios no desempenho. O desempenho é calculado com base no tempo necessário para cada atividade. Esses parâmetros são calculados e associados no nível de execução da integração. Cada parâmetro é codificado por cores para facilitar a identificação.
- Qualys Rendimento de desempenho de ingestão de itens vulneráveis: compare o rendimento de ingestão de itens vulneráveis diários para a integração Qualys de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

detecção de host. O rendimento é medido em itens por hora. Este relatório mostra o desempenho geral em um dia específico e não no nível de parâmetro individual.



Transformação de dados da Qualys

Os dados recuperados da Qualys são processados por meio de um conjunto de fontes de dados e transformações.

A maioria das transformações para Qualys Vulnerability Integration é realizada usando scripts de transformação. Esses scripts são para uso interno. A exclusão não é recomendada. As modificações exigem codificação ou conhecimento avançado ServiceNow ou Qualys Vulnerability Integration. Os mapas restantes são listados nesta seção e usam mapas de campo.

Nota: Durante a instalação, mapas de severidade normalizados, que transformam níveis de severidade Qualys Cloud Platform importados em níveis de severidade ServiceNow padrão, são instalados no módulo Mapeamento de Severidade Normalizada Resposta a vulnerabilidades. Para obter mais informações, consulte Criar um Resposta a vulnerabilidades mapa de severidade.

Importação de lista de pesquisa dinâmica

O mapa de transformação da lista de pesquisa dinâmica da Qualys é usado para transformar e importar listas de pesquisa dinâmica da Qualys. As mudanças nesta transformação alteram a forma como as listas de pesquisa dinâmica são processadas e inseridas no sistema.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas de conjunto para importação** > **Importação da lista de pesquisa dinâmica**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos do mapa de transformação da lista de pesquisa dinâmica da Qualys

Campo de origem	Campo de destino	Descrição
u_id	ID	Usado como o identificador da lista de pesquisa dinâmica da Qualys.
[Script]	lista_tipo	O tipo de lista de pesquisa. Dinâmico é o padrão para a transformação da Lista de Pesquisa Dinâmica.
título_u	título	O nome em Qualys para esta lista de pesquisa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação da lista de pesquisa dinâmica da Qualys

Quando o script é executado	Finalidade do script
onAfter (depois que um conjunto de importação concluiu a transformação).	Cria os relacionamentos entre listas de pesquisa e suas vulnerabilidades relacionadas. Para uso interno. Não é recomendável modificar ou excluir.

Importação de lista de pesquisa estática

O mapa de transformação da lista de pesquisa estática da Qualys é usado para transformar e importar listas de pesquisa estática da Qualys. As mudanças nesta transformação alteram a forma como as listas de pesquisa estática são processadas e inseridas no sistema.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas de conjunto para importação** > **Importação de lista de pesquisa estática**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos do mapa de transformação da lista de pesquisa estática da Qualys

Campo de origem	Campo de destino	Descrição
u_id	ID	Usado como o identificador da lista de pesquisa estática da Qualys.
título_u	título	O nome em Qualys para esta lista de pesquisa.
[Script]	lista_tipo	O tipo de lista de pesquisa. Estático é o padrão para a transformação da Lista de Pesquisa Estática.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação da lista de pesquisa estática da Qualys

Quando o script é executado	Finalidade do script
onAfter (depois que um conjunto de importação concluiu a transformação).	Cria os relacionamentos entre listas de pesquisa e suas vulnerabilidades relacionadas. Para uso interno. Não é recomendável modificar ou excluir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de grupo de ativos

O mapa de transformação de dispositivo do grupo de ativos da Qualys é usado para transformar dados do grupo de ativos da Qualys para criar registros do dispositivo scanner. As mudanças nesta transformação alteram a forma como os dispositivos scanner são criados e modificados.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas de conjunto para importação** > **Importação de grupo de ativos**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos do mapa de transformação do grupo de ativos da Qualys

Campo de origem	Campo de destino	Descrição
u_id	ID	Usado como identificador para o grupo de ativos da Qualys.
[Script]	manual	Valor em script para determinar como o registro de destino foi criado. Quando criado por meio de transformações, este campo é sempre falso.
[Script]	ips	Os endereços IP associados ao grupo de ativos que está sendo transformado.
u_default_appliance_id	id_do_dispositivo	O identificador do dispositivo Qualys para o dispositivo padrão neste grupo de ativos.
título_u	asset_group_name	O nome do grupo de ativos da Qualys.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação do grupo de ativos da Qualys

Quando o script é executado	Finalidade do script
onBefore (antes de um conjunto para importação concluir a transformação).	O script que restringe as importações do grupo de ativos somente para grupos de ativos com um dispositivo padrão e um conjunto de endereços IP mapeados. Para uso interno. Não é recomendável modificar ou excluir.

Importação de dispositivo

O mapa de transformação do dispositivo Qualys é usado para transformar dados do dispositivo Qualys em registros do dispositivo. Isso é usado para atualizar os registros do dispositivo que seriam criados inicialmente a partir da importação de grupo de ativos. As mudanças nesta transformação alteram a forma como os registros do dispositivo são atualizados com os detalhes do dispositivo.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas de conjunto para importação** > **Importação de dispositivo**.

A tabela mostra os campos que estão sendo transformados no momento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação do dispositivo Qualys

Campo de origem	Campo de destino	Descrição
u_name	Appliance_name	O nome do dispositivo scanner da Qualys.
u_status	status_do_dispositivo	O último status relatado do dispositivo scanner da Qualys.
u_id	id_do_dispositivo	O identificador do dispositivo Qualys.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação do dispositivo Qualys

Quando o script é executado	Finalidade do script
onBefore (antes de um conjunto para importação concluir a transformação).	Usado para atualizar nomes e status do dispositivo para o ID fornecido. Para uso interno. Não é recomendável modificar ou excluir.

Mensagens REST da Qualys

As mensagens REST da Qualys são usadas para fazer chamadas para a API da Qualys.

A partir da versão 12.9.2 de Qualys, você tem a opção de escolher entre Autenticação básica ou OAuth. O método de autenticação em nuvem da Qualys de parâmetro de instância é pré-configurado para Autenticação básica. Se você preferir usar o OAuth, deverá modificar o parâmetro de instância de integração e configurar a mensagem REST diretamente para o OAuth.

Mensagem REST de detecção de host da Qualys

A mensagem REST de detecção de host da Qualys faz a chamada inicial para a API de detecção de lista de hosts para a integração de detecção de host da Qualys.

Parâmetros de mensagem REST de detecção de host da Qualys

Nome do Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. As mudanças não são necessárias.
output_format	XML	Define o formato do relatório retornado pela Qualys. Os vários scripts e transformações assumem XML, portanto, não são recomendadas mudanças no valor.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de detecção de host da Qualys

Nome do Parâmetro	Valor	Descrição
detecção_processada_após	${lastScanDate}	Mostra somente detecções cujo status de detecção mudou após uma determinada data e hora. Para detecções que nunca mudaram, a data é aplicada à data da última detecção.
truncation_limit	500	O número de hosts dos quais os dados serão recuperados, de acordo com a solicitação. Este parâmetro é usado para fins de paginação. O valor padrão é 500, mas valores maiores ou menores podem ser usados. Não defina para menos de 100, pois isso aumenta significativamente a carga do sistema. Valores menores exigem mais chamadas para a API da Qualys e valores maiores resultam em conjuntos de resultados maiores para processar e possíveis tempos limites de recuperação/processamento de dados.
status	Novo, Corrigido, Ativo, Reaberto	Status de detecção a serem recuperados da Qualys. O padrão é recuperar todos os status. Para extrações de dados grandes (geralmente a extração inicial de dados), pode ser útil excluir os status Fixo desta lista. É importante incluir o status Corrigido ao atualizar vulnerabilidades que já estão no sistema.

Mensagem REST de paginação de detecção de host da Qualys

A mensagem REST de paginação de detecção de host lida com solicitações de paginação para a API de detecção de host.

Quando a detecção de host primário é executada, se a API da Qualys fornece um URL para buscar a próxima página de dados, esta mensagem REST recupera esses dados adicionais. Esses dados são usados pelo Manipulador de Paginação de Detecção de Host.

REST de paginação de detecção de host é uma mensagem REST especializada e não deve ser modificada.

Mensagem REST da base de conhecimento da Qualys (preenchimento)

A mensagem REST da Base de conhecimento da Qualys (preenchimento) recupera os dados da base de conhecimento da Qualys com base no carimbo de data/hora da última modificação dos dados de vulnerabilidade para a integração da Base de conhecimento da Qualys.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações da base de conhecimento.

A tabela a seguir mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (preenchimento)

Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação que está sendo solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
detalhes	Todos	Indica o nível de detalhe mostrado para vulnerabilidades recuperadas. É seguro modificar conforme necessário.
IDs	${qids}	Especifica quais QIDs serão recuperados da Qualys. Referenciado no código. Modificações não são recomendadas.

Mensagem REST da base de conhecimento da Qualys (baseada em data)

A mensagem REST da Base de conhecimento da Qualys (baseada em data) é usada para recuperar dados da base de conhecimento da Qualys com base no carimbo de data/hora da última modificação dos dados da vulnerabilidade. Esta mensagem é usada pela integração da Base de conhecimento da Qualys.

As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações da base de conhecimento.

A tabela a seguir mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (baseada em data)

Campo de origem	Campo de destino	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
detalhes	Todos	Indica o nível de detalhe mostrado para vulnerabilidades recuperadas. É seguro modificar conforme necessário.
last_modified_after	${dateStart}	Indica quando começar a recuperar dados históricos. Usado pelo código para determinar a hora de início e para ajudar na paginação. Modificações ou remoção não são recomendadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (baseada em data)

Campo de origem	Campo de destino	Descrição
last_modifiedbefore	${dateEnd}	Indica quando terminar a recuperação de dados históricos. Usado pelo código para determinar a hora de término e para ajudar na paginação. Modificações ou remoção não são recomendadas.

Mensagem de REST de tíquetes da Qualys

A mensagem REST de tíquetes da Qualys recupera informações do tíquete da Qualys para a integração de tíquete da Qualys. As mudanças no registro do método de mensagem REST afetam as solicitações feitas à Qualys para recuperar informações do tíquete.

A tabela mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST de tíquetes da Qualys

Nome do Parâmetro	Valor	Descrição
modificado_desde_data/hora	${lastRunDatetime}	Indica a data da última execução da integração e a data após a qual os dados serão extraídos. Usado pelo código. Mudanças não são recomendadas.
desde_número_do_ticket	${lastTicketNumber}	Indica qual tíquete foi recuperado pela última vez da Qualys. Usado para paginação. Mudanças não são recomendadas.
mostrar_vuln_detalhes	1	Indica se os detalhes da vulnerabilidade foram recuperados.

Noções básicas sobre Integração com Rapid7 Vulnerability

O ServiceNow® Integração com Rapid7 Vulnerability usa dados importados do data warehouse [Rapid7 ou dos produtos Rapid7 InsightVM para ajudar você a determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas.

Rapid7 Nexpose sensores coletam dados e os enviam automaticamente para os produtos Rapid7 de data warehouse (no local) ou Rapid7 InsightVM (baseados na nuvem), que analisam e correlacionam continuamente as informações. Ele se integra facilmente com ServiceNow® Resposta a vulnerabilidades para mapear vulnerabilidades para ICs e serviços. O Integração com Rapid7 Vulnerability aprimora os dados de vulnerabilidade em sua instância.

Rapid7 integrações são pontos de entrada que interagem com o data warehouse [Rapid7 ou produtos Rapid7 InsightVM, invocados como trabalhos agendados. Os trabalhos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Os trabalhos agendados são executados automaticamente e na ordem especificada. Você também pode executar trabalhos agendados individuais manualmente.

Nota:

Se você usar o data warehouse [Rapid7 e Rapid7 InsightVM como origens para seus dados, corre o risco de ter registros de vulnerabilidade duplicados.

Nota: Ao migrar do tipo de integração de **data warehouse** para o tipo **InsightVM**, você pode desduplicar os registros de data warehouse existentes. Para obter mais informações, consulte Desduplicar Integração com Rapid7 Vulnerability registros de data warehouse.

Se você tiver várias implantações da integração de vulnerabilidade Rapid7 InsightVM, poderá adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com o seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados obtidos de cada implantação são identificados e estão disponíveis em uma única instância de Resposta a vulnerabilidades.

Nota: Você não pode excluir a integração de vulnerabilidade original, mas pode desativá-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Versão de lançamento para Xanadu	**Notas de versão**
Integração com Rapid7 Vulnerability v13.6, 13.7	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Rapid7 As tarefas de integração de vulnerabilidade envolvem as funções a seguir.

- sn_vul_r7.admin: pode ler, gravar e excluir registros.
- sn_vul_r7.user: pode ler e gravar registros.
- sn_vul_r7.read: pode ler registros.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Integração com Rapid7 Vulnerability

Para exibir o Integração com Rapid7 Vulnerability, navegue até **Rapid7** > **Administração** > **Integrações**.

As seguintes integrações estão incluídas no sistema de base.

Rapid7 integrações de data warehouse

Integração	Descrição
Integração com Rapid7 Vulnerability	Recupera dados de vulnerabilidade de Rapid7 Nexpose e os processa em sua instância.
Rapid7 Integração da lista de ativos	Recupera dados de verificação uma vez por semana do Rapid7 Nexpose data warehouse e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando a data **da última verificação**. Exiba a hora da **última verificação** na lista de itens descobertos em Resposta a vulnerabilidades.
Rapid7 Integração de categoria	Recupera informações de categoria de Rapid7 Nexpose. As categorias fornecem classificação de alto nível para vulnerabilidades.
Rapid7 Explorar integração	Recupera informações de exploração de Rapid7 Nexpose.
Rapid7 Integração do kit de malware	Recupera informações do kit de malware de Rapid7 Nexpose.
Rapid7 Integração de referência	Recupera referências a documentos de autoridade externa, como CVEs ou referências de vulnerabilidade específicas do fornecedor.
Rapid7 Integração de solução	Recupera dados de solução de Rapid7 Nexpose, que fornece soluções recomendadas para vulnerabilidades específicas.
Rapid7 Integração da solução de substituição	Recupera informações sobre quais soluções foram substituídas por outras soluções.
Rapid7 Integração da solução de pré-requisito	Recupera informações sobre as soluções que são pré-requisitos para outras soluções. Quando esta integração é executada, ela busca o mapeamento de soluções e soluções de pré-requisito do data warehouse Rapid7. **Nota:** Esta integração funciona somente se o plug-in Solução de gestão de vulnerabilidade estiver ativado.
Rapid7 Integração do mapa de solução de vulnerabilidade	Recupera o mapeamento para associar soluções a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rapid7 integrações de data warehouse

Integração	Descrição
Rapid7 Integração de item vulnerável	Recupera dados de item vulnerável de Rapid7 Nexpose e os processa em sua instância. As saídas desta integração são itens vulneráveis.
Rapid7 Integração de resolução de item vulnerável	Recupera informações sobre quais itens vulneráveis estão marcados como encerrados em Rapid7 Nexpose e fecha os itens vulneráveis correspondentes em Resposta a vulnerabilidades.
Rapid7 Integração de site	Recupera dados do site de Rapid7 Nexpose. Um site é uma coleção de ativos que são direcionados para uma verificação.
Rapid7 Integração da lista de ativos	Recupera marcadores de host e dados de verificação uma vez por semana do data warehouse Rapid7 e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando a data **da última verificação**. Exibir a hora da **última verificação** na lista de itens descobertos em Resposta a vulnerabilidades
Rapid7 Integração Abrangente de Item Vulnerável	Importa todas as detecções do Rapid7 para todos os itens de configuração verificados desde a última execução de integração bem-sucedida. Com base nos dados importados mais atuais, os itens vulneráveis encontrados não recentemente durante as verificações são transicionados automaticamente para "Fechado" quando o módulo de fechamento automático de itens vulneráveis obsoletos está habilitado.

Integrações do Rapid7 InsightVM

Integração	Descrição
Rapid7 Integração de item vulnerável — API	Recupera dados de itens vulneráveis do Rapid7 InsightVM e os processa em sua instância.
Integração com Rapid7 Vulnerability — API	Recupera dados de referência, categoria, exploração, kit de malware e vulnerabilidade do Rapid7 InsightVM e os processa em sua instância.
Rapid7 Integração da lista de ativos - API	Recupera marcadores de host e dados de verificação uma vez por semana de Rapid7 InsightVM e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando a data **da última verificação**. Exiba a hora da **última verificação** na lista de itens descobertos em Resposta a vulnerabilidades.
Rapid7 Integração abrangente de item	Importa todas as detecções do Rapid7 para todos os itens de configuração verificados desde a última execução de integração bem-sucedida. Com base nos dados importados mais atuais, os itens vulneráveis encontrados não recentemente durante as verificações são transicionados automaticamente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Rapid7 InsightVM

Integração	Descrição
vulnerável - API	para "Fechado" quando o módulo de fechamento automático de itens vulneráveis obsoletos está habilitado.
Rapid7 Integração de site	Recupera dados do site do produto Rapid7 InsightVM. Esta integração está definida para ser executada semanalmente às 00:00:00.

Durante a importação, os registros CVE que ainda não estão presentes são criados como registros do NVD e referenciados em entradas de terceiros para Rapid7 por padrão. A integração de modelo para Rapid7 não pode ser excluída. Em vez disso, desabilite-o.

O Conector do Service Graph para Rapid7

A partir da versão 2.0, o Conector do Service Graph para Rapid7 está disponível no ServiceNow® Store. Para obter mais informações, consulte Conector do Service Graph para Rapid7 (2.0.0) .

Regras de Pesquisa de IC

As Regras de pesquisa de IC determinam como preencher o campo **Item de configuração** em um registro de item vulnerável.

Para obter mais informações sobre como as regras de pesquisa de IC funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.

Para criar ou editar regras de pesquisa, consulte Criar uma regra de pesquisa de IC de resposta a vulnerabilidades.

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Itens Descobertos

Este módulo lista os itens de configuração detectados durante a importação das Rapid7 Integrações de itens vulneráveis (data warehouse ou API do InsightVM) e da Rapid7 Integração da lista de ativos - API. A Rapid7 Asset List Integration - API importa todos os ativos do Rapid7 verificados quanto a vulnerabilidades desde a última execução da integração. A Integração da lista de ativos do data warehouse Rapid7 está incluída.

Nota: O filtro padrão para esta lista está definido como **Incompatível**. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Consulte Itens Descobertos em Resposta a vulnerabilidades para obter mais informações sobre o módulo Itens descobertos.

Marcadores de host

Os marcadores de host são importados como parte da Rapid7 Asset List Integration - Integração de API para Rapid7 InsightVM. Eles são usados principalmente para filtragem em Resposta a vulnerabilidades Regras de atribuição e tarefa de correção em Rapid7 InsightVM. Eles são exibidos no formulário Item descoberto.

Marcadores de host

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A integração Rapid7 de lista de ativos - integração de API deve ser executada antes da criação de Regras de atribuição ou de tarefa de correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Se um marcador **San Diego** for criado, um marcador **SAN DIEGO** não poderá ser armazenado na tabela de marcadores do host. “San Diego” e “SAN DIEGO” são considerados o mesmo marcador de host. O marcador que foi importado primeiro vence.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags**. Esta propriedade é definida como verdadeira por padrão. A desativação dos marcadores os desativa em todas as instâncias.

Sites

Um site é uma coleção de ativos direcionados para uma verificação. Um site consiste em ativos de destino, um modelo de verificação, um ou mais mecanismos de verificação e outras configurações relacionadas à verificação, como cronogramas ou alertas. Os sites são gerenciados por Rapid7 aplicações.

Integração com Rapid7 Vulnerability A filtragem de site durante a configuração permite categorizar e solicitar ativos por site durante a importação. Consulte Filtrando por Rapid7 sites para obter mais informações sobre como filtrar importações.

As integrações de data warehouse Rapid7 InsightVMRapid7 e Sites [] importam sites como um trabalho agendado semanalmente.

Para exibir os sites importados em uma lista, navegue até **Rapid7** > **Sites**.

Reabrir itens vulneráveis resolvidos não encerrados por verificações

Itens vulneráveis definidos como "Resolvidos" em sua instância Now Platform, mas não transicionados para "Fechados/Corrigidos" pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Para Rapid7 detecções, uma opção agora está disponível na página de configuração do Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como "Resolvidos", mas não transicionados para "Fechados/Corrigidos" pelas verificações subsequentes, retornam para "Aberto" após o número de dias inserido.

Criar ICs usando o Mecanismo de Identificação e Reconciliação (IRE)

Você pode usar o Mecanismo de Identificação e Reconciliação para criar novos ICs quando um IC existente não puder ser correspondido com um host importado de um scanner de terceiros. Habilite o plug-in Modelos de classe de IC do CMDB para criar ICs usando as novas classes, caso contrário, ICs incompatíveis serão criados nas classes de IC incompatível. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos em nuvem incompatíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar novamente itens vulneráveis

Inicie novas verificações na plataforma Rapid7 para verificar se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Consulte Iniciar nova verificação para a integração de vulnerabilidade Rapid7.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Rapid7 gestão de soluções

Se você ativou o plug-in Solução de gestão de vulnerabilidade, as soluções Rapid7Rapid7 para o data warehouse [] e Rapid7 InsightVM] serão preenchidas na tabela Soluções de vulnerabilidade [sn_vul_solution]. No entanto, se você não ativou o plug-in Solução de gestão de vulnerabilidade, o Integração com Rapid7 Vulnerability funcionará como está e importará as soluções na tabela [sn_vul_r7_solution] personalizada. Para obter mais informações, consulte Rapid7 gestão de soluções.

Preparando para o Integração com Rapid7 Vulnerability

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Integração com Rapid7 Vulnerability pressupõe que você esteja familiarizado e execute Rapid7 data warehouse ou Rapid7 InsightVM verificações de produto em seu ambiente.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Os scanners Rapid7 são desativados por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Antes de baixar a aplicação Integração com Rapid7 Vulnerability do ServiceNow® Store e instalá-la em sua instância, revise as seguintes informações sobre os tipos de integração e configure as informações:

Existem dois tipos de integrações incluídas com o Integração com Rapid7 Vulnerability que estão disponíveis no ServiceNow® Store:

- Rapid7 InsightVM
- Rapid7 data warehouse

O Rapid7 tipo de data warehouse:

- Requer a URL do servidor de data warehouse Rapid7 e as credenciais de autenticação
- Requer um MID Server
- Usa um driver PostgresSQL para executar consultas no data warehouse
- Não é compatível com várias instâncias

O tipo de integração Rapid7 InsightVM :

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- É baseado em nuvem e usa uma REST API. Esta integração requer uma chave de API de dentro da sua conta do Rapid7 Insight.
- Oferece suporte a várias instâncias.

Consulte Configurar para a integração de data warehouse Rapid7 (data warehouse) e Configurar para a integração Rapid7 InsightVM para obter mais informações sobre os requisitos de configuração para esses tipos de integração.

Configurar para a integração de data warehouse Rapid7

A integração Rapid7 de data warehouse é um dos tipos de integração incluídos com o Integração com Rapid7 Vulnerability Integração com Rapid7 Vulnerability.

Antes de Iniciar

Antes de executar a integração de data warehouse Rapid7, conclua as seguintes tarefas de configuração:

- Obtenha o Rapid7 complemento de data warehouse. Consulte o Rapid7 site e a documentação para adquirir e instalar este complemento.
- Obtenha o driver PostgresSQL mais atual. Vá para https://jdbc.postgresql.org/ e baixe o driver mais recente.
- Um MID Server para executar consultas no data warehouse. Consulte MID Server para obter mais informações sobre como configurar um MID Server.

  Anote o nome do data warehouse. O tipo de integração de data warehouse Rapid7 só oferece suporte a MID Servers autônomos. MID Servers em cluster não são compatíveis.

- Obtenha a URL do servidor de data warehouse Rapid7 e as credenciais de autenticação e deixe-as acessíveis.

Função necessária: o administrador do sistema [admin] baixa e instala o app. O sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Faça login na instância Now Platform em que você deseja instalar a aplicação Integração com Rapid7 Vulnerability.
2. Instale o arquivo JAR do PostgreSQL que você baixou nas tarefas de configuração listadas anteriormente.

   a. Em sua instância Now Platform, navegue até **Todos** > **MID Server** > **Arquivos JAR**.

   b. Clique em **Nova**.

   c. Insira o nome do driver PostgresSQL que você baixou anteriormente.

      Opcionalmente, insira as informações de **Versão**, **Origem**e **Descrição**. Deixe a caixa de seleção **Ativo** marcada.

   d. Anexe o arquivo JAR baixado usando o ícone de clipe de de papel no cabeçalho.

   e. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você concluiu a configuração da integração de data warehouse Rapid7. Se você não revisou os requisitos para a integração Rapid7 InsightVM, antes de instalar o Integração com Rapid7 Vulnerability, consulte Configurar para a integração Rapid7 InsightVM e Preparando para o Integração com Rapid7 Vulnerability.

Para obter as etapas para obter direitos, baixar e instalar o Integração com Rapid7 Vulnerability, consulte Instalar o Integração com Rapid7 Vulnerability.

Configurar para a integração Rapid7 InsightVM

A integração Rapid7 InsightVM é um dos tipos de integração incluídos com o Integração com Rapid7 Vulnerability Integração com Rapid7 Vulnerability.

Antes de Iniciar

Antes de executar a integração Rapid7 InsightVM, conclua as tarefas de configuração a seguir.

Função necessária: o administrador do sistema [admin] baixa e instala o app. O sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Para o tipo de integração Rapid7 InsightVM, tenha sua região e chave de API prontas. Entre em contato com Rapid7 para obter a região e a chave de API apropriadas. Você concluiu a configuração da integração Rapid7 InsightVM. Se você não revisou os requisitos para a integração de data warehouse Rapid7, antes de instalar o Integração com Rapid7 Vulnerability, consulte Configurar para a integração de data warehouse Rapid7 e Preparando para o Integração com Rapid7 Vulnerability.
2. Para obter as etapas para obter direitos, baixar e instalar o Integração com Rapid7 Vulnerability, consulte Instalar o Integração com Rapid7 Vulnerability.

Instalar o Integração com Rapid7 Vulnerability

Depois de concluir as etapas de configuração da integração para que ela se integre corretamente com Resposta a vulnerabilidades, obtenha direitos, baixe e instale a aplicação em sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: administrador para download e instalação, sn_vuln.admin supervisiona a configuração e verifica os resultados esperados.

1. Consulte Preparando para o Integração com Rapid7 Vulnerability, Configurar para a integração de data warehouse Rapid7 e Configurar para a integração Rapid7 InsightVM para obter mais informações sobre os tipos de integração e requisitos de configuração para o Integração com Rapid7 Vulnerability.
2. Conclua a check-list de configuração a seguir antes de baixar e instalar. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.
3. Depois que a aplicação for ativada, siga as etapas listadas abaixo para configurar o Integração com Rapid7 Vulnerability.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem as funções Now Platform necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados. Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades. • O administrador do sistema [admin] instala o app. Se ainda não estiver atribuído, o administrador atribuirá a função de Administrador de vulnerabilidade [sn_vul.vulnerability_admin ou sn_vul.admin]. • O administrador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados. A função de administrador Rapid7 é herdada quando você recebe uma função administrativa na aplicação Resposta a vulnerabilidades (VR).
Valide o dimensionamento da instância com base no número de itens vulneráveis que você espera importar.	Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.
Configurar filtragem	Use a filtragem para limitar o número de itens para importação inicial e fasear

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	sua implantação ajustando os filtros nas importações subsequentes.
Desabilitar calculadoras de vulnerabilidade	Se você não usar calculadoras de vulnerabilidade, Desabilitar a calculadora de vulnerabilidade padrão se não for usada, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.
Manter valor padrão para executar como usuário	Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.
Como usar marcadores de host	Se você planeja usar marcadores de host em Resposta a vulnerabilidades Regras de atribuição ou de tarefa de correção, execute a integração da lista de ativos do Rapid7 antes de criar regras.
Desduplicar registros de dados existentes	Ao migrar do tipo de integração de **data warehouse** para o tipo **InsightVM**, você pode desduplicar os registros de data warehouse existentes. Para obter mais informações, consulte Desduplicar Integração com Rapid7 Vulnerability registros de data warehouse.

Procedimento

1. Faça login na instância em que você deseja instalar a aplicação Integração com Rapid7 Vulnerability.
2. Navegue até ServiceNow Store e faça login.
3. Em ServiceNow Store, pesquise a aplicação Integração com Rapid7 Vulnerability.

   Nota: No ServiceNow Store, a aplicação é chamada de Rapid7 Integration for Security Operations. Esta aplicação requer uma assinatura.

4. Clique no bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira o **Nome** e **o motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Em sua instância Now Platform, navegue até **Aplicações do sistema** > **Todas as aplicações** > **Todos**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Na caixa de diálogo Instalar, seu status de dependência é exibido. Se você precisar de uma aplicação de dependência, a aplicação necessária será exibida. Siga os avisos na caixa de diálogo para instalar a aplicação Integração com Rapid7 Vulnerability em sua instância.

    Nota: O administrador de vulnerabilidades agora pode concluir a configuração da aplicação. Consulte Configure o Integração com Rapid7 Vulnerability.

Configure o Integração com Rapid7 Vulnerability

Configure o Integração com Rapid7 Vulnerability depois que a aplicação for instalada e ativada em seu Now Platform®.

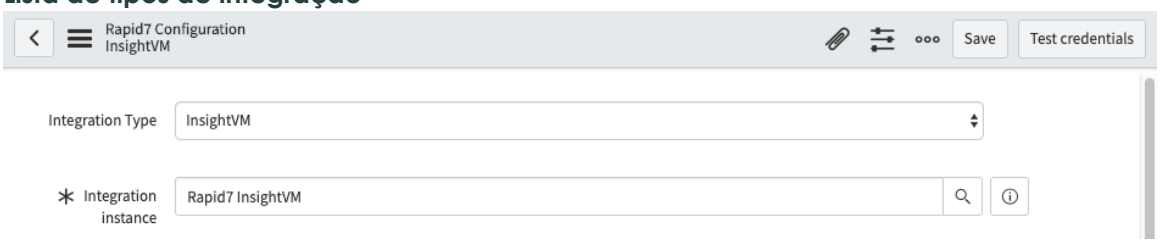
Antes de Iniciar

Função necessária: o administrador [admin] baixa e instala o app. O sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Depois que a aplicação for ativada (instalada), navegue até **Integração com Rapid7 Vulnerability** > **Administração** > **Configuração**.
2. Selecione um tipo de integração na lista.

Lista de tipos de integração



3. Selecione uma instância de integração.
   A instância de integração padrão Rapid7 InsightVM é selecionada por padrão. Se esse for o tipo de integração desejado, siga estas etapas. Se você quiser configurar o tipo de integração de data warehouse Rapid7, prossiga para a etapa 4.

   a. Com a guia **Configuração de integração** selecionada no formulário exibido, preencha os campos:

Guia Configuração de integração para o tipo de integração do InsightVM

Campo	Descrição
Região do InsightVM	A URL do servidor que você adquiriu do site Rapid7.
Chave de API	A chave de API que você adquiriu da sua conta do Rapid7 Insight.
Status de Validação	Somente leitura: status do processo de validação de credenciais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Verifique a configuração bem-sucedida clicando em **Testar credenciais**.
Se uma mensagem de erro for exibida durante a configuração, insira novamente os dados.

c. Depois de um teste bem-sucedido, clique em **Salvar**.

d. Clique na guia **Importar configuração**.

No formulário exibido, preencha os campos.

Guia Importar configuração do InsightVM

Campo	Descrição
Pontuação mín. do CVSS	Pontuação mínima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Pontuação máxima de CVSS	Pontuação máxima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Filtro do site	Limita os dados aos Rapid7 InsightVM sites escolhidos na lista Sites. Consulte Filtrando por Rapid7 sites. Você pode escolher mais de um site. O padrão (vazio) traz todos os sites. Para preencher previamente a lista de locais, execute a API Rapid7 Site Integration - antes de definir este campo. Para obter informações sobre como usar a filtragem de site, consulte Filtrando por Rapid7 sites.
Criar entrada de CVE automaticamente	A propriedade do sistema para criar uma entrada CVE está ativa (verdadeira) por padrão. Os espaços reservados do CVE serão criados automaticamente com a ingestão de conhecimento do Rapid7 se o ID do CVE não existir. Se você quiser que este recurso fique inativo, desative a propriedade [sn_vul_r7.create_cve_for_vulnerability] na lista Propriedades do sistema.
Reabrir resolvido por idade	Quando selecionados, os itens vulneráveis são reabertos automaticamente quando o número de dias em que eles foram resolvidos, mas não encerrados, corresponde ao valor exibido no campo **Reabrir resolvido após**.

e. Clique em **Salvar**.

Para várias implantações do tipo de integração Rapid7 InsightVM :

f. No campo **Instância de integração**, abra o lista de pesquisa e selecione uma instância de integração existente ou clique em **Novo** no menu pop-up.

g. Em **Novo**, insira um **Nome** para a instância de integração e clique em **Enviar**.
O tipo de integração aparece no formulário de configuração Rapid7.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode excluir qualquer instância de integração, exceto a padrão. A exclusão de uma instância exclui o seguinte (exceto IVs):

- Integrações
- Parâmetros de instância
- Execuções de Integração
- Processos de integração
- A coluna de instância no VI está marcada como vazia

h. Verifique a configuração bem-sucedida clicando em **Testar credenciais**.

i. Depois de um teste bem-sucedido, clique em **Salvar**.

4. No campo Tipo de integração, expanda a lista e clique em **Depósito de dados**.

a. Selecione a guia **Configuração de integração**.

No formulário exibido, preencha os campos.

Guia Configuração de integração para o tipo de integração de data warehouse

Campo	Descrição
Nome da credencial JDBC	Nome das credenciais do data warehouse.
Nome de usuário	Nome de usuário do data warehouse do Rapid7.
Senha	Senha do data warehouse da Rapid7.
Status de Validação	Somente leitura: status do processo de validação de credenciais.
Detalhe da Validação	Somente leitura: somente data warehouse. Mostra informações adicionais sobre a verificação de validação depois que você clica em Testar credenciais pelo menos uma vez. Isso pode ser útil para depurar sua configuração (por exemplo, validar se o MID Server estiver configurado incorretamente ou se você tiver apenas as credenciais incorretas.
DNS/IP do servidor de banco de dados	DNS ou endereço IP do seu data warehouse.
Porta do banco de dados	Porta a ser usada para a integração do data warehouse.
Nome do banco de dados	Nome do seu data warehouse.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Deslocamento de atraso de dados (Dias)	A compensação de atraso de dados considera o atraso entre os dados em tempo real no scanner Rapid7 Nexpose e os dados no data warehouse.
MID Server	MID Server a ser usado. Somente MID Servers autônomos são compatíveis. MID servers em cluster não são compatíveis.
Tempo limite do MID Server (mín.)	Número de minutos para aguardar a resposta do MID Server antes de atingir o tempo limite da execução da integração.

b. Verifique a configuração bem-sucedida clicando em **Testar credenciais**.

c. Depois de um teste bem-sucedido, clique em **Salvar**.

d. Clique na guia **Importar configuração**.

No formulário exibido, preencha os campos.

Guia Configuração de importação do Data Warehouse

Campo	Descrição
Antes da v12.0: caixa de seleção Criar entrada de CVE	Quando marcados, os espaços reservados para CVEs, ainda não presentes, são criados como registros do NVD e referenciados na entrada de terceiros para Rapid7. Quando desmarcados, esses CVEs são ignorados.
Pontuação mín. do CVSS	Pontuação mínima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Pontuação máxima de CVSS	Pontuação máxima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Filtro do site	Limita os dados de integração de sites importados aos sites escolhidos. Você pode escolher mais de um. **Nota:** Como a configuração padrão é importar dados de todos os sites, você não precisa usar o filtro se quiser todos os sites. Isso torna a solicitação mais lenta.
Reabrir resolvido por idade	Quando selecionados, os itens vulneráveis são reabertos automaticamente quando o número de dias em que eles foram resolvidos, mas não encerrados, corresponde ao valor exibido no campo **Reabrir resolvido após**.

5. Clique em **Salvar**.

6. Opcional: Se você quiser definir uma data de início nos registros de integração de vulnerabilidade - API Rapid7 e integração de item vulnerável do Rapid7 - API para recuperar dados históricos durante a importação inicial da verificação de Rapid7, siga estas etapas.
Você pode usar esses dados para ajudá-lo com Fechando detecções obsoletas em Resposta a vulnerabilidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Integração com Rapid7 Vulnerability** > **Administração** > **Integrações**.
A lista de integrações Rapid7 é exibida.

b. Clique em um dos registros de integração para abri-lo.

(Optional) Próximo à parte superior do formulário, clique no link **aqui** para editar o registro.

O campo **Importar desde** a data nas integrações Rapid7 está em branco, por padrão, exceto para a Integração de vulnerabilidade Rapid7 - API e a Integração de item vulnerável Rapid7 - API. Para essas integrações, esses campos são definidos como 1998-12-31 ou 1999-01-01.

Para recuperar dados históricos durante a importação inicial da verificação Rapid7, defina uma data de início nos registros de integração apropriados. Este processo funciona para qualquer integração Rapid7, com as seguintes exceções:

- As integrações de exploração e kit de malware Rapid7 não mostram o campo **Importar desde** porque não fazem atualizações delta e, portanto, não usam esse campo.
- A integração Rapid7 Lista de ativos ignora o campo, já que sua intenção é recuperar todos os dados.
- Para a execução inicial da Rapid7 InsightVM Integração de item vulnerável abrangente – API quando o módulo de fechamento automático de itens vulneráveis obsoletos está habilitado e o campo **Importar desde** é deixado em branco.

  Quando você habilita o recurso de fechamento automático, é necessária uma execução bem-sucedida da Integração de item vulnerável abrangente do Rapid7 ou da Integração de item vulnerável abrangente do Rapid7 - API. Essas integrações estão desabilitadas por padrão.

  Ao habilitar a Rapid7 InsightVM Integração Abrangente de Item Vulnerável – API, se você deixar o campo **Importar desde** em branco na página de configuração de integração, o valor no campo **dias atrás** do formulário Fechar automaticamente itens vulneráveis obsoletos também será usado para **Importar desde** data na primeira execução de integração. O valor padrão para Itens vulneráveis obsoletos de fechamento automático é (90 dias).

  Por exemplo, se o campo de **dias atrás** no formulário de fechamento automático de itens vulneráveis obsoletos for 90 e o campo **Importar desde** na página Integração abrangente de itens vulneráveis do Rapid7 - API estiver em branco, a primeira execução de integração importará os dados dos últimos 90 dias.

  Este relacionamento entre os campos **Importar desde** e **dias atrás** se aplica somente à primeira execução de integração. Depois disso, alterar o campo **dias atrás** no formulário de fechamento automático de itens vulneráveis obsoletos não afeta o campo **Importar desde** na página Integração abrangente de itens vulneráveis do Rapid7 – API. O campo é alterado para a hora de início da primeira execução para que as execuções de integração subsequentes importem somente as informações delta

  O campo **Importar desde** é editável e você pode inserir os valores desejados para cada uma das integrações.

7. Navegar até **Todos** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. O parâmetro de instância de integração **import_startime_buffer_comprehenctive** define um tempo de buffer de 24 horas antes do tempo especificado no campo **Importar desde** para que os ativos verificados a partir desse tempo de buffer sejam obtidos durante a execução da **Integração de item vulnerável abrangente do Rapid7 - API**. Você pode modificar este tempo de buffer de acordo com seus requisitos.

b. Opcional: Defina o parâmetro **close_stale_detections** como *verdadeiro* para fechar as detecções obsoletas que não estão mais chegando por meio da API Rapid7 para os ativos que são verificados e recuperados por meio da API Rapid7 por meio da **Integração abrangente de itens vulneráveis do Rapid7 - API**.

Você concluiu com sucesso as etapas de instalação e configuração do Integração com Rapid7 Vulnerability. Agora você está pronto para revisar e verificar os dados importados.

O que Fazer Depois

Os scanners Rapid7 e Qualys são desativados por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto de scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto ativado é exibido no campo Origem nos registros de item vulnerável e de tarefa de correção após a próxima importação, e **Verificar novamente** está disponível como uma ação de IU.

Se o seu ambiente exigir importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração.

Para criar ou refinar suas regras de pesquisa antes da importação, consulte Criar uma regra de pesquisa de IC de resposta a vulnerabilidades.

Filtrando por Rapid7 sites

Filtrar por site para Rapid7 InsightVM tipos de integração, bem como Rapid7 Nexpose tipos de integração de data warehouse.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Nota: O uso da filtragem de site pode ter um impacto no desempenho. Para obter informações sobre desempenho e outras considerações antes de usar a filtragem de sites, consulte KB0789221 .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

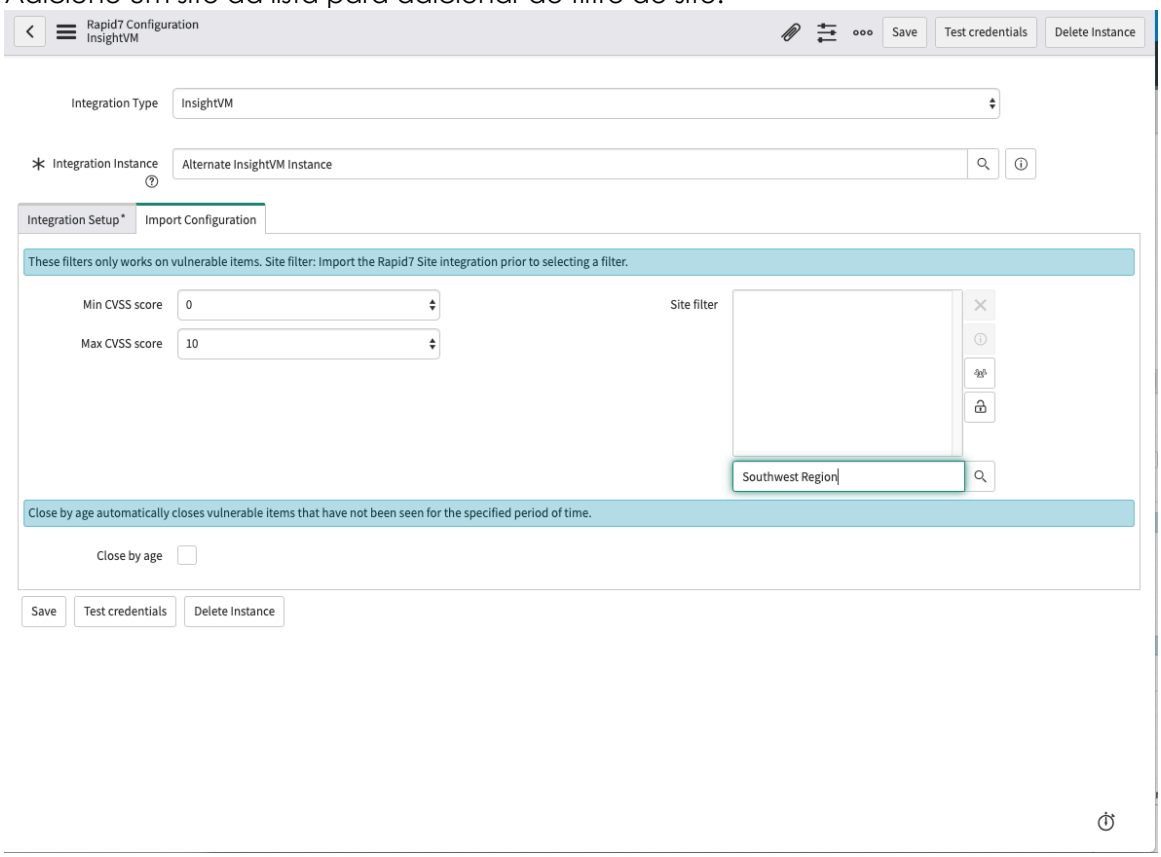
Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Todos** > **Integração com Rapid7 Vulnerability** > **Configuração**.
2. Selecione uma instância de integração.
3. Clique na guia **Importar configuração**.

> **Nota:** Se você quiser todos os sites, deixe o campo de filtro do site em branco. Nenhum filtro de site é equivalente à adição de todos os sites.
>
> Os sites são específicos da instância de integração. A lista de pesquisa para filtragem de site exibe Rapid7 InsightVM e Rapid7 Nexpose sites de instância de integração de data warehouse. Verifique se o site escolhido corresponde à instância de integração selecionada. Por exemplo, se você escolher um site de data warehouse, por engano, esse site não funcionará para a filtragem de sites por Rapid7 InsightVM.

4. Clique na lista de pesquisa para exibir os registros de site da instância de integração atual.
5. Adicione um site da lista para adicionar ao filtro de site.



6. Repita a seleção para adicionar outros locais.
7. Clique em **Salvar**.
   Esses sites são usados para filtrar por site durante a próxima importação. Consulte Anexar SITE aos marcadores do site do Rapid7 InsightVM para obter informações sobre como adicionar o prefixo SITE aos dados do site.

Anexar SITE aos marcadores do site do Rapid7 InsightVM

Adicione o prefixo SITE aos marcadores do site Rapid7 InsightVM para destacá-los na lista de marcadores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Nota: Se necessário, alterne seu escopo para a Integração Rapid7 para Operações de segurança.

Procedimento

1. Na caixa de navegação à esquerda, digite: *sys_properties.list*.
2. Em **Nome**, pesquise por: *sn_vul_r7.prefix_site_to_rapid7_tags*.
3. Abra o *sn_vul_r7.prefix_site_to_rapid7_tags*.
4. Mude o **Valor** para **verdadeiro**.
5. Clique em **Atualizar**.
   Marcadores de site novos e existentes são prefixados durante a próxima importação de Rapid7 InsightVM.

Desduplicar Integração com Rapid7 Vulnerability registros de data warehouse

Ao migrar para o tipo de integração **InsightVM** do tipo de integração de **Data Warehouse**, você pode desduplicar itens vulneráveis de data warehouse existentes, desde que eles pertençam aos mesmos dados de origem que seus dados Rapid7 InsightVM.

Antes de Iniciar

Função necessária: sn_vul_r7.admin ou, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

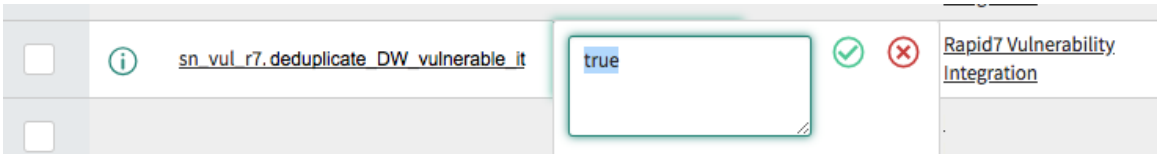
Essa desduplicação funciona somente ao migrar do data warehouse [Rapid7 Nexpose para a integração de item vulnerável Rapid7 InsightVM.

Procedimento

1. Navegar até **Todos** > **Rápido 7** > **Integrações**.
2. Defina todas as Rapid7 Nexpose integrações de data warehouse Configurações da coluna **ativa** como **Falso**, desabilitando as integrações.
3. Insira `sys_properties.list` no painel de navegação esquerdo.
4. Pesquise o **Nome**: `sn_vul_r7.deduplicate_DW_vulnerable_item`.
5. Altere o campo **Valor** para **Verdadeiro**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique no ícone de marca de seleção .
   Durante a próxima Rapid7 InsightVM importação de integração de item vulnerável, qualquer correspondência com registros de data warehouse existentes impedirá a criação de um item vulnerável duplicado.

Integração com Rapid7 Vulnerability gráfico de status de execução

Os sensoresRapid7 Nexpose coletam os dados e os enviam automaticamente para os produtos Rapid7 Nexpose ou Rapid7 InsightVM, que analisam e correlacionam continuamente as informações.

Visualizações de dados nos espaços Resposta a vulnerabilidades

Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços, Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Integração com Rapid7 Vulnerability funciona facilmente com Resposta a vulnerabilidades para mapear vulnerabilidades para ICs e serviços de negócio para determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas. O módulo Integração com Rapid7 Vulnerability Status de execução é uma exibição gráfica do status de Integração com Rapid7 Vulnerability execuções.

Para exibir esses dados na exibição legada, navegue até **Todos** > **Todos Integração de vulnerabilidade do Rapid7** > **Status da Execução da Integração**.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Versões anteriores de Resposta a vulnerabilidades

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois novos gráficos foram adicionados para comparar as métricas de desempenho:

- Rapid7 Métricas de desempenho de ingestão de itens vulneráveis: compare as métricas diárias de desempenho para regras de atribuição, regras de grupo, regras de risco, tempo de espera na fila, tempo de processamento da fila e outras estatísticas de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

itens vulneráveis nos últimos 30 dias para identificar a causa de quaisquer desvios no desempenho.

- Rapid7 Taxa de transferência de desempenho de ingestão de itens vulneráveis: compare a taxa de transferência diária de ingestão de itens vulneráveis para a Rapid7 Integração de item vulnerável - API. O rendimento é medido em itens por hora.

Nota: Em Rapid7, esses gráficos são compatíveis somente com a integração de VM do Insight.

Status de execução da integração do Rapid7

Amostra Integração com Rapid7 Vulnerability de gráfico de status de execução

- O valor na coluna Itens importados representa o número total de itens vulneráveis que são criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de itens vulneráveis que são criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que itens vulneráveis são atualizados durante uma execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
- A coluna Itens inalterados exibe itens vulneráveis encontrados durante a execução de integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campos relevantes foi alterado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A integração é executada sem resultados para todos os quatro dos seguintes valores: **Novos ICs**, **ICs existentes**, **Novos itens**e **Itens atualizados** são filtrados da lista de execuções de **integração do Rapid7**.

Integração com Rapid7 Vulnerability executar relatórios de gráfico de status

Nome	Descrição
Resultados dos últimos 30 dias Rapid7	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Rapid7 Novos IVs	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Rapid7 VIs atualizados	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Rapid7 duplicados	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Rapid7 Execuções de integração	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções desta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na contagem de detecção ou descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem de data até" na instância, após a conclusão da execução da integração.
Últimos 30 dias Rapid7 Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparados nos últimos 30 dias.
Últimos 30 dias Rapid7 Taxa de transferência de desempenho de ingestão de item vulnerável	Taxa de transferência de ingestão de item vulnerável diária para a Rapid7 Integração de item vulnerável - API medida nos últimos 30 dias.

Exibir o Integração com Rapid7 Vulnerability painel de status de execuções de importação

Use o Rapid7 painel de status de execução de importação de vulnerabilidade para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar
Funções necessárias: sn_vuln.admin

Por Que e Quando Desempenhar Esta Tarefa
Este procedimento faz as seguintes suposições.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você tem Resposta a vulnerabilidades e Integração com Rapid7 Vulnerability instalados e configurados.
- Integração com Rapid7 Vulnerability importações estão programadas e em execução.
- Rapid7 gráficos de status de execução de integração estão em uso.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 19.0 do Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Rapid7** > **Status da Execução da Integração**.

   A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

   Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

2. Se você não estiver usando o gráfico de status de execução de integração Rapid7, navegue até **Rapid7** > **Integrações**.
   a. Escolha uma integração.
   b. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
3. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns de falha na execução:

   - Interrupção de rede
   - Declínio de bits na transferência de dados, resultando em dados corrompidos durante a transformação

   Para todas essas condições, clique em **Executar agora** e execute novamente a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar nova verificação para a integração de vulnerabilidade Rapid7

Inicie novas verificações na plataforma Rapid7 para verificar se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados.

Antes de Iniciar

Nota: Novas verificações para Rapid7 itens vulneráveis de data warehouse não são compatíveis.

Você pode iniciar novas verificações nos espaços da Resposta a vulnerabilidades. Para obter mais informações, consulte Verificar novamente registros e tarefas de correção no Espaço do gerenciador de vulnerabilidades e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Funções necessárias: funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Por Que e Quando Desempenhar Esta Tarefa

Para novas verificações no ambiente clássico, consulte as seções a seguir.

Novas verificações são compatíveis. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis importados de integrações Rapid7 InsightVM da sua instância Now Platform®.

Nota: O scanner Rapid7 está desativado por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou tarefas de correção que tenham a aplicação Rapid7 como origem, o botão Verificar novamente não estará disponível.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de itens vulneráveis (VI), tarefas de correção (RT), entradas de terceiros (TPE) ou registros de itens descobertos da sua instância Now Platform®.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada a partir de seus Now Platform para Rapid7 itens vulneráveis. Você pode exibir resultados atualizados em seus itens vulneráveis com a próxima importação agendada de Rapid7 InsightVM Integrações de vulnerabilidade e item vulnerável.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável a partir do qual você deseja acionar uma nova verificação e abra-o.

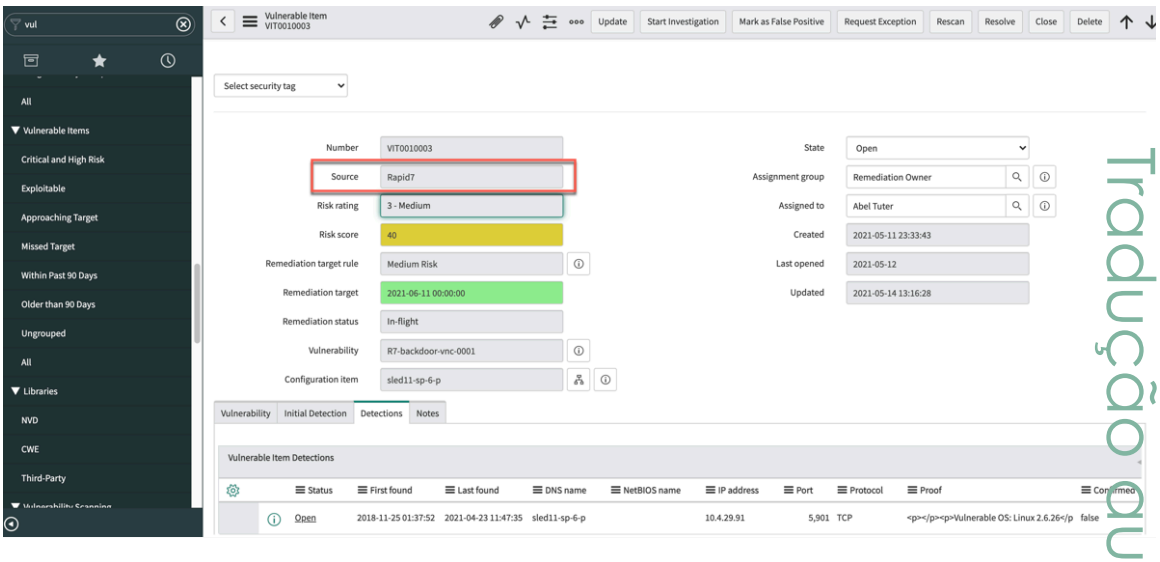
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Inicie novas verificações de IVs com Rapid7 como origem. Verifique se Rapid7 é exibido na coluna **Origem** nas exibições de lista de VI ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condições para agrupar IVs por origem. Ou, se a coluna **Origem** não for exibida na exibição Lista de VI, no canto superior esquerdo da lista, clique no ícone de engrenagem e mova a **Origem** de **Disponível** para **Selecionado**.

Ao iniciar novas verificações, evite acionar simultaneamente verificações para um ID de origem de várias origens. A solicitação de verificação mais recente gerará erro.

Por exemplo, se você iniciar uma nova verificação de um VI a partir de um registro de VI e também solicitar outra nova verificação a partir de um registro de tarefa de correção que contém o mesmo VI, é provável que a segunda solicitação falhe.



3. Como alternativa, navegue até **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **terceiro** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de VI, o VI deve ser do produto Rapid7 e estar em qualquer estado diferente de Encerrado. Para vários registros de VI, todos os IVs selecionados na exibição de lista devem ser do produto Rapid7 e estar em qualquer estado diferente de Encerrado.
   - Em um registro de tarefa de correção, a tarefa de correção pode estar em qualquer estado diferente de Encerrado e todos os IVs associados devem ser do produto Rapid7.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do produto Rapid7 em qualquer estado diferente de Fechado.
   - Em um registro de item descoberto, o VI deve ser do produto Rapid7 e estar em qualquer estado diferente de **Closed**.

4. No canto superior direito do registro, clique em **Verificar novamente**.
   Para exibições de lista, selecione os IVs na lista que você deseja verificar novamente e, na lista **Ação nas linhas selecionadas**, selecione **Verificar novamente**.

5. No pop-up exibido, confirme a nova verificação.
   Uma mensagem é exibida indicando que a verificação está sendo processada (**Em fila**).
   Na mensagem, clique no link **Exibir detalhes** para verificar o status da nova verificação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

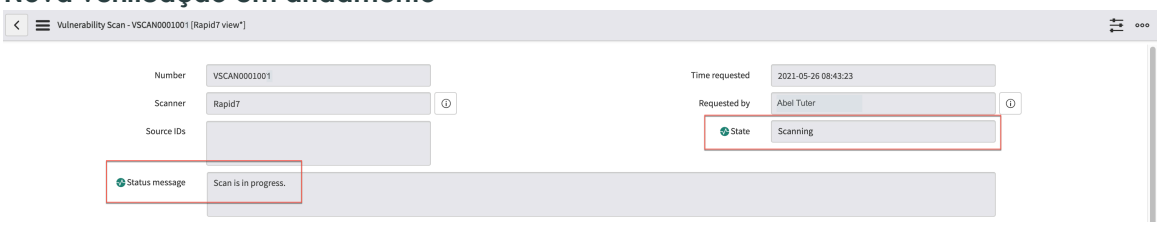
(verificação secundária) e exibir outras verificações iniciadas a partir do registro. O status de todas as novas verificações pode ser encontrado a qualquer momento na lista relacionada Verificações na parte inferior do VI, tarefa de correção, TPE e registros de itens descobertos que você usa para iniciar as novas verificações.

Quando a verificação está em andamento, o campo Estado muda para **Verificação**e o campo Mensagem de status exibe **A verificação está em andamento**.

Nota: Cada nova verificação oferece suporte a 500 ativos por verificação. Se sua solicitação tiver mais de 500 ativos, mais verificações secundárias serão solicitadas.

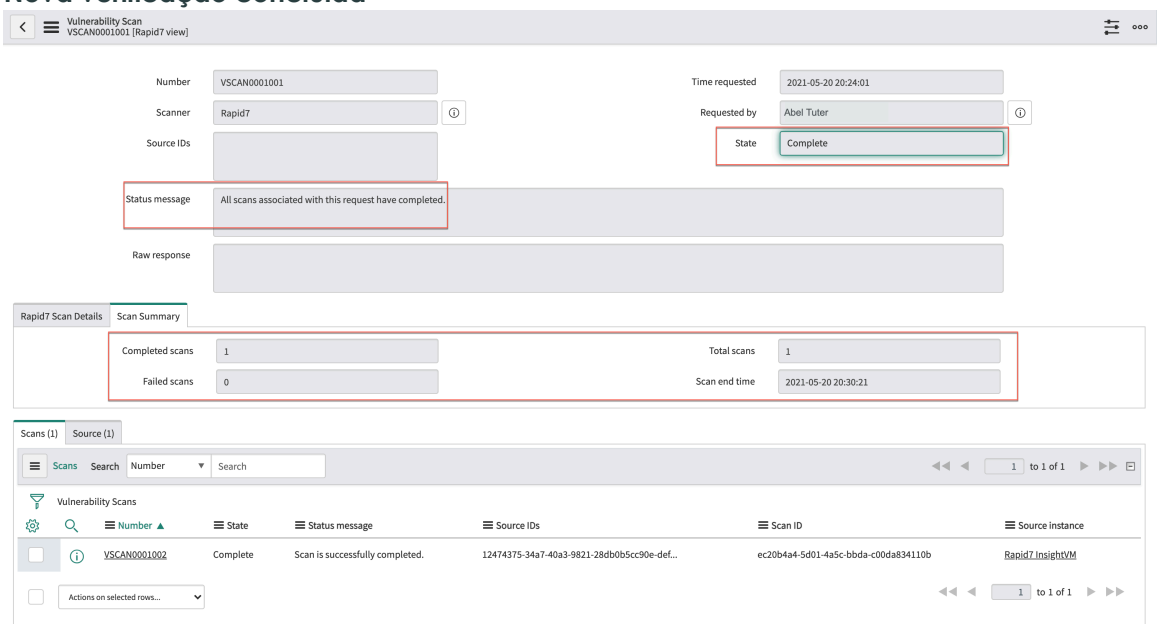
Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

Nova verificação em andamento



O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram ou farão a transição para Encerrado/ Corrigido são importados com a próxima importação agendada das Rapid7 integrações.

Nova verificação concluída



Como alternativa, você pode iniciar uma nova verificação sob demanda para uma vulnerabilidade específica em um ativo específico. Você pode exibir os resultados dessas verificações depois que a verificação for concluída no VI atualizado, na tarefa de correção, no TPE e nos registros de itens descobertos a partir dos quais você iniciou a verificação.

Tradução automática

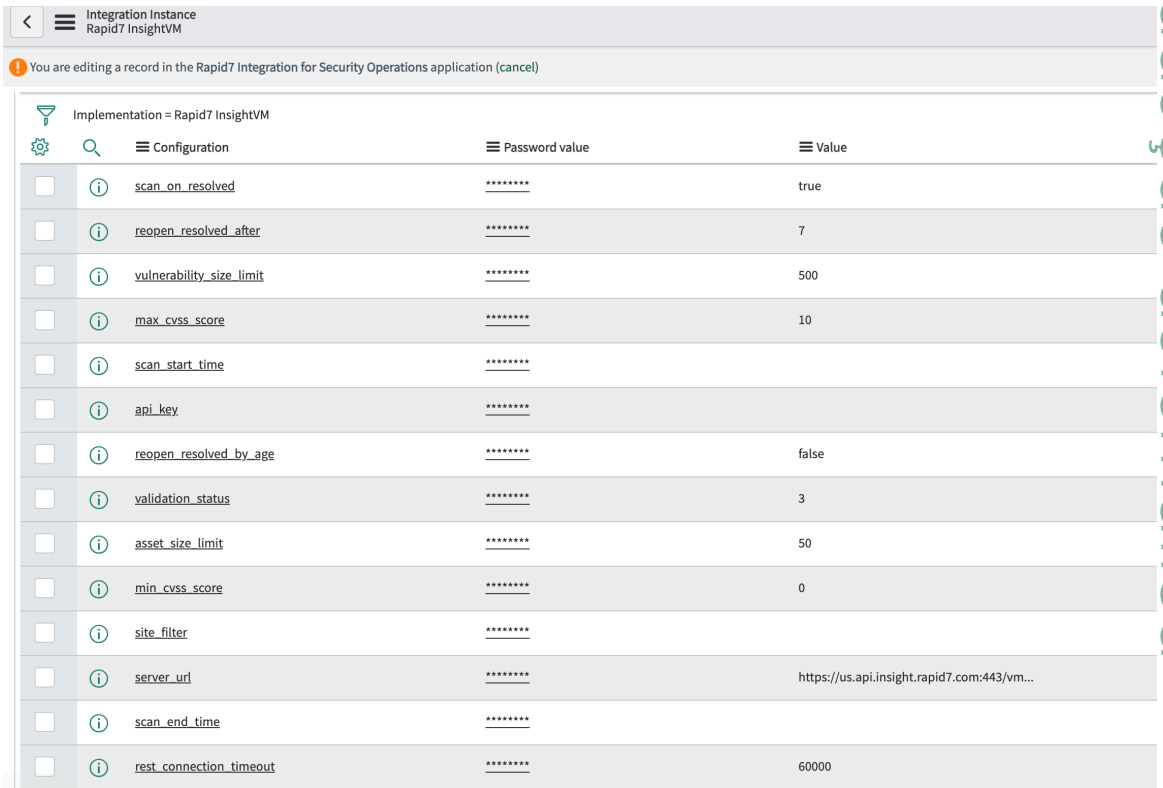
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor do campo Estado nos registros de Verificação de vulnerabilidades é importado de Rapid7. Quando a verificação é concluída com sucesso, o estado é definido como Concluído. Se a verificação não for concluída com sucesso, um valor de erro será exibido.

Verificações automáticas e verificações programadas

Como gerente ou analista de vulnerabilidade, você pode especificar e programar quando novas verificações são iniciadas para IVs e RTs. Você também pode habilitar verificações automáticas para IVs e tarefas de correção definidas para resolver.

6. Para modificar os parâmetros de integração na instância de integração, navegue até **Integração com Rapid7 Vulnerability** > **Administração** > **Configuração**.
7. No registro de configuração do Rapid7, se não estiver selecionado, na lista **Tipo de integração**, selecione **Rapid7 InsightVM**.
8. À direita do campo **Instância de integração**, clique no ícone de informações e, em seguida, em **Abrir registro**.
9. No registro da Instância de integração do Rapid7 InsightVM, localize os parâmetros para programar verificações e edite conforme necessário.



scan_on_resolved indica se a verificação é iniciada quando uma vulnerabilidade é resolvida. O padrão é **falso** (desabilitado).

Se este parâmetro estiver definido como `verdadeiro`, sempre que um VI ou RT for definido como Resolvido, o fluxo de trabalho para verificar novamente o respectivo VI e a tarefa de correção será acionado automaticamente.

scan_start_time

Defina a hora de início da verificação em **HH:mm** (formato de 24 horas) no fuso horário UTC para a hora de início da janela em que você deseja que novas verificações estejam disponíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor padrão é `00:00`.

scan_end_time

Defina a hora de término da verificação em **HH:mm** (formato de 24 horas) no fuso horário UTC para a hora de término da janela de verificação disponível.

O valor padrão é `23:59`.

Se uma verificação for iniciada dentro da janela de tempo programada, ela será iniciada instantaneamente. Se a verificação for iniciada fora da janela, ela será enfileirada para a próxima janela programada.

Por exemplo, se você inserir uma hora de início de `00:00` para o parâmetro *scan_start_time* e uma *scan_end_time* de 10:00 AM na mesma manhã, as verificações programadas ou iniciadas manualmente fora da janela de tempo da meia-noite às 10 AM serão enfileiradas e iniciadas na hora de início da janela de tempo do dia seguinte `00:00`.

No mesmo exemplo, se você iniciar manualmente uma nova verificação às 11h, a nova verificação não será iniciada imediatamente, pois está fora dos tempos de verificação configurados disponíveis. A solicitação de verificação permanece na fila até o início da janela de tempo do dia seguinte, neste exemplo `00:00`.

Definir parâmetros de filtro adicionais para Rapid7 InsightVM importações

Personalize os parâmetros de filtragem das suas consultas programadas com Integração Rapid7 para Operações de segurança para ajudá-lo a refinar ainda mais os dados de vulnerabilidade importados com o produto Rapid7 InsightVM.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para que você possa revisar somente os detalhes específicos da vulnerabilidade. Por exemplo, talvez você queira exibir somente as vulnerabilidades importadas que são `Críticas` e `Graves`.

Para ajudá-lo a coletar esses dados, adicione parâmetros Rapid7 para ajudá-lo a importar os detalhes específicos da vulnerabilidade necessários.

Sem adicionar chamadas de API ou codificação adicionais, a partir da v13.4, o recurso permite que você personalize suas informações de solicitação HTTP com parâmetros Rapid7 InsightVM em seu Now Platform. As seguintes integrações Rapid7 InsightVM são compatíveis com a filtragem adicionando conteúdo JSON ao corpo da solicitação:

- Rapid7 InsightVM API de integração de item vulnerável
- Rapid7 InsightVM API de integração de vulnerabilidade
- Rapid7 InsightVM

Você deve saber como usar cadeias de caracteres JSON para este recurso.

Função necessária: sn_vul.vulnerability_admin

Procedimento

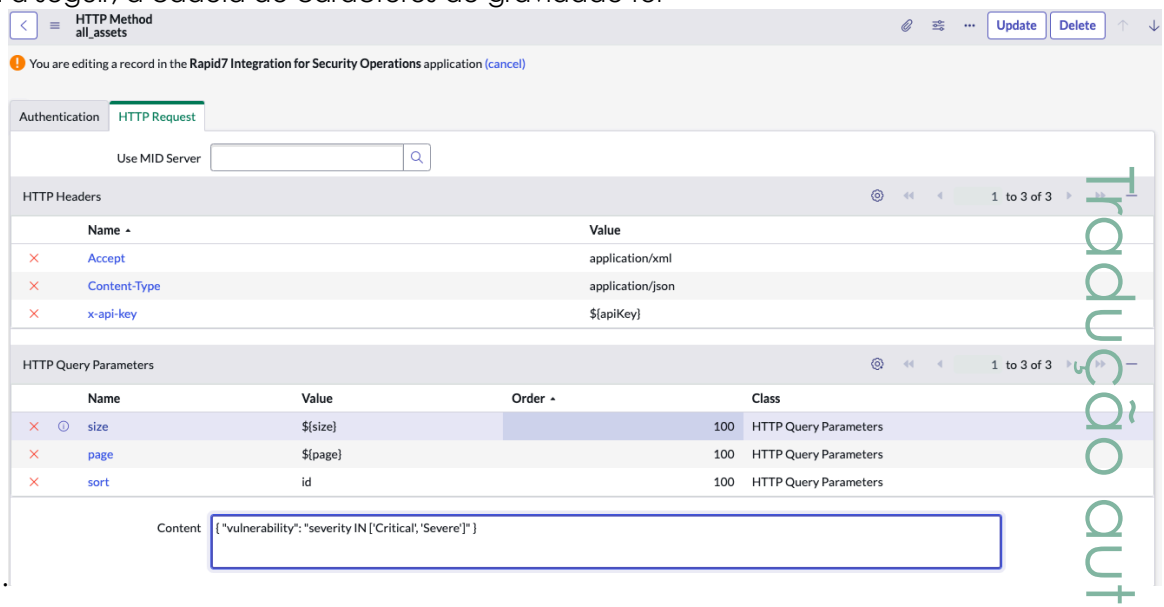
1. Localize os parâmetros compatíveis com o produto [Rapid7 InsightVM no site do desenvolvedor Rapid7 que você deseja usar para a filtragem.

   Você pode criar os parâmetros para o corpo da solicitação consultando a documentação Rapid7. Os parâmetros e valores inseridos no produto Rapid7 InsightVM são compatíveis somente no nível da instância de integração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Navegar até **Todos** > **Integração com Rapid7 Vulnerability** > **Administração** > **Integrações**.
3. Na página da lista Integrações do Rapid7, clique no registro da integração Rapid7 InsightVM que você deseja abrir.
4. À direita da página, clique no ícone de informações (I) da mensagem REST, seguido por **Abrir registro**.
5. Com a guia Solicitação HTTP selecionada, em Métodos HTTP, na coluna Nome, clique em um item para abrir seus parâmetros de consulta HTTP.
6. Em Registro de método HTTP, em Parâmetros de consulta HTTP, no campo Conteúdo, insira os valores de parâmetro que você encontrou no site do desenvolvedor Rapid7.

   Na imagem a seguir, a cadeia de caracteres de gravidade foi adicionada.



   Se você quiser inserir mais de um parâmetro, consulte a documentação Rapid7 para obter mais informações sobre como separar cada valor.

7. Clique em **Atualizar**.

Noções básicas sobre a integração de exploração do Shodan

A aplicação Integração de exploração ServiceNow® Shodan usa dados importados do mecanismo de pesquisa Shodan para ajudá-lo a determinar o impacto e a prioridade de explorações potencialmente mal-intencionadas.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Shodan Exploit Integration

O mecanismo de pesquisa Shodan coleta dados de exploração e a API do Shodan disponibiliza esse banco de dados para o Now Platform®. Ele se integra facilmente à aplicação ServiceNow® Resposta a vulnerabilidades para mapear explorações para vulnerabilidades de terceiros, enriquecendo os dados de exploração em sua instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente na ordem em que são listadas. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento para Xanadu	**Notas de versão**
Integração com Shodan Exploits v10.6, 10.7	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Shodan As tarefas de integração de exploração envolvem as funções a seguir.

- sn_vul_shodan.admin: usuários com essa função podem ler, gravar e excluir registros.
- sn_vul_shodan.user: usuários com essa função podem ler e gravar registros.
- sn_vul_shodan.read: usuários com esta função podem ler registros.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Integrações de exploração do Shodan

Para exibir as integrações de exploração Shodan, navegue até **Todos** > **Shodan Exploit Integration** > **Integrações**.

As seguintes integrações estão incluídas no sistema de base. Essas integrações estão ativas por padrão.

Integrações de exploração do Shodan

Integração	Descrição
Shodan ExploitDB Integration	Recupera dados do ExploitDB de Shodan e aprimora seus dados de vulnerabilidade de terceiros. Esta integração está definida para ser executada diariamente às 03:15:00.
Shodan Metasploit Integration	Recupera informações do Metasploit de Shodan e aprimora seus dados de vulnerabilidade de terceiros. Esta integração está definida para ser executada diariamente à 01:15:00.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para alterar a hora de início padrão das importações de integração programadas, consulte Definir Shodan Tempo de importação da integração de exploração.

Para exibir dados de exploração em vulnerabilidades de terceiros, consulte Exibir Resposta a vulnerabilidades bibliotecas de vulnerabilidades.

Alterar outras configurações de integração de exploração Shodan requer conhecimento avançado ServiceNow e Resposta a vulnerabilidades e está além do escopo da documentação do produto.

Preparando para a integração de exploração Shodan

Uma integração de exploração Shodan bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. A integração de exploração Shodan pressupõe que você esteja familiarizado com o mecanismo de pesquisa Shodan e a API.

Antes de Iniciar

A integração de exploração Shodan requer uma chave de API. Registre-se no Shodan site para obter uma assinatura gratuita para adquirir esta chave.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

- Se você não importou dados do banco de dados de vulnerabilidades do NIST (NVD) para Resposta a vulnerabilidades, faça-o antes de instalar a integração de exploração Shodan. A importação dos dados do NVD garante que os dados de CVE (Common Vulnerability and Exposure, vulnerabilidade e exposição comuns) preencham automaticamente os registros de exploração.

  Sem dados do NVD, um espaço reservado é criado no registro de exploração e não é inserido até a próxima atualização do NVD. Para obter mais informações sobre o NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

- Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Instalar e configurar o Integração com Shodan Exploits para Operações de segurança

Antes de executar o Integração com Shodan Exploits em sua instância, baixe-o e instale-o a partir do ServiceNow Store. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tradução automática

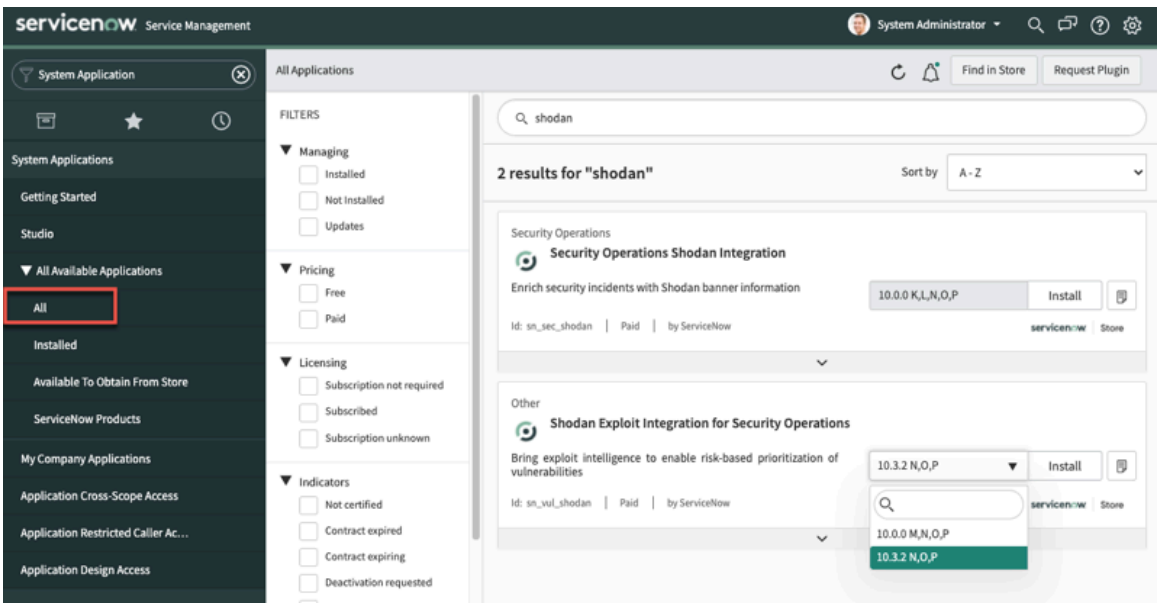
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se você tem direitos ServiceNow válidos para a aplicação Resposta a vulnerabilidades e os direitos [Integração com Shodan Exploits para a aplicação Operações de segurança.	Para verificar direitos, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre como obter direitos para uma aplicação Operações de segurança do ServiceNow Store, consulte .
(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros.	Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte, Como instalar Resposta a vulnerabilidades.
Tenha a chave de API de integração de exploração Shodan à mão.	Consulte Preparando para a integração de exploração Shodan.

Função necessária: administrador

Procedimento

1. Faça login na instância Now Platform em que você deseja instalar a aplicação Integração com Shodan Exploits.
2. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
3. Localize a aplicação Integração com Shodan Exploits para Operações de segurança, selecione a versão desejada e clique em **Instalar**.



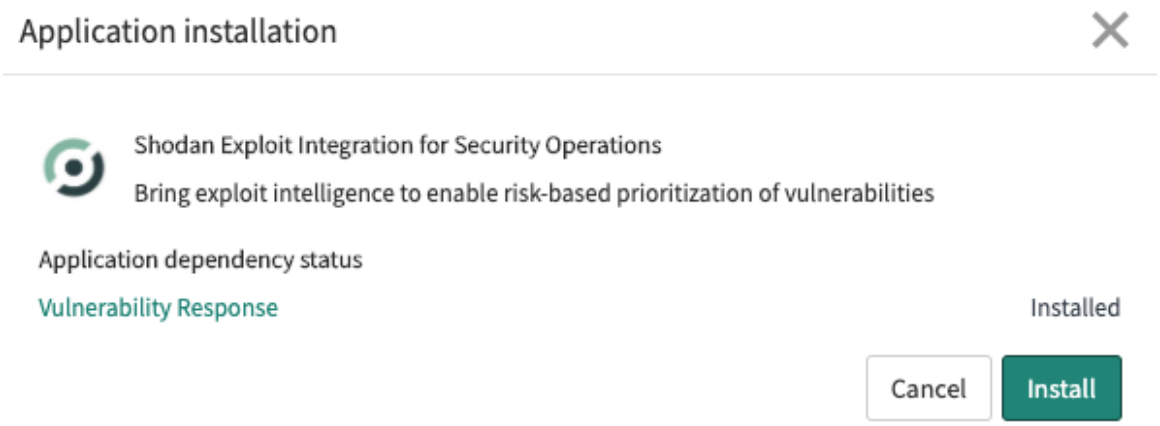
Nota: Se você tiver direito a uma atualização para esta aplicação, o botão **Atualizar** será exibido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

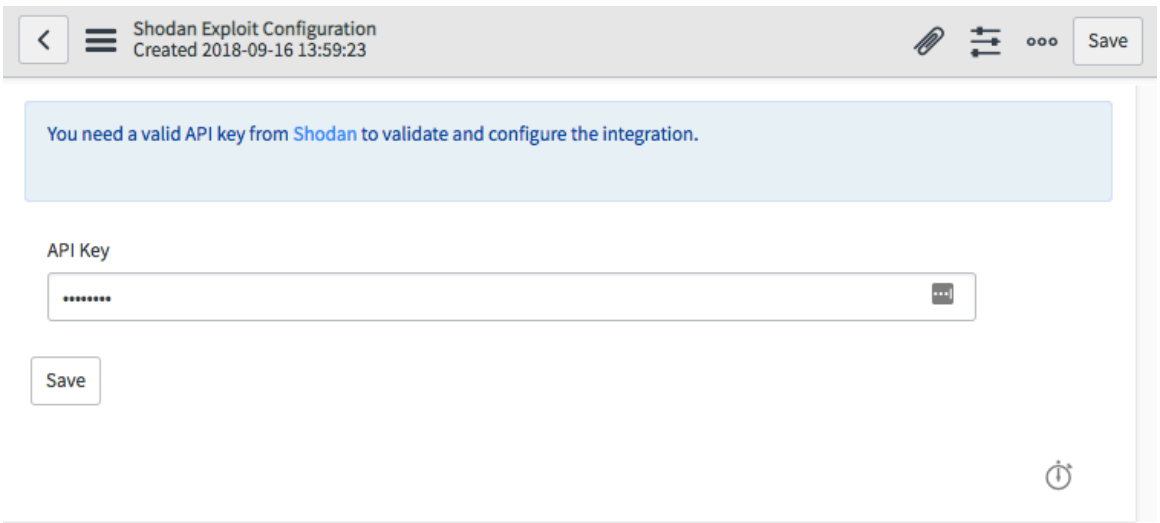
A caixa de diálogo de instalação da aplicação exibe o status de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.

4. Na caixa de diálogo, clique em **Instalar**.



A caixa de diálogo Instalar indica quando a instalação foi concluída com sucesso.

5. Feche a caixa de diálogo Instalar.
6. Navegar até **Shodan Exploit Integration** > **Configuração**.
7. Insira sua chave de API Shodan.



8. Clique em **Salvar**.
   Sua configuração Integração com Shodan Exploits está concluída.

Definir Shodan Tempo de importação da integração de exploração

Para sua conveniência, você pode redefinir a hora de início das integrações de exploração Shodan.

Antes de Iniciar
Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, Shodan exploram integrações que retornam dados delta, a menos que uma importação completa seja solicitada. Consulte Executar uma importação de exploração manual Shodan para obter mais informações sobre importações completas.

Procedimento

1. Navegar até **Todos** > **Shodan Exploit Integration** > **Integrações**.
2. Escolha uma integração.
3. Clique no link para editar o registro.
4. Defina as novas opções **Executar** e **Tempo**.
   O tempo é calculado como Horas no horário local. O tempo padrão para as importações de exploração Shodan é 03:15:00.
5. Clique em **Atualizar**.
   A nova hora será usada para a próxima importação agendada.

Executar uma importação de exploração manual Shodan

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independente do trabalho agendado diariamente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Shodan Exploit Integration** > **Integrações**.
2. Escolha uma integração.
3. Marque a caixa de seleção **Importação de dados completa**.
4. Clique em **Executar Agora**.
   Quando a importação for concluída, a caixa de seleção será desmarcada e as importações delta serão retomadas.

Exibir o Shodan status de execução da importação da integração de exploração

Use a lista relacionada de execuções de integração de vulnerabilidade para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas, e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status de execução de importação do Shodan:

- A aplicação Resposta a vulnerabilidades e a integração de exploração Shodan devem ser instaladas e configuradas.
- As importações de integração de exploração Shodan devem estar programadas e em execução.

Função necessária: sn_vuln.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Shodan Exploit Integration** > **Integrações**.
2. Selecione uma integração.
3. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

Trouble?

As causas mais comuns de falha na execução incluem:

- Interrupção de rede
- Declínio de bits na transferência de dados, resultando em dados corrompidos durante a transformação

Se você encontrar alguma dessas condições, marque a caixa de seleção **Importação de dados completa**, clique em **Executar agora**e execute novamente a integração.

Noções básicas sobre a integração de vulnerabilidade da Tenable

A aplicação Integração de Resposta a vulnerabilidades com Tenable desenvolvida pela engenharia ServiceNow para a integração de vulnerabilidade da Tenable usa dados importados dos produtos Tenable.io e Tenable.sc para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. A aplicação está disponível com uma assinatura separada do ServiceNow® Store.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

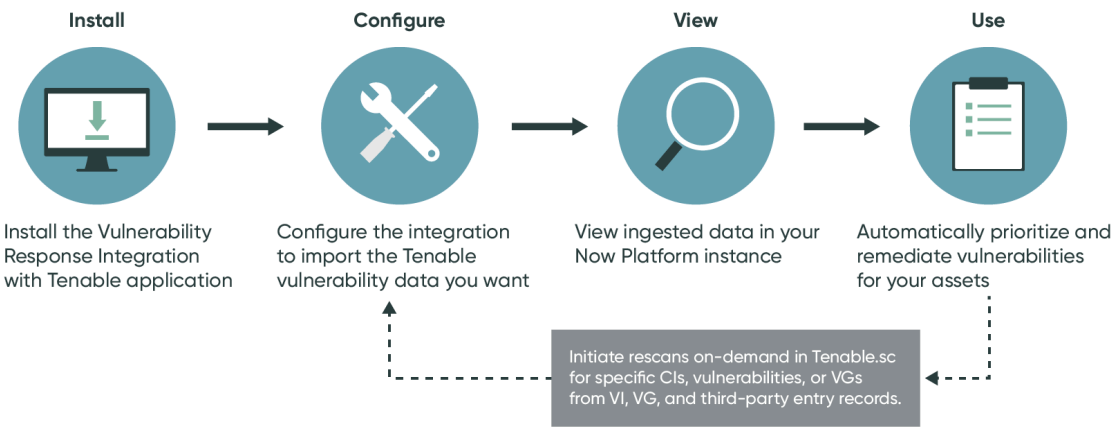
A integração de vulnerabilidade da Tenable emprega duas integrações da Tenable, Tenable.io e Tenable.sc, para importar dados de scanners de terceiros sobre seus ativos e vulnerabilidades. A aplicação Integração de Resposta a vulnerabilidades com Tenable é compatível com o produto Tenable.sc a partir da versão 5.13.

- Tenable.io é uma integração empresarial baseada na nuvem.
- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

A aplicação Integração de Resposta a vulnerabilidades com Tenable está disponível no ServiceNow Store com uma assinatura separada.

Para obter listas e descrições das integrações no Integrações de vulnerabilidade da Tenable, consulte Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações e Tenable.sc integrações com a aplicação Resposta a vulnerabilidades.

Integração de vulnerabilidade Tenable



Versões disponíveis para Xanadu

Versão de lançamento	Notas de versão
Integração de Resposta a vulnerabilidades com Tenable v3.5, v3.6	Para obter informações de compatibilidade, consulte KB0856498 Matriz de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão de lançamento	Notas de versão
	compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado em sua instância Now Platform quando:

- Uma vulnerabilidade importada de um scanner de terceiros é correspondida com um ativo existente (um item de configuração em seu CMDB). O produto da Tenable se refere a essas correspondências como **vulnerabilidades**.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente em seu CMDB. Nesse caso, um IC incompatível também é criado junto com um item vulnerável.

  Para ICs não correspondentes, você também pode usar o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido com um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatível. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação.

Entradas de vulnerabilidade e plug-ins de terceiros

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros e listadas na tabela Entradas de vulnerabilidade de terceiros na instância Now Platform. As entradas de vulnerabilidade de terceiros da Tenable são ingeridas em Resposta a vulnerabilidades e correspondidas aos ativos existentes listados em CMDB. A Tenable se refere às entradas de vulnerabilidade de terceiros como Plug- **ins**.

IC (Configuration Item, item de configuração)

Itens de configuração são os ativos existentes listados em seu CMDB.

Item descoberto

Os ativos ingeridos da importação de ativos da Tenable são correspondidos com os itens de configuração existentes em seu CMDB. Ativos importados são atualizados.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Se o plug-in Modelos de classe de IC do CMDB estiver habilitado, o Mecanismo de Identificação e Reconciliação (IRE) criará novos ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação. Se o IC original incompatível for reclassificado, os registros de itens descobertos serão atualizados para refletir o estado. Os itens descobertos dão visibilidade sobre como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados de uma integração de terceiros, a Resposta a vulnerabilidades usa automaticamente os dados do host (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). Regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os IVs são criados para ajudá-lo na correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nova verificação e verificação de correção

Você pode iniciar um comando de nova verificação direcionada em um item de configuração específico, tarefa de correção ou entrada de terceiro diretamente do item vulnerável, tarefa de correção e registros de entrada de vulnerabilidade de terceiros em sua instância Now Platform. A Tenable se refere a esta nova verificação como uma **verificação de correção**.

Fechar automaticamente IVs mais antigos

Com o módulo de fechamento automático de itens vulneráveis obsoletos em seu Now Platform, você pode limpar itens vulneráveis (VI) obsoletos mais antigos que não foram encontrados recentemente por suas integrações de terceiros. Mover esses IVs para **Encerrado** ajuda a reduzir o número de itens vulneráveis ativos e tarefas de correção e reconciliar ativos em seu CMDB. Você pode usar todas as integrações com Integração de Resposta a vulnerabilidades com Tenable para fechar automaticamente IVs obsoletos.

Instância

Este termo se refere a uma ocorrência distinta da sua aplicação Now Platform®.

Integração

Uma integração é uma referência específica de produto a uma integração, como a Tenable.io Assets Integration, ou a Tenable.sc Plugin Integration. Essas são as integrações separadas que pertencem a produtos específicos da Tenable na integração de vulnerabilidade da Tenable em sua instância.

Instância de integração

Este termo se refere às integrações separadas da Tenable listadas por seus produtos Tenable.io e Tenable.sc.

Implantação

Quando uma integração oferece suporte a várias origens, uma existência de integração única e distinta é chamada de implantação da sua integração. O termo é usado para se referir à(s) integração(ões) e produto(s) em seu ambiente. Por exemplo, você pode ter várias implantações de várias integrações dos produtos Tenable.io e Tenable.sc em seu ambiente.

As integrações Tenable.io e Tenable.sc também incluem os seguintes recursos principais:

- As descobertas da avaliação de configuração, ou seja, resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas podem ser importadas para a aplicação Conformidade de configurações com o produto Tenable.io. Consulte Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações e Explorando Conformidade de configurações para obter mais informações sobre como essa integração funciona com a aplicação Conformidade de configurações.
- A partir da v2.1 do Integrações de vulnerabilidade da Tenable, crie itens de configuração (ICs) exclusivos que incluem diferentes identificadores de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. Identifique os ativos distintos em seu ambiente e atualize os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações Tenable.io e Tenable.sc. Você também pode executar trabalhos agendados manualmente sob demanda.
- Para importações de ativos com Tenable.io, você pode habilitar etiquetas do ativo para organizar e rastrear os ativos listados em seu ambiente CMDB no Tenable.io.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As integrações Tenable.io e Tenable.sc permitem configurar regras de pesquisa de IC para definir como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (ICs) em seu Now Platform CMDB.
- As integrações Tenable.io e Tenable.sc permitem que você defina filtros de importação na importação de vulnerabilidades para importar somente as vulnerabilidades desejadas da Tenable. Para Tenable.io, você tem a opção de importar vulnerabilidades **fixas** da Tenable com a importação de vulnerabilidades.
- Para Tenable.sc, você tem a opção de iniciar novas verificações sob demanda diretamente do item vulnerável, da tarefa de correção e dos registros de entrada de terceiros em sua instância Now Platform. Se os IVs tiverem sido transicionados para **Encerrado/Corrigido**, mas ainda não estiverem atualizados em sua instância, você poderá verificar se as vulnerabilidades em itens de configuração específicos foram corrigidas. Consulte Iniciar nova verificação para a integração Tenable.sc.

As seções a seguir listam mais detalhes sobre as integrações da Tenable.

Funções necessárias de Now Platform

As tarefas de integração exigem as funções a seguir em sua instância Now Platform.

administrador

O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das integrações da Tenable no Assistente de configuração. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. O administrador de vulnerabilidades configura todas as aplicações e regras de VR para integrações de terceiros instaladas.

sn_vul_tenable.configure_integration

Essa função contém a função granular sn_vul_tenable.read_integration e os usuários com essa função podem configurar a aplicação Integração de Resposta a vulnerabilidades com Tenable.

sn_vul_tenable.read_integration

Usuários com essas funções podem exibir (ler), mas não editar registros da aplicação Integração de Resposta a vulnerabilidades com Tenable.

Grupo de Resposta a vulnerabilidades

Por padrão, o grupo de Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Itens vulneráveis

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de tarefa de correção e atribuídos para correção com base nas regras de atribuição. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral e Resposta a vulnerabilidades visão geral das regras de atribuição.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de pesquisa de item de configuração (IC)

As Regras de pesquisa de IC identificam ICs e determinam quando adicioná-los a um item vulnerável. Para obter mais informações sobre como as regras de pesquisa de IC funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desabilite-as ao criar novas.

As regras de pesquisa Tenable.io a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nome do host
- DNS
- IP

As regras de pesquisa Tenable.sc a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Nota: Vários valores para ip_address, mac_address, fqdns e network_interfaces são usados para um ativo. Todos os valores são considerados nas regras de pesquisa de IC para correspondência. Todos os valores são usados para criar vários adaptadores de rede usando o IRE.

Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos em nuvem incompatíveis.

Novas propriedades para ignorar endereços IP

Em Tenable.io, há duas propriedades disponíveis se você quiser ignorar vários endereços IP ou vários endereços Mac como parte de suas regras de pesquisa de IC:

ignorarEndereçoIP

Uma lista de endereços IP a serem ignorados para pesquisa de IC e criação de IC.

ignoreMacAddress

Uma lista de endereços MAC a serem ignorados para pesquisa de IC ou criação de IC.

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação das integrações de itens vulneráveis da Tenable e das integrações de ativos da Tenable.

Nota: O filtro padrão para esta lista está definido como `Incompatível`. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre o módulo Itens descobertos, consulte Itens Descobertos.

Etiquetas do ativo

As etiquetas do ativo (também chamadas de etiquetas de host) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos. Em seguida, ao iniciar verificações, você pode selecionar marcadores associados aos ativos que deseja verificar. O módulo Etiquetas do ativo permite que você baixe dados de etiqueta do ativo de Tenable.io para sua instância de forma programada. Os dados de ativos que incluem etiquetas de ativos são extraídos de Tenable.io e transformados usando os mapas de transformação de integração de transformação de ativo da Tenable.io.

Todas as etiquetas do ativo são importadas como parte da integração do ativo Tenable.io. As etiquetas do ativo geralmente são usadas para filtrar em Resposta a vulnerabilidades regras de atribuição e Regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Nota: Execute a integração de ativo Tenable.io antes de criar regras de atribuição Resposta a vulnerabilidades ou regras de tarefa de correção na aplicação Resposta a vulnerabilidades para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Por exemplo, se você criar um marcador para descrever ativos em seu local de San Diego e criar o marcador `San Diego`, também não poderá criar um marcador `SAN DIEGO` e armazená-lo na tabela de etiquetas do ativo. `San Diego` e `SAN DIEGO` são consideradas a mesma etiqueta do ativo pelo sistema. O marcador que for importado primeiro será o marcador armazenado e reconhecido daqui em diante.
- O uso de etiquetas do ativo como chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As etiquetas do ativo devem ser usadas somente no Construtor de condições.
- As etiquetas do ativo são controladas pela propriedade do sistema global sn_vul.import_asset_tags. Esta propriedade é definida como `verdadeira` por padrão. Desabilitar os marcadores os desabilita em todas as Now Platform® instâncias.

Filtros de recuperação de dados

As configurações de recuperação de dados ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da aplicação Tenable para sua instância Now Platform®. Para obter uma lista das configurações mais usadas, consulte Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable.

Classificação de prioridade de vulnerabilidade (VPR)

A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com uma nova calculadora de risco padrão em Resposta a vulnerabilidades. A Regra de risco da Tenable é instalada com a aplicação Integração de Resposta a vulnerabilidades com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade de Resposta a vulnerabilidades.

Esta regra de risco está desabilitada por padrão.

Ao habilitar a regra da calculadora de risco da Tenable, os valores de VPR importados são usados para calcular a pontuação de risco dos itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR = 70%, Ativo = 15% e Criticalidade dos negócios = 15%. Habilitar esta regra da Calculadora de risco da Tenable pode afetar o desempenho de ingestão de dados. Para obter mais informações sobre Resposta a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades calculadoras e a regra da calculadora de risco da Tenable, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Instalação e configuração

Depois de baixar o Integração de Resposta a vulnerabilidades com Tenable do ServiceNow® Store, a instalação e a configuração são compatíveis com o Assistente de configuração em Resposta a vulnerabilidades. Para obter mais informações, consulte Configuração de Resposta a vulnerabilidades usando o Assistente de configuração.

Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações

As integrações Integração de Resposta a vulnerabilidades com TenableTenable.io na aplicação [] estão disponíveis nas aplicações Resposta a vulnerabilidades e Conformidade de configurações.

Lista de Tenable.io integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente a partir do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura a aplicação Integração de Resposta a vulnerabilidades com Tenable no Assistente de configuração.

Tenable.io é uma integração empresarial baseada na nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com o produto Tenable.io.

A Tenable.io Integração de resultados de conformidade e a Tenable.io Integração de aterramento de resultados de conformidade estão inativas por padrão.

Para ativá-los:

1. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações da Tenable, clique no nome de uma integração para abrir o registro e marque a caixa de seleção **Ativo** para habilitá-lo. Você pode preferir deixar as configurações de programação em seus valores padrão para que essas integrações sejam iniciadas.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de ativos	• Recupera todos os dados de ativos, incluindo etiquetas de ativos, do produto Tenable.io e os processa em sua instância. • A partir da v3.0, se a integração de resultados de conformidade Tenable.io estiver ativada, você poderá importar dados de avaliação de configuração segura junto com os dados de ativos importados. Esses dados podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativos. • A saída desta integração são itens descobertos. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. • A partir da v2.2, *Last Scan Time* é importado e atualizado somente para ativos que têm vulnerabilidades.
Tenable.io Integração de resultados de conformidade	• A partir da versão 3.0, os dados importados de avaliação de configuração segura da Integração de resultados de conformidade junto com os dados importados da Integração de ativos podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Se habilitado, recupera dados de avaliação de configuração segura de alto nível e os processa em sua instância Now Platform. Os dados importados incluem resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas. • Dados de avaliação para ativos ausentes ou ativos sem IDs de ativo não são importados. • Se um resultado de testes for importado e o ativo correspondente não puder ser correspondido em sua instância, o resultado do teste será ignorado e o ID do ativo ausente será armazenado em um registro temporário na tabela [sn_vul_tenable_missing_asset]. • O valor total de ativos ignorados (ausentes) é listado no campo **ICs ignorados** na guia **Configuração** no registro de execução de integração para esta integração.
Tenable.io Integração de preenchimento de resultados de conformidade	• Quando ativada, essa integração é executada automaticamente depois que a integração de ativos é concluída com sucesso como parte de uma execução de integração encadeada. Esta integração corresponde aos dados de avaliação de configuração com ativos ausentes listados na tabela [sn_vul_tenable_missing_asset]. • Importa até 200 IDs de ativo para todos os ativos ausentes descobertos ou presentes na instância após a conclusão bem-sucedida da importação de integração de ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Remove os registros temporários da tabela [sn_vul_tenable_missing_asset] quando os ativos podem ser correspondidos com os dados de avaliação de configuração correspondentes.
Tenable.io Verificar integração de credenciais	• Esta integração recupera as credenciais de verificação configuradas em Tenable.io. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential],. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.io Integração de modelo	Um registro de modelo é enviado para Tenable.io durante uma nova verificação. Esta integração recupera Tenable.io credenciais disponíveis para usar em novas verificações. As credenciais são específicas da instância e um único registro de modelo é importado e armazenado com segurança temporariamente na tabela [sn_vul_tenable_io_template].
Tenable.io Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.io. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma execução de integração Tenable.io. • Esta importação garante que os Tenable.io Identificadores (Dez IDs) sejam atuais. • Coordena as chamadas de mensagem REST para a API do plug-in. • A saída desta integração são vulnerabilidades de terceiros.
Tenable.io Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de gravidade do produto Tenable.io e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **fixas**, mas os itens vulneráveis não serão criados para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	detecções **fixas** por padrão, porque a Tenable considera as vulnerabilidades **fixas** como **mitigadas**. • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidade fixa** estiver ativado no Assistente de configuração, novos IVs serão criados no estado **Fixo** para que você tenha visibilidade sobre as detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem na sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. Esta execução de integração está programada. É uma integração em cadeia, o que significa que depois que uma execução é concluída com sucesso, a integração de vulnerabilidades aberta descrita abaixo é acionada. A partir do Tenable v3.3, você pode exibir as seguintes informações para as execuções de integração de vulnerabilidade: • **Total de blocos:** número total de blocos gerados pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow
Tenable.io Integração de vulnerabilidades abertas	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.io Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de gravidade do produto Tenable.io e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são Itens vulneráveis (IVs) **novos/reabertos**. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. A Tenable considera as vulnerabilidades ativas **cumulativas** (atuais). • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. A partir do Tenable v3.3, você pode exibir as seguintes informações para as execuções de integração de vulnerabilidade: • **Total de blocos:** número total de blocos gerados pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow

Tenable.sc integrações com a aplicação Resposta a vulnerabilidades

As Tenable.sc integrações na aplicação Integração de Resposta a vulnerabilidades com Tenable.

A partir de Resposta a vulnerabilidades v20.0, se um ativo for verificado por um agente, a coluna Agente existe exibirá o valor verdadeiro na lista Itens descobertos, o que indica que se trata de uma verificação autentica.

Lista de Tenable.sc integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente a partir do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura a aplicação Integração de Resposta a vulnerabilidades com Tenable no Assistente de configuração.

- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de ativos	Para evitar a criação de itens descobertos duplicados com dados de ativos importados, a integração de ativos do produto Tenable.sc é composta por duas integrações. A Tenable.sc Integração de Ativos Abertos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Cumulativos** (atuais) ou **Abertos**. Os itens vulneráveis (IVs) criados em sua instância com esses dados de ativo importados são considerados abertos, ou seja, no estado **Aberto**. Esses itens vulneráveis requerem investigação e podem precisar de correção. A Tenable.sc integração de ativos fixos Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Mitigados** (não mais vulneráveis) ou **Corrigidos**. Os itens vulneráveis desses ativos fazem a transição do estado **Aberto** para o estado **Fechado/Corrigido** em sua instância, pois os resultados das verificações mostram que eles não estão mais vulneráveis. • Recupera todos os dados de ativos do produto Tenable.sc e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativos. • A saída desta integração são itens descobertos. • O filtro de consulta da Tenable selecionado no Assistente de configuração também se aplica à integração de ativos Tenable.sc. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.
Tenable.sc Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.sc. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma execução de integração Tenable.sc. • Esta importação garante que os Tenable.sc Identificadores (Dez IDs) sejam atuais e que somente as vulnerabilidades ativas sejam importadas. • Coordena as chamadas de mensagem REST para a API de plug-ins. • A saída desta integração são vulnerabilidades de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de gravidade do produto Tenable.sc e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **fixas**, mas os itens vulneráveis não serão criados para detecções **fixas** por padrão, porque a Tenable considera as vulnerabilidades **fixas** como **mitigadas**. • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidade fixa** é ativado no Assistente de configuração, ele cria novos IVs no estado **Fixo** para que você tenha visibilidade sobre as detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem na sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. Esta execução de integração é uma execução programada. É uma integração em cadeia, o que significa que, depois que uma execução é concluída com sucesso, a Tenable.sc Integração de vulnerabilidades abertas descrita abaixo é acionada. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de vulnerabilidades abertas	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.sc Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de consulta selecionados no produto Tenable.sc e os processa em sua instância. • Cria itens vulneráveis correspondentes para vulnerabilidades ativas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	• Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é **Atualizar/Criar novos** itens vulneráveis (IVs), caso eles ainda não existam. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Verificar integração de credenciais	• Esta integração recupera as credenciais de verificação configuradas em Tenable.sc. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.sc Integração de vulnerabilidades de preenchimento	• Esta integração de aterramento importa todas as vulnerabilidades abertas e corrigidas que possam ter sido perdidas durante uma importação. • Esta integração importa vulnerabilidades abertas e corrigidas dos últimos sete dias para atualizar suas detecções e itens vulneráveis. • Esta integração pode afetar seu desempenho. • Esta integração está desabilitada por padrão. • Para atualizar seus dados de vulnerabilidade e evitar possíveis problemas de desempenho, talvez você prefira programar as Integrações de vulnerabilidades corrigidas e abertas do Tenable.sc para serem executadas quando nenhuma outra verificação estiver em execução. • A saída desta integração é:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	◦ Itens vulneráveis (IVs)**encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. ◦ para **atualizar/criar novos** itens vulneráveis (IVs) se eles ainda não existirem. Ele também cria itens de configuração e entradas de terceiros se eles não existirem.

Autenticação de usuário e Tenable.sc

A autenticação de usuário é compatível com sua instância Now Platform® e a versão 5.13 do produto Tenable.sc. A autenticação de usuário será necessária se você estiver usando a versão 5.12 e anterior do produto Tenable.sc.

Quando você seleciona a autenticação de usuário para as integrações Tenable.sc, os tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de Execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, `Erro: falha na validação de token`. Nenhuma ação será necessária se esta mensagem for exibida. Os tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro no processo de integração.

Preparação para a integração de vulnerabilidade da Tenable

Prepare-se para a integração de vulnerabilidade ServiceNow® da Tenable executando as seguintes tarefas de configuração.

Antes de começar

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Para uma instalação e configuração tranquilas da aplicação Integração de Resposta a vulnerabilidades com Tenable, talvez você prefira imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para sua instância Now Platform®.

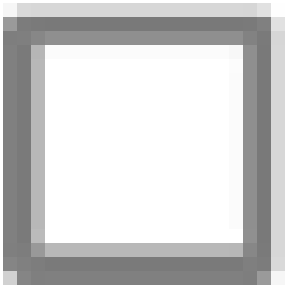
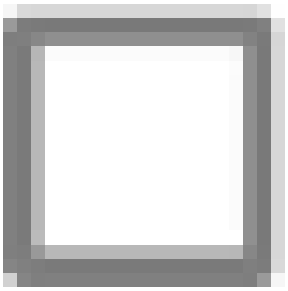
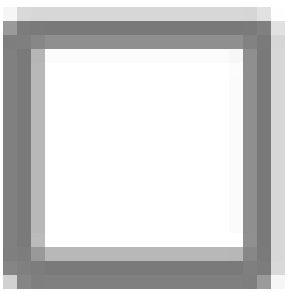
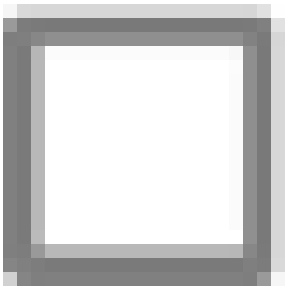
Nota: Se você estiver importando dados com a integração criada pela Tenable e quiser começar a usar a Integração de resposta a vulnerabilidades ServiceNow® com a Tenable, consulte

Para obter informações atuais de limpeza e migração de dados da integração criada pela Tenable para a integração criada por ServiceNow, consulte o artigo Diretrizes para migrar da Integração de resposta a vulnerabilidades da Tenable para a Integração de resposta a vulnerabilidades da ServiceNow com a Tenable [KB0960667] .

Função necessária: administrador para baixar e instalar a aplicação.

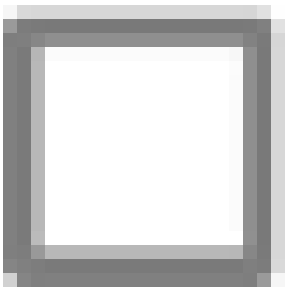
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte, Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 12.1 de Resposta a vulnerabilidades ou posterior.
	Se você ainda não o tiver em sua instância, obtenha direitos e baixe a aplicação Integração de Resposta a vulnerabilidades com Tenable para sua instância Now Platform®. A aplicação Integração de Resposta a vulnerabilidades com Tenable é compatível com o produto Tenable.sc a partir da versão 5.13. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou precisar de assistência, entre em contato com o ServiceNow® Suporte técnico.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. administrador O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. sn_vul.vulnerability_admin Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das integrações da Tenable. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Configura todas as aplicações e regras de VR e configura integrações de terceiros. sn_vul_tenable.configure_integration

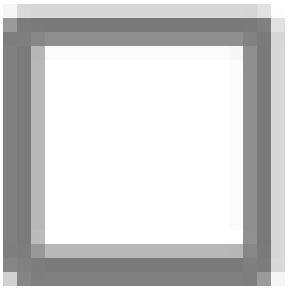
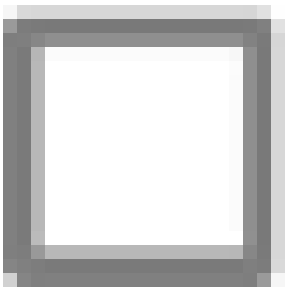
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Pode configurar a integração de vulnerabilidade da Tenable. Esta função contém a função granular sn_vul_tenable.read_integration. sn_vul_tenable.read_integration Pode exibir (ler) registros da integração de vulnerabilidade da Tenable. Grupo de Resposta a vulnerabilidades Por padrão, o grupo de Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos no Assistente de configuração para a integração. Por padrão, o grupo de Resposta a vulnerabilidades está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Consulte Criação de um grupo de usuários . Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.
	Para promover um desempenho aprimorado para sua primeira importação, talvez você prefira desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não as usar. Essas calculadoras, além de qualquer outra que você tenha definido, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Consulte Desabilitar calculadoras de vulnerabilidade. • Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, talvez você prefira Desabilitar regras de negócio relacionadas a notificações, conforme descrito em Importar modificações para a integração de vulnerabilidade da Tenable.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. • Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Integração de Resposta a vulnerabilidades com Tenable e sua instância Now Platform estiverem no mesmo ambiente. Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . • Verifique se o plug-in IntegrationHub está instalado e ativado. Este plug-in permite que os componentes do sistema de base chamem sistemas externos usando APIs de integração e ative etapas de protocolo como REST. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.
	Obter credenciais da Tenable. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seus produtos Tenable para que você tenha acesso a eles. Tenable.io requer acesso de administrador com um atributo de permissão maior ou igual a 64. Tenable.sc requer acesso de analista de segurança ou gerente. **Nota:** A partir da v3.8 de Integração de Resposta a vulnerabilidades com Tenable, o acesso a Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

Você está pronto para Instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable usando o Assistente de configuração.

Instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable usando o Assistente de configuração

Antes de executar a ServiceNow® Tenable Vulnerability Integration, você precisa baixar a aplicação Integração de Resposta a vulnerabilidades com Tenable da ServiceNow Store, instalar e configurar usando o Assistente de configuração na aplicação Resposta a vulnerabilidades.

Antes de Iniciar

Antes de instalar a aplicação Tenable, verifique se você concluiu todos os itens na check-list em Preparação para a integração de vulnerabilidade da Tenable.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Tenable no Assistente de configuração. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) para configurar a aplicação no Assistente de configuração após sua instalação.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Depois de alguns momentos, as aplicações que estão disponíveis para instalação em sua instância são exibidas.

2. Localize o bloco **Tenable (Plataforma Tenable)** e clique em **Instalar**.

   Esta ação instala a aplicação Integração de Resposta a vulnerabilidades com Tenable que você baixou de ServiceNow Store.

3. Siga os avisos fornecidos no Assistente de configuração para continuar com a instalação.
4. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de integração>Integrações do scanner** no Assistente de configuração para continuar com a configuração. Se você quiser obter mais informações para complementar os avisos fornecidos no Assistente de configuração, consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração.

Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable

As configurações de recuperação de dados a seguir ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da ServiceNow® Integração de vulnerabilidade da Tenable para sua instância Now Platform®.

As configurações descritas nas seções a seguir ajudam a controlar os dados que você deseja importar. Além disso, você pode definir os valores desses filtros em Instâncias de integração. Para exibir instâncias de integração, navegue até **Integração de vulnerabilidade Tenable** > **Instâncias de Integração** e clique na sua integração, Tenable.io ou Tenable.sc.

Na página Instância de integração exibida, clique em Parâmetros de instância de integração para exibir uma lista de parâmetros ou nas guias Integrações de vulnerabilidade para uma programação, Detalhes de REST, Detalhes de integração, Fontes de dados e informações de execução de integração.

Configurações e filtros comuns de gravidade e recuperação para Tenable.io e Tenable.sc em sua instância Now Platform

As configurações a seguir estão disponíveis para as integrações Tenable.io e Tenable.sc em sua instância Now Platform. Essas e outras definições de configuração são exibidas na página Instância de integração da sua instância Now Platform. Você pode preferir deixar essas configurações em seus padrões para as primeiras execuções de integração.

Tenable.io

inserir_fixo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

severidade_crítica

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade crítica das Tenable.io Integrações de Vulnerabilidades Abertas e Tenable.io Vulnerabilidades Corrigidas.

gravidade_alta

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade de alto nível das Tenable.io Integrações de Vulnerabilidades Abertas e Tenable.io Vulnerabilidades Corrigidas.

gravidade_média

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade média das integrações de Tenable.io vulnerabilidades abertas e Tenable.io vulnerabilidades fixas.

sever_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade no nível de informação das integrações de Tenable.io vulnerabilidades abertas e Tenable.io vulnerabilidades fixas.

severidade_baixa

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade baixa das integrações de Tenable.io vulnerabilidades abertas e Tenable.io vulnerabilidades fixas.

tamanho

Esta configuração define o número de registros de plug-in a serem incluídos no conjunto de resultados da Tenable.io Integração de plug-ins. Deve estar no formato int32. O valor padrão é 1.000. O tamanho máximo é 10.000.

num_assets

O número máximo de vulnerabilidades por bloco exportado das Tenable.io Integrações de Vulnerabilidades Corrigidas e Tenable.io de Vulnerabilidades Abertas. O valor padrão é 50.

chunk_size

Especifica o número de ativos por bloco exportado pela Tenable.io Integração de ativos. O padrão é 1.000.

Tenable.sc

assíncrono_request

Este parâmetro está inativo por padrão (falso). Habilite ou desabilite este parâmetro para fazer chamadas de API assíncronas ou síncronas com Tenable.sc, respectivamente. Para chamadas síncronas, se houver um tempo limite de 30 segundos, entre em contato com o suporte do produto Tenable para ajustar a caixa. Este parâmetro, uma vez habilitado, é aplicável a todas as integrações de Tenable.sc. Para clientes existentes que usam chamadas assíncronas, um script de correção está disponível, o que adiciona um novo parâmetro async_request às instâncias de integração Tenable.sc existentes. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Scripts de correção**.

inserir_fixo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

deslocamento

Especifica o número de ativos, plug-ins e vulnerabilidades importados em uma execução de integração.

Filtros de consulta

Os filtros de consulta são configurados no console da Tenable. Esses filtros de consulta têm IDs que podem ser selecionados no Assistente de configuração ou na página Instâncias de integração em sua instância Now Platform. Esses filtros são aplicados ao recuperar os dados das integrações Tenable.sc.

Mensagens de REST para a integração de vulnerabilidade da Tenable

As ServiceNow® mensagens REST de integração de vulnerabilidade da Tenable são usadas para fazer chamadas para a API da Tenable.

Tenable.io Mensagem REST de ativos

A mensagem Tenable.io Assets REST recupera informações de ativos para a integração de ativos Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de ativos. O trabalho de exportação de ativos é enviado com os seguintes filtros:

- "is_deleted": falso
- "is_licensed": verdadeiro

Tenable.io Mensagem REST de plug-ins

A mensagem REST Tenable.io de plug-ins recupera informações de plug-in para a integração de plug-in Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de plug-ins.

Tenable.io Mensagem REST de vulnerabilidades

A mensagem Tenable.io de REST de vulnerabilidades recupera informações de vulnerabilidade para vulnerabilidades abertas e fechadas da integração de vulnerabilidade Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de vulnerabilidades.

Mensagem REST de consultas da Tenable.sc

A mensagem de REST de consultas do Tenable.sc recupera as informações do filtro de consulta para a integração de ativos do Tenable.sc e a integração de vulnerabilidades do Tenable.sc em que o filtro de consulta está configurado.

Tenable.sc Mensagem REST de plug-ins

A mensagem REST de plug-in Tenable.sc recupera informações de plug-in para a integração de plug-ins Tenable.sc. As mudanças no registro do método Obter plug-ins da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar informações de plug-ins.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do parâmetro	Valor	Descrição
tipo	ativo	Indica a origem da qual a Tenable extrai dados. Usado pelo código. Mudanças não são recomendadas.
campos	id, descrição, cvssVector,cvssV3Vector, cvssV3TemporalVector, sinopse, cvssVector, baseScore, temporalScore, cvssV3Vector, cvssV3BaseScore, cvssV3TemporalVector, name, vprScore, vprContext, plug-inPubDate, plug-inModDate, xrefs, família, riscoFator, cpe, vprContext, plug-inPubDate, plug-inModDate, xrefs, família, riscoFator, cpeArame, soluções para trabalho, explorar tipo, direitos autorais, versão, sourceFile, dependências, necessáriosPorts, necessáriosUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stígSeverity, patchPubDate, patchModDate, vulnPubDate, modificadoTempo, md5	Indica a lista de campos importados da Tenable.

Tenable.sc Mensagem REST de vulnerabilidades

A mensagem REST Tenable.sc de vulnerabilidades recupera informações de vulnerabilidade da integração Tenable.sc. As mudanças na mensagem REST do método Buscar vulnerabilidades ou Buscar vulnerabilidades corrigidas ou, a partir da versão v14.0 Resposta a vulnerabilidades e v2.2 da Integração de vulnerabilidades da Tenable, Buscar registro de vulnerabilidades de preenchimento afetam as solicitações feitas a Tenable.sc para recuperar informações de vulnerabilidades.

Tenable.sc Verificar mensagem REST de credenciais

Tenable.sc Mensagem de REST da política

A mensagem POST REST da política Tenable.sc adiciona uma política para os plug-ins solicitados. A política gerada será usada em Tenable.sc solicitações de verificação.

Tenable.sc Verificar mensagem REST

A mensagem POST REST de verificação do Tenable.sc adiciona uma verificação que depende do acesso e da permissão definidos no corpo da solicitação da mensagem REST. Ele usa política, ID de plug-in e IP(s) no corpo da solicitação para a solicitação de verificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.sc Mensagem REST do resultado da verificação

A mensagem Tenable.sc Resultado da verificação GET REST fornece detalhes da verificação gerada usando a mensagem Scan REST. Ele usa o scanResultId na resposta das mensagens REST de verificação e recupera detalhes da verificação acionada.

Tenable.sc Verificar credenciais

A mensagem REST Tenable.sc de verificação de credenciais recupera as informações de credenciais de Tenable.sc. As mudanças no registro do método "Importar" da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar as informações de credenciais.

Nome do parâmetro	Valor	Descrição
campos	ID, nome, descrição, tipo	Indica a lista de campos importados de Tenable.sc
filtros	utilizável	Indica que a integração extrai somente credenciais utilizáveis de Tenable.sc Mudanças em qualquer um dos parâmetros não são recomendadas.

Transformação de dados para a integração de vulnerabilidade da Tenable

Depois de identificar os dados a serem importados, eles são recuperados do produto Tenable e processados por meio de um conjunto de fontes de dados e transformações em sua instância.

Durante a instalação, os mapas de severidade normalizada são instalados no módulo Mapeamento de severidade normalizada. Esses mapas transformam os níveis de severidade importados da Tenable em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de severidade, consulte Criar um mapa de severidade da Resposta a vulnerabilidades na documentação Resposta a vulnerabilidades.

Importação de ativo da Tenable.io

Os dados de ativos importados são carregados primeiro na tabela Importação de ativos do Tenable.io [sn_vul_tenable_io_asset_import].

O mapa de transformação de integração de ativos da Tenable.io é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de ativos da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise `Tenable.io Asset Transform`.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
u_id	source_id	A Tenable fornece um ID exclusivo para ativos e

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
		mapas para o registro do item descoberto e é usado para pesquisa de IC.
u_ipv4s	ip_address	Mapeia o primeiro valor de IP para o campo ip_address no registro de item descoberto.
u_mac_address	mac_address	Mapeia o primeiro valor de mac_address para o campo de endereço mac no registro de item descoberto.
u_fqdns	fqdn	Mapeia o primeiro valor de fqdn para o campo fqdn no registro de item descoberto.
u_netbios_names	netbios	Mapeia o primeiro valor netBIOS para o campo netBIOS no registro do item descoberto.
u_operating_systems	os	Mapeia o primeiro valor de SO para o campo de SO no registro de item descoberto.
(Antes da v 14.0 Resposta a vulnerabilidades e v2.2 da Integração de vulnerabilidade da Tenable)u_last_scan_time	última_scan_date	Mapeia para o campo last_scan_date no registro do item descoberto.
u_last_authenticated_scan_date	last_auth_scan_date	Mapeia para o campo last_auth_scan_date no registro do item descoberto.
[script]	nome	Mapeia o nome do host usando a lógica do script.
u_tags		Os marcadores são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo e finalidade do script do mapa de transformação de ativo da Tenable.io

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Uma função usada para atualizar valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Integração de plug-ins Tenable.io

O mapa de transformação de plug-ins do Tenable.io é usado para transformar plug-ins importados do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados recebidos dos plug-ins da Tenable são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise a transformação do plug-in Tenable.io.

A carga dos plug-ins da Tenable.io contém todos os campos na coluna u_attributes da tabela sn_vul_tenable_io_plugin_import. O campo de atributos é analisado e mapeado para os registros da tabela de entrada de terceiros, conforme listado na tabela a seguir.

Campo de origem	Campo de destino	Descrição
ID	ID	Mapeia o ID da origem e adiciona o prefixo TEN- a ele. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
Descrição	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	A origem do TPE importado é Tenable.io.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família	categoria	Mapeia a família do plug-in para a coluna de categoria

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
plug-in_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
plug-in_publication_date	date_published	Mapeia o plugin_publication_date para a data de publicação.
tem_patch	correção_tipo	Mapeia o tipo de correção do valor has_patch.
synopsis	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
cvss_base__pontuação	pontuação	Mapeia a pontuação base de cvss para a coluna de pontuação na tabela de entrada de terceiros.
solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
exploit_available	exploração	Mapeia o exploit_available fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros
pontuação.vpr	pontuação_risco_origem	Mapeia a pontuação de vpr fornecida pelo scanner para o source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para a coluna age_of_vuln na tabela de entrada de terceiros.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		na tabela de entrada de terceiros.
vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
vpr.drivers.threat_sources_last28	ameaças_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para o Threat_sources na tabela de terceiros.
vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.
vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_reCency na tabela de entrada de terceiros.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto cvss3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
pontuação_temporais_cvss	pontuação_temporais_cvss	Mapeia a pontuação temporal do CVSS v2.
cvss_v3_pontuação_temporais	v3_tempo_pontuação	Mapeia a pontuação temporal do CVSS v3.
risk_factor	gravidade_origem	Mapas para a severidade de origem na tabela de entrada de terceiros.
nome	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
sting_severity	sting_severity	Mapeia a pontuação de vpr fornecida pelo scanner para o source_risk_score na tabela de entrada de terceiros.
plug-in_type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor para a coluna unsupported_by_vendor.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base nas colunas exploit_available e v3_attack_vector.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados ao CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como uma referência.
[script]	A lista de explorações para esse plug-in e insere o mapeamento da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Uma função usada para atualizar os valores na entrada de terceiros e verificar se a entrada de terceiros já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A inclusão de script TenableIOPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.io e a transforma em Now Platform entradas de vulnerabilidade de terceiros. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados dos plug-ins Tenable.io na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.io

O mapa de transformação de item vulnerável do Tenable.io é usado para transformar informações de vulnerabilidades abertas e fixas importadas do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades da Tenable são processados.

O mesmo mapa de transformação é usado para a integração de vulnerabilidades fixas do Tenable.io e a integração de vulnerabilidades abertas do Tenable.io. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise o `mapa de transformação de item vulnerável da Tenable.io`.

Campo de origem	Campo de destino	Descrição
u_asset.uuid	ID	Uuid é mapeado para o campo de ID do registro cmdb_ci.
u_asset.ipv4	ip_address	O campo IPv4 é mapeado para o campo de endereço IP do registro cmdb_ci.
u_asset .last_authenticated_results	last_auth_scan_date	A data da última verificação autenticada é mapeada para a data da última verificação autenticada do registro cmdb_ci.
u_ativo.mac_addess	mac_address	O endereço MAC é mapeado para o campo de endereço MAC do host do registro cmdb_ci.
u_asset.netbios_name	netbios	O NetBIOS é mapeado para o campo netBIOS do registro cmdb_ci.
u._plugin.cvss3_base_score	v3_base_score	A pontuação base do CVSS v3 é mapeada para a pontuação base v3 do registro de entrada de terceiros.
u._plugin.cvss3_tempo_score	v3_tempo_pontuação	A pontuação temporal do CVSS v3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u._plugin.cvss_base_score	pontuação	A pontuação base do CVSS é mapeada para o campo de pontuação do registro de entrada de terceiros.
u._plugin.cvss_tempo_score	pontuação_ temporal	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_plugin.description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada de terceiros.
u_plugin.family	categoria	Mapeia a família do plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plugin.modification_date	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_plugin.publication_date	date_published	A data de publicação é mapeada para o campo de data de publicação do registro de entrada de terceiros.
plug-in.risco_fator	gravidade_origem	O fator de risco é mapeado para o campo source_severity do registro de entrada de terceiros.
u_plugin.solução	solução	A solução é mapeada para o campo de solução do registro de entrada de terceiros.
u_plugin.sinopsis	ameaça	A sinopse é mapeada para o campo de ameaça do registro de entrada de terceiros.
u_severity_id	prioridade	A prioridade é mapeada para o ID de severidade da carga. O valor padrão é 5.
u_plugin.exploit_available	exploração	Mapeia o exploit_available

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
pontuação.vpr	pontuação_risco_origem	Mapeia a pontuação de vpr fornecida pelo scanner para o source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_plugin.vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_sources_last28	ameaças_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para Threat_sources na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plugin.vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_reCency na tabela de entrada de terceiros.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS3 v3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
u_plugin.type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor no plug-in para a coluna unsupported_by_vendor.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base nas colunas exploit_available e v3_attack_vector.
u_plugin.family_id	ID da família	Mapeia o ID de família do plug-in para a colunafamily_id na tabela de entrada de terceiros.
porta	porta	A porta é mapeada para o campo de porta do registro de item vulnerável.
protocolo	protocolo	O protocolo é mapeado para o campo de protocolo do registro de item vulnerável.
u_first_found	first_found	Primeiro encontrado é mapeado para o primeiro campo encontrado do registro de item vulnerável.
u_last_found	último_encontrado	O último encontrado é mapeado para o último campo encontrado do registro do item vulnerável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_state	estado	O estado é mapeado para o campo Estado no registro do item vulnerável
[script]	origem	A origem da integração está preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.io como origem.
[script]	integração_instance	O integration_instance é o nome da instância da qual o item vulnerável é importado.
u_plugin.name	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
u_plugin.sting_severity	sting_severity	Mapeia a severidade de sting do plug-in para a coluna de severidade de sting na tabela de entrada de terceiros

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados ao CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como uma referência.
[script]	A lista de explorações desse plug-in e o mapeamento de inserções da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação aciona o TenableIOVulnerabilitiesProcessor, que importa dados do Tenable.io usando o conjunto para importação e carrega cada registro na tabela de IC do CMDB, na tabela de itens vulneráveis e na tabela de vulnerabilidade de terceiros. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Uma função para verificar se a entrada e as detecções de terceiros já existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para atualizar a contagem de ICs, IVs e Detecções conforme importados do Tenable.io. Para uso interno. Não é recomendável modificar ou excluir.

Importação de ativo da Tenable.sc

Os dados de ativos importados do Tenable.sc são carregados primeiro na tabela Importação de ativos do Tenable.sc (sn_vul_tenable_sc_asset_import). O mapa de transformação de integração de ativos da Tenable.sc é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de ativos da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise a `transformação de ativo Tenable.sc`.

Campo de origem	Campo de destino	Descrição
u_uuid	ID	O UUID não é preenchido pela API da Tenable, portanto, o atributo "u_uniqueness" é usado para criar um campo UUID exclusivo para ativos e mapeá-lo para o registro cmdb_ci.
u_ip	ip_address	Mapeia o campo IP da API para o campo ip_address em um registro cmdb_ci.
u_macaddress	mac_address	Mapeia o campo de endereço eletrônico da API para o campo de endereço no registro cmdb_ci.
u_dnsname	fqdn	Mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_netbiosname	netbios	Mapeia o campo netBIOS da API para o campo netBIOS no registro cmdb_ci.
u_oscpe	os	As informações do sistema operacional são extraídas do atributo oscpe na carga e mapeadas para o campo do sistema operacional no registro cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mapeia o campo lastauthrun da API para o campo last_auth_scan_date no registro do item descoberto.
u_lastauthrun e u_lastauthrun	última_scan_date	O lastauthrun é extraído da API da Tenable ou lastauthrun. Com base no valor que aparece na carga útil, o campo last_scan_date no registro do item descoberto é preenchido.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Função usada para atualizar os valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Importação de plug-ins Tenable.sc

Os dados de plug-ins importados do Tenable.sc são carregados primeiro na tabela de importação de plug-ins do Tenable.sc (sn_vul_tenable_sc_plugin_import). O mapa de transformação do plug-in Tenable.sc é usado para transformar as informações de plug-in que foram importadas. As mudanças nesta transformação alteram como os dados de importação do plug-in Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise o mapa de transformação do `plug-in Tenable.sc`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_id	ID	Mapeia o ID da origem e adiciona o prefixo TEN-. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
u_description	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	O TPE importado desta integração tem o Tenable.sc como origem.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família_u	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria.
u_plugin_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
u_plugin_publication_date	date_published	Mapeia o plugin_publication_date para a data de publicação.
u_has_patch	Tipo_de_correção	Mapeia o tipo de correção do valor has_patch.
sinopse_u	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
u_cvss_pontuação_base	pontuação	Mapeia a pontuação base do CVSS para a coluna de pontuação na tabela de entrada de terceiros.
u_solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
u_cvss_pontuação_temporais	pontuação_temporais_cvss	Mapeia a pontuação temporal do CVSS v2.
u_cvss_v3_tempo_score	v3_tempo_pontuação	Mapeia a pontuação temporal do CVSS v3.
u_risk_factor	severidade de origem	Mapas para a severidade de origem na tabela de entrada de terceiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_cvss_v3_base_score	v3_base_score	Mapeia a pontuação base do CVSS na tabela de entrada de terceiros.
u_exploit_available	exploração	Mapeia o exploitAvailable fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
pontuação_u_vpr	pontuação_risco_origem	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id="threat_sources_last_28"]	ameaça_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.
u_vpr_context[id="threat_intensity_last_28"]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id="threat_recency"]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		Threat_reCency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_name	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_sting_severity	sting_severity	Mapeia o campo stíg_severity no plug-in para stíg_severity na tabela de entrada de terceiros.
u_check_type	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in "family_id" para "family_id" na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base nas colunas exploit_available e v3_attack_vector.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
u_cpe	A lista de CPEs é adicionada como uma referência.
u_ver_também	A lista de URLs é adicionada como uma referência.
u_exploit_frameworks	A lista de explorações para esse plug-in e insere o mapeamento da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Função usada para atualizar os valores na entrada de terceiros e verificar se a entrada de terceiros já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de plug-ins criados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

A inclusão de script TenableSCPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.sc e a transforma em entradas de vulnerabilidade de terceiros da ServiceNow. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados de plug-ins Tenable.sc na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.sc

O mapa de transformação de vulnerabilidades abertas do Tenable.sc é usado para transformar dados importados da integração de vulnerabilidades abertas do Tenable.sc, e o mapa de transformação de vulnerabilidades fixas e Tenable.sc é usado para transformar dados importados da integração de vulnerabilidades fixas do Tenable.sc.

Nota: As mudanças nesses mapas de transformação alteram como os dados da importação de vulnerabilidades fixas/abertas da Tenable são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e corrigidas do Tenable.sc, navegue até **Integração de vulnerabilidade Tenable** > **Administração** > **Instâncias de Integração** > **Tenable.sc Integração de vulnerabilidades fixas/abertas** > **Fontes de dados** > **Vulnerabilidades abertas/corrigidas do Tenable.sc** > **Transformações**.

Campo de origem	Campo de destino	Descrição
u_pluginID	Id	Usado como o identificador do plug-in. Este campo é mapeado para o ID do plug-in no registro de entrada de terceiros.
u_riskfactor	gravidade_origem	Este campo é mapeado para source_severity no registro de entrada de terceiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
gravidade_u	prioridade	O campo de prioridade é mapeado com a gravidade. O valor padrão é 5.
u_hasbeenmitigado	estado	Hasbeenmitigado é mapeado para o campo de estado do registro de vulnerabilidade. Para a integração de vulnerabilidades corrigidas, todos os IVs estão no estado "Encerrado".
u_ip	ip_address	O endereço IP é mapeado para o campo de IP do host da tabela cmdb_ci.
u_port	porta	A porta é mapeada para o campo de porta do registro de item vulnerável.
u_protocol	protocolo	O protocolo está mapeado para o campo de porta do registro de item vulnerável.
u_firstVisto	first_found	O primeiro valor visto é mapeado para o primeiro campo encontrado do registro VI.
u_lastVisto	último_encontrado	O último valor visto é mapeado para o último campo encontrado do registro VI.
u_exploitDisponível	exploração	ExploitAvailable é mapeado para o campo de exploração no registro de entrada de terceiros.
sinopse_u	ameaça	A sinopse é mapeada para o campo de ameaça no registro de entrada de terceiros.
u_description	resumo	A descrição é mapeada para o campo de resumo no

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		registro de entrada de terceiros.
u_solução	solução	A solução é mapeada para o campo de solução no registro de entrada de terceiros.
u_basescore	pontuação	BaseScore é mapeado para o campo de pontuação no registro de entrada de terceiros.
Pontuação_temporal	pontuação_ temporal	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_cvssv3basescore	v3_base_score	Cvssv3basescore é mapeado para a pontuação base v3 no registro de entrada de terceiros.
u_cvsspontuação temporal	v3_tempo_pontuação	A pontuação temporal Cvssv3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.
u_pluginpublicar	date_published	A data de publicação do plug-in é mapeada para a data de publicação do plug-in no registro de entrada de terceiros.
u_pluginmoddate	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_dnsname	fqdn	DnsName é mapeado para o campo FQDN do registro cmdb_ci.
u_macaddress	mac_address	MacAddress é mapeado para o campo mac_address do registro cmdb_ci.
u_netbiosNome	netbios	O NetBIOSName é mapeado para o

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		campo NETBIOS do registro cmdb_ci.
u_ip	ip	O IP está mapeado para o campo IP do registro cmdb_ci.
hostUniqueness	uuid	A exclusividade do host não é mapeada para nenhum campo, mas é usada para determinar o UUID do host.
família_u	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plugintext	prova	O texto do plug-in é mapeado para a prova no registro de TPE.
[script]	origem	A origem da integração está preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.sc como origem.
[script}	integração_instance	O integration_instance é o nome da instância da qual o item vulnerável é importado.
pontuação_u_vpr	pontuação_risco_origem	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		• 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id="threat_sources_last_28]	ameaças_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.
u_vpr_context[id="threat_intensity_last_28]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id="threat_recency"]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_reCency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_pluginname	nome	Mapeia o nome do plug-in para a coluna

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		de nome na tabela de entrada de terceiros.
gravidade_ust	sting_severity	Mapeia o campo stíg_severity no plug-in para stíg_severity na tabela de entrada de terceiros.
u_checktype	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in "family.id" para "family_id" na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela third_party_entry é preenchida com base nas colunas exploit_available e v3_attack_vector.

Campo de origem	Descrição
u_cve	Insere dados relacionados ao CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento é encontrado em sn_vul_m2m_entry_cve.
u_bid	A lista de traqs de erros é adicionada como uma referência.
u_cpe	A lista de CPEs é adicionada como uma referência.
u_seetambém	A lista de URLs é adicionada como uma referência.
u_xrefs	A lista de X-REFs é adicionada como uma referência.
u_exploitframeworks	A lista de explorações desse plug-in e o mapeamento de inserções da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Função usada para atualizar os valores na vulnerabilidade e verificar se a vulnerabilidade já existe. Com base nos resultados, modifica os valores em uma tabela de itens vulneráveis. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos IVs criados e VIs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Definir parâmetros de filtro adicionais para Tenable.io importações

Personalize os parâmetros de filtragem das suas consultas programadas com Integrações de vulnerabilidade da Tenable para ajudá-lo a refinar ainda mais os dados de vulnerabilidade importados com o produto Tenable.io.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para que você possa revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por *cidr_range*, *num_assets*, *indexed_at*e *plugin_family*. Ou digamos que você queira executar uma integração Tenable.io, de modo que uma execução importe somente vulnerabilidades críticas a cada quatro horas e outra seja executada a cada 24 horas para buscar todas as outras vulnerabilidades não críticas.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros compatíveis com a Tenable para ajudá-lo a importar os detalhes específicos da vulnerabilidade necessários.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com parâmetros Tenable em seu Now Platform. As seguintes integrações Tenable.io oferecem suporte à filtragem fornecendo conteúdo JSON no corpo da solicitação:

- Integração de ativos
- Integração de vulnerabilidade fixa
- Integração de vulnerabilidades abertas

Você deve saber como usar cadeias de caracteres JSON para este recurso.

Função necessária: sn_vul.vulnerability_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

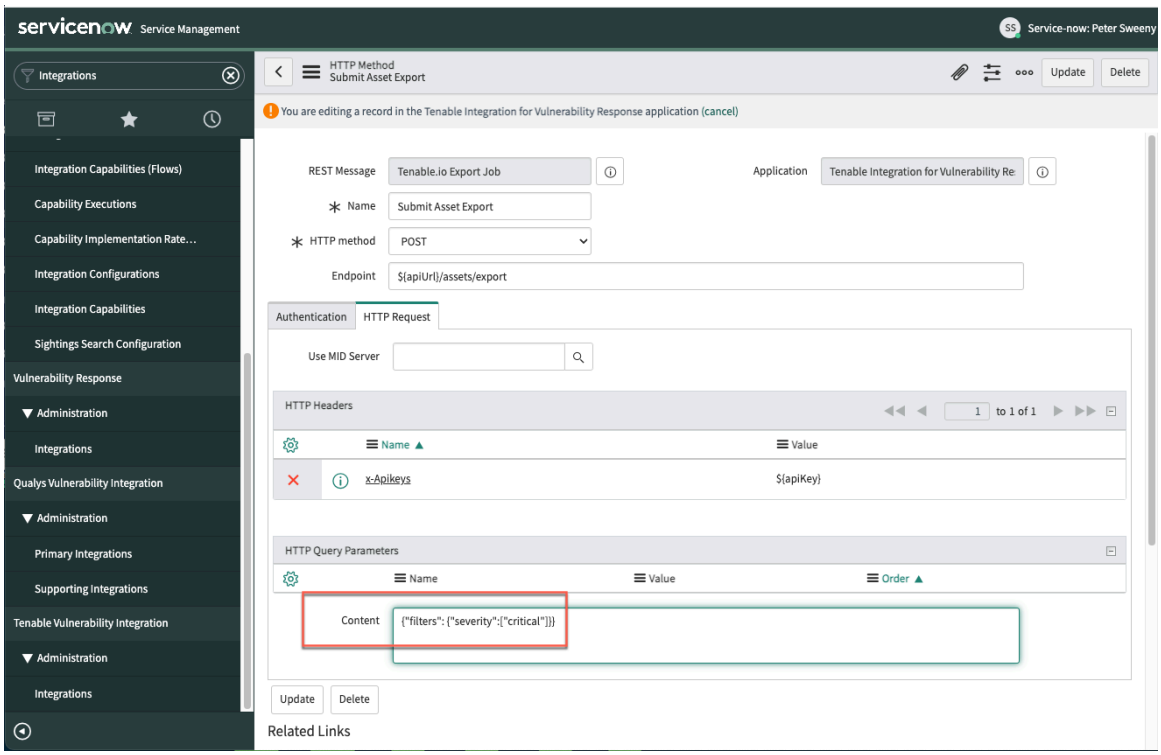
Procedimento

1. Localize os parâmetros compatíveis com o produto Tenable.io no site do desenvolvedor que você deseja usar para a filtragem.

   Os parâmetros e valores inseridos no produto Tenable.io são compatíveis somente no nível da instância de integração.

2. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
3. Na página da lista Integrações da Tenable, clique no registro da integração Tenable.io que você deseja abrir.
4. Com a guia Métodos REST da Tenable selecionada, clique no ícone de informações (I) para o método REST, seguido por **Abrir registro**.
5. Selecione a guia **Solicitação HTTP**.
6. Para editar o registro, na parte superior da página, clique no link em. Para editar o registro, clique **aqui**.
7. No registro Método REST no campo Conteúdo, insira o conteúdo JSON que você deseja como parte do corpo da solicitação.

   Na imagem a seguir, como exemplo, o parâmetro de severidade para vulnerabilidades importadas, `{"filters": {"severity": ["critical"]}}` foi personalizado para a integração de Tenable.io ativos. Este valor importa somente vulnerabilidades críticas (pontuação de CVSS de 10,0).



   Se você quiser inserir mais de um parâmetro, consulte a documentação Tenable.io para obter mais informações sobre como separar cada valor.

8. Clique em **Atualizar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Emissão de relatórios de integração de vulnerabilidade da Tenable

Exiba relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Resposta a vulnerabilidades.

Visualizações de dados nos espaços Resposta a vulnerabilidades

Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços, Explorar o Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Versões anteriores de Resposta a vulnerabilidades

O painel de visão geral da Resposta a vulnerabilidades (Gestão de vulnerabilidades) fornece uma exibição executiva das vulnerabilidades e itens vulneráveis, ajudando o Administrador de vulnerabilidades a identificar rapidamente as áreas de preocupação. O painel de correção da Resposta a vulnerabilidades (Correção de vulnerabilidades) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Para obter mais informações, consulte Usando os painéis padrão Resposta a vulnerabilidades.

Função necessária: responsável pela correção.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

para exibir o painel, navegue até **Resposta a vulnerabilidades** > **Visão Geral da Correção**.

Gráfico de status de execução de integração para a integração de vulnerabilidade da Tenable

O módulo Status da execução de integração da Tenable fornece uma exibição gráfica do status das execuções de integração da Tenable.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer parte do gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: administrador de vulnerabilidade.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

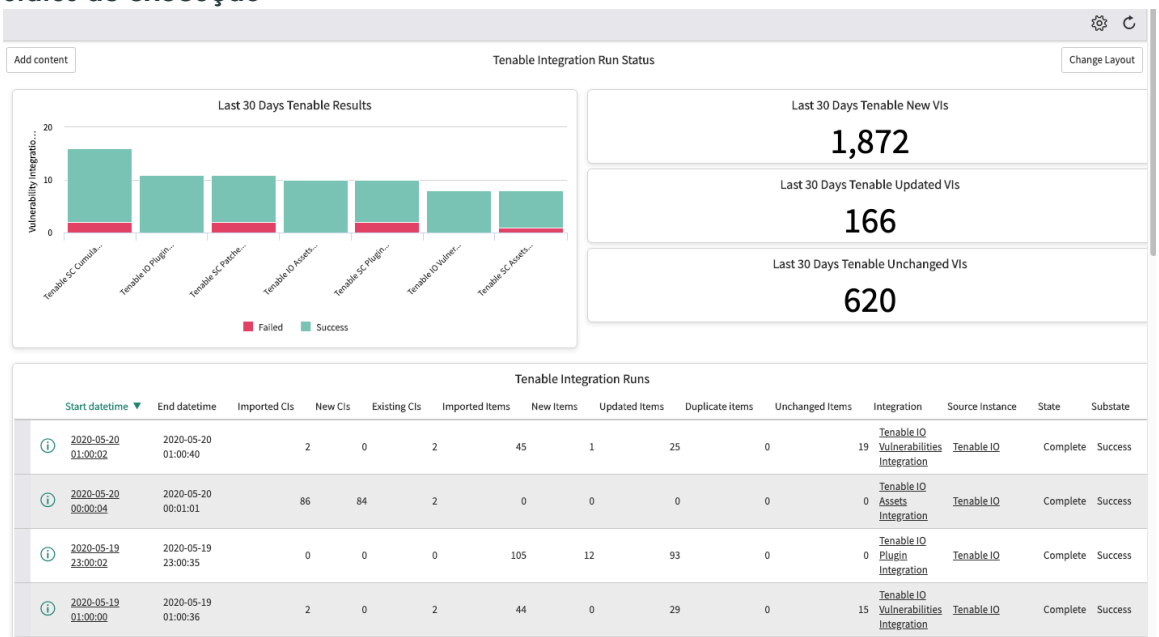
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir os dados, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Status da Execução da Integração**.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Status de execução



Relatórios do gráfico de status de execução da integração da Tenable

Nome	Descrição
Resultados do Tenable nos últimos 30 dias	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Cada execução é exibida como uma barra no gráfico.
VIs novos do Tenable nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs atualizados do Tenable nos últimos 30 dias	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs inalterados do Tenable nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Execuções de integrações do Tenable	Os registros de execução de integração em uma lista.

Tradução automática

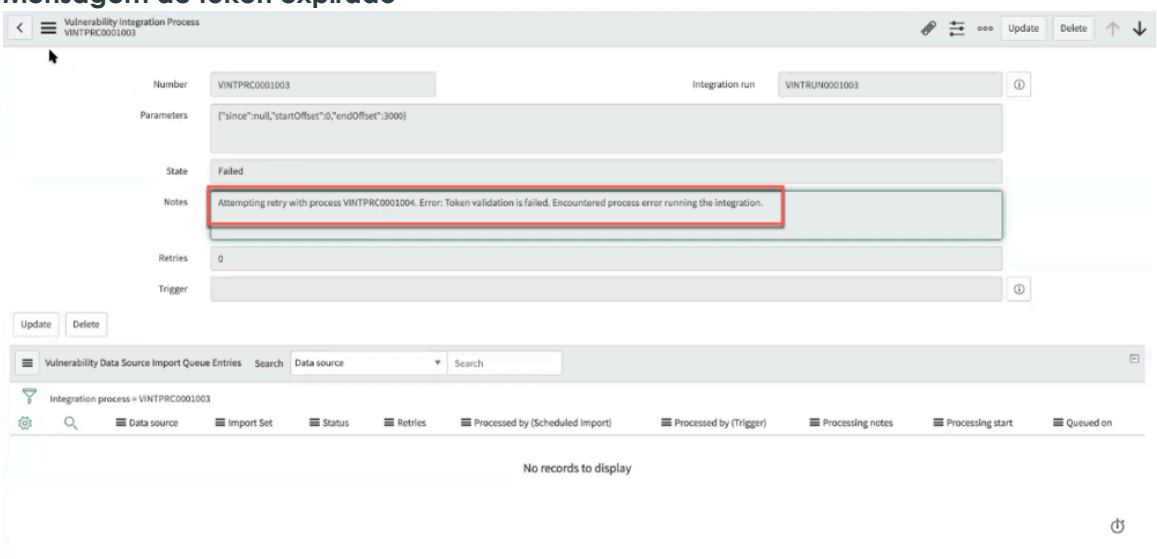
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: **V16.1:** para verificar as detecções desta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow[*sn_vul_detection*] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na contagem de detecção ou descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem de data até" na instância, após a conclusão da execução da integração.

Expiração da validação do token

Se uma execução de integração do Tenable.sc falhar por qualquer motivo, o token de autenticação do Tenable.sc expirará automaticamente e uma mensagem será exibida no registro do processo de integração de vulnerabilidade.

Mensagem de token expirado



Um novo token é gerado automaticamente para o próximo processo de integração. Todos os processos de integração, com falha e bem-sucedidos, são exibidos na guia Processo de integração de vulnerabilidade no registro Processo de integração de vulnerabilidade.

Iniciar nova verificação para a integração Tenable.sc

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.sc da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Nota: Tenable.sc não é compatível com o início de uma nova verificação em máquinas baseadas em agente.

Verifique se o scanner está ativado antes de começar. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
Para iniciar uma nova verificação a partir dos espaços, consulte Verificar novamente itens vulneráveis Tenable.io e Tenable.sc dos espaços Resposta a vulnerabilidades.

Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de itens vulneráveis (VI), tarefas de correção (RT), entradas de terceiros (TPE) ou registros de itens descobertos da sua instância Now Platform.

As novas verificações permitem que os proprietários de correção e os analistas de vulnerabilidade verifiquem se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada a partir de seus Now Platform para Tenable.sc itens vulneráveis.

Nota: Ao solicitar uma nova verificação da instância Now Platform®, a seleção das credenciais Integração de Resposta a vulnerabilidades com Tenable é opcional. A ServiceNow® Tenable.sc Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.sc em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais de conta da Tenable. A ServiceNow® Tenable.sc Integração de credencial de verificação é habilitada (`Ativo`) automaticamente no Assistente de configuração em sua instância quando você configura as Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades abertas e corrigidas).

Observe as seguintes informações sobre as credenciais importadas para que os usuários possam vê-las conforme necessário na instância Now Platform :

- As credenciais criadas com a função de usuário de administrador Tenable.sc estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.sc estão disponíveis somente para usuários dentro dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

Consulte o site de documentação Tenable.sc para obter mais informações.

Consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração para obter mais informações sobre como configurar a aplicação Tenable.sc. Para exibir mais informações sobre a Integração de credencial de verificação, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.sc**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável a partir do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Você só pode iniciar novas verificações de IVs com Tenable.sc como origem. Verifique se Tenable.sc é exibido na coluna **Origem** nas exibições de lista de VI ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condições para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição de lista de VI, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **Origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de VI, o VI deve ser do produto Tenable.sc e estar em qualquer estado diferente de **Closed**. Para vários registros de VI, todos os IVs devem ser do produto Tenable.sc e estar em qualquer estado diferente de **Closed**.
   - Em um registro de RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Tenable.sc.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do produto Tenable.sc em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro, clique em **Verificar novamente**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você será solicitado a escolher as credenciais do scanner para acessar o scanner. Estas são as credenciais importadas pela Tenable.sc Scan Credential Integration.

5. Na caixa de diálogo, selecione os filtros e tipos de credenciais desejados.
6. Clique **em Solicitar verificação**.

   Uma mensagem é exibida indicando que a verificação está sendo processada. O status de todas as novas verificações pode ser encontrado a qualquer momento nas listas relacionadas a Verificação nos registros VI, RT e TPE usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e outras verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. O registro de verificação primário é um contêiner para as verificações secundárias.

   Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram ou farão a transição para **Encerrado/Corrigido** são importados com a próxima importação programada da Integração de vulnerabilidades fixas da Tenable.sc.

Iniciar nova verificação para a integração Tenable.io

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.io da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Verifique se o scanner está ativado antes de começar. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

- Consulte e Verificar novamente registros e tarefas de correção no Espaço do gerenciador de vulnerabilidades e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI para iniciar uma nova verificação nos espaços da Resposta a vulnerabilidades.
- Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Nota: Tenable.io não é compatível com o início de uma nova verificação em máquinas baseadas em agente.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, como responsável pela correção, especialista em TI, analista de vulnerabilidade ou gerente de vulnerabilidades, você pode iniciar novas verificações direcionadas sob demanda. você pode verificar vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de itens vulneráveis (VI), tarefas de correção (VUL), entrada de terceiros (TPE) ou registros de itens descobertos (SDI) da instância Now Platform. As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao solicitar uma nova verificação da instância Now Platform®, a seleção das credenciais Integração de Resposta a vulnerabilidades com Tenable é opcional. A ServiceNow® Tenable.io Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.io em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais de conta da Tenable.

As informações a seguir descrevem as credenciais que você importa para que os usuários possam vê-las conforme necessário na sua instância Now Platform :

- As credenciais criadas com a função de usuário de administrador Tenable.io estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.io estão disponíveis somente para usuários dentro dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

  Consulte o site de documentação Tenable.io para obter mais informações.

- A integração de modelo Tenable.io e a integração de credencial de verificação Tenable.io precisam ser ativadas antes de iniciar novas verificações. Para exibir mais informações sobre a Integração de credencial de verificação, navegue até **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.io**.

  Por padrão, as integrações de credencial de modelo e verificação estão desativadas. Quando você insere suas credenciais para Tenable.io, todas as integrações Tenable.io são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

  1. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
  2. Na lista exibida, localize os registros de integração Tenable.io desejados.
  3. Abra cada registro e marque a caixa de seleção **Ativo** para ativar a integração.
  4. Clique em **Atualizar** para salvar suas mudanças.
  5. Retorne ao Assistente de configuração para continuar com a configuração para Integrações de vulnerabilidade da Tenable com Resposta a vulnerabilidades.

Consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração para obter mais informações sobre como configurar os produtos Tenable.io e Tenable.sc.

Digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada a partir de seus Now Platform para Tenable.io itens vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação agendada da Integração de vulnerabilidades corrigidas.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável a partir do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Se você estiver usando o Tenable.io Scanner, só poderá iniciar novas verificações de IVs com Tenable.io como origem. Verifique se Tenable.io é exibido na coluna **Origem** nas exibições de lista de VI ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condições para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição de lista de VI, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **Origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para os registros que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de VI, o VI deve estar em qualquer estado diferente de **Closed**. Para vários registros de VI, todos os IVs devem ser do produto Tenable.io e estar em qualquer estado diferente de **Closed**.
   - Para registros de tarefa de correção, somente tarefas de correção em qualquer estado diferente de **Encerrado** são compatíveis. Todos os IVs associados devem estar em qualquer estado diferente de **Encerrado** e usar Tenable.io como origem.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.

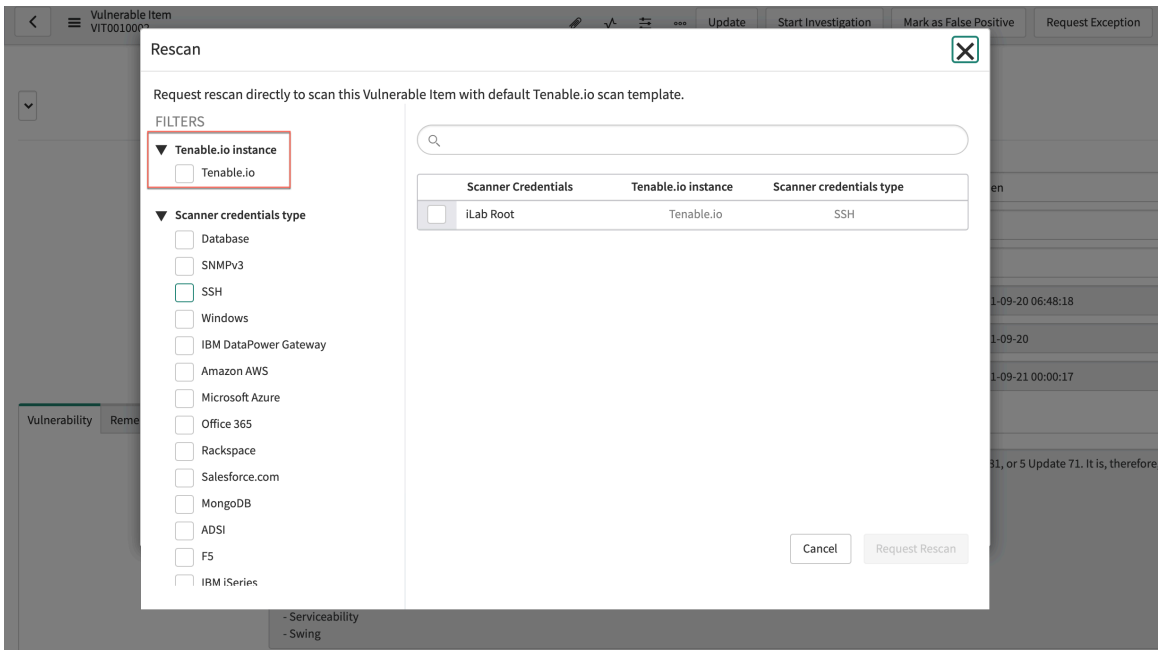
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em registros de Itens descobertos, o registro deve ter pelo menos um registro VI associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.
- Na lista Itens vulneráveis, você pode selecionar itens vulneráveis individuais que deseja verificar novamente. Use o menu Ações nas linhas selecionadas no canto inferior esquerdo da tela para iniciar a nova verificação. Você será solicitado a inserir suas credenciais.

4. No canto superior direito de um registro, clique em **Verificar novamente**.
Você será solicitado a escolher a instância ou as instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pela Tenable.io Scan Credential Integration.
5. Na caixa de diálogo, selecione a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Na imagem a seguir, uma instância de integração, `Tenable.io`, é exibida. Se você tiver mais de uma instância Tenable.io, todas elas serão exibidas na seção `Tenable.io` no formulário.



Campo	Descrição
Instância da Tenable.io	Escolha uma instância de integração Tenable.io a partir da qual você deseja iniciar a nova verificação. Todas as suas instâncias de integração para Tenable.io são exibidas. Se houver um VI em mais de uma instância de integração, você poderá usar este filtro para limitar ou expandir as instâncias que deseja verificar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se você optar por verificar novamente os IVs de um registro de tarefa de correção para uma única instância de integração, somente os VIs ativos que estão associados a essa tarefa de correção, para essa instância, usando as credenciais selecionadas serão verificados.
Filtro de tipo de credenciais do scanner	Use este filtro para exibir credenciais por tipo.
Painel com credenciais do scanner, instância Tenable.io, tipo de credenciais do scanner	Estas são as credenciais de scanner disponíveis importadas dos produtos Tenable.io. Escolha uma ou mais credenciais a serem usadas na verificação.

6. Clique **em Solicitar nova verificação**.

Uma mensagem é exibida indicando que a verificação está sendo processada e que um registro de verificação primário foi criado. O status de todas as verificações secundárias pode ser encontrado a qualquer momento nas listas relacionadas a Verificação nos registros de VI, tarefa de correção, TPE e SDI usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e outras verificações iniciadas a partir de um determinado registro.

O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. Cada verificação oferece suporte a uma combinação exclusiva de instância de integração, TPE, IP e ID de rede. Você pode ver várias verificações secundárias em um registro de verificação primário. Por exemplo, o número máximo de endereços IP que uma verificação secundária pode suportar é 1000. Se houver 1002 IPs para um item vulnerável, duas verificações secundárias serão criadas e listadas na lista relacionada Verificações para oferecer suporte à solicitação. O registro de verificação primário é um contêiner para as verificações secundárias e seu estado de reflete o status das verificações secundárias.

Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** são importados com a próxima importação agendada da Tenable.io Integração de vulnerabilidades corrigidas.

Para verificações com erro, você pode verificar as verificações secundárias no registro de verificação primário. Exiba o erro na carga de resposta da verificação secundária.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação agendada da Integração de vulnerabilidades corrigidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizar itens de configuração com o identificador de partição de rede para o Integrações de vulnerabilidade da Tenable

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão na aplicação Resposta a vulnerabilidades, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC `(IC 1)` durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	Network_id	Item de configuração
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	Repository_id	Item de configuração
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. A partir de uma nova importação de dados, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para as integrações de ativos e vulnerabilidades fixas e abertas dos produtos Tenable.io e Tenable.sc no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

Tradução automática

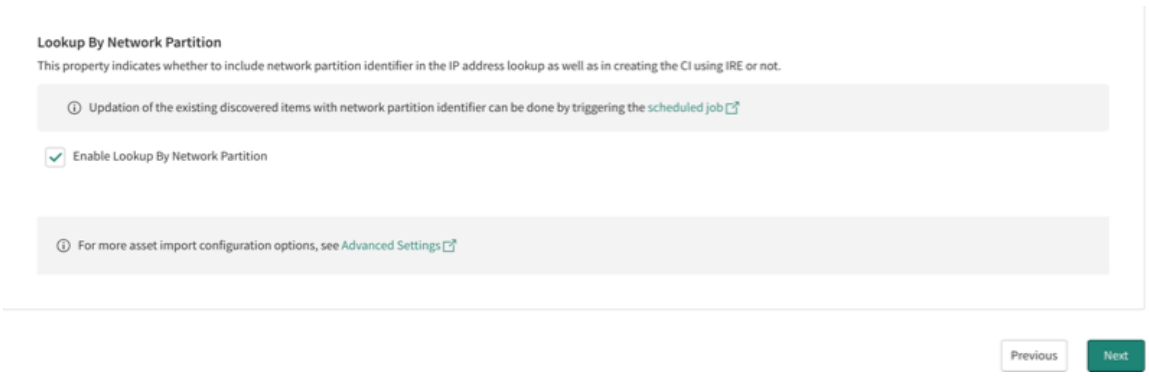
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando você faz upgrade a partir da v14.0 de Resposta a vulnerabilidades e v2.2 da Integração de vulnerabilidade da Tenable, os modelos de classe de IC do CMDB (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. Os ICs dos dados existentes da Tenable são criados ou atualizados para incluir a granularidade do identificador de partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são todos atualizados com os novos ICs.
Aguarde as importações de novos dados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo trabalho agendado. IC, item vulnerável e registros de detecção são todos atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Selecione Tenable.io integrações ou Tenable.sc integrações.
3. **Edite** a integração necessária.
4. Selecionar **Configuração de importação de ativo**.
5. Selecionar **Habilitar pesquisa por partição de rede** caixa de seleção do **Habilitar pesquisa por partição de rede** seção.



6. Clique em **Avançar**.

   Os identificadores de partição de rede NETWORK_ID e REPOSITORY _ID estão incluídos e atualizam os ICs existentes ou criam ICs com o próximo trabalho agendado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo do identificador de partição de rede incluído na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

Com o próximo trabalho agendado, as regras de pesquisa de identificação de endereço IP e IC de endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para os produtos Tenable.io e Tenable.sc.

Depois de habilitar a propriedade do sistema e salvar os registros, você também pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando os trabalhos agendados sob demanda.

Importar modificações para a integração de vulnerabilidade da Tenable

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração de importação de vulnerabilidades da Tenable na ServiceNow® Integração de vulnerabilidade da Tenable.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação e conhecimento avançado sobre o Now Platform.

Siga estas etapas para criar importações separadas por domínio para as integrações de vulnerabilidades da Tenable. O exemplo a seguir é para a integração Tenable.io Open Vulnerabilities, mas este conteúdo é aplicável a outras integrações da Tenable.

Procedimento

1. Crie um domínio.
2. Para cada domínio criado, crie um usuário e atribua o usuário a esse domínio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

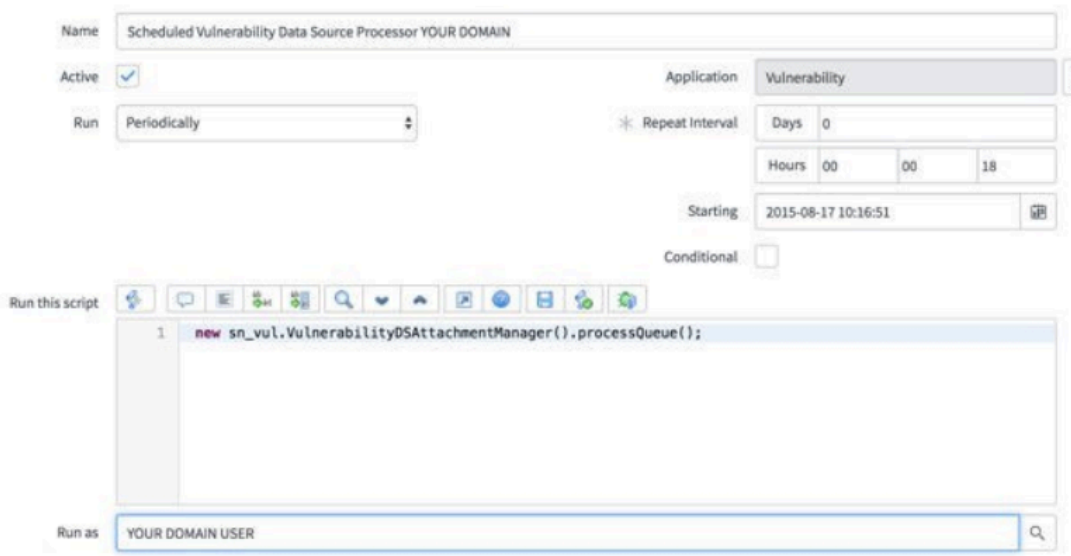
Pense neste usuário como um espaço reservado run_as para o domínio no Tenable.io.

3. Integração de vulnerabilidades abertas.
   O usuário é o equivalente ao usuário VR.System no domínio global e deve ter as seguintes funções: sn_vul.tenable_configure_integration, import_admin e sn_vul.vulnerability_write. Este usuário requer acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota: Considere este usuário como específico para esta função. O usuário não deve ter outra finalidade

4. Em cada domínio, crie um trabalho agendado copiando o Processador da Fonte de Dados de Vulnerabilidade Programada encontrado em **Definição do Sistema** > **Trabalhos agendados**.
5. Anexe o domínio ao nome para identificar o trabalho agendado.
6. Altere o usuário run_as para o usuário que você criou na etapa anterior.

   Nota: Edite a ação de IU a seguir para que a integração seja executada no domínio do usuário run_as.



7. Edite a ação de IU Executar agora na integração de vulnerabilidades abertas do Tenable.io para adicionar este bloco de código à parte superior do arquivo.
   ```
   //sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
   ```

   Nota: Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário run_as.

8. Edite o método de inclusão de script VulnerabilityIntegrationUtils addIntegrationRun para adicionar o código realçado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edite o método de inclusão de script VulnerabilityIntegrationUtils addProcessRun para adicionar o código realçado.

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edite o método de inclusão de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups para alterar este código original: código _processFromDataSourcesGroups original para código _processFromDataSourcesGroups editado.

11. Edite o método de inclusão de script VulnerabilityDSAttachmentManager, queueItem para adicionar os seguintes blocos de código realçados queueItem, _getNext, _processQueueEntry.

Você está pronto para importações de detecção de host separadas por domínio.

Desabilitar calculadoras antes da importação

Siga estas etapas para desabilitar a calculadora padrão se não for usada. Se você não usar calculadoras de vulnerabilidade, é melhor desabilitar as calculadoras padrão, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é acessado e pode afetar o desempenho da instância.

Função necessária: sn_vul.vulnerability_admin.

12. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Calculadoras de vulnerabilidade**.

13. Abra o grupo Impacto de vulnerabilidade.

14. Abra a calculadora de impacto baseado em pontuação e serviço.

15. Desmarque o campo Ativo para desativar a calculadora.

16. Clique em Atualizar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você desativou a calculadora padrão.

Desabilitar regras de negócio baseadas em notificação antes da importação inicial

Siga estas etapas para desabilitar Regras de negócio relacionadas a notificações antes da importação do registro inicial. Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem gerar muitas notificações, afetando o desempenho. Essas regras de negócio devem ser modificadas para desativá-las durante a importação.

A função necessária é sn_vul.vulnerability_admin.

17. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócio**.
18. Pesquise notificações de ICs afetados.
19. Abra a regra de negócio e insira a seguinte condição: *`current.sys_class_name != "sn_vul_vulnerable_item"`*.
20. Clique em **Atualizar**.
21. Repita este procedimento para as seguintes regras de negócio:
    - Notificações do centro de custos afetado
    - Notificações do grupo afetado
    - Notificações de locais afetados

    Nota: Após a conclusão da importação do registro inicial, você tem a opção de habilitar novamente essas regras de negócio. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Modificar uma data de início inicial

Siga estas etapas para modificar uma data de início inicial. Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações da Tenable. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado nas etapas a seguir.

22. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
23. Clique em qualquer integração.
24. Clique em Detalhes da integração.
25. Defina o campo Hora de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde essa hora sejam detectadas.

    Se você configurou a Tenable usando o Assistente de configuração, o campo Hora de início será preenchido previamente, inicialmente até três meses antes da data de hoje e, posteriormente, até a data de hoje. Observação: considere definir o valor para no máximo um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Tenable, bem como o acionamento de tempos limites de execução.

26. Clique em **Enviar** ou **Atualizar**.
27. Opcional: Clique **em Executar agora** para executar imediatamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre a integração [Atlassian Jira com Resposta a vulnerabilidades

A integração [Atlassian Jira com Resposta a vulnerabilidades permite que você aproveite diferentes ferramentas de acompanhamento de problemas e gestão ágil para acompanhar os esforços de correção de vulnerabilidades.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

ServiceNow® Resposta a vulnerabilidades está integrado a Atlassian Jira para criar problemas correspondentes a vulnerabilidades e sincronizou a entidade de problema em Jira e a entidade de item de vulnerabilidade em Resposta a vulnerabilidades bidirecionalmente para refletir as atualizações mais recentes. Os Gerenciadores de vulnerabilidade exigem que os itens de vulnerabilidade presentes em ServiceNow Resposta a vulnerabilidades sejam criados e atribuídos a usuários de correção (desenvolvedores no caso de Resposta a vulnerabilidades de aplicações) em seu sistema preferencial de registro e ferramenta de gestão de problemas, como Atlassian Jira. Qualquer andamento realizado nas vulnerabilidades na ferramenta de gestão de problemas deve ser atualizado em ServiceNow Resposta a vulnerabilidades para visibilidade para os gerentes de vulnerabilidade. Além disso, todas as atualizações feitas por gerentes de vulnerabilidade em Resposta a vulnerabilidades para itens de vulnerabilidade também devem ser passadas para a ferramenta de gestão de problemas para visibilidade aos usuários de correção.

Versões disponíveis

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades	Notas de versão da Integração de resposta a vulnerabilidades
Vulnerability Response e Configuration Compliance para contêiner	Notas de versão da Resposta a vulnerabilidades do contêiner
Spoke do Jira	Notas da versão do spoke do Jira

Jira Integrações de vulnerabilidade

Para exibir a Jira Integração de vulnerabilidade, navegue até **Todos** > **Gestão do Agile para VR** > **Configurar ferramentas Agile** .

As seguintes integrações estão incluídas no sistema de base. Essas integrações não estão ativas por padrão.

Após a execução inicial, todos os dias, os trabalhos agendados são encadeados para executar as integrações automaticamente na ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparando para a integração Jira Resposta a vulnerabilidades

Uma integração Jira de vulnerabilidade bem-sucedida requer planejamento e execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. A integração Jira Resposta a vulnerabilidades pressupõe que você esteja familiarizado com o produto Jira e a API.

Componentes instalados com a Integração Agile para Resposta a vulnerabilidades e Integração Jira para Resposta a vulnerabilidades

Vários tipos de componentes são instalados com a ativação do plug-in Agile Integration for Vulnerability Response e Jira Integration for Vulnerability Response, incluindo tabelas e funções de usuário.

Funções instaladas

Título da função [name]	Descrição
Administrador da ferramenta Agile [sn_vul_agile.agile_tool_admin]	Permite que você crie uma regra de configuração para que a Gestão ágil crie ou atualize problemas. Crie configurações de regra para Agile Management.
Administrador do JIRA [sn_vul_jira.admin]	Permite que você selecione a ferramenta Agile para criar problemas para a tabela de entidade selecionada.

Tabelas instaladas

Tabela	Descrição
Configuração da ferramenta Agile [sn_vul_agile_tool_rule_config]	Contém regras de configuração para criar problemas na plataforma Agile.
Mapeamento do campo da ferramenta Agile [sn_vul_agile_tool_field_mapping]	Contém o mapeamento de campo da regra de configuração.
Mapeamento de estado da ferramenta Agile [sn_vul_agile_tool_state_mapping]	Contém o mapeamento de estado do status do problema do JIRA com o estado do Item vulnerável da aplicação, Item vulnerável do contêiner, Tarefa de correção da aplicação e Tarefa de correção do contêiner.
Manifesto da ferramenta Agile [sn_vul_agile_tool_manifest]	Contém carga para criação de problemas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instaladas

Tabela	Descrição
Recurso de dados da ferramenta Agile [sn_vul_agile_tool_data_resource]	Contém as informações sobre o problema do JIRA criado.
Administrador do JIRA [sn_vul_jira.admin]	Permite que você selecione a ferramenta Agile para criar problemas para a tabela de entidade selecionada.

Instalar a Integração de resposta a vulnerabilidades com Jira

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Jira se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Função necessária: administrador

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	• A Integração do Jira para Resposta a vulnerabilidades requer a aplicação Resposta a vulnerabilidades. • Para a versão mais atual da Integração do JIRA para Resposta a vulnerabilidades, verifique se você tem a versão mais atual da Resposta a vulnerabilidades instalada. Consulte KB0856498 Matriz de compatibilidade da Resposta a vulnerabilidades e mudanças no esquema da versão . • Se a aplicação não estiver instalada e ativada, consulte Instalar Resposta a vulnerabilidades .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se o plug-in Integration Hub está instalado.	• O Jira Spoke requer o Hub de integração. • Consulte KB1112383 para instalação do hub de integração. • Para obter mais informações, consulte Cronogramas jurídicos-Visão geral do IntegrationHub .
Verifique se a versão mais recente de Jira Spoke está instalada.	Consulte KB0792632 para instalação do Spoke do Jira.
Verifique se a Integração da Resposta a vulnerabilidades com Gestão ágil está instalada.	A integração da Resposta a vulnerabilidades com o Atlassian Jira requer essa integração.

Procedimento

1. Faça login na instância em que você deseja instalar a integração Jira Resposta a vulnerabilidades.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a integração [Resposta a vulnerabilidades com a aplicação Jira.
4. Clique no bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira o **Nome** e **o motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

Configurar regras na configuração da ferramenta Agile

Jira problemas serão criados na plataforma Jira se os registros criados no item vulnerável da aplicação, no item vulnerável do contêiner, na tarefa de correção da aplicação e na tarefa de correção do contêiner corresponderem às regras criadas na configuração da ferramenta Agile.

Antes de Iniciar

Funções necessárias: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

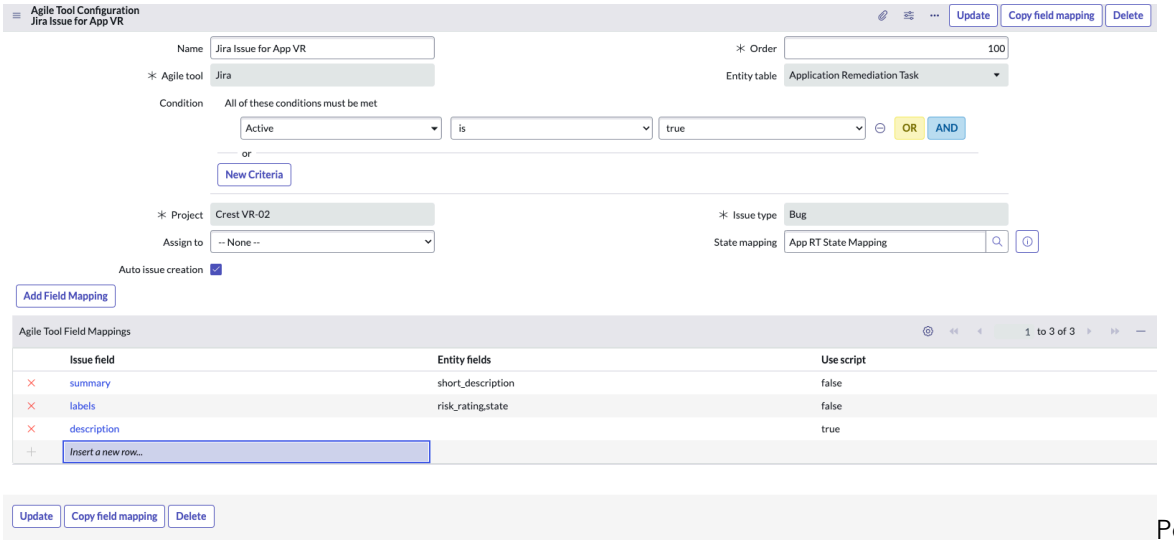
1. Navegar até **Todos** > **Gestão do Agile para VR** > **Configurar ferramentas Agile**.
2. Para criar uma nova regra de configuração na configuração da ferramenta Agile, selecione **Novo**.
3. No formulário, preencha os campos.

Formulário de configuração da ferramenta Agile

Campo	Descrição
Nome	Nome da configuração da ferramenta Agile.
Ordem	Ordem da configuração da ferramenta Agile.
Ferramenta Agile	A ferramenta Agile para criar problemas na plataforma Agile específica.
Tabela da entidade	Tabela na qual a regra de configuração será aplicada.
Condição	Filtrar a condição na tabela de entidade selecionada para criar problemas na plataforma Agile.
Criação automática de problemas	A regra de configuração será consultada quando qualquer novo registro for criado na tabela de entidade selecionada, somente se a caixa de seleção estiver marcada. **Nota:** O usuário deve usar a ação de lista para criar problemas para registros de entidade existentes.
Projeto	O projeto no qual o problema do Jira será criado.
Tipo de Problema	O tipo de problema a ser criado em um projeto específico.
Atribuir a	O designado a quem o problema deve ser atribuído após a criação do problema. Para manter os problemas criados como não atribuídos, selecione "Nenhum".
Mapeamento de Estado	Os mapeamentos de estado existentes da tabela Mapeamento de estado da ferramenta Agile ou criam um novo mapeamento de estado entre o status do problema na plataforma Agile e os estados da tabela de entidade ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, quando a aplicação está instalada, a Tarefa de correção de aplicação e a Tarefa de correção de contêiner são exibidas no campo Tabela de entidade no formulário de configuração da ferramenta Agile.

4. Para adicionar o item vulnerável da aplicação e o item vulnerável do contêiner na lista de seleção Tabela da entidade, navegue até **Propriedades do sistema** > **sn_vul_agile.tablesToShow** e adicione tudo no campo Valor.

Formulário de propriedade do sistema

Campo	Descrição
Escolhas	Valores separados por vírgula para uma lista de seleção.
Valor	Defina o valor desejado para a propriedade. Todos os valores de propriedade são armazenados como cadeias de caracteres. Ao recuperar propriedades por meio do método gs.getProperty (), trate os resultados como cadeias de caracteres. Por exemplo, uma propriedade verdadeiro | falso retorna 'verdadeiro' ou 'falso' (cadeias de caracteres), não o equivalente booliano.

5. Selecione o registro de mapeamento de estado existente ou crie um novo mapeamento de estado na ferramenta Agile Mapeamento de estado.

Formulário Mapeamento de estado da ferramenta Agile

Campo	Descrição
Nome	Insira o nome exclusivo do Mapeamento de estado.
Ferramenta Agile	Selecione a ferramenta Agile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela da entidade	Selecione a tabela de origem na qual o mapeamento de estado será criado.
Projeto	Selecione o projeto no qual o estado será mapeado.
Estado da entidade da ServiceNow	Selecione o estado que você deseja mapear com o status da ferramenta Agile.
Status da ferramenta Agile	Selecione o estado que você deseja mapear a partir dos estados de item de vulnerabilidade.

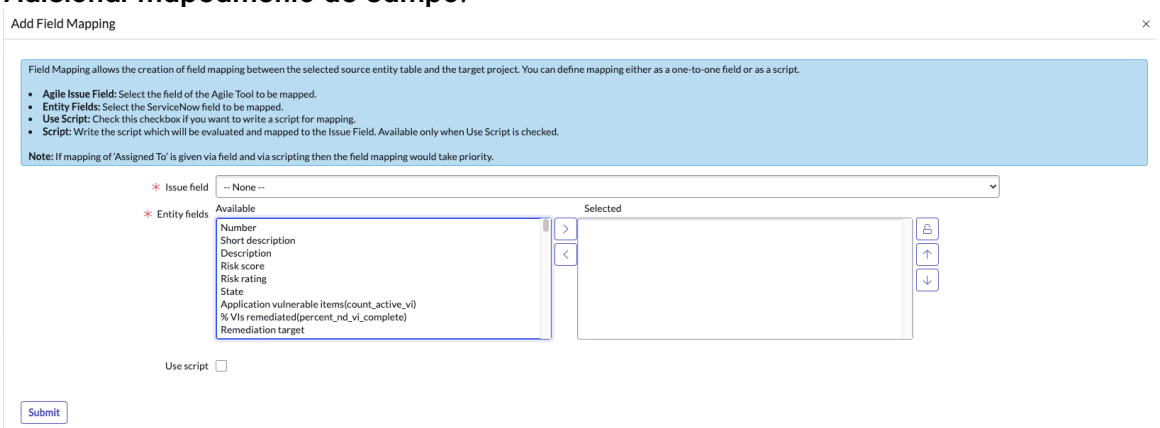
6. Clique em **Salvar e buscar projetos** para buscar os projetos na regra de configuração do campo Projeto e validar as credenciais da ferramenta Agile.

   Dica: Você pode definir a propriedade do **sistemaprojectsPageSize** para buscar um número específico de projetos por página.

7. Navegue até **Propriedades do sistema** > **sn_vul_jira.projectsPageSize** e adicione o número de projetos a serem obtidos por página no campo Valor do Jira Cloud.
8. Selecione o Projeto, o Tipo de Problema e Atribuir a na Regra de configuração depois que os projetos forem obtidos.

   O mapeamento de campo padrão será preenchido na lista incorporada de mapeamentos de campo da ferramenta Agile. Por padrão, os campos Resumo e Descrição dos problemas são mapeados.

9. Para mapear outros campos de problema com os campos ServiceNow, clique em **Adicionar mapeamento de campo**.



Nota:

- Você deve mapear somente campos do tipo Cadeia de caracteres e Opção.
- Todos os campos de problema obrigatórios da ferramenta Agile precisam estar mapeados corretamente com o campo de entidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Mapeamento de estado da ferramenta Agile

Campo	Descrição
Campo do problema	Contém os campos de problema do projeto selecionado no momento e o tipo de problema na regra de configuração.
Campos da entidade	Contém os campos da tabela de entidade selecionada na Regra de configuração.
Usar o Script	Selecione para usar o script para mapear os campos de problema com campos de entidade.
Script	Script para mapear o campo do problema com os campos da entidade.

10. Clique em **Enviar** no modal do glide para enviar o registro de mapeamento de campo na tabela Mapeamentos de campo da ferramenta Agile.

    Nota: Se você não mapear os campos obrigatórios, os problemas não serão criados para essa regra de configuração.

    Os campos obrigatórios são exibidos na parte superior do formulário de configuração da ferramenta Agile.
    Todos os mapeamentos de campo para uma regra de configuração específica são exibidos na lista incorporada da tabela Mapeamento de campo da ferramenta Agile na tabela Configuração da ferramenta Agile.
11. Clique com o botão direito do mouse no cabeçalho para salvar suas mudanças.
    O registro salvo fica visível na tabela Configuração da ferramenta Agile. Se algum registro for criado no item vulnerável da aplicação, o item vulnerável do contêiner, a tarefa de correção da aplicação e a tarefa de correção de contêiner corresponderem a qualquer regra de configuração, o problema será criado para o registro de acordo com o mapeamento na regra de configuração.
12. Navegue até **Propriedades do sistema** > **sn_vul_jira.cloudBulkSize** e defina o número de problemas a serem criados por lote no campo Valor.

    Nota: O número máximo de problemas que podem ser criados por lote na nuvem do Jira é 50).

    Você pode definir o tamanho do lote para criar problemas no servidor Jira.
13. Navegue até **Propriedades do sistema** > **sn_vul_jira.onPremBulkIssue** e defina o número de problemas a serem criados por lote no campo **Valor**.
    Você também pode definir a contagem de erros no campo Valor na propriedade do sistema para processar os registros na tabela de manifesto e criar problemas do Jira até uma contagem de erros específica.
14. Navegue até **Propriedades do sistema** > **sn_vul_agile.ManifestErrorCount** e defina o número máximo de vezes até o qual o manifesto com erro deve ser processado.

Criar problema ágil manualmente usando a ação de lista

Quando uma ação de lista: Criar problema do Jira é acionada, os registros que correspondem aos critérios de configuração de regra devem ser considerados para "Criar problema do Jira" e esses registros devem ser ingeridos na tabela sn_vul_agile_tool_manifest com o mapeamento selecionado na regra de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedimento
1. Navegar até **Todos** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista** > **Tarefas de correção/itens vulneráveis da aplicação/itens vulneráveis de contêiner**.
2. Selecione vários registros para criar problemas do Jira e clique em **Criar problema do Jira**.
   Os registros selecionados devem considerar o mapeamento de campo e o mapeamento de estado da ferramenta Agile associada.
   Os registros selecionados que atendem à condição da regra de configuração devem estar qualificados para a criação de problemas do Jira e esses registros devem ser adicionados à tabela *sn_vul_agile_tool_manifest*.

Criar problema ágil manualmente usando a ação de formulário

Crie um problema ágil manualmente usando a ação de formulário. Se o registro corresponder a qualquer condição de regra de configuração, uma caixa pop-up será preenchida com os valores selecionados na regra de configuração e, se não corresponder a nenhum critério, o usuário terá permissão para selecionar valores predefinidos campos.

Antes de Iniciar
Certifique-se de que todos os campos de problema obrigatórios da ferramenta Agile estejam mapeados corretamente com o campo de entidade.

Funções necessárias: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedimento
1. Navegar até **Todos** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista** > **Tarefas de correção/itens vulneráveis da aplicação/itens vulneráveis de contêiner**.
2. Selecione qualquer registro para criar um problema ágil manualmente.
3. Selecione **Criar problema do Agile**.
4. Insira detalhes válidos para os campos mencionados.

   Se o registro atender à condição de qualquer regra de configuração, os campos abaixo deverão ser preenchidos com o valor configurado e o usuário poderá modificar os valores do campo.

Campo	Descrição
Projeto	Selecione o projeto no qual o problema do JIRA será criado.
Tipo de Problema	Selecione o tipo de problema a ser criado em um projeto específico.
Atribuir a	Selecione o designado a quem o problema deve ser atribuído após a criação do problema.
Mapeamento de Campos	Selecione os campos de tipo de problema da ferramenta Agile e insira os valores diretos para o campo selecionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Criar problema do Agile** para enviar o registro.
   Depois de enviar o registro, a entrada de registro será criada na tabela sn_vul_agile_tool_manifest.

Sincronizar manualmente o status do problema Jira

Atualize o estado do registro único clicando no botão **Sincronizar status do Agile** do menu de contexto do formulário e atualize os estados de vários registros clicando na ação de lista **Sincronizar status do Agile** do item vulnerável da aplicação, do item vulnerável do contêiner e da tabela Tarefa de correção em o Espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Funções necessárias: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Por Que e Quando Desempenhar Esta Tarefa

O estado será sincronizado de ServiceNow para a ferramenta Agile se o estado da entidade for fechado em ServiceNow ou se qualquer entidade for reaberta (ou seja, o estado for Aberto). Todos os outros estados serão refletidos da ferramenta Agile para ServiceNow. O usuário não terá permissão para sincronizar o estado dos registros cuja regra configurada associada não tenha mapeamento de estado ou os problemas criados diretamente a partir da ação do formulário.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista** > **Tarefas de correção/itens vulneráveis da aplicação/itens vulneráveis de contêiner**.
2. Selecione vários registros para criar problemas do Jira e clique em **Sincronizar status do Agile**.
   Os estados dos registros para os quais os problemas já foram criados serão atualizados se o registro não estiver no estado fechado e se o mapeamento de estado existir para os registros selecionados na regra de configuração.
3. Abra um registro e o **status do Sync Agile ficará** visível no menu de contexto do formulário se as seguintes condições forem atendidas.
   - O problema foi criado para o registro e o registro não está no estado Encerrado
   - Existe um mapeamento de estado para o registro
4. Clique em **Sincronizar status ágil** para sincronizar o status ágil com o estado mapeado. Você pode definir a propriedade do sistema para definir o tamanho do lote para buscar o status do problema do JIRA.
5. Navegue até **Propriedade do sistema** > **sn_vul_jira.bulkIssueStatusSize**.
   - Para o Jira Server, o número máximo de problemas a serem retornados (o padrão é 50). O valor máximo permitido é determinado pela propriedade do JIRA 'jira.search.views.default.max'. Se você especificar um valor maior que este número, os resultados da pesquisa serão truncados).
   - Se o problema for criado a partir da ação do formulário ou se a regra configurada não tiver nenhum mapeamento de estado, esses registros não serão considerados para a sincronização de estado.

Configurar programador para criar problemas automaticamente

Configure o programador para executar e criar automaticamente os problemas Jira para os registros que foram criados na tabela sn_vul_agile_tool_manifest.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: admin ou schedule_admin.

Por Que e Quando Desempenhar Esta Tarefa
Todos os registros do Item vulnerável da aplicação, Item vulnerável do contêiner, Tarefa de correção da aplicação e Correção de contêiner criados na tabela sn_vul_agile_manifest serão considerados para Jira a criação do problema.

Procedimento
1. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos agendados** > **Criar problemas do Jira**.
2. Você pode modificar os campos Executar, Fuso horário e Hora no Script programado.

Formulário Execução de script agendada

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho agendado: ◦ Diariamente: é executado diariamente, em um horário designado. ◦ Semanalmente: é executado semanalmente, em dia e hora designados. ◦ Mensal: é executado mensalmente, em uma hora e dia do mês designados. ◦ Periodicamente: é executado em um intervalo de repetição designado. ◦ Uma vez: é executado somente para uma única ocorrência. ◦ Sob demanda: é executado imediatamente sob demanda. ◦ Calendário comercial: início da entrada: é executado nas datas de entrada iniciais do calendário comercial selecionado no campo. Um trabalho agendado é executado para a data de início de cada entrada de negócios definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho agendado será executado no primeiro dia de cada mês. ◦ Calendário de negócios: fim da entrada: é executado na data de término do calendário de negócios selecionado no campo. Esta seleção é executada da mesma maneira que Calendário de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	negócios: início da entrada, mas para as datas de término das entradas do calendário de negócios associadas. **Nota:** Ao selecionar Calendário de negócios: início de entrada ou Calendário de negócios: fim de entrada, você pode aplicar um fator de deslocamento para programar o trabalho para ser executado antes ou após o período de tempo do calendário de negócios selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Deslocamento. Para saber mais sobre como criar e usar calendários de negócios e definir entradas de calendário de negócios, consulte Criar um calendário de negócios e Definir entradas do calendário de negócios .
Dia	Dia em que o trabalho agendado deve ser executado. ◦ Se Executar estiver definido como Semanalmente, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ◦ Se Executar estiver definido como Mensal, selecione o dia do mês. Por exemplo, selecione 25 para o dia 25 do mês. Este campo aparecerá somente se você selecionar Mensal ou Semanal no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho agendada. Insira a duração no número de dias, horas ou minutos. Por exemplo: ◦ Para executar o trabalho agendado a cada quatro dias, insira 04 no campo Dias. ◦ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ◦ Se ele repetir em um intervalo de 13:30:25, insira 13 no campo Horas e, em seguida, insira 30 e 25 nos dois campos não rotulados após ele.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora	Hora do dia em que o trabalho agendado deve ser executado, expressa em horas, minutos e segundos no formato de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo Hora ao especificar a hora em que o trabalho agendado deve ser executado. Selecione uma entrada de fuso horário: ◦ **Nenhum**: use o fuso horário padrão para o usuário conectado que está criando o trabalho agendado. Por exemplo, o trabalho agendado será executado às 16h45, horário dos EUA/Pacífico, se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Horário. ◦ **Usar fuso horário do sistema**: use o fuso horário do sistema padrão especificado para a instância na qual ele é executado. Por exemplo, o trabalho agendado será executado às 22h15, horário de Londres, se Europa/London for o fuso horário padrão do sistema para a instância e você inserir 22:15 no campo Horário. ◦ Fuso horário real. ◦ Por exemplo, o trabalho agendado será executado às 13h30 no fuso horário do Leste dos EUA se você selecionar EUA/Leste e inserir 13:30 no campo Horário.
run_as	Por padrão, run_ como o valor do campo deve estar vazio. O usuário pode definir o valor como o valor do usuário do domínio para criar um problema para um domínio específico.

Tradução automática

Configurar programador para atualizar problemas automaticamente

Configure o programador para atualizar os problemas Jira automaticamente para os registros que foram adicionados à tabela sn_vul_agile_tool_manifest.

Antes de Iniciar

Função necessária: admin ou schedule_admin.

Por Que e Quando Desempenhar Esta Tarefa

Todos os registros do item vulnerável da aplicação, item vulnerável do contêiner, tarefa de correção da aplicação e correção de contêiner criados na tabela sn_vul_agile_manifest são considerados para Jira atualização de problema. Se o registro for encerrado e os comentários forem adicionados, esses valores também deverão ser atualizados para o problema Jira associado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- O trabalho agendado "atualizar problemas" não atualizará o estado Jira se o fluxo de trabalho do projeto de problema ágil escolhido restringir qualquer usuário de mudar diretamente o estado de outro estado.
- Se você fechar qualquer registro de entidade com comentários adicionais, somente o último comentário será considerado no momento da atualização e, para a próxima atualização, todos os comentários serão adicionados ao Jiraassociado.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos agendados** > **Atualizar problemas do Jira**.
2. Você pode modificar os campos **Executar**, **Fuso horário**e **Hora** no script Programado.

Formulário Execução de script agendada

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho agendado: ◦ Diariamente: é executado diariamente, em um horário designado. ◦ Semanal: é executado semanalmente, em uma hora e dia designados. ◦ Mensal: é executado mensalmente, em uma hora e dia do mês designados. ◦ Periodicamente: é executado em um intervalo de repetição designado. ◦ Uma vez: é executado somente para uma única ocorrência. ◦ Sob demanda: é executado imediatamente sob demanda. ◦ Calendário comercial: início da entrada: é executado nas datas de entrada iniciais do calendário comercial selecionado no campo. Um trabalho agendado é executado para a data de início de cada entrada de negócios definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho agendado será executado no primeiro dia de cada mês. ◦ Calendário de negócios: Término da entrada: é executado na data de término do calendário de negócios selecionado no campo. Esta seleção é executada da mesma maneira que Calendário de negócios: início da

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	entrada, mas para as datas de término das entradas do calendário de negócios associadas. **Nota:** Ao selecionar Calendário de negócios: início de entrada ou Calendário de negócios: fim de entrada, você pode aplicar um fator de deslocamento para programar o trabalho para ser executado antes ou após o período de tempo do calendário de negócios selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Deslocamento. Para saber mais sobre como criar e usar calendários de negócios e definir entradas de calendário de negócios, consulte e Criar um calendário de negócios Definir entradas do calendário de negócios .
Dia	Dia em que o trabalho agendado deve ser executado. ◦ Se Executar estiver definido como Semanalmente, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ◦ Se Executar estiver definido como Mensal, selecione o dia do mês. Por exemplo, selecione 25 para o dia 25 do mês. Este campo aparecerá somente se você selecionar Mensal ou Semanalmente no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho agendada. Insira a duração no número de dias, horas ou minutos. Por exemplo: ◦ Para executar o trabalho agendado a cada quatro dias, insira 04 no campo Dias. ◦ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ◦ Se ele repetir em um intervalo de 13:30:25, insira 13 no campo Horas e, em seguida, insira 30 e 25 nos dois campos não rotulados após ele.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora	Hora do dia em que o trabalho agendado deve ser executado, expressa em horas, minutos e segundos no formato de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo Hora ao especificar a hora em que o trabalho agendado deve ser executado. Selecione uma entrada de fuso horário: ◦ Nenhum: use o fuso horário padrão para o usuário conectado que está criando o trabalho agendado. Por exemplo, o trabalho agendado é executado às 16h45. Horário dos EUA/Pacífico se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Horário. ◦ Usar fuso horário do sistema: use o fuso horário padrão do sistema especificado para a instância na qual ele é executado. Por exemplo, o trabalho agendado será executado às 22h15, horário de Londres, se Europa/London for o fuso horário padrão do sistema para a instância e você inserir 22:15 no campo Horário. ◦ Fuso horário real. ◦ Por exemplo, o trabalho agendado será executado às 13h30 no fuso horário do leste dos EUA se você selecionar EUA/Leste e inserir 13h30 no campo Horário.
run_as	Por padrão, o valor do campo **run_ as** está vazio. Você pode definir o valor como um usuário de domínio para criar um problema para um domínio específico.

Tradução automática

Configure o programador para sincronizar o status [Jira para ServiceNow® automaticamente

Configure o programador para sincronizar o estado de Jira problemas com o item de vulnerabilidade da aplicação, itens de vulnerabilidade do contêiner e tarefas na tabela sn_vul_agile_manifest.

Antes de Iniciar

Função necessária: schedule_admin ou admin

Por Que e Quando Desempenhar Esta Tarefa

O programador é executado automaticamente de acordo com a programação configurada. O estado dos registros criados no item vulnerável de aplicação, no item vulnerável de contêiner, na tarefa de correção de aplicação e na tabela de tarefas de correção de contêiner que têm problemas criados em Jira é atualizado de acordo com o

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

status atual do problema na plataforma Jira com base no mapeamento de estado na regra de configuração.

Todos os registros de item vulnerável de aplicação, item vulnerável de contêiner, tarefa de correção de aplicação e correção de contêiner criados na tabela sn_vul_agile_manifest serão considerados para Jira criação de problemas.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos agendados** > **Status da sincronização**.
2. Você pode modificar os campos Executar, Fuso horário e Hora no Script programado.

Formulário Execução de script agendada

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho agendado: ◦ Diariamente: é executado diariamente, em um horário designado. ◦ Semanal: é executado semanalmente, em uma hora e dia designados. ◦ Mensal: é executado mensalmente, em uma hora e dia do mês designados. ◦ Periodicamente: é executado em um intervalo de repetição designado. ◦ Uma vez: é executado somente para uma única ocorrência. ◦ Sob demanda: é executado imediatamente sob demanda. ◦ Calendário de negócios: início de entrada: é executado nas datas de entrada iniciais do calendário de negócios selecionado no campo. Um trabalho agendado é executado para a data de início de cada entrada de negócios definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho agendado será executado no primeiro dia de cada mês. ◦ Calendário de negócios: Término da entrada: é executado na data de término do calendário de negócios selecionado no campo. Esta seleção é executada da mesma maneira que Calendário de negócios: início da entrada, mas para as datas de término das entradas do calendário de negócios associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Ao selecionar Calendário de negócios: início de entrada ou Calendário de negócios: fim de entrada, você pode aplicar um fator de deslocamento para programar o trabalho para ser executado antes ou após o período de tempo do calendário de negócios selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Deslocamento. Para saber mais sobre como criar e usar calendários de negócios e definir entradas de calendário de negócios, consulte Criar um calendário de negócios e Definir entradas do calendário de negócios.
Dia	Dia em que o trabalho agendado deve ser executado. ◦ Se Executar estiver definido como Semanalmente, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ◦ Se Executar estiver definido como Mensal, selecione o dia do mês. Por exemplo, selecione 25 para o dia 25 do mês. Este campo aparecerá somente se você selecionar Mensal ou Semanal no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho agendada. Insira a duração no número de dias, horas ou minutos. Por exemplo: ◦ Para executar o trabalho agendado a cada quatro dias, insira 04 no campo Dias. ◦ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ◦ Se ele repetir em um intervalo de 13:30:25, insira 13 no campo Horas e, em seguida, insira 30 e 25 nos dois campos não rotulados após ele.
Hora	Hora do dia em que o trabalho agendado deve ser executado, expressa em horas, minutos e segundos no formato de 24

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo Hora ao especificar a hora em que o trabalho agendado deve ser executado. Selecione uma entrada de fuso horário: ◦ -Nenhum-: use o fuso horário padrão para o usuário conectado que está criando o trabalho agendado. Por exemplo, o trabalho agendado será executado às 16h45, horário dos EUA/ Pacífico, se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Horário. ◦ Usar fuso horário do sistema: use o fuso horário padrão do sistema especificado para a instância na qual ele é executado. Por exemplo, o trabalho agendado será executado às 22h15, horário de Londres, se Europa/ London for o fuso horário padrão do sistema para a instância e você inserir 22:15 no campo Horário. ◦ Fuso horário real. ◦ Por exemplo, o trabalho agendado será executado às 13h30 no fuso horário do Leste dos EUA se você selecionar EUA/ Leste e inserir 13h30 no campo Horário.
run_as	Por padrão, o valor do campo run_ as está vazio. Você pode definir o valor como o valor do usuário do domínio necessário para criar um problema para um domínio específico.

Tradução automática

Criar manualmente uma integração de vulnerabilidade

As integrações de vulnerabilidade permitem que clientes e fornecedores enriqueçam os dados de vulnerabilidade em suas instâncias, recuperando dados de sistemas e fornecedores externos. Essa capacidade pode simplificar o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Para obter instruções detalhadas sobre como criar integrações, consulte Definir uma nova integração de vulnerabilidade.

Definir uma nova integração de vulnerabilidade

Uma integração de vulnerabilidade extrai dados de relatório de um sistema de terceiros, geralmente para recuperar dados de vulnerabilidade e processar esses dados de relatório usando fontes de dados ou um processador personalizado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Integrações**.
2. Clique em **Nova**.
3. Preencha os campos conforme necessário.

Integração da vulnerabilidade

Campo	Descrição
Nome	Um nome descritivo para a integração.
Ativo	Se a integração está ativa. Se você não quiser que ele seja executado por um período específico, poderá configurar os parâmetros que deseja usar e desativar o trabalho.
Executar	A frequência com que você deseja que a integração seja executada: Diariamente, Semanalmente, Periodicamente e assim por diante. Conforme observado, os campos subsequentes são exibidos ou não com base na sua configuração neste campo.
Dia	O dia em que você deseja que a integração seja executada. ◦ Se você selecionou **Semanalmente** no campo **Executar**, este campo exibirá os dias da semana. ◦ Se você selecionou **Mensal** no campo **Executar**, este campo exibirá os dias do mês.
Hora	A hora em que você deseja que a integração seja iniciada. Este campo aparecerá somente se você tiver selecionado **Diariamente**, **Semanalmente**ou **Mensalmente** no campo **Executar**.
Aplicação	[Somente leitura] O nome da aplicação para a qual esta integração foi criada.
Intervalo de repetição	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	o número de dias e horas antes que a integração seja executada novamente.
Início	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá as datas e a hora a serem usadas como ponto de partida para atualizações periódicas.
Condicional	Selecione este campo se quiser adicionar parâmetros condicionais.
Condição	Se você marcou a caixa de seleção **Condicional**, insira as condições aqui.
Detalhes de Integração	
Script de integração	Selecione a inclusão de script que estende o VulnerabilityIntegrationBase a ser executado quando a integração é executada. Este script define como recuperar dados de um sistema de terceiros.
Script de fábrica de integração	Insira um script que defina como construir a inclusão de script selecionada para o **script de integração**. Para obter mais informações, consulte Campos de script de fábrica de integração. **Nota:** Os scripts exigem a experiência ServiceNow e Resposta a vulnerabilidades.
Estratégia do processador de relatórios	Selecione a estratégia que você deseja usar para lidar com os dados retornados pelo script de integração quando a integração é executada. ◦ Selecione **Anexo de fonte de dados** se quiser processar dados usando uma fonte de dados. ◦ Selecione **Processador de relatório personalizado** para selecionar um processador personalizado.
Processador de relatórios	Se você selecionou **Processador de relatório personalizado** no campo **Estratégia do processador** de relatório, selecione a inclusão de script que estende a inclusão de script VulnerabilityReportProcessorBase a ser executada quando a integração for executada. Este script define como processar os dados retornados pelo script de integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Script de fábrica do processador	Insira um script que defina como construir a inclusão de script selecionada para o **Processador de relatório**.

4. Clique em **Enviar**.

Informações relacionadas

- Script de integração de vulnerabilidade
- Estratégias do processador de relatórios
- Campos de script de fábrica de integração
- Executar manualmente uma integração de vulnerabilidade

Script de integração de vulnerabilidade

No formulário Integração de vulnerabilidade, o script de integração é uma referência a uma inclusão de script que estende a inclusão de script VulnerabilityIntegrationBase.

A funcionalidade contida neste script é chamada pelo VulnerabilityIntegrationController para gerenciar os meios pelos quais os dados são recuperados de uma fonte de dados externa. Cada subclasse de VulnerabilityIntegrationBase tem acesso a informações contextuais sobre o processo de chamada. Essas informações estão disponíveis por meio das seguintes variáveis de membro:

- integrationGr — um GlideRecord do registro de integração de vulnerabilidade que solicitou a execução da integração.
- integrationProcessGr — um GlideRecord que fornece informações contextuais para o processo atual de uma integração.

O processo de vulnerabilidade contém parâmetros especiais a serem usados em uma integração, geralmente para fins de paginação. Cada execução de uma integração de vulnerabilidade (chamada de Execução de integração de vulnerabilidade) tem pelo menos um processo de integração de vulnerabilidade associado. Para integrações de várias chamadas, há um ou mais registros do processo de integração de vulnerabilidade para cada execução de integração de vulnerabilidade.

A inclusão de script deve fornecer uma implementação para o método `recuperaData()` e retornar um objeto que é processado pelo script do processador de relatório. O objeto retornado por recuperaData é um objeto simples com propriedades para conteúdo, contentType e extensão.

Esta é uma captura de tela de VulnerabilityIntegrationBase.retrieveData():

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

VulnerabilityIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

A lógica em `recuperaData()` depende da interface necessária para recuperar os dados. Por exemplo, se a origem dos dados extraídos tiver uma REST API, o corpo desse método poderá chamar o endpoint REST, provavelmente por meio de RESTMessageV2. A resposta da chamada pode ser analisada ou colocada em um anexo, e os detalhes podem ser usados para construir o objeto de retorno.

Integrações de chamada única

Os scripts de integração de chamada única (página única) são os tipos mais simples de integrações. Eles exigem uma chamada, geralmente para uma fonte externa de dados, para recuperar dados. Somente recuperaData() é necessário para ser implementado para integrações de página única/chamada única.

Segue um exemplo que demonstra um script simples de integração de chamada única. Ele cria uma RESTMessageV2 e a executa. Em seguida, ele retorna um objeto usando o corpo da resposta como conteúdo, junto com um contentType e uma extensão presumidos.

Script de integração de chamada única

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

Integrações de várias chamadas

Os scripts de integração de várias chamadas (ou várias páginas) são um pouco mais complicados. Eles exigem várias chamadas para uma fonte de dados para recuperar dados.

Como uma integração de chamada única, uma integração de várias chamadas também deve ter recuperaData() implementado. No corpo de recuperaData(), a integração usa os métodos hasMoreData() e setNextRunParameters() fornecidos por VulnerabilityIntegrationBase.

O método hasMoreData() aceita um único booliano que instrui o VulnerabilityIntegrationController a inserir mais processos para extrair mais dados. Ao passar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

verdadeiro para hasMoreData(), uma chamada para setNextRunParameters() é feita para fornecer contexto para o próximo processo.

O método setNextRunParameters() aceita um único objeto que fornece informações de contexto a serem usadas pela próxima chamada para recuperaData(). Este objeto é usado para passar o estado para chamadas subsequentes para RecuperarData(). Um exemplo de caso de uso é passar um objeto que indica o número e o tamanho da página atual para um serviço web.

Para várias integrações de chamadas, cada chamada de recuperaData() verifica primeiro os parâmetros do processo atual. O método _getProcessParameters() é fornecido para todos os VulnerabilityIntegrationBase como uma conveniência para obter os parâmetros definidos pelo processo anterior. Se não houver parâmetros, isso indica que é o primeiro processo.

Segue uma captura de tela de um exemplo de script de integração de várias chamadas. Estendendo no exemplo de integração de chamada única, este script demonstra como fazer chamadas para um endpoint REST que tem suporte de paginação básica. Ele mostra como você pode obter uma única página de dados, reconhecer que há mais dados para recuperar e informar ao próximo processo qual página recuperar.

Script de integração de várias chamadas

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Anexos como valores de retorno de getData()

Às vezes, é preferível retornar um anexo de recuperaData(). A lógica para criar e/ou recuperar um anexo é específica da implementação, mas depois que o anexo é conhecido, suas informações podem ser retornadas.

Para fornecer um anexo, recuperaData() retorna um objeto como:

```
{
        contents: "attachment-sys-id",
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
        contentType: "sys_attachment"
}
```

Segue um exemplo que se estende ao exemplo anterior, mas salva o corpo da resposta da Mensagem REST no registro do processo de integração. Em seguida, ele retorna esse identificador de anexo como o conteúdo do objeto de retorno.

Retornar anexo de recuperaData

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Estratégias do processador de relatórios

O campo **Estratégia do processador de relatório** no formulário Integração de vulnerabilidade é usado para selecionar o método de processamento dos dados retornados pelo script de integração de vulnerabilidade quando o processo de integração de vulnerabilidade é executado.

O valor padrão é **Anexo de fonte de dados**. Este método é a implementação de linha de base que obtém os dados recuperados e os passa para uma fonte de dados a ser importada para o sistema. Selecionar **Processador de relatório personalizado** permite selecionar um script de processador personalizado para processar os dados.

Usar a estratégia do processador de relatório de anexo de fonte de dados

A estratégia do processador de relatório de anexo de fonte de dados é usada para passar dados recuperados pelo script de integração para fontes de dados configuradas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Integrações** e crie uma nova integração.
2. No campo **Estratégia do processador de relatórios**, selecione **Anexo de fonte de dados**.
3. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
4. Na lista relacionada **Fontes de dados de integração de vulnerabilidade**, clique em **Novo**.
5. Defina a fonte de dados a ser usada.
6. Clique em **Enviar**.
7. Repita as etapas 4 a 6 se precisar de fontes de dados adicionais.
   Certifique-se de especificar a ordem em que as várias fontes de dados enviam informações no campo **Ordem**.
8. Clique em **Atualizar**.

Sobre scripts do processador de relatório personalizado

No formulário Integração de vulnerabilidade, o processador de relatório é uma referência a uma inclusão de script que estende a inclusão de script VulnerabilityReportProcessorBase. A funcionalidade contida neste script é chamada pelo VulnerabilityIntegrationController e define os meios pelos quais os dados retornados pelo script de integração são processados.

Cada subclasse de VulnerabilityReportProcessorBase tem acesso a informações contextuais sobre o processo de chamada. Essas informações estão disponíveis por meio das seguintes variáveis de membro:

- integrationGr — um GlideRecord do registro de integração de vulnerabilidade que solicitou a execução da integração.
- integrationProcessGr — GlideRecord do processo de vulnerabilidade que fornece informações contextuais para o processo atual de uma integração.

A inclusão de script deve fornecer uma implementação para o método `processReport()`. O objeto passado para processReport() é o objeto retornado por recuperaData e, como tal, é um objeto simples com propriedades para conteúdo, contentType e extensão. A lógica real em processReport() é específica da implementação e depende dos dados do relatório fornecidos.

Esta é uma captura de tela do VulnerabilityReportProcessorBase.processReport():

Script do processador de relatório personalizado

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Campos de script de fábrica de integração

O formulário Integração de vulnerabilidade contém o script de fábrica de integração e, quando a estratégia do processador de relatório do **Processador** de relatório personalizado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

é selecionada, o script de fábrica do processador. Esses campos são usados para fornecer a lógica para realmente instanciar o objeto definido pelos campos de referência de inclusão de script, script de integração e processador de relatório, respectivamente.

Quando a inclusão de script é selecionada, ambos os campos são preenchidos previamente com uma chamada de construtor sem argumentos. Frequentemente, isso é suficiente, mas pode haver ocasiões em que mais lógica é necessária para instanciar o objeto de script.

O registro integrationProcessGr é exposto aos campos de script de fábrica para que informações específicas do processo possam ser usadas, conforme necessário.

Executar manualmente uma integração de vulnerabilidade

Uma integração de vulnerabilidade está configurada para ser executada de forma programada. No entanto, você pode executá-los manualmente quando necessário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Integrações**.
2. Abra a integração que você deseja executar.
3. Clique em **Executar Agora**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ingestão manual de vulnerabilidades

Inclua vulnerabilidades manualmente na aplicação Resposta a vulnerabilidades para que você possa corrigi-las rapidamente sem ter que esperar pelos resultados do scanner.

Verificadores de terceiros, como Rapid7, ajudam a importar dados de vulnerabilidade para Resposta a vulnerabilidades e processam os dados para relatar as descobertas. Com a integração de ingestão manual, você pode ingerir proativamente as vulnerabilidades e corrigi-las em vez de esperar que os scanners relatem os ativos que estão em risco. A ingestão manual de vulnerabilidades protege efetivamente os ativos contra ameaças desconhecidas, como explorações de dia zero.

Ingestão manual de vulnerabilidades

Você pode importar os dados de vulnerabilidade carregando um modelo nos seguintes formatos de arquivo:

- Excel
- Valor separado por vírgula (CSV)

Para acessar e baixar o modelo, navegue até **Todos** > **Resposta a vulnerabilidades** > **Ingestão manual de item de vulnerabilidade** > **Carregar IU de arquivo**.

Certifique-se de seguir estes pontos-chave ao preencher os registros no modelo:

- Não cometa erros de digitação nos registros da coluna Gravidade/Estado. Se houver um erro de digitação, o registro será ignorado.
- Não mude os nomes das colunas.
- Não coloque nomes de coluna em nenhuma linha, exceto na primeira linha.
- Não altere a ordem das planilhas no modelo do Excel. Os dados de vulnerabilidades devem estar sempre presentes na segunda planilha.
- Não coloque detalhes de vulnerabilidades em nenhuma folha, exceto na folha Detecções manuais de entrada.
- Não use nenhum caractere, exceto caracteres alfanuméricos e especiais, como hífen (-), ponto (.), adição (+), sublinhado (_), espaço, colchetes '(' ')' e símbolo de arroba (@) para o nome do arquivo.

Para obter instruções sobre como preencher os dados no modelo, consulte Modelo para ingestão manual de vulnerabilidades.

Integrações de ingestão manual

A integração é acionada quando um arquivo é carregado. Com base no tipo de arquivo carregado, a integração relacionada é acionada.

Para exibir as integrações, navegue até **Todos** > **Resposta a vulnerabilidades** > **Ingestão manual de item de vulnerabilidade** > **Integrações**.

As seguintes integrações de ingestão manual do sistema base estão disponíveis por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações

Tipo de integração	Descrição
Integração do Excel de ingestão manual	Recupera dados buscando o arquivo do Excel mais recente carregado da tabela Fila de envio de ingestão de vulnerabilidade e copia o anexo para a respectiva execução de integração.
Integração de CSV de ingestão manual	Recupera dados buscando o arquivo CSV mais recente carregado da tabela Fila de envio de ingestão de vulnerabilidade e copia o anexo para a respectiva execução de integração.

A integração de terceiros por ingestão manual cria uma instância de integração, por padrão, com os dois parâmetros de instância de integração a seguir:

- max_input_records: define o número de registros que podem ser criados no modelo. Se você adicionar mais registros do que o especificado neste parâmetro, os registros adicionais serão ignorados. O número de registros pode ser atualizado na coluna Valor. O número recomendado de criações de registros no modelo é 1000. Qualquer coisa acima desse valor pode representar desafios de desempenho.
- insert_fixed: importa detecções de vulnerabilidades fixas.

Para exibir os parâmetros da instância de integração, navegue até **Todos** > **Resposta a vulnerabilidades** > **Ingestão manual de item de vulnerabilidade** > **Integrações** e clique na instância de origem de qualquer integração. Como alternativa, você pode navegar até **Todos** > **Resposta a vulnerabilidades** > **Instâncias de Integração** e clique em **Ingestão manual**.

Ingerir vulnerabilidades manualmente

Ingerir vulnerabilidades manualmente carregando um modelo com dados de vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar IU de arquivo**.
2. Clique nos links Excel ou CSV e baixe o modelo no respectivo formato.
3. No modelo, insira os dados de vulnerabilidade nos registros.
   Para obter instruções sobre como preencher os dados no modelo, consulte Modelo para ingestão manual de vulnerabilidades.
4. Clique **em Importar arquivo** e carregue o modelo atualizado.
5. Clique em **Enviar**.
   A página Filas de envio de integração de vulnerabilidade é exibida. Você pode exibir a lista de instâncias de integração, o status das execuções de integração e as anotações de log após a conclusão da execução de integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de carregar o arquivo, navegue até **Todos** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Integrações**. Verifique se a execução da integração foi bem-sucedida.

Verificar execução de integração manual

Verifique se a execução da integração foi bem-sucedida. Exiba o número de detecções individuais e os itens vulneráveis (IVs) criados ou atualizados devido à execução da integração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Integrações**.
2. Clique no nome da integração com base no tipo de arquivo carregado.
3. Clique na guia **Execuções de integração de vulnerabilidade**.
4. Clique no número da execução de integração.
5. Clique na guia **Itens**.
6. Revise as informações na guia **Itens**.

Guia Itens

Guia/Campo	Descrição
Guia Itens	Exibe o número total de IVs importados. Você pode ver o total de detecções importadas adicionando os números listados na guia Detecções.
Novos itens	Exibe o número de itens vulneráveis criados a partir desta execução de integração.
Itens importados	Exibe a soma de todos os campos nesta seção.
Itens duplicados	Exibe itens duplicados. Este campo não está mais preenchido.
Itens atualizados	Exibe o número de vezes que os itens vulneráveis são atualizados durante esta execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
Itens inalterados	Exibe itens vulneráveis encontrados durante a execução de integração que existem no banco de dados, mas não foram atualizados porque nenhum dos valores de campos relevantes foi alterado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de verificar se a execução da integração foi bem-sucedida, navegue até **Todos** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar histórico de arquivos**. Verifique se há registros com falha das Anotações.

Configurar detecções manuais de fechamento automático

Habilite o fechamento automático de detecções manuais para fechar automaticamente as detecções manuais obsoletas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar IU de arquivo**.
2. Clique **em Mudar configuração de fechamento automático**.
3. Clique na guia **Detecções manuais**.
4. Certifique-se de que a caixa de seleção Encerrar automaticamente **as detecções manuais** esteja marcada.
5. No campo **Últimas detecções manuais encontradas (dias atrás)**, insira o número de dias após o qual as detecções manuais devem ser encerradas.
   O padrão é 90 dias. Você pode inserir qualquer valor positivo para o número de dias.

Verificar status de carregamento

Verifique se a execução da integração de vulnerabilidade foi bem-sucedida, parcialmente bem-sucedida ou uma falha.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Ingestão de item vulnerável manual** > **Carregar histórico de arquivos**.
2. Na tabela Filas de envio de integração de vulnerabilidade, verifique a hora do upload e o status do upload nas colunas Criado e Estado, respectivamente.
3. Opcional: No campo **Anotações**, exiba o motivo da falha.

Modelo para ingestão manual de vulnerabilidades

O modelo fornece colunas que devem ser preenchidas com dados de vulnerabilidade e item de configuração (IC). Depois que o modelo é preenchido e carregado, os dados são processados.

Instruções para preencher o modelo

Para inserir os detalhes no modelo, siga as instruções fornecidas na tabela a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instruções do modelo

Coluna	Obrigatório/ opcional?	Tamanho da cadeia de caracteres (máximo)/ valores válidos	Descrição
ID do ativo	Opcional	255	Identificador exclusivo universal (UUID) ou ID do ativo. Pode ser o valor gerado por um scanner.
Insira informações em pelo menos uma das cinco colunas a seguir:			
Endereço MAC	Obrigatório	24	Informações de host ou ativo. A combinação de todos os valores fornecidos deve ser exclusiva para um ativo.
FQDN	Obrigatório	255	
NETBIOS	Obrigatório	255	
Endereço IP	Obrigatório	255	
Nome do host	Obrigatório	255	
As colunas restantes não dependem umas das outras.			
ID de vulnerabilidade	Obrigatório	255	Representa uma vulnerabilidade no banco de dados nacional de vulnerabilidades (NVD) ou um ID retornado de um scanner de terceiros.
Resumo de vulnerabilidade	Opcional	512	Breve descrição da vulnerabilidade. Ele é adicionado ao banco de dados somente quando o ID de vulnerabilidade não está disponível.
Gravidade	Opcional	crítico, alto, médio, baixo, nenhum	Gravidade da vulnerabilidade. Ele é adicionado ao banco de dados somente quando o ID de vulnerabilidade não está disponível. Se o registro estiver vazio, por padrão, ele será considerado crítico.
Porta	Opcional	Não aplicável	Porta pela qual a vulnerabilidade é detectada. O valor deve ser um número inteiro válido. Se houver uma entrada inválida, o registro será ignorado.
Protocolo	Opcional	40	Tipo de protocolo de rede usado.
Prova	Opcional	4000	Representa o local ou o caminho do sistema da vulnerabilidade.
Estado	Opcional	aberto, fixo	Status da detecção. Se o registro estiver vazio, por padrão, ele será considerado aberto.

Tradução automática

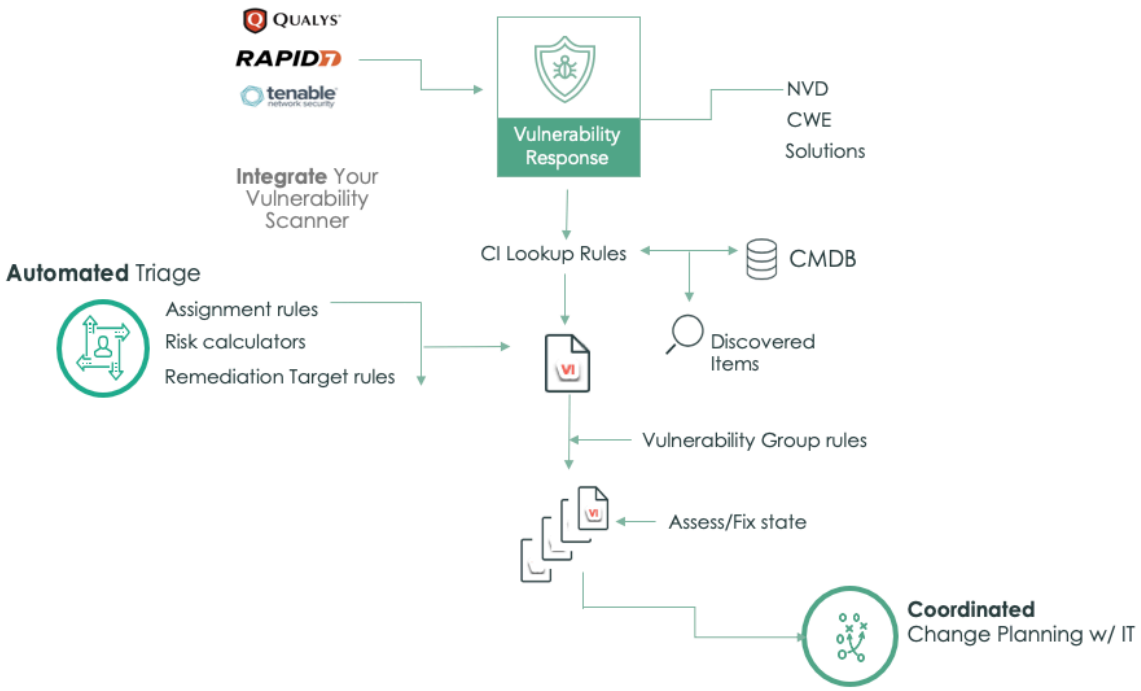
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades visão geral da correção

Resposta a vulnerabilidades A correção é um processo em fases que consiste na verificação da conclusão da importação, na triagem de novas vulnerabilidades e no monitoramento do andamento até a conclusão. Abordada dessa forma, a correção se torna gerenciável, oportuna e, de várias maneiras, automatizada.

Compreender sua postura de segurança em todos os ativos da empresa ajuda a identificar as vulnerabilidades mais críticas para correção. Este processo de correção requer que Resposta a vulnerabilidades e uma integração de terceiros, como Qualys Vulnerability Integration, estejam instalados e configurados.

Fluxo do processo de integração da Resposta a vulnerabilidades



Verificar a conclusão bem-sucedida das importações de integração de terceiros

A primeira fase deste processo é garantir que tudo esteja funcionando corretamente. Resposta a vulnerabilidades está predefinido para baixar vulnerabilidades do Banco de dados nacional de vulnerabilidades (NVD) e vulnerabilidades de enumeração comum (CWE). As importações de terceiros fornecem os dados necessários para criar itens vulneráveis e tarefas de correção. A correção bem-sucedida depende da importação consistente e bem-sucedida de vulnerabilidades e itens vulneráveis.

Durante a importação, as regras de pesquisa de IC correspondem a ativos de terceiros com ativos no Configuration Management Database (CMDB). Todos os ativos são armazenados no módulo Itens descobertos. As informações de IC são essenciais para a implementação da solução.

Nota: Depois que uma integração de terceiros foi instalada e configurada, há algumas instâncias em que uma importação pode falhar, por exemplo, se o fornecedor de terceiros limitar suas chamadas de API. Quando as importações falham, elas exigem atenção imediata.

Os relatórios de execução de status da integração para as integrações de terceiros compatíveis são enviados com as aplicações para fornecer uma visão geral gráfica de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

suas importações. Use este relatório, ou crie o seu próprio, para determinar facilmente se a importação mais recente foi bem-sucedida. Para obter mais informações sobre integrações compatíveis, consulte Integrações do Resposta a vulnerabilidades.

Revisar e fazer a triagem de vulnerabilidades e itens vulneráveis

A próxima fase da correção exige a revisão de novas vulnerabilidades e itens vulneráveis. Um item vulnerável (VI) é uma combinação detectada de vulnerabilidade e item de configuração (IC). Conforme os itens vulneráveis são formados, várias regras são executadas para atribuir IVs, determinar o risco que eles representam e definir metas de correção. Ajuste as regras, conforme necessário, para garantir que os itens vulneráveis tenham sido triados com sucesso.

Monitorar o andamento da correção de vulnerabilidades existente

A fase final da correção consiste em monitorar seu andamento.

- Revise o status das importações de implementações de patch que não apareceram e faça o acompanhamento com as Operações de TI.
- Acompanhe o andamento das obrigações de conformidade regulatória e garanta sua conclusão.
- Revise o status do item adiado e revise ou implemente correções.
- Monitore os painéis da Gestão de vulnerabilidades. Para revisar tendências, exibir relatórios em tempo real e usar métricas que rastreiam suas taxas de obtenção de meta de correção, talvez você prefira monitorar seus processos com a aplicação Performance Analytics para Resposta a vulnerabilidades.
- Fechando detecções obsoletas em Resposta a vulnerabilidades.

Verificar a conclusão bem-sucedida de Resposta a vulnerabilidades importações de integração

A maneira mais fácil de determinar se suas importações foram bem-sucedidas é usar um painel de status de execução de integração. O painel Status de execução de integração fornece um exemplo de uma exibição gráfica do status de execuções de integração de terceiros.

As integrações de vulnerabilidade Qualys e Rapid7 têm um painel de status de execução de integração. Consulte Qualys gráfico de status de execução de integração ou Integração com Rapid7 Vulnerability gráfico de status de execução para obter informações detalhadas sobre o conteúdo do gráfico.

Nota: Gráficos, para integrações não fornecidas por ServiceNow®, podem ser criados a partir de relatórios em um painel, mas podem exigir experiência de ServiceNow. Para obter mais informações sobre como criar relatórios e painéis, consulte Introdução a relatórios e painéis.

Exibir Resposta a vulnerabilidades dados de detecção de itens vulneráveis

Os dados completos coletados por suas integrações de scanner de terceiros com Resposta a vulnerabilidades são exibidos nas guias Detecções e Detecções iniciais nos registros de itens vulneráveis (VIT). Também é exibido em registros de Detecção na lista de Detecção de Item Vulnerável em sua instância Now Platform®.

Antes de Iniciar

As integrações de terceiros recuperam dados de detecção de itens vulneráveis. As detecções são ocorrências distintas de vulnerabilidades conforme relatadas pelos scanners. Os dados de detecção são emparelhados com itens vulneráveis e o estado de VI é

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atualizado com base no estado das detecções. Se um IV não for encontrado, um novo será criado. As detecções são abertas ou fechadas somente por dados encontrados diretamente por um scanner.

Função necessária:

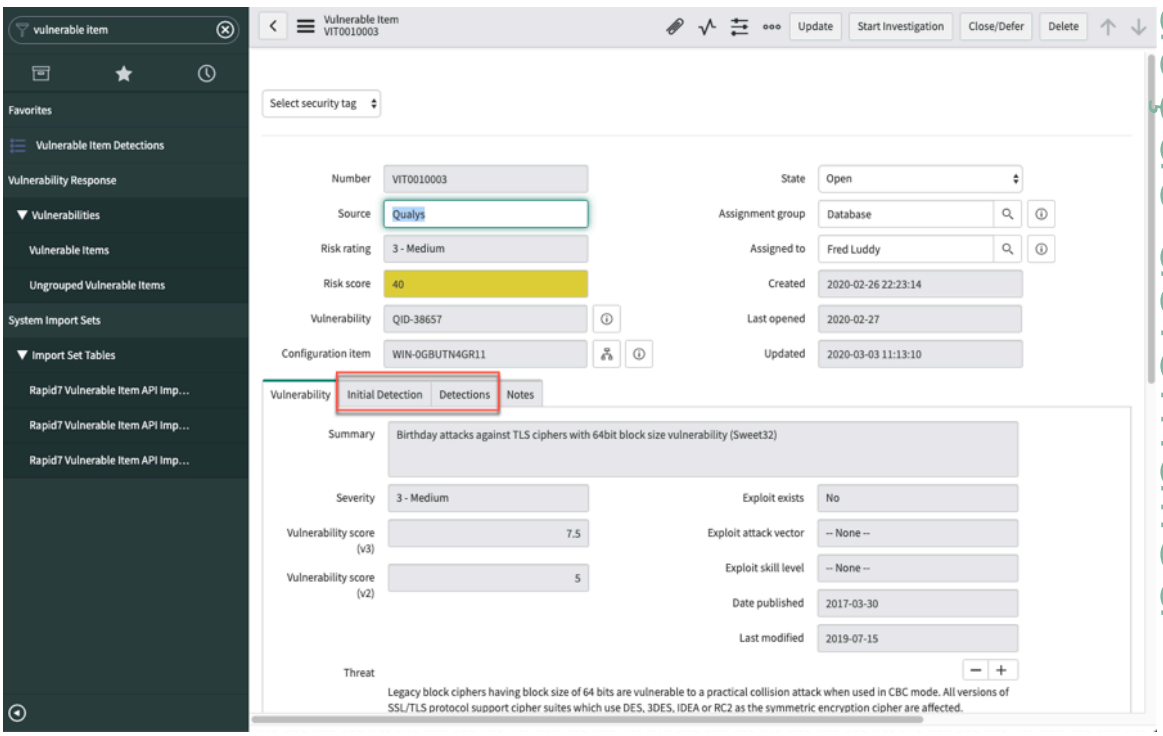
- sn_vuln.admin inicia execuções de integração e exibe dados de detecção de itens vulneráveis.
- sn_vul.remediation_owner está atribuído a itens vulneráveis criados a partir de detecções de itens vulneráveis e exibe dados em registros de VI.

Procedimento

1. Para exibir os dados de detecção de item vulnerável, navegue até um registro de item vulnerável e abra-o.

   O registro é exibido com as guias Detecções iniciais e Detecções.

   Nota: Os dados exibidos anteriormente na guia Detalhes da configuração são exibidos junto com outros dados de detecção nas guias Detecção inicial e Detecções.

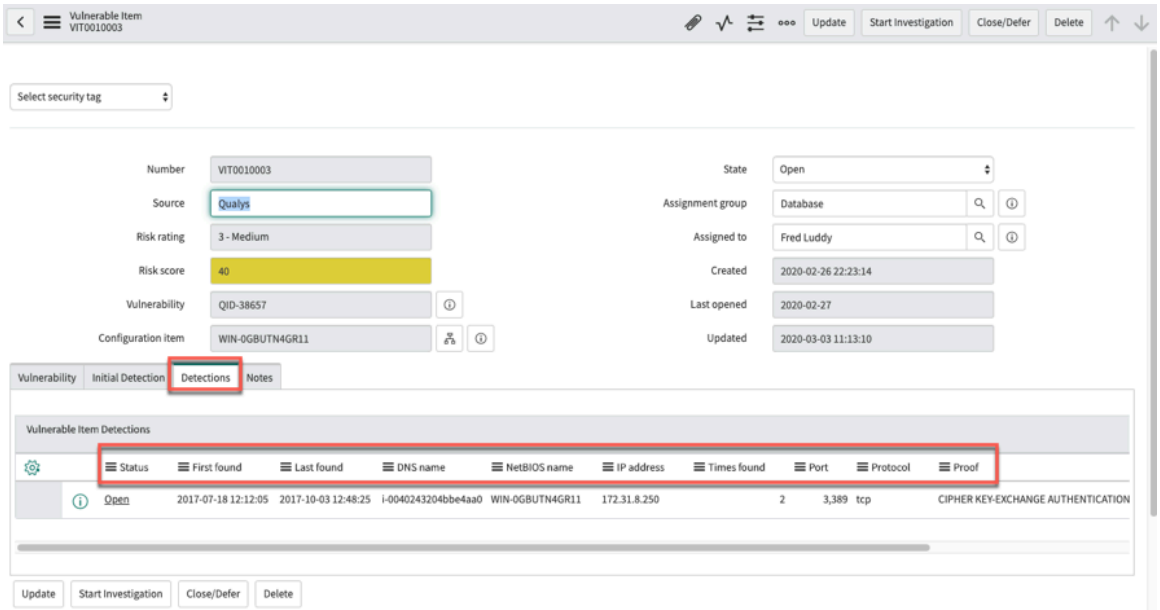


2. Clique na guia **Detecções**.

   Quando um item vulnerável é criado a partir dos resultados de uma verificação de terceiros, os dados da verificação são exibidos no registro de detecção, conforme mostrado na figura a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cada linha na seção Detecções de itens vulneráveis representa dados de uma detecção distinta. Na coluna Primeiro encontrado, a data em que o item vulnerável foi detectado pela primeira vez pelo scanner é exibida. Na coluna Último encontrado, a data da detecção mais atual é exibida. O campo Origem exibe o scanner que recuperou os dados.

Nota: Para Qualys, com detecções de item vulnerável, os seguintes campos estão obsoletos no registro VI e não são mais preenchidos:

- Qualys severidade
- Última atualização pela origem

Também para Qualys, conforme mostrado na figura anterior, quando um VI é criado a partir de uma verificação, o valor da verificação de Resultados é exibido na coluna Prova no registro de detecção. No entanto, este valor não é exibido na parte superior do registro VI.

Para Rapid7, quando um VI é criado a partir de uma verificação, o valor da Prova da verificação pode ser exibido na coluna Prova no registro de detecção e na parte superior do registro de VI, mas não por padrão. Para exibir este valor na parte superior do registro VI, selecione o campo Prova no layout do formulário.

3. Opcional: Para configurar o layout da guia Detecções no registro, siga estas etapas.

a. As colunas a seguir são exibidas na guia Detecções por padrão.

- Status
- Primeiro encontrado (dados)
- Último encontrado (data)
- Nome DNS
- Net BIOSname
- Endereço IP
- Horas encontradas
- Porta

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Protocolo
- Prova
- SSL

Nota:

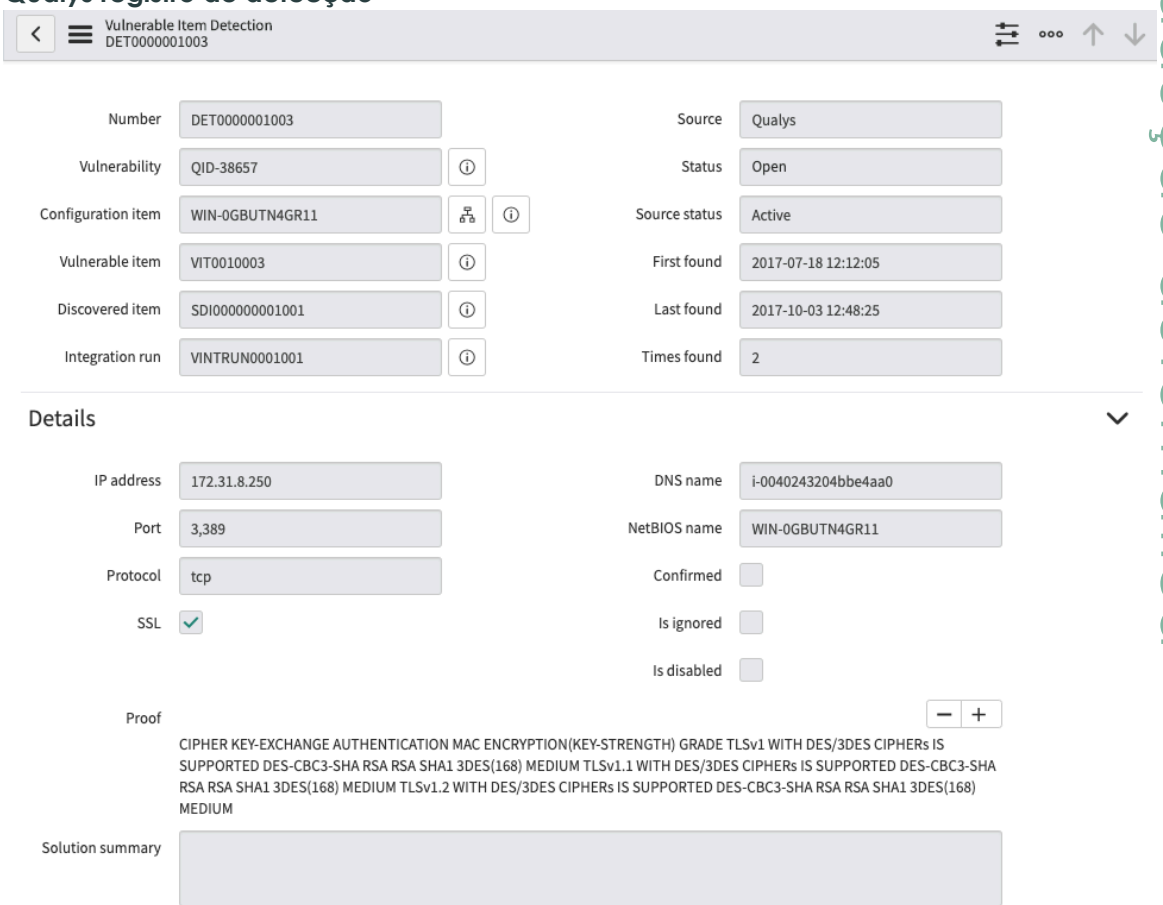
Observação: se não houver valor em uma coluna, os dados desse campo não foram detectados pelo scanner.

b. Clique no ícone de engrenagem (ícone de) para personalizar sua exibição.

c. Selecione as colunas do slushbucket para exibir dados específicos e clique em **OK**.

4. Com a guia Detecções selecionada, na coluna Status, clique em um item para abrir o registro de detecção e exibir os detalhes associados a esse item vulnerável, incluindo um Resumo da solução (somente integração do Rapid7 InsightVM).

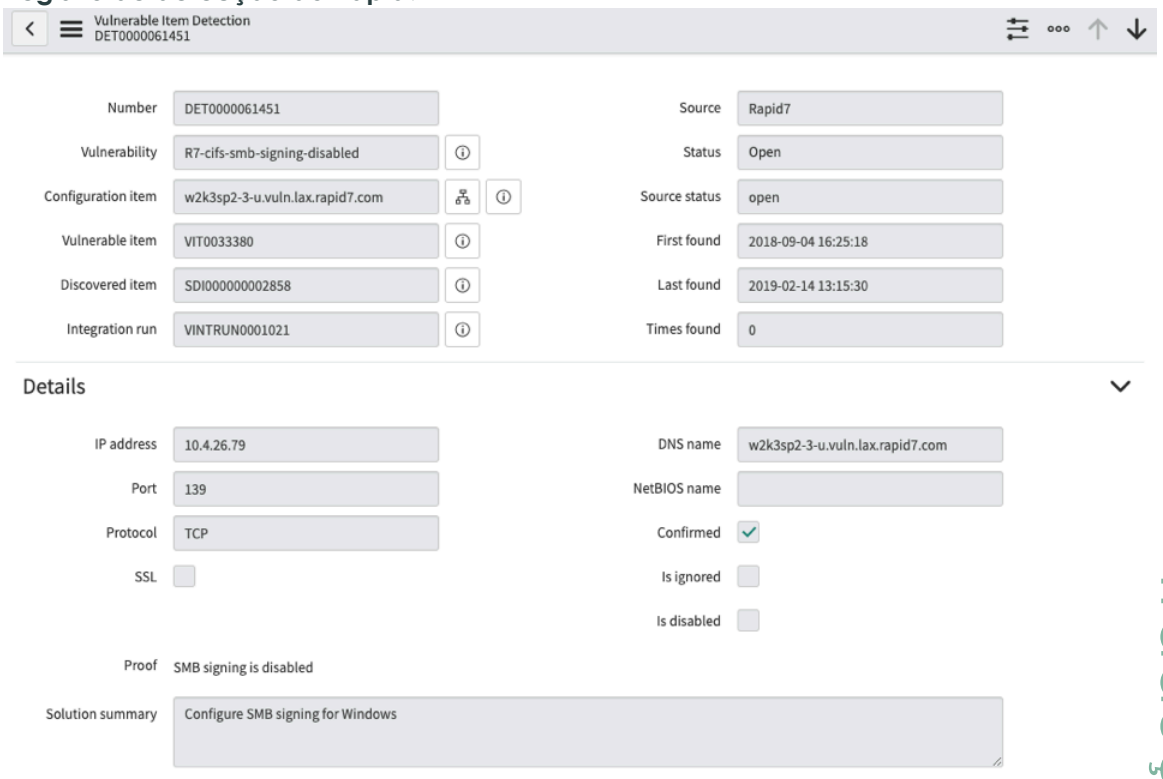
Qualys registro de detecção



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de detecção do Rapid7

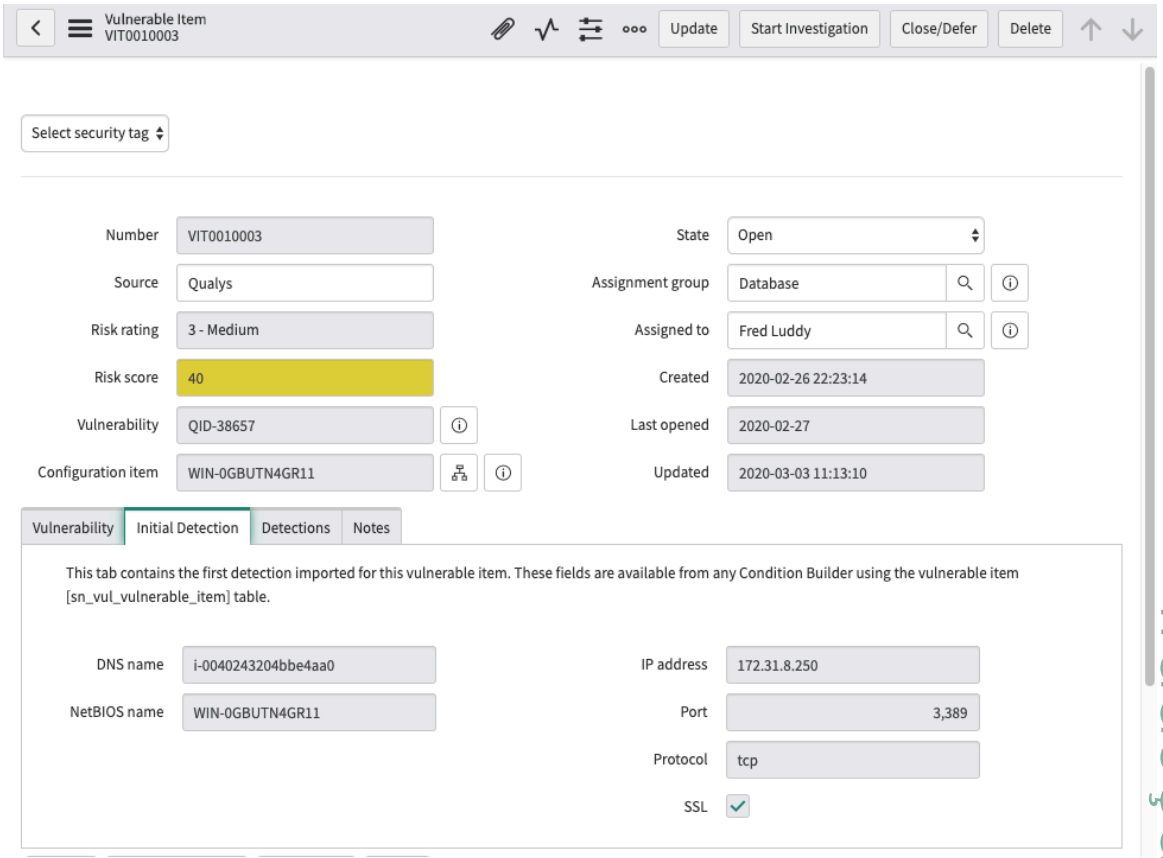


5. Retorne ao registro e selecione a guia Detecção inicial.

A guia Detecções iniciais exibe os dados importados do scanner de terceiros na primeira ocorrência da detecção. Essas informações na guia de detecção inicial não mudam conforme os dados de detecção são atualizados.

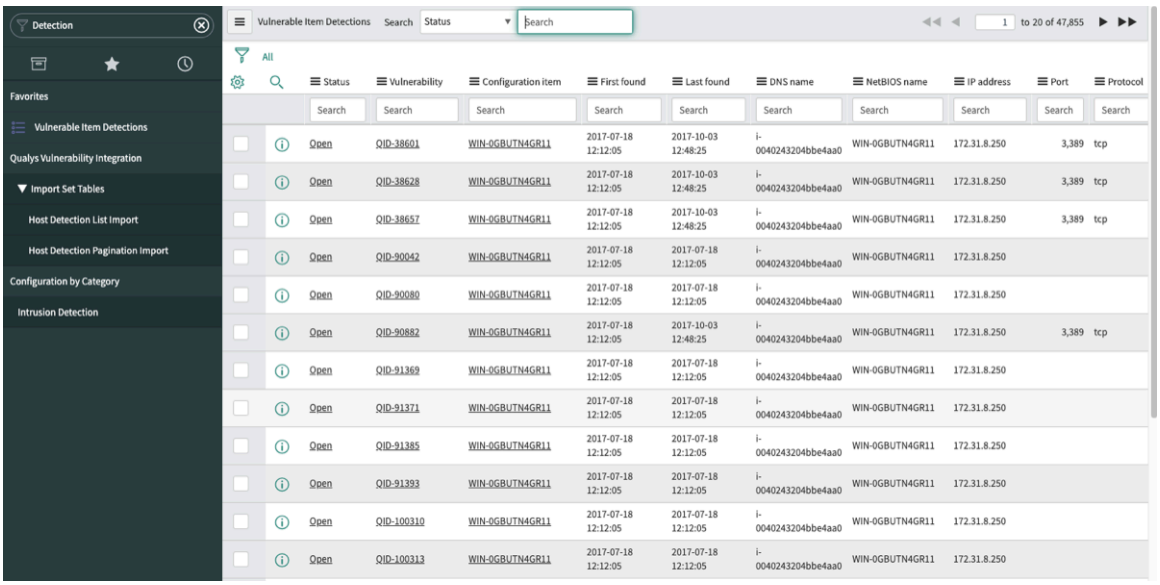
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Opcional: Navegue até Detecções de itens vulneráveis para exibir a Lista de detecção de itens vulneráveis.

(Optional) A lista de Detecção de item vulnerável é exibida. Cada linha na lista de Detecções de itens vulneráveis representa uma detecção distinta. As colunas exibem os mesmos dados que o registro VI.



As detecções são abertas ou fechadas somente pelos dados encontrados por um scanner. Eles não são acumulados a partir de IVs. Conforme as detecções são importadas, elas são usadas para criar IVs e atualizar os estados dos IVs. Se todas as

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

detecções de um item vulnerável forem encerradas, esse item vulnerável será encerrado. No registro VI, o estado é `fechado`e o subestado é `fixo`.

Nota: Os erros são registrados enquanto:

- Processando anexos recuperados do scanner.
- Criar ou atualizar detecções ou itens vulneráveis.

Para obter informações sobre como lidar com erros de detecção, consulte Manipulação de erros para detecções.

Quando todos os IVs são encerrados para uma tarefa de correção, a tarefa de correção é encerrada.

IVs encerrados com um subestado **fixo** ou **obsoleto** serão reabertos se uma nova detecção for criada e os VIs puderem ser correspondidos com a nova vulnerabilidade.

Itens vulneráveis definidos como **Resolvidos** em sua instância, mas não transicionados para **Encerrado/Corrigido** pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Quando todos os IVs são encerrados para uma tarefa de correção, o registro é encerrado.

Itens vulneráveis definidos como "Resolvidos" em sua instância, mas não transicionados para "Fechados/Corrigidos" pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Para Rapid7 detecções, uma opção agora está disponível na página de configuração do Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como **Resolvidos**, mas não transicionados para **Encerrado/Corrigido** por verificações subsequentes, retornam para **Aberto** após o número de dias inserido.

Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como "Resolvidos", mas que não foram transicionados para **Encerrado/Corrigido** por verificações subsequentes, esses VIs voltarão para **Aberto** quando a última data encontrada for posterior à data de Resolvido.

O que Fazer Depois

Para exibir mais dados, incluindo contagens de item e detecção, você pode Verificar Resposta a vulnerabilidades dados de detecção de item vulnerável em registros de execução de integração (VINTRUN).

Verificar Resposta a vulnerabilidades dados de detecção de item vulnerável em registros de execução de integração (VINTRUN)

A partir de registros de execução de integração em sua instância Now Platform®, você pode localizar dados de detecção de item vulnerável de integração de terceiros com base na data e hora das verificações. Verifique se a verificação foi concluída com sucesso e exiba o número (contagens) de detecções individuais, bem como todos os itens vulneráveis (IVs) que foram criados ou atualizados diretamente como resultado das verificações.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vuln.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode preferir que as informações de execução de integração, data e hora da verificação ou o número do registro de execução de integração (VINTRUN#) do item vulnerável ou registros de detecção para ajudá-lo a localizar registros específicos nas listas a seguir.

Procedimento

1. Escolha um para continuar.

Integração	Descrição
Navegar até **Integração com Rapid7 Vulnerability** > **Administração** > **Integrações**	Na lista Integrações do Rapid7, escolha a integração para a qual você deseja exibir os resultados da verificação de detecção. **a.** Depósito de dados da Rapid7: ▪ Integração de item vulnerável da Rapid7 ▪ Integração de resolução de item vulnerável da Rapid7 ▪ Integração abrangente de item vulnerável da Rapid7 **b.** Integração de resolução de item vulnerável da Rapid7 (InsightVM) ▪ Integração de item vulnerável da Rapid7 - API ▪ Integração abrangente de item vulnerável da Rapid7 - API
Navegar até **Qualys** > **Integração de vulnerabilidade da Qualys** > **Integrações Primárias**	Na lista Integrações da Qualys, escolha entre: ◦ Qualys Host Detection Integration ◦ Integração de Detecção Abrangente de Host da Qualys
Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**	Na lista Integrações da Tenable, escolha a integração para a qual você deseja exibir os resultados da verificação de detecção.
Navegar até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integrações**	Na lista Integrações do Microsoft TVM, escolha a integração para a qual você deseja exibir os resultados da verificação de detecção.

2. Na parte inferior da página exibida, clique na guia **Execuções de integração de vulnerabilidade**.

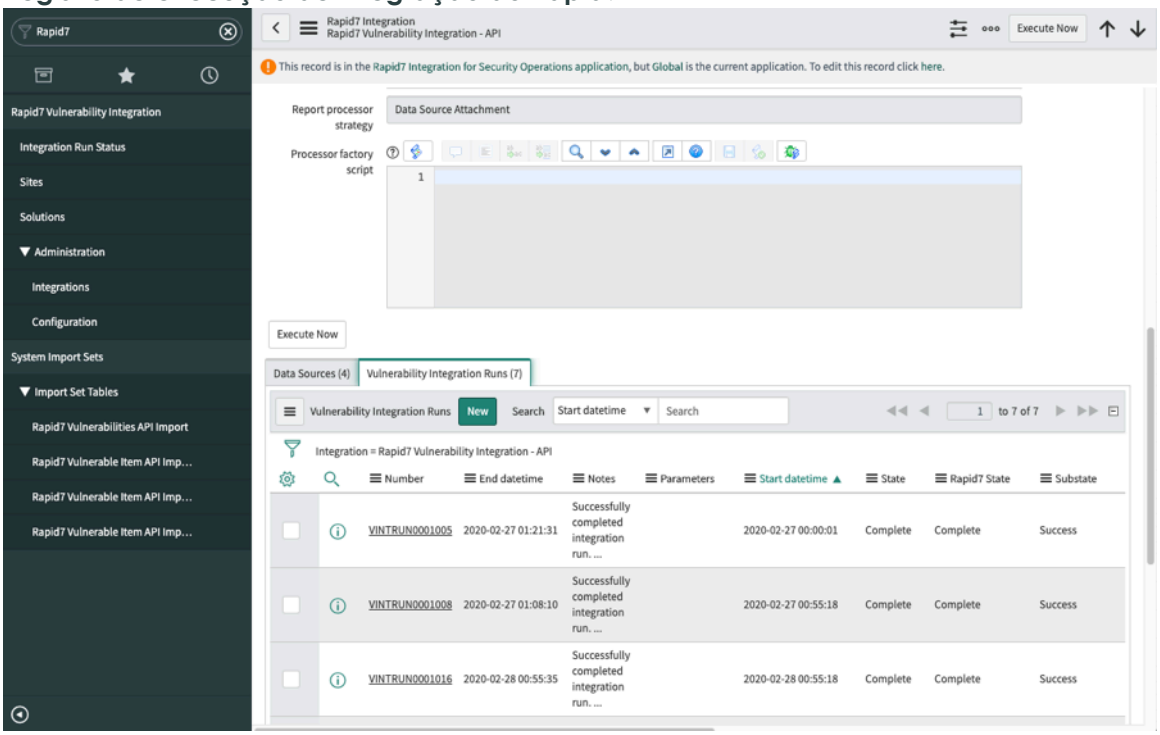
3. Clique em um item nas colunas Número ou Origem da importação para abrir um registro.

O registro de execução de integração é exibido.

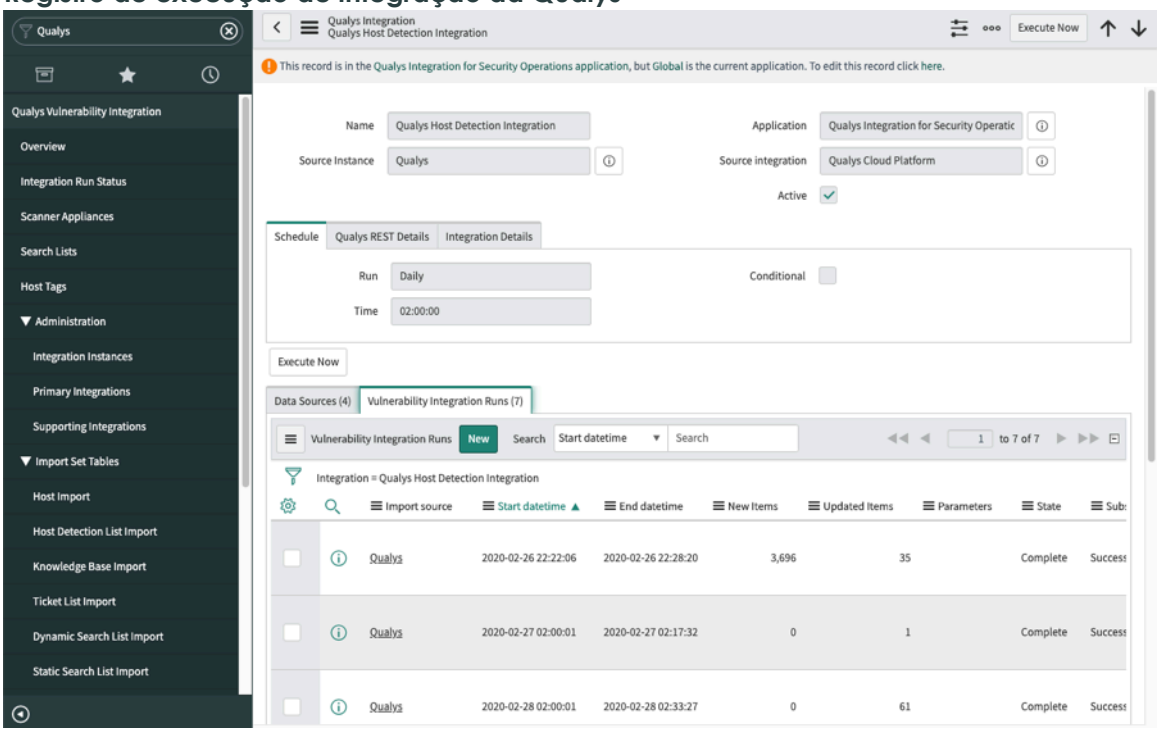
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de execução de integração do Rapid7



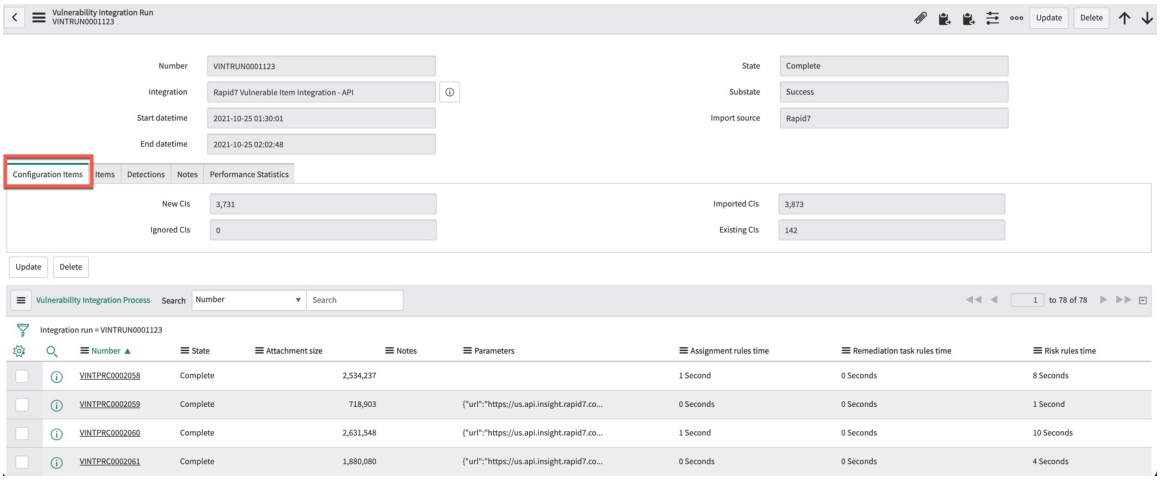
Registro de execução de integração da Qualys



O registro de execução de integração é exibido. Você pode verificar no campo Estado que a integração foi executada com sucesso. Selecione a guia **Itens de configuração**.

Tradução automática

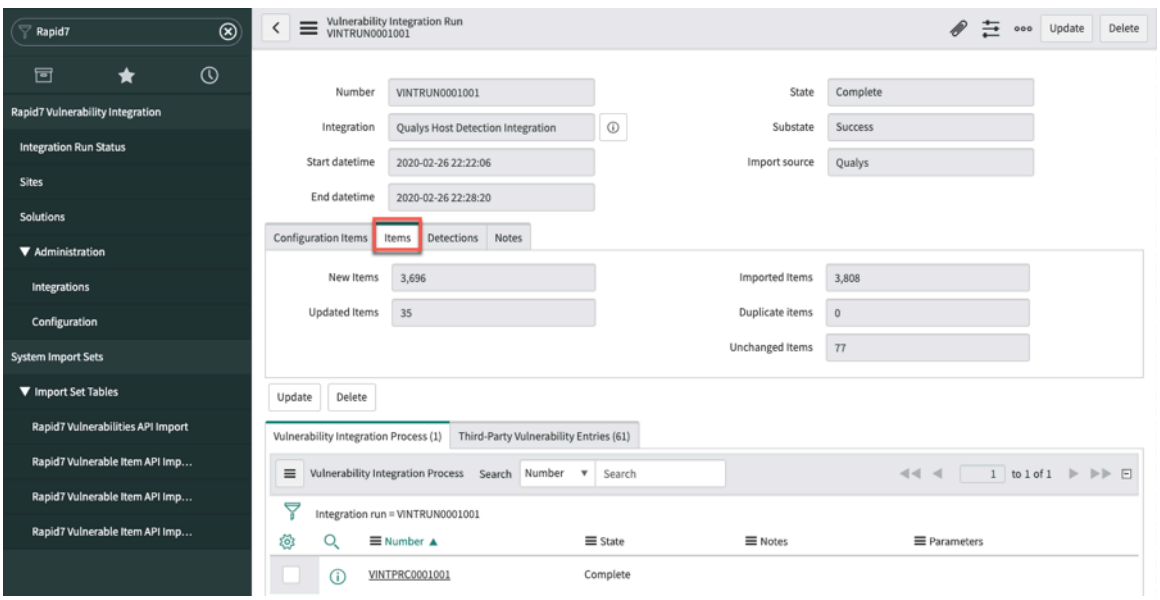
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia Itens de configuração exibe as seguintes informações:

- A guia Itens de configuração exibe o número total de itens de configuração importados.
- O campo Novos ICs exibe o número de ICs criados como parte desta execução de integração.
- O campo ICs importados exibe a soma de todos os ICs nesta seção.
- O valor do campo ICs ignorados é sempre 0 para as integrações Resposta a vulnerabilidades.
- O campo ICs existentes exibe o número total de ICs que já existem.

Clique na guia **Itens**.



A guia Itens exibe as seguintes informações:

- A guia Itens exibe o número total de IVs importados. Você pode ver o total de detecções importadas adicionando os números listados na guia Detecções.
- O campo Novos itens exibe o número de itens vulneráveis que são criados a partir desta execução de integração.
- O campo Itens importados exibe a soma de todos os campos nesta seção.
- O campo Itens duplicados não está mais preenchido.

Tradução automática

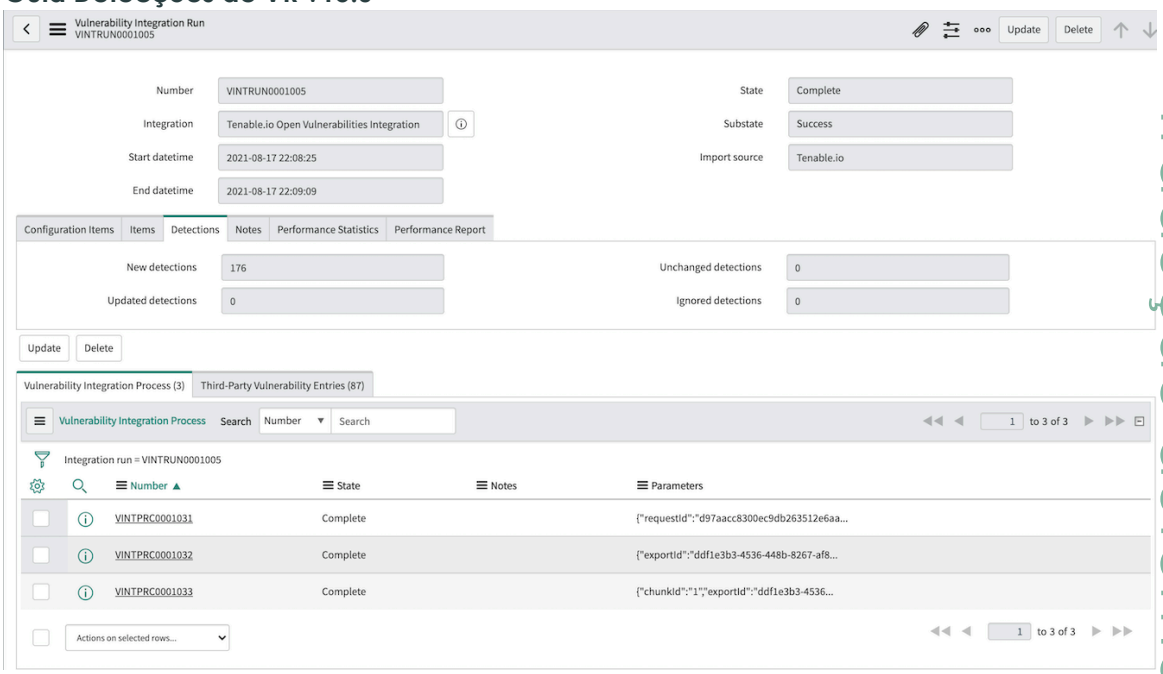
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O campo Itens atualizados exibe o número de vezes que os itens vulneráveis são atualizados durante esta execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
- O campo Itens inalterados exibe itens vulneráveis encontrados durante a execução de integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campos relevantes foi alterado.

4. Clique na guia **Detecções**.

Esta guia só será exibida se a execução da integração tiver detecções. Você pode verificar o total de detecções importadas adicionando os números listados.

Guia Detecções de VR v15.0



Nota: Antes da v15.0, não havia campo para detecções ignoradas.

A guia Detecções exibe as seguintes informações:

- A partir da v15, um novo campo Detecções ignoradas foi adicionado para rastrear as detecções que antes eram ignoradas. Com esta implementação, a contagem de detecções importadas e a contagem rastreada nos registros de execução de integração se tornam consistentes. Esta funcionalidade foi implementada para todos os scanners, ou seja, Qualys Vulnerability Integration, Integração com Rapid7 Vulnerability, Integrações de vulnerabilidade da Tenable e Microsoft TVM.
- O campo Novas detecções exibe novas detecções que são criadas durante esta execução de integração.
- O campo Detecções inalteradas exibe as detecções encontradas durante a execução de integração que já existem no banco de dados, mas não foram atualizadas porque nenhum dos valores de campos relevantes foi alterado.
- O campo Detecções atualizadas exibe o número de vezes que as detecções são atualizadas durante esta execução de integração. Este valor não é o número de detecções exclusivas atualizadas. Se, por exemplo, uma detecção for atualizada duas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vezes como parte da execução de integração, ela será contada duas vezes e exibida como 2 detecções atualizadas.

Nota: As detecções que não são exibidas nessas contagens são detecções que estão em um estado fechado (Fixo), porque registros fixos são usados para atualizar IVs existentes. Se você quiser mais visibilidade para esses registros de detecção, poderá exibir os IVs encerrados que são criados quando não houver um VI correspondente existente em um estado aberto. Para obter mais informações sobre vulnerabilidades no estado fixo que você pode habilitar no Assistente de configuração para a integração da Qualys, consulte Configuração de Resposta a vulnerabilidades usando o Assistente de configuração.

5. Clique em um item nas colunas Número ou Origem da importação para abrir um registro.

Exibição de dados de patch e programação de patches no Resposta a vulnerabilidades

A partir da v16.1 de Resposta a vulnerabilidades, você pode programar patches e exibir dados de patch junto com a solução e outras informações de vulnerabilidade em registros no ambiente clássico e nos espaços Resposta a vulnerabilidades na sua instância Now Platform.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para importar seus patches para exibir dados e programar patches. Consulte as integrações compatíveis para obter mais informações.

- Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades e Noções básicas sobre a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM.
- Exibição de dados de orquestração de patches nos painéis Resposta a vulnerabilidades no ambiente clássico.
- Exiba dados em cartões de pontuação no Resposta a vulnerabilidades Espaços.

Programação de patches

Você pode programar patches dos seguintes registros:

- Atualização de patch (VPU)
- Tarefa de correção (RT)
- Item descoberto (SDI)

Dados de patch no ambiente clássico

No ambiente clássico na aplicação Resposta a vulnerabilidades :

- Para exibir registros de atualização de patch, navegue até **Todos** > **Resposta a vulnerabilidades** > **Patches**.
- Para exibir Soluções, navegue até **Todos** > **Resposta a vulnerabilidades** > **Soluções**.
- Para exibir IVs atribuídos a você que tenham patches, navegue até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Atribuído a mim com patches**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para exibir tarefas de correção, navegue até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Atribuído a mim com patches**
- Para exibir registros de itens descobertos, navegue até **Todos** > **Operações de segurança** > **Itens descobertos**.

Dados de patch e rollup de estado para orquestração de patches no Resposta a vulnerabilidades

A partir da v16.1 de Resposta a vulnerabilidades, os dados e estados de patch são acumulados para Patch Update e outros registros na aplicação Resposta a vulnerabilidades.

Registros de atualização de patch nos espaços no ambiente clássico do Resposta a vulnerabilidades

Informações sobre patches, soluções de vulnerabilidade e vulnerabilidades estão todas conectadas na aplicação Resposta a vulnerabilidades.

Os dados de patch e os dados e status de rollup de patch são exibidos em registros em sua instância. Os registros de patch são incluídos como parte do recurso de orquestração de patches desta integração com Resposta a vulnerabilidades. Exiba os registros de patch (VPU) nos Espaços de resposta a vulnerabilidades na Exibição de lista no Espaço de correção de TI. Os registros de Atualização de patch na exibição clássica e nos Espaços de resposta a vulnerabilidades incluem os seguintes dados:

- Dados de solução de vulnerabilidade e informações de fornecedores de patch importados pela aplicação Gestão de soluções de vulnerabilidade.
- Status de correção de origem que inclui o número total de dispositivos que têm uma vulnerabilidade que pode ser corrigida por um patch e todos os dispositivos sem atualizações.
- Status de correção que inclui % de IVs corrigidos e o total de VIs que têm um patch como preferencial.
- Dispositivos associados, itens vulneráveis, implantações de patch e solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos Espaços de resposta a vulnerabilidades.
- Solicitações de patch que os proprietários de correção enviaram para aprovação.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para exibir dados e programar patches. Consulte as integrações compatíveis para obter mais informações.

- Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades e Noções básicas sobre a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM.
- Exibição de dados de orquestração de patches nos painéis Resposta a vulnerabilidades no ambiente clássico.
- Exiba dados em cartões de pontuação no Resposta a vulnerabilidades Espaços.

Tradução automática

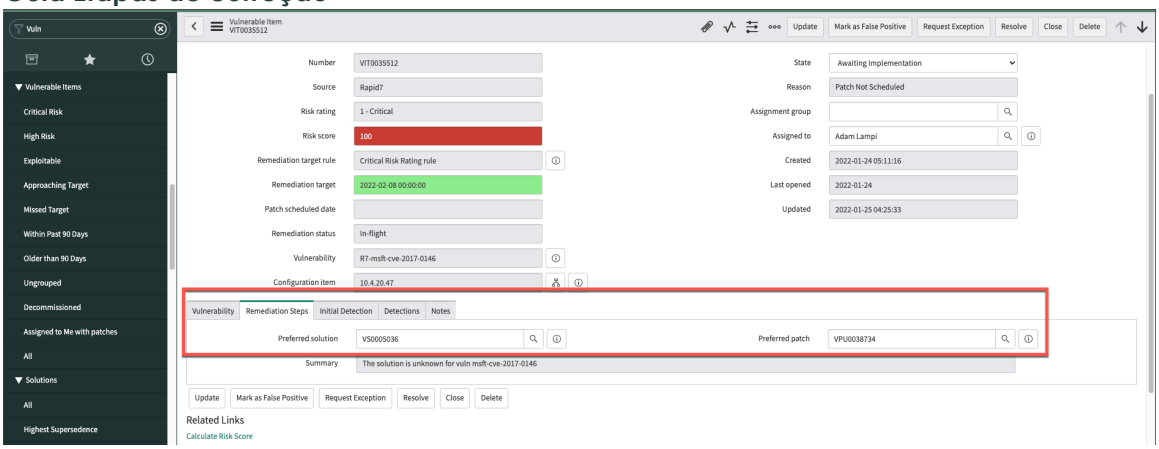
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acúmulo de dados e estado do patch

Para exibir os itens vulneráveis que têm patches e que estão atribuídos a você no ambiente clássico, navegue até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Atribuído a mim com patches**.

Se um registro de item vulnerável for preenchido com um patch preferencial, ele fará a transição automaticamente para **Aguardando implementação** somente se o estado do VI não for **Encerrado**, **Resolvido**, **Adiado** ou **Em revisão**. Para detalhar os dados para exibir a solução preferencial e outros dados, clique na guia **Correção** no registro de VI.

Guia Etapas de correção



Um VI com um patch preferencial muda para **Aguardando implementação** nos seguintes casos:

- Se um patch estiver programado para implantação em um IC que faz parte de uma importação de coleção e o IC tiver um VI associado, o motivo pelo qual o VI está **Aguardando Implementação** será **Patch programado**.
- Se um patch estiver programado para implantação em um IC que faz parte de uma importação de coleção e o IC tiver um VI associado e a data de meta de correção (prazo) posterior à data de tempo de correção (TTR), o estado de o VI está **Aguardando Implementação** com o motivo como **Patch programado (Data de destino ausente)**.
- Se um patch não estiver programado para implantação em um IC que faz parte de uma importação de coleção, o estado do VI será **Aguardando implementação**, com o motivo como **Patch não programado**.

Clique no ícone Informações do **patch preferencial** para abrir as atualizações de patch e exibir as seguintes informações nos Links relacionados:

Itens vulneráveis

Itens vulneráveis que estão associados a este patch.

Dispositivos associados

Dispositivos com atualizações e dispositivos sem atualizações.

Implantações de patch

Implantações programadas para este patch em máquinas individuais (ativos) ou em grupos de ativos.

Solicitações de patches

Uma lista de solicitações de patch que foram enviadas para aprovação antes de serem programadas para implantação.

Patches em potencial

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Patches que podem resolver uma vulnerabilidade.

Clique no ícone **Informações do patch preferencial** para abrir o registro e exibir as informações listadas anteriormente, além dos seguintes dados de atualização de patch:

Status de correção da fonte

O total de dispositivos que exigem este patch e quaisquer dispositivos que não tenham o patch.

Status da Correção

O status (total de VIs, percentual corrigido, VIs adiados) dos IVs que têm este patch preferencial.

Patches e soluções preferenciais

Quando uma vulnerabilidade importada corresponde a um ativo em seu Configuration Management Database (CMDB), um item vulnerável (VI) é criado em Resposta a vulnerabilidades. Se o item de configuração (IC) associado a este VI também for importado de um fornecedor de patch de terceiros e for mostrado como um patch ausente para a mesma vulnerabilidade, um patch preferencial será listado e acumulado para suas soluções. Essas informações permitem que você saiba que um ativo (IC) tem uma correção de um patch disponível que é a melhor correspondência para sua vulnerabilidade.

Exibição de patches sem soluções

Após uma importação, se nenhum dado de solução de vulnerabilidade estiver disponível, o campo **Solução de vulnerabilidade** no registro de Atualização de patch será deixado em branco. Para obter mais informações sobre como exibir informações para esses tipos de patches, consulte Exibir patches sem soluções em Resposta a vulnerabilidades.

Exibir patches sem soluções em Resposta a vulnerabilidades

A partir da v16.0 de Resposta a vulnerabilidades, para patches que não têm soluções após uma importação, o sistema pesquisa IDs de patch nos dados de referência de vulnerabilidade para que você possa exibir esses patches nos registros de vulnerabilidade.

Patches sem soluções

Função necessária: sn_vul.vulnerability_admin.

Os dados importados das aplicações de orquestração de patches e soluções de vulnerabilidade, bem como integrações de scanner de patch, são processados, conectados e exibidos na aplicação Resposta a vulnerabilidades em registros de atualização de patch.

Quando existe uma solução para uma vulnerabilidade, as informações relacionadas são correlacionadas em sua instância e são acumuladas dos patches, para as soluções de vulnerabilidade e para as vulnerabilidades. Para exibir essas informações, navegue até **Todos** > **Resposta a vulnerabilidades** > **Patches** > **Todos**.

Após uma importação, se nenhum dado de solução de vulnerabilidade estiver disponível, o campo **Solução de vulnerabilidade** no registro de Atualização de patch será deixado em branco. Para que você possa ver as informações da solução relacionada a esses patches, uma propriedade do sistema, [**sn_vul_patch_orch.no_solution_patch_rollup**], é ativada por padrão em sua instância. Esta propriedade pesquisa IDs de boletim e IDs de artigo nos dados de referência de vulnerabilidade das importações do scanner. Se uma correspondência for encontrada, os dados associados serão preenchidos na tabela de possíveis patches e essas informações serão exibidas nas listas relacionadas de registros de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você tiver um grande número de vulnerabilidades ou o trabalho agendado de acúmulo estiver demorando muito para ser concluído, talvez prefira desativar esta propriedade do sistema para evitar possíveis problemas de desempenho. No entanto, observe que se você desativar esta propriedade do sistema, os dados da solução importados não serão pesquisados nem acumulados para suas vulnerabilidades sem soluções.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema, siga estas etapas:

1. Navegar até **sys.properties.list**.
2. Localize **sn_vul_patch_orch.no_solution_patch_rollup** e clique nele para abrir o registro.
3. No campo Valor, digite `falso`.
4. Clique em **Atualizar**.

Exibição de dados de orquestração de patches nos painéis Resposta a vulnerabilidades

A partir da v16.1, você pode exibir dados de atualização de patch no ambiente clássico nos painéis incluídos com a aplicação Resposta a vulnerabilidades.

Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Para obter mais informações, consulte Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI.

Você também pode exibir esses dados nos painéis do CISO e da Gestão de vulnerabilidades (PA) se tiver uma assinatura do Performance Analytics.

Você também pode exibir dados de patch no ambiente clássico. Para obter mais informações sobre as funções necessárias e como exibir dados nos painéis Resposta a vulnerabilidades no ambiente clássico que estão incluídos com a aplicação Resposta a vulnerabilidades e aqueles que exigem uma assinatura separada, consulte Usando os painéis padrão Resposta a vulnerabilidades.

Exibir uma solução

Exiba todas as soluções, soluções com maior substituição e soluções associadas a itens vulneráveis para informar suas atividades de correção.

Antes de Iniciar

Função necessária: sn_vul.read, sn_vul.vulnerability_admin ou sn_vul.remediation_owner
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Como Analista de vulnerabilidade ou Proprietário de correção, você pode exibir diferentes conjuntos de soluções relacionados a itens vulneráveis.

Nota: Os registros de solução são somente leitura, exceto em **Anotações** na seção **Anotações internas** ou em soluções criadas pelo usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Soluções**.
2. Escolha uma lista de soluções.

   Nota: Você pode filtrar uma lista de soluções usando caracteres curinga para o nome do produto.

3. Para revisar, clique em cada item.
4. Opcional: Insira anotações na guia **Anotações** e clique com o botão direito do mouse em **Salvar** para permanecer na página ou clique em **Atualizar** para salvar e retornar à lista de **Soluções de vulnerabilidade**.

   Nota: Se você tiver apenas a função sn_vul.read, não poderá executar esta etapa.

Criar uma solução de vulnerabilidade

Crie uma solução de vulnerabilidade para que você possa rastrear soluções de vulnerabilidade que não são cobertas pelo conteúdo da solução de terceiros.

Antes de Iniciar

Função necessária: administrador, sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou Vulnerability.write
Solução de gestão de vulnerabilidade é um recurso disponível na aplicação Resposta a vulnerabilidades. Solução de gestão de vulnerabilidade requer uma assinatura separada.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar uma solução a partir de qualquer uma das listas de soluções. Você deve instalar a aplicação Gestão de soluções de vulnerabilidade antes de criar uma solução.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Soluções**.
2. Escolha uma lista de soluções: **Todos**, **Substituição mais elevada** ou **Com itens vulneráveis**.
3. Clique em **Nova**.
4. Preencha os campos editáveis no formulário, conforme apropriado.
   Você pode deixar em branco todos os campos não utilizados. Para obter mais informações sobre campos individuais, consulte Campos do formulário de solução.
5. Clique com o botão direito do mouse em **Salvar** no cabeçalho.
   O registro da solução é adicionado e aparece nas listas **Todos** e **Substituição mais alta**, por padrão.
6. As listas relacionadas são exibidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode associar esta solução às seguintes listas relacionadas: **Itens vulneráveis , Vulnerabilidadesde terceiros**, **CVEs**, **Soluções substitutas** e **Soluções anteriores**. Escolha uma vulnerabilidade ou solução e clique em **Enviar**.

Nota:

Solução de gestão de vulnerabilidade O associa automaticamente itens vulneráveis e tarefas de correção a soluções quando os registros de vulnerabilidade são associados manualmente a soluções.

Itens vulneráveis reatribuídos manualmente a outra solução não são atualizados automaticamente com as mudanças de solução no nível da vulnerabilidade.

Se você quiser excluir o relacionamento entre uma vulnerabilidade de terceiros e uma solução porque não é relevante para o IC que você está corrigindo ou não é uma preocupação em seu ambiente, consulte Excluir manualmente soluções de registros de terceiros ou vice-versa.

Excluir manualmente soluções de registros de terceiros ou vice-versa

Exclua o relacionamento entre uma vulnerabilidade de terceiros e uma solução porque ele não é relevante para o IC que você está corrigindo ou não é uma preocupação em seu ambiente. Exclua manualmente as soluções usando uma vulnerabilidade de terceiros ou um registro de solução.

Antes de Iniciar

Função necessária:

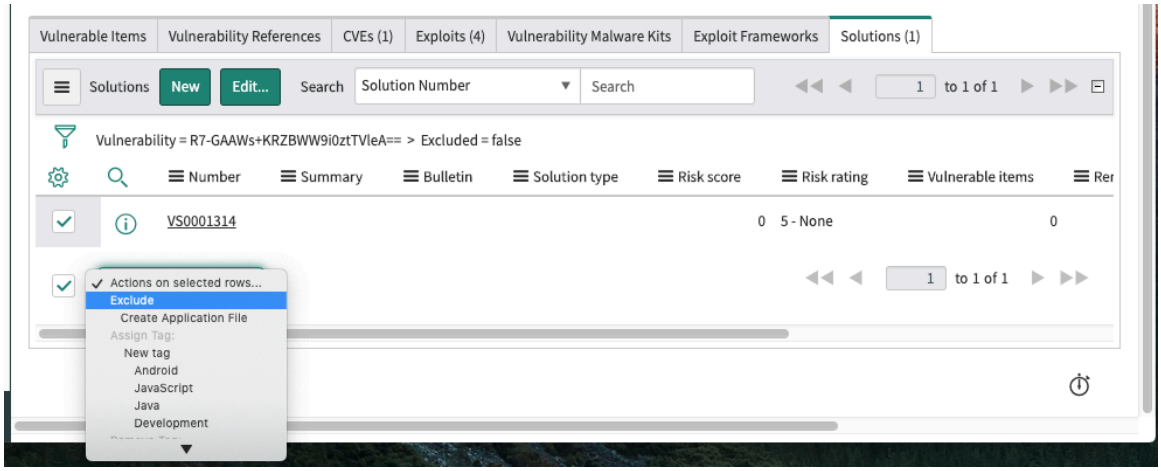
- sn_vul.write
- sn_vul.remediation_owner

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** ou **Resposta a vulnerabilidades** > **Todas as soluções**
2. Abra uma vulnerabilidade ou registro de solução de terceiros.
   a. Para um registro de terceiros: selecione a guia relacionada **Soluções**.
   b. Para um registro de solução: selecione a guia relacionada **Vulnerabilidades de terceiros**.
3. Marque a caixa ao lado de cada registro de vulnerabilidade ou solução que você deseja excluir.
4. No menu suspenso **Ações em linhas selecionadas**, escolha **Excluir**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro de terceiros ou da solução não aparece mais na guia relacionada.

Os relacionamentos de vulnerabilidade de terceiros com as soluções também são excluídos quando as soluções são atualizadas ou se o trabalho noturno estiver habilitado.

Os relacionamentos de vulnerabilidade de terceiros com as soluções são excluídos durante o trabalho agendado à noite.

Excluir vulnerabilidades de terceiros significa que a solução não é mais um fator para qualquer avaliação de solução preferencial. Impactos da exclusão:

- Tudo conta para soluções, já que a vulnerabilidade de terceiros, os itens vulneráveis (IVs) e os itens de configuração (ICs) anexados à vulnerabilidade de terceiros não contam mais para a solução.
- Determinar a solução preferencial para a vulnerabilidade de terceiros e, por extensão, a solução preferencial de quaisquer IVs anexados e tarefas de correção que contenham o VI.

Triagem de vulnerabilidades automaticamente

A revisão e a triagem de novas vulnerabilidades são necessárias para garantir a correção bem-sucedida. Transforme importações de vulnerabilidade em tarefas de correção com atribuição automatizada de item vulnerável (VI), cálculo de risco, metas de correção e agrupamento de VI.

Começando com vulnerabilidades importadas, reconcilie os ativos não encontrados no CMDB, priorize os resultados, traduza isso em atividades de correção que são atribuídas automaticamente, orquestre o processo de correção e confirme a conclusão com uma verificação de validação.

Novos itens vulneráveis geralmente são classificados em tarefas de correção na importação, com base nas regras de tarefas de correção. Às vezes, os itens vulneráveis não podem ser agrupados ou não contêm um item de configuração reconhecido.

Uma visão geral do processo de triagem de vulnerabilidades:

- Faça login na sua instância Resposta a vulnerabilidades.
- Valide se suas regras (Pesquisa de IC, Atribuição) para o item vulnerável estão funcionando conforme o esperado. Para obter informações sobre como revisar as Regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros. Para obter informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Devido ao grande volume nas importações de dados, é necessário ter cuidado com a atribuição automatizada de itens vulneráveis.

- Valide se suas metas de correção estão corretas. Consulte Resposta a vulnerabilidades regras de destino de correção para obter informações sobre como as regras de destino de correção funcionam e como revisá-las.
- Exibir itens vulneráveis não agrupados.
  - Observando os itens vulneráveis desagrupados, considere revisar suas regras de grupo e executar uma nova verificação. Para obter mais informações, consulte Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção.
  - Agrupe manualmente os itens vulneráveis. Criar manualmente uma tarefa de correção no Resposta a vulnerabilidades para obter mais informações.
  - Revise as pontuações de risco dos itens vulneráveis em suas tarefas de correção. Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
  - Feche itens vulneráveis mais antigos não detectados recentemente por suas integrações de terceiros. Para obter mais informações, consulte Fechamento automático de itens e detecções vulneráveis.
- Exibir e reclassificar itens de configuração incompatíveis.
- Pesquise o que precisa ser feito para correção.

  Esta etapa pode incluir:

  - Determine com o que lidar agora e o que você pode adiar. Essa determinação geralmente se baseia na pontuação de risco, nos sistemas afetados e nos patches com janelas de mudança.

    Nota: As regras de destino de correção pertencem a itens vulneráveis. Essas regras são executadas quando o item vulnerável é importado. Essas regras foram criadas anteriormente no Assistente de configuração.

  - Atualizar itens vulneráveis, se necessário, e Exibir o status da meta de correção de um Resposta a vulnerabilidades item vulnerável.
  - Crie uma **solicitação de mudança** e atribua a tarefa de correção a um grupo de atribuição (Operações de TI) para correção.

    Nota: Se a vulnerabilidade constitui um incidente de segurança e o plug-in Security Incident Response (com.snc.security_incident) estiver ativado, você poderá criar registros de incidentes de segurança a partir das tarefas de correção.

  - Depois de enviar uma ou mais solicitações de mudança, mova o estado do grupo para Sob investigação.

Editar itens vulneráveis em massa no Resposta a vulnerabilidades

Edite itens vulneráveis em massa para economizar tempo selecionando campos e executando um trabalho assíncrono de edição em massa em segundo plano.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Importante: O recurso Edição em massa está disponível para itens vulneráveis de host no Vulnerability Manager Workspace. Para obter mais informações, consulte Como usar a edição em massa no Vulnerability Manager Workspace.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Selecione os itens vulneráveis executando uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo #unique_122_Connect_42_entry-be-record-selection.
   - Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** ao campo #unique_122_Connect_42_entry-be-record-selection.
3. Selecione o botão **Edição em massa**.
4. No modal de edição em massa, preencha os campos.

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ Somente Itens vulneráveis selecionados ◦ Todos os itens vulneráveis que correspondem ao filtro ◦ Tarefa de correção ◦ Entrada de vulnerabilidade
Estado	Mudança para o **Estado** no item vulnerável. As opções são: ◦ Não atualizar ◦ Aberto ◦ Sob Investigação ◦ Aguardando Implementação ◦ Adiado **Nota:** ▪ Quando você seleciona essa opção, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você adia VITs, uma tarefa de correção é criada e essa tarefa é enviada para aprovação. ◦ Fechado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ▪ Quando você seleciona esta opção para marcar os registros como falso-positivos, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você marca os registros como falso-positivos, uma tarefa de correção é criada e essa tarefa é enviada para aprovação. ◦ Resolvido
Solução preferencial	Solução que é direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa. Selecione a mudança para o campo **Solução preferencial** nos itens vulneráveis (VITs). As opções são de uma lista de pesquisa de soluções preferenciais disponíveis para os VITs selecionados. **Nota:** ◦ O conjunto de soluções preferenciais disponíveis é uma interseção de todas as possíveis soluções das vulnerabilidades em todos os VITs selecionados. ◦ Ao selecionar **Seleção de registro** > **Entrada de Vulnerabilidade** para uma edição em massa, todos os VITs da vulnerabilidade serão definidos para a solução preferencial selecionada. **Nota:** Esta operação não define a **solução preferencial** no nível de entrada de vulnerabilidade. Definir a **solução preferencial** no nível de entrada de vulnerabilidade definiria a **solução preferencial** para todos os novos VITs daqui em diante. A edição em massa modifica somente o conjunto atual de VITs. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir a **solução preferencial**. ◦ O número total de soluções que podem ser mostradas na lista de pesquisa é limitado a 170. Se houver mais de 170 soluções, uma mensagem de aviso será exibida. O valor atualizado é mostrado na exibição de lista de itens vulneráveis.
Patch preferencial	Patch destinado a corrigir todos os itens de vulnerabilidade selecionados para edição em massa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Você deve instalar a Orquestração de patches para exibir a lista de patches preferenciais. ◦ O conjunto de patches preferenciais disponíveis é uma interseção de todos os possíveis patches em todos os VITs selecionados. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir o **patch preferencial**. ◦ O número total de patches que podem ser mostrados na lista de pesquisa é limitado a 170. Se houver mais de 170 patches, uma mensagem de aviso será exibida.
Motivo	Motivo para adiar registros: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Redução do controle no local ◦ Outro Motivo para fechar registros: ◦ Falso-positivo **Nota:** ▪ Quando você seleciona esta opção, os campos Descrição resumida, Até e Informações adicionais são exibidos. ▪ Uma tarefa de correção é criada quando você marca os registros como falso-positivos e essa tarefa é enviada para aprovação. ◦ Cancelado(a) ◦ Fixo **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Nota resumida descrevendo o motivo do adiamento e das solicitações falso-positivos encerradas. Essas informações são refletidas no campo Descrição da Tarefa de correção criada para solicitações de adiamento e falso-positivo encerradas. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Até	Data até a qual o registro permanece adiado. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado.
Informação adicional	Outras informações necessárias. Essas informações são refletidas no campo Informações adicionais na guia Visão geral. Se sua solicitação de adiamento for aprovada, essas informações adicionais serão exibidas como notas de adiamento no VIT e na tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.
Cancelar atribuição	Todos os itens selecionados não estão atribuídos ao grupo de atribuição e ao responsável pela correção. Para obter mais informações sobre como um proprietário de correção pode remover as atribuições de itens vulneráveis, consulte Remover atribuições de itens vulneráveis para você ou seus grupos. **Nota:** ◦ Este campo aparece quando você seleciona o Estado como Não atualizar. ◦ Quando você cancela a atribuição de registros, uma tarefa de correção é criada e essa tarefa é enviada para aprovação.
Grupo de atribuição	Grupo de atribuição para o VIT. Selecione manualmente ou use as Recomendações de atribuição se estiver habilitado. **Nota:** Este campo é desabilitado quando você marca a caixa de seleção **Cancelar atribuição**.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

Tradução automática

5. Selecione **OK**.
   Um trabalho assíncrono de edição em massa atualiza os registros selecionados. O número do trabalho com um link é exibido na página Itens vulneráveis, onde você pode exibir seu status. Uma tarefa de correção é criada com os itens vulneráveis selecionados quando você adia, cancela a atribuição ou fecha (falso-positivo) itens vulneráveis em massa. E esta tarefa de correção é enviada para aprovação.

Itens vulneráveis desagrupados Resposta a vulnerabilidades

Itens vulneráveis são atribuídos automaticamente a uma tarefa de correção quando são importados. No entanto, às vezes, se um item vulnerável (VI) for criado manualmente, por exemplo, o VI pode se tornar órfão. O módulo de item vulnerável não **agrupado** lista os itens vulneráveis sem um grupo.

Nota: Os processos automatizados de integração não criam órfãos, portanto, espera-se que este caso de uso seja pequeno.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O desagrupamento ocorrerá se um item vulnerável tiver sido criado sem uma vulnerabilidade ou se não houver uma regra de tarefa de correção que atribua o VI a um grupo.

Nesse caso, revise a lista de itens vulneráveis não agrupados navegando até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Desagrupado**.

Após a revisão, suas escolhas são as seguintes:

- Você pode Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção para capturar todos os itens que aparecem nesta lista.
- Você pode Criar manualmente uma tarefa de correção no Resposta a vulnerabilidades e adicionar manualmente itens desta lista ao grupo ou definir uma condição que corresponda a esses itens.
- Você pode abrir uma tarefa de correção existente e adicionar itens vulneráveis relevantes ao grupo, desde que ele esteja no estado Aberto ou Sob investigação.

Nota: Itens vulneráveis adicionados manualmente não são removidos automaticamente das tarefas de correção por regras de tarefa de correção ou condições de grupo.

Para obter mais informações sobre como as tarefas de correção e as regras de tarefa se comportam, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral.

Exibir Resposta a vulnerabilidades itens vulneráveis não agrupados

Itens vulneráveis que não estão atribuídos a um grupo são colocados em uma lista visível.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis desagrupados**.
2. Revise os itens vulneráveis na lista.
3. Clique em cada item vulnerável para exibir e determinar como incluir em um grupo.

Adicionar manualmente um item vulnerável a uma tarefa de correção

Se um item vulnerável for deixado desagrupado, você poderá adicioná-lo a uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Registre o número vulnerável.
2. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
3. Escolha uma tarefa de correção (VUL) para o item vulnerável.
4. Selecione **Editar** no canto inferior direito.
5. Insira o número do **item vulnerável** no campo de pesquisa de Coleção.
6. Selecione o item vulnerável da coleção e adicione-o à lista.
7. Clique em **Salvar**.

Remover atribuições de itens vulneráveis

Reatribuir registros de itens vulneráveis nas aplicações Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Se você determinar que itens vulneráveis (VITs) não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou a seus grupos, você poderá remover a si mesmo ou seus grupos dos campos **Atribuído a** e **Grupo de atribuição** em registros de item vulnerável e tarefa de correção.

O botão **Cancelar atribuição** é exibido nos seguintes registros em qualquer estado diferente de Encerrado ou Resolvido:

- Tarefas de correção (VULs) no ambiente clássico e nos espaços Resposta a vulnerabilidades. Se uma tarefa de correção for atualizada com este recurso, os campos **Atribuído a** e**Grupo de atribuição** em todos os VITs associados também serão limpos.
- Itens vulneráveis (VITs) no ambiente clássico e nos espaços Resposta a vulnerabilidades.
- Itens vulneráveis da aplicação (AVITs).
- Itens vulneráveis de contêiner (CVITs).

Importante: Você pode cancelar a atribuição de itens vulneráveis de host em massa no Vulnerability Manager Workspace. Para obter mais informações, consulte Como usar a edição em massa no Vulnerability Manager Workspace.

Procedimento

1. No ambiente clássico ou no Espaço de trabalho do proprietário de correção de TI, navegue até um registro de item vulnerável (VIT) atribuído a você que esteja em qualquer estado diferente de Encerrado ou Resolvido.
2. Para limpar os campos **Atribuído a** e **Grupo de atribuição**, na parte superior do registro, selecione **Cancelar atribuição**.
3. Opcional: Como alternativa, navegue até um AVIT atribuído a você ou aos seus grupos e clique em **Cancelar atribuição** para limpar os campos de atribuição.
4. Na caixa de diálogo Cancelar atribuição, forneça anotações de trabalho e selecione **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Opcional: Se você quiser limpar os campos de atribuição de vários VITs em uma lista, selecione os VITs desejados e selecione **Edição em massa**.

   a. Na caixa de diálogo Edição em massa de item vulnerável, selecione **Somente itens vulneráveis selecionados** no campo **Seleção de registro**, marque a caixa de seleção **Cancelar atribuição** e clique em **OK**.
   Para obter mais informações sobre edições em massa, consulte Edição em massa de itens vulneráveis da Respostaa vulnerabilidades.

   b. Selecione o ID da tarefa de correção que é exibido na notificação.

6. Exiba as seguintes informações:
   - As anotações de trabalho fornecidas são exibidas na seção Anotações.
   - Na guia **Aprovação** de mudança de estado, o registro de aprovação de mudança de estado é exibido com o estado Em revisão, o que ajuda a rastrear o fluxo de trabalho de aprovação.
   - Na guia **Aprovações solicitadas**, sua solicitação para a remoção de você ou seu grupo de atribuição é exibida no estado Solicitado.

Resultados

A solicitação é aprovada usando um fluxo de trabalho de aprovação padrão de um nível. Para obter mais informações, consulte Aprovação de solicitações nos espaços do gerenciador de vulnerabilidades.

- Se sua solicitação for aprovada, o registro de aprovação de mudança de estado e o registro de aprovação solicitada passarão para o estado Aprovado. Você e seus grupos são removidos dos campos **Atribuído a** e **Grupo de atribuição**. `Não atribuído` é exibido no campo **Tipo de atribuição** e a tarefa de correção e os VITs são exibidos na lista do módulo Não atribuído para Conformidade de configurações.

  As notificações de que os registros não estão atribuídos são enviadas automaticamente para gerentes de vulnerabilidade ou analistas no grupo Notificação de não atribuição. Para configurar o sinalizador de aprovação, as notificações e o grupo de atribuição padrão, consulte Remoção de atribuições de itens vulneráveis e tarefas de correção.

- Se sua solicitação for rejeitada, o estado do registro de aprovação de mudança e do registro de aprovação solicitada passará para o estado Rejeitado.

Nota: Como administrador de vulnerabilidades, você pode definir a propriedade do sistema *`sn_vul.unassign_vr.approval_required`* como **falsa** para desabilitar o processo de aprovação.

O que Fazer Depois

Navegue até os Módulos não atribuídos das aplicações Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações Contêiner de Resposta a vulnerabilidades, monitore todos os registros não atribuídos em busca de itens que possam se enquadrar no seu escopo e reatribua-os a você.

Aprovar ou rejeitar uma solicitação de não atribuição no Resposta a vulnerabilidades

Aprove solicitações para a remoção de itens vulneráveis de um grupo de atribuição ou de um usuário individual na aplicação Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: para aprovações não atribuídas, é necessário um aprovador no grupo Aprovador – Nível 1.

- sn_vul.unassign_approver para AVITs e VITs
- sn_vul_container.unassign_approver para CVITs

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, uma configuração de aprovação é fornecida e um grupo de aprovação não atribuído é criado. Os usuários do grupo Aprovador não atribuído - Nível 1 podem aprovar a solicitação. Este grupo contém uma função de aprovador não atribuído, sn_vul.unassign_approver, por padrão. Você pode modificar ou criar um novo grupo e atualizar a configuração de aprovação. Para configurar uma regra de aprovação, selecione qualquer uma das seguintes regras de aprovação no módulo Regras de aprovação e navegue até a configuração de aprovação na guia **Configurações** de aprovação:

- *`Vulnerable item field change request`* para um item vulnerável.
- *`Vulnerability field change request`* para uma tarefa de correção.
- *`Application vulnerability field change request`* para um item vulnerável da aplicação (AVIT).
- *`Approval for container management`* para um item vulnerável de contêiner (CVIT).

Para obter mais informações sobre regras de aprovação e configurações, consulte Configurações do fluxo de trabalho de aprovação para solicitação de cancelamento de atribuição.

Importante: Você pode aprovar ou rejeitar solicitações no Vulnerability Manager Workspace. Para obter mais informações, consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Minhas aprovações** para VITs e AVITs. Como alternativa, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações** para CVITs.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação adicionando os comentários apropriados.

Fechamento automático de itens e detecções vulneráveis

Você pode fechar automaticamente detecções obsoletas e itens vulneráveis (IVs) associados a ICs desativados usando o módulo Configuração de fechamento automático.

Para configurar a opção de fechamento automático, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Configuração de fechamento automático**. Você pode fechar automaticamente detecções e IVs obsoletos nos seguintes cenários:

- Fechar automaticamente detecções obsoletas no Resposta a vulnerabilidades
- Fechar automaticamente itens vulneráveis relacionados a ICs desativados

Para obter informações sobre como trabalhar com itens de configuração desativados, consulte Como trabalhar com itens de configuração desativados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como trabalhar com itens de configuração desativados

Itens de configuração (ICs) desativados são movidos para o estado desativado, arquivado ou excluído no Configuration Management Database (CMDB). Resposta a vulnerabilidades contém itens vulneráveis (VIs) que são compostos por ICs. Quando o estado de um IC é atualizado para desativado, os IVs associados são encerrados com o subestado "IC desativado".

Se o CMDB mudar o status da fase do ciclo de vida de um IC para descontinuado, você poderá optar por fechar automaticamente os IVs associados. Para obter mais informações sobre como fechar automaticamente os IVs associados, consulte Fechar automaticamente itens vulneráveis relacionados a ICs desativados.

O IC desativado será eventualmente arquivado ou excluído permanentemente do CMDB.

Impacto da descontinuação dos ICs:

- **Impacto nos itens descobertos:** quando o IC é descontinuado, o item descoberto (DI) relacionado é marcado como "IC desativado".
- **Impacto em itens vulneráveis:** quando o estado de um DI é atualizado para "IC desativado", o VI associado é encerrado e a seção de anotações é atualizada automaticamente.

> **Nota:** O estado de um DI é atualizado automaticamente para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um IV é atualizado para Encerrado somente quando a opção **Fechar automaticamente IVs vinculados a ICs desativados** está habilitada. Para obter mais informações sobre como fechar automaticamente os IVs associados, consulte Fechar automaticamente itens vulneráveis relacionados a ICs desativados.

O trabalho agendado *Close detections/VIs for decommissioned CIs* é executado diariamente para as DIs atualizadas. Se a opção de configuração de fechamento automático estiver habilitada para ICs desativados, ela identificará a DI que contém um IC desativado e fechará o VI relacionado com o subestado "IC desativado". Se todos os IVs em uma tarefa de correção estiverem encerrados e seu subestado for IC desativado, a tarefa de correção também será encerrada com o subestado "Cancelado". Para exibir os IVs desativados, navegue até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Desativado**.

> **Nota:** Se um IC voltar ao estado original do estado "Descontinuado", a entrada "Itens descobertos" também será atualizada. Os IVs são abertos automaticamente quando os dados são ingeridos novamente do scanner.

Fechar automaticamente itens vulneráveis relacionados a ICs desativados

Se o Configuration Management Database (CMDB) mudar o status da fase do ciclo de vida de um item de configuração (IC) para descontinuado, você poderá optar por fechar automaticamente as detecções e itens vulneráveis (IVs) associados.

Antes de Iniciar

Função necessária: sn_vul.admin

Por Que e Quando Desempenhar Esta Tarefa

A partir da v22.0 de Resposta a vulnerabilidades, para fechar automaticamente os IVs e detecções associados, você deve habilitar a propriedade do sistema *sn_vul_cmn.auto_close_vis_linked_retired_cis* para fechar automaticamente os IVs associados a ICs desativados. Para habilitar a opção, defina o campo Valor como "1". Por outro lado, para desabilitar a opção, defina o campo Valor como '0'.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante um upgrade, se a propriedade do sistema *sn_vul_cmn.auto_close_vis_linked_retired_cis* for selecionada na v21.0 de Resposta a vulnerabilidades, o valor permanecerá como '1'. Quando esta opção está habilitada, todos os VIs e detecções novos ou existentes relatados para o mesmo IC são criados ou atualizados automaticamente com um status de "Encerrado". Isso se baseia no ID do ativo na carga útil do scanner e no status da entrada de itens descobertos. Para obter mais informações sobre o impacto de ICs desativados, consulte Como trabalhar com itens de configuração desativados

.

Nota: O estado de uma DI é atualizado para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um IV é atualizado para Encerrado somente quando a opção **Fechar automaticamente IVs vinculados a ICs desativados** está habilitada.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Configuração de fechamento automático** > **Ciclo de vida do item de configuração**.
2. Para fechar automaticamente itens vulneráveis associados aos ICs desativados, marque a caixa de seleção Fechar automaticamente **IVs vinculados a ICs desativados**.
3. Selecione **Atualizar**.

Nota: Se um IC já tiver sido descontinuado antes **de a opção Fechar VIs automaticamente vinculados a ICs descontinuados** ser habilitada, os IVs serão criados somente para novas detecções de scanners. O estado desses IVs é Encerrado e o subestado é IC desativado.

Você não pode reabrir manualmente IVs cujo estado é IC desativado, usando as opções **Reabrir** ou **Edição em massa**.

IVs encerrados com um subestado fixo ou obsoleto serão reabertos se uma nova detecção for criada e os VIs puderem ser correspondidos com a nova vulnerabilidade. Para obter mais informações, consulte Detecções, tarefas de correção e estados de itens vulneráveis.

Fechando detecções obsoletas em Resposta a vulnerabilidades

O módulo Encerrar automaticamente detecções obsoletas ajuda a limpar automaticamente detecções vulneráveis mais antigas e obsoletas que não foram encontradas recentemente por suas integrações de terceiros. Mover essas detecções para Encerrado reduz o número de itens vulneráveis ativos e tarefas de correção em sua instância Now Platform e ajuda a reconciliar ativos em seu CMDB.

Visão geral e termos-chave

Para acumular dados de detecção com mais precisão para seus itens vulneráveis, o módulo de fechamento automático de detecções obsoletas ajuda a limpar detecções de itens vulneráveis mais antigas e obsoletas que não foram encontradas recentemente por suas integrações de terceiros. Para obter mais informações sobre esse recurso, consulte o caso de uso abaixo e o artigo Encerramento automático de detecções obsoletas [KB 0958638] .

Nas versões anteriores do Resposta a vulnerabilidades, o módulo de fechamento automático de itens vulneráveis fazia a transição automática de itens vulneráveis não encontrados recentemente ou atualizados por suas integrações de scanner de terceiros para o estado Encerrado - Obsoleto.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de habilitar o recurso de fechamento automático de detecções obsoletas, revise os termos a seguir, como os estados são acumulados para itens vulneráveis e tarefas de correção e os pré-requisitos para suas integrações de terceiros que importam dados de detecção.

Para habilitar o recurso, consulte Fechar automaticamente detecções obsoletas no Resposta a vulnerabilidades.

Termos principais

Detecções obsoletas

Refere-se a detecções associadas a itens vulneráveis em sua instância Now Platform® que são antigos e não foram encontrados, atualizados ou detectados por verificações de integração de terceiros por um período significativo.

Últimas detecções encontradas

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data e hora mais atuais ou mais recentes em que as detecções foram encontradas novamente pelo scanner.

Última verificação de ativos

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data e hora mais atuais em que um ativo foi verificado pela última vez por um scanner de terceiros.

Caso de uso

Às vezes, os ativos (itens de configuração) podem ser desativados em seu ambiente ou limpos por scanners de terceiros, e as detecções associadas não são atualizadas pelas detecções de itens vulneráveis. Como resultado, as detecções e os itens vulneráveis relacionados não são atualizados na aplicação Resposta a vulnerabilidades e se tornam inativos (obsoleto).

Para fechar essas detecções antigas que têm dados de item vulnerável inalterados e reduzir o número de IVs ativos e tarefas de correção (RTs), habilite o fechamento automático de detecções obsoletas. Este recurso fecha automaticamente as detecções de itens vulneráveis que não foram encontrados ou atualizados recentemente por suas integrações de scanner de terceiros com base nos critérios de pesquisa e em uma duração em número de dias que você define.

Por exemplo, suponha que um item de configuração (IC) específico tenha vários IDs de ativo e um desses IDs não tenha sido importado em uma detecção de um scanner de terceiros nos últimos 90 dias. Este recurso fecha automaticamente esta detecção que não tem novos dados de vulnerabilidade para que o VI associado possa ser fechado.

Como um VI pode ter mais de uma detecção associada a ele, este recurso faz a transição somente das detecções determinadas como obsoletas pelos parâmetros definidos. Por exemplo, se um VI tiver quatro detecções associadas a ele e duas detecções forem obsoletas, ou seja, nenhum novo dado de vulnerabilidade foi importado nos últimos 90 dias, este recurso fechará somente as detecções obsoletas. Antes que o VI possa ser encerrado, você deve primeiro corrigir as outras duas detecções em aberto.

Acúmulo de estados de detecção para IVs

Para diferenciar as detecções encerradas automaticamente das detecções encerradas por scanners de terceiros, um novo valor para o campo Status, Obsoleto, foi adicionado. Os valores possíveis para este campo são Aberto, Fechado e Obsoleto. Obsoleto indica que uma detecção foi encerrada pelo recurso de detecção de fechamento automático.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Precedência de estado: Aberto > Fechado > Obsoleto.

1. Se alguma detecção estiver Aberta, o estado de VI associado permanecerá Aberto.
2. Se nenhuma detecção estiver Aberta, algumas estiverem Encerradas e algumas estiverem Obsoletas, o estado de VI associado passará para Fechado - Fixo.
3. Se todas as detecções forem obsoletas, o estado de VI associado passará para Encerrado - obsoleto.

   A partir de Resposta a vulnerabilidades 20.0, se a detecção for Obsoleta e o VI associado estiver no estado Encerrado, o estado do VI não fará a transição para Encerrado - Obsoleto. Isso evita que o VI seja reaberto quando uma nova detecção for identificada para que você possa evitar passar por todo o processo de aprovação e solicitação de falso-positivo. Para reverter esse comportamento, desmarque a caixa de seleção **Ignorar detecções obsoletas para IVs encerrados** no formulário Configuração de fechamento automático. Para obter mais informações, consulte Fechar automaticamente detecções obsoletas no Resposta a vulnerabilidades.

Acúmulo de estados de VI para tarefas de correção (VUL)

Precedência de estado: Aberto > Encerrado - Fixo > Encerrado - Obsoleto.

1. Se algum IV em uma VUL (tarefa de correção) estiver Aberto, o estado da VUL não será alterado.
2. Se pelo menos um VI for Encerrado - Fixo e o restante for Encerrado - Obsoleto, o estado do VUL passará para Encerrado - Fixo.
3. Se todos os IVs em uma VUL forem Encerrado - Obsoleto, o estado da VUL passará para Encerrado - Cancelado.

Detecções de fechamento automático e requisitos de integração de terceiros

Usuários do Microsoft TVM e fechamento automático de detecções obsoletas

Item de check-list	Descrição
Integração de vulnerabilidade do Microsoft TVM	Com a integração de vulnerabilidade do Microsoft TVM, se você selecionar **Últimas detecções encontradas** para basear sua pesquisa, esse recurso exigirá uma execução bem-sucedida da integração de vulnerabilidades da máquina do Microsoft TVM (importação completa) nos últimos sete dias. Esta integração é executada semanalmente. Se o fechamento automático de detecções obsoletas estiver habilitado e configurado para **Últimas detecções encontradas**, e a integração de vulnerabilidades da máquina com Microsoft TVM estiver desabilitada ou uma importação de dados não tiver sido concluída com sucesso nos últimos sete dias, o trabalho programado para fechar detecções ainda será executado diariamente, mas alguns detecções obsoletas podem não ser encerradas conforme o esperado. Se você selecionar **Últimos ativos verificados** para basear sua pesquisa, a execução da integração de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	vulnerabilidades de máquina com Microsoft TVM não será necessária. Para ativar esta integração: 1. Navegar até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integração**. 2. Localize e habilite a **integração de vulnerabilidades da máquina com Microsoft TVM (importação completa)**.
(Opcional) Implante várias instâncias das integrações do Microsoft TVM em seu ambiente.	Opcionalmente, você pode implantar várias instâncias das integrações em seu ambiente. O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para obsoletas nas instâncias que concluíram com sucesso as execuções de integração. Se o fechamento automático de detecções obsoletas estiver habilitado e você desabilitar as integrações que são executadas semanalmente em uma instância, o trabalho agendado para fechar detecções ainda será executado diariamente, mas algumas detecções podem não fazer a transição para obsoleto automaticamente como esperado.

Qualys usuários e fechamento automático de itens vulneráveis obsoletos

- Todas as integrações de terceiros ativadas Qualys que recuperam dados de detecção podem ser executadas com este módulo. Não há aplicações Qualys específicas necessárias.
- Opcionalmente, você pode implantar várias instâncias das integrações Qualys em seu ambiente.
- O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para obsoletas em todas as instâncias.

Rapid7 usuários e fechamento automático de detecções obsoletas

Item de check-list	Descrição
A Rapid7 integração de vulnerabilidade	Se você selecionar **Últimas detecções encontradas** para basear sua pesquisa, este recurso exigirá uma execução bem-sucedida de uma das Rapid7 integrações de item vulnerável abrangentes nos últimos sete dias. Essas integrações abrangentes são executadas semanalmente:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	• Para o Rapid7 Nexpose data warehouse, é necessária uma execução bem-sucedida da Rapid7 Integração Abrangente de Item Vulnerável. • Para Rapid7 InsightVM, é necessária uma execução bem-sucedida da Rapid7 Integração Abrangente de Item Vulnerável - API. Se o fechamento automático de detecções obsoletas estiver habilitado e configurado para **Últimas detecções encontradas**, e as Rapid7 integrações de itens vulneráveis abrangentes estiverem desabilitadas ou uma importação de dados não tiver sido concluída com sucesso nos últimos sete dias, o trabalho programado para fechar detecções ainda será executado diariamente, mas algumas detecções obsoletas podem não ser encerradas conforme o esperado. Se você selecionar **Ativos verificados pela última vez** para basear sua pesquisa, nenhuma execução de integração abrangente Rapid7 será necessária. Para ativar essas integrações: **1.** Navegar até **Integração com Rapid7 Vulnerability** > **Administração** > **Integração**. **2.** Localize e habilite a Rapid7 Integração Abrangente de Item Vulnerável necessária. **Nota:** Além dessas integrações que são executadas semanalmente, Rapid7 Nexpose e Rapid7 InsightVM têm integrações de VI que são executadas diariamente, a integração de item vulnerável do Rapid7 e a integração de item vulnerável do Rapid7 - API. Se as integrações diária e semanal Rapid7 estiverem habilitadas, somente uma integração será executada por vez. Se um desses trabalhos de integração estiver em execução, o trabalho da outra integração será ignorado até o próximo trabalho agendado.
(Opcional) Implante várias instâncias das integrações Rapid7 em seu ambiente.	Opcionalmente, você pode implantar várias instâncias das integrações abrangentes em seu ambiente. O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para obsoletas nas instâncias que concluíram com sucesso as execuções de integração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	Se o fechamento automático de detecções obsoletas estiver habilitado e você desabilitar as integrações que são executadas semanalmente em uma instância, o trabalho agendado para fechar detecções ainda será executado diariamente, mas algumas detecções podem não fazer a transição para obsoleto automaticamente como esperado.

Usuários de integração de vulnerabilidade da Tenable e itens vulneráveis obsoletos com fechamento automático

- Todas as integrações ativadas da integração de vulnerabilidade da Tenable que recuperam dados de detecção podem ser executadas com este módulo. Não há integrações de vulnerabilidade específicas da Tenable necessárias.
- Opcionalmente, você pode implantar várias instâncias da integração de vulnerabilidade da Tenable em seu ambiente.
- O fechamento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para **obsoletas** em todas as instâncias.

Depois de verificar se suas integrações estão configuradas corretamente, consulte Fechar automaticamente detecções obsoletas no Resposta a vulnerabilidades para habilitar o recurso.

Informações de upgrade de itens vulneráveis obsoletos de fechamento automático para fechamento automático de detecções obsoletas

Para o módulo Encerramento automático de detecções obsoletas, se você já usou o Encerramento automático de itens vulneráveis obsoletos:

- O valor do número de dias que você inseriu para a opção **Ativos verificados** pela última vez em Encerrar automaticamente itens vulneráveis obsoletos é preservado automaticamente para **Ativos verificados pela última vez** em Detecções obsoletas de encerramento automático.
- O valor do número de dias que você inseriu para a opção Itens vulneráveis **encontrados** pela última vez em Fechar automaticamente itens vulneráveis obsoletos é preservado automaticamente para **Detecções encontradas pela última vez** em Detecções obsoletas de fechamento automático.
- As detecções em aberto existentes com itens vulneráveis como Encerrado - Obsoleto passarão para Obsoleto de acordo com as definições de configuração de fechamento automático quando o trabalho agendado *`Auto-Close Stale Detections`* for executado após o upgrade.

Informações de acúmulo

- Se um item vulnerável foi Encerrado - Obsoleto antes do upgrade e todas as suas detecções forem marcadas como Obsoleto após o upgrade, o estado do IV permanecerá Encerrado - Obsoleto.
- Se um item vulnerável foi Encerrado - Obsoleto antes do upgrade e somente algumas de suas detecções forem marcadas como Obsoleto após o upgrade e o restante tiver sido encerrado pelo scanner, o item vulnerável passará para Encerrado - Corrigido de acordo com a lógica de acúmulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fechar automaticamente detecções obsoletas no Resposta a vulnerabilidades

Habilite o fechamento automático de detecções obsoletas para fechar automaticamente as detecções vulneráveis obsoletas que não foram encontradas recentemente por suas integrações de terceiros.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vuln.admin (descontinuado) ou um gerenciador de vulnerabilidades com a função granular sn_vul.manage_auto_close_stale_vi.

Para obter mais informações sobre este recurso, termos-chave e qualquer configuração que possa ser necessária para suas integrações de terceiros que importam dados de detecção, consulte Fechando detecções obsoletas em Resposta a vulnerabilidades para obter mais informações.

Nota: As informações fornecidas no procedimento a seguir são aplicáveis somente a versões anteriores à v22.0 de Resposta a vulnerabilidades. A partir da v22.0 de Resposta a vulnerabilidades, você tem a opção de configurar opções de pesquisa adicionais. ConsulteCriar regras de fechamento automático para obter mais informações.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Administração** > **Configuração de fechamento automático** > **Detecções obsoletas**.
   O formulário Configuração obsoleta de fechamento automático é exibido.
2. Preencha os campos.
3. Para o campo **Fechar automaticamente detecções obsoletas com base em**, escolha uma opção para sua pesquisa.

   Ambas as pesquisas correspondem à idade de detecções mais antigas e obsoletas em número de dias até uma data fornecida pelo seu scanner.

   Nota: A partir da v22.0 de Resposta a vulnerabilidades, as opções Últimas **detecções encontradas** e **Ativos verificados pela última vez** são criadas como uma lista.

   - **Últimas detecções encontradas**. Esta opção pesquisa a data mais atual ou mais recente em que as detecções foram encontradas novamente pelo scanner.

     Nota: Para usuários de Rapid7 e Microsoft TVM, uma mensagem de aviso é exibida sobre a solicitação de informações de detecção atuais.

     Se você selecionar **Últimas detecções encontradas** para basear sua pesquisa, este recurso exigirá uma execução de integração bem-sucedida de uma das Rapid7 integrações de item vulnerável abrangentes nos últimos sete dias.

     Se você selecionar **Últimas detecções encontradas** para basear sua pesquisa, este recurso exigirá uma execução bem-sucedida da integração de vulnerabilidades de máquina do Microsoft TVM (importação completa) nos últimos sete dias.

   - **Última verificação de ativos**. Esta opção pesquisa a data mais atual em que um ativo foi verificado pela última vez por um scanner de terceiros.
4. Somente para usuários Rapid7 e Microsoft de TVM, verifique se todas as integrações necessárias estão habilitadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Noções básicas sobre Integração com Rapid7 Vulnerability e Noções básicas sobre a integração de vulnerabilidade da Gestão de ameaças e vulnerabilidades da Microsoft.

5. Para habilitar o módulo, clique na caixa de seleção Ativo para marcá-lo.
6. No campo **Últimas detecções encontradas (dias atrás)**, insira a idade das detecções mais antigas e obsoletas no número de dias.

   O padrão é 90 dias. Você pode inserir qualquer valor positivo para o número de dias. Este valor é usado para corresponder a uma data fornecida pelo seu scanner. Com 90 e **Últimas detecções encontradas** exibidos, todas as detecções não encontradas nos últimos 90 dias são encerradas automaticamente. Com 90 e **Últimos ativos verificados** exibidos, todas as detecções associadas a ativos não verificados nos últimos 90 dias são encerradas automaticamente.

   Nota:

   Há um relacionamento entre o campo Últimas **detecções encontradas/Últimas verificações de ativos (dias atrás)** para este recurso e o campo **Importar desde** na API Integração abrangente de itens vulneráveis do Rapid7 e a integração de vulnerabilidades da máquina com Microsoft TVM.

   Para essas integrações, o campo **Importar desde** nas páginas de configuração está vazio por padrão.

   Se você não inserir um valor ou o campo não tiver nenhum valor, os dados do número de dias configurados no campo **Últimas detecções encontradas/Última verificação de ativos (dias atrás)** serão usados.

   Por exemplo, se o número de dias definido no formulário de configuração de fechamento automático for `90`e o campo **Importar desde** estiver vazio nas páginas de configuração de integração, a primeira execução de integração importará os dados dos últimos 90 dias. Os campos **Importar desde** da Rapid7 Integração abrangente de item vulnerável - API e a integração de vulnerabilidades da máquina com Microsoft TVM são editáveis, portanto, você também pode fornecer os valores desejados. O valor de 90 dias será fornecido como padrão se o campo permanecer vazio para que o recurso de fechamento automático não feche os falsos positivos.

   Este relacionamento entre esses campos se aplica somente à primeira execução de integração. Depois disso, a alteração do campo **Últimas detecções encontradas/ Última verificação de ativos (dias atrás)** no formulário de fechamento automático de detecções vulneráveis obsoletas não afeta o campo **Importar desde** nas páginas de configuração da integração. O campo é alterado para a hora de início da primeira execução para que as execuções de integração subsequentes importem somente as informações delta.

7. Opcional: Marque a caixa de seleção **Ignorar detecções obsoletas para VIs adiados** para ignorar detecções obsoletas que são mapeadas para VIs adiadas ou para VIs atualmente em revisão para adiamento.

   (Optional) Se você deixar esta opção desabilitada, todas as detecções que corresponderem aos seus critérios serão fechadas e mapeadas para VIs adiados ou para VIs que estão em revisão para adiamento. Os VIs adiados ou VIs que estão em revisão e que correspondem a essas detecções também são encerrados automaticamente com base na lógica de acúmulo. Para obter mais informações sobre a lógica de acúmulo, consulte Fechando detecções obsoletas em Resposta a vulnerabilidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você habilitar esta opção, todas as detecções que correspondam aos seus critérios que mapeiam para VIs adiados ou para VIs que estão em revisão para adiamento serão ignoradas durante o fechamento automático.

8. Opcional: Desmarque a caixa de seleção **Ignorar detecções obsoletas para IVs encerrados**.

   (Optional) Por padrão, esta caixa de seleção é marcada para que o VI encerrado não seja reaberto quando uma nova detecção relacionada a este VI encerrado for identificada. Para obter mais informações sobre a lógica de acúmulo, consulte Fechando detecções obsoletas em Resposta a vulnerabilidades.

9. Clique em **Atualizar** para salvar suas mudanças.

   O trabalho agendado *Auto-Close Stale Detections* é executado diariamente. O trabalho determina se você selecionou a data em que as detecções foram encontradas pela última vez ou a data em que os ativos foram verificados pela última vez. Em seguida, ele faz a transição das detecções correspondentes para o estado Obsoleto. É importante observar que o recurso de fechamento automático de detecção obsoleta encerra somente detecções obsoletas para instâncias de integração ativas. Itens vulneráveis e detecções associados a instâncias de integração ativas são encerrados. A partir da v22.0 de Resposta a vulnerabilidades, o trabalho agendado foi modificado para considerar a tabela comum [sn_vul_cmn_auto_close_rule].

   Depois que as detecções forem marcadas como obsoletas, se o scanner relatar que encontrou essa detecção novamente, o campo Status das detecções mudará para Aberto. Os itens vulneráveis correspondentes à detecção também são reabertos.

   Além disso, se a detecção estiver marcada como Obsoleta e o scanner descobrir que ela é Fixa, a detecção muda para Encerrada. O estado também é acumulado para os IVs.

Criar regras de fechamento automático

Use regras de fechamento automático para fechar detecções mais antigas automaticamente com base nas condições de filtro que você definir.

Antes de Iniciar

Função necessária: sn_vul.manage_auto_close_stale_vi

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de encerramento automático**.

   O sistema de base fornece as seguintes regras de fechamento automático:

   - **Última verificação de ativos**: as detecções associadas a ativos que não foram verificados nos últimos 90 dias são transferidas para o estado **Obsoleto**.
   - **Últimas detecções manuais encontradas**: detecções manuais que não foram encontradas nos últimos 90 dias. Se você ativar o **último registro encontrado de Detecções**, este recurso exigirá uma execução de integração bem-sucedida de Rapid7 Integrações Abrangentes de Item Vulnerável e Integração de Vulnerabilidades da Máquina com Microsoft TVM (importação completa) nos últimos sete dias.
   - **Últimas detecções encontradas**: detecções que não foram encontradas nos últimos 90 dias.

2. Selecione **Novo** para criar uma nova regra de fechamento automático.
3. No formulário, preencha os campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
Nome	Nome da regra de fechamento automático.
Ativo	Opção para ativar a regra. Se ativado, ele fechará automaticamente todas as detecções que correspondam aos critérios de filtro.
Ignorar itens adiados	Se selecionado, todas as detecções mapeadas para os estados **Em revisão** ou **Adiado** serão ignoradas e não encerradas. Se você desmarcar esta opção, todas as detecções que corresponderem aos seus critérios serão encerradas.
Ordem de execução	Valor exclusivo para a execução da regra de fechamento automático. Este valor determina a ordem de execução. O valor padrão é 100.
Descrição	Descrição da regra de fechamento automático.
Condição	Condições de filtro usadas para identificar detecções que devem ser encerradas.

4. Selecione **Enviar**.

   O trabalho agendado *Auto-Close Stale Detections* é executado diariamente. Ele identifica detecções com base nas condições especificadas e faz a transição das correspondentes para o estado **Obsoleto**. O trabalho lida com os seguintes cenários:

   - Se todas as detecções em um item vulnerável (VIT) forem marcadas como obsoletas, o VIT será encerrado com o subestado definido como "Obsoleto".
   - Se pelo menos uma detecção permanecer aberta em um VIT, enquanto outras estiverem com o status Obsoleto, o VIT permanecerá aberto.
   - Nos casos em que há detecções com status "Encerrado" e "Obsoleto" em um VIT, o VIT é encerrado com o subestado definido como "Fixo".

   Quando você faz upgrade para a versão mais recente do Resposta a vulnerabilidades, as condições definidas nas regras de fechamento automático também são atualizadas de acordo. Além disso, se as regras estiverem associadas a domínios diferentes, as regras serão criadas especificamente nesses domínios.

Reclassificar hardware não classificado

Reclassifique o hardware não classificado atualizando as regras de pesquisa de IC.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa

A tabela Mapa de importação de host [sn_sec_cmn_src_cmdb_map] exibe as variáveis de entrada da carga útil e suas atribuições correspondentes na tabela Itens descobertos. Ocasionalmente, discrepâncias nas convenções de nomenclatura entre o scanner e a Descoberta podem fazer com que o hardware seja deixado sem classificação. Ao criar um novo IC de hardware não classificado, certifique-se de que o nome na carga útil contenha somente o nome do host. Posteriormente, quando a Descoberta identificar o ativo, ele poderá ser reclassificado na classe de IC apropriada. Se necessário, um script pode ser gravado para gerar um valor derivado que se alinhe com o nome dos ICs na Descoberta e no Configuration Management Database (CMDB).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o Mecanismo de identificação e reconciliação (IRE) estiver ativado, a opção de reclassificação de Itens descobertos não será compatível.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Mapas de importação de host**.
2. Selecione uma origem.
3. Na lista Campo de destino, selecione **Nome**.
   A caixa de seleção **Usar script** se torna visível.

   Nota:

   - O script estará disponível somente se **Nome** for selecionado na lista Campo de destino.
   - Para adicionar um script para outras opções na lista do campo de destino, você deve desabilitar a política de IU:
     - Desabilitando o "Definir script de uso falso".
     - Desativação de "Mostrar ou ocultar script de uso".
     - Removendo a condição "campo de destino é nome" na "política Mostrar ou ocultar script".
   - A tabela Mapas de importação de host foi atualizada com duas novas colunas: Script e Usar script.

4. Marque a caixa de seleção **Usar script**.
   O campo **Script** exibe o script padrão, mas você tem a opção de criar um personalizado. Neste campo, você pode especificar os valores de origem e derivados para alinhar com a convenção de nomenclatura do banco de dados. O valor gerado pelo script é armazenado em sourcePayload['DERIVED'][rule.source_field]. Certifique-se de que as regras de pesquisa de IC estejam ajustadas para utilizar carga de origem, valores de atributo derivados e de destino ao fazer check-in das tabelas correspondentes.
5. Para aplicar o script a registros duplicados mais antigos, faça o seguinte:

   a. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens Descobertos**.

   b. Selecione os registros duplicados.

   c. Na lista Ação em linhas selecionadas, selecione **Reaplicar regras de pesquisa de IC**.
   Mostra uma correspondência com um ativo existente.

6. Para aplicar o script para Tenable.io, faça o seguinte:

   a. Navegar até **Resposta a vulnerabilidades Mapas de importação de host**.

   b. Selecione o script para a linha com os nomes NetBIOS, HOSTNAMES e FQDNS como o campo **Origem**.

   c. Atualize o script para cada elemento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para Tenable.io, o scanner retorna uma matriz para nomes NetBIOS, HOSTNAMES e FQDNS, para os quais o script não funciona conforme o esperado.

Como o Mapa de importação de host para Tenable.io contém **netbios_name** no campo **Origem**, você deve gravar um script. Durante a pesquisa, outro campo de origem **NETBIOS** é usado, que tem uma matriz de valores. Portanto, uma nova linha é adicionada à tabela e a mesma lógica deve ser gravada em um loop no script. Da mesma forma, para **FQDNS** e **HOSTNAMES**.

7. Para aplicar o script para Rapid7, faça o seguinte:
   a. Navegar até **Todos** > **Resposta a vulnerabilidades Mapas de importação de host**.
   b. Para linhas Rapid7 com FQDN e HostName, atualize o Método de pesquisa para Script.

Nota: Para Rapid7, o método Pesquisa de IC é definido como Correspondência de campo para FQDN e Nome do host, o que ajuda a impedir que ele use o script.

Criar manualmente uma tarefa de correção no Resposta a vulnerabilidades

A criação de uma tarefa de correção manualmente é feita quando você deseja agrupar itens vulneráveis por algo diferente dos critérios de Regras de tarefa de correção. Por exemplo, você pode criar tarefas para um gerente específico ou para novas explorações ativas, como ransomware que incluem diferentes vulnerabilidades. Você também pode usá-lo para agrupar itens vulneráveis não agrupados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.

   As regras de tarefa de correção funcionam da mesma forma que as regras de grupo de vulnerabilidades funcionavam anteriormente e ainda estão disponíveis para você. No entanto, talvez você prefira deixar as regras de tarefa de correção inativas enquanto se acostuma com os recursos que estão disponíveis para seus gerentes de segurança e equipes de TI nos espaços.

2. Selecione uma das categorias de tarefas para abrir a lista.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.
   Para obter informações sobre campos específicos, consulte Campos do formulário da tarefa de correção.
5. Clique em **Enviar**.
   Quando a tarefa é criada, usando o tipo de filtro **Condição** ou **Grupo** de filtros, a lista relacionada ao **item vulnerável** pesquisa e exibe todos os itens vulneráveis correspondentes.

   Você pode usar o Link relacionado, Verificar novamente se **há vulnerabilidades** para acionar manualmente uma verificação iniciada por ServiceNow®. Para obter informações sobre como configurar um scanner de vulnerabilidades, consulte Configurar e gerenciar Qualys scanners e verificações de vulnerabilidade.

   Para uma integração de vulnerabilidade da Qualys, um scanner padrão é pré-instalado no módulo **Scanners de vulnerabilidade**. Este scanner está desativado por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marque as caixas de seleção **Ativo** e **Padrão** para ativar o scanner da Qualys para funcionar usando o link relacionado **Verificar vulnerabilidades** na tarefa de correção e nos formulários de itens vulneráveis.

O link relacionado **Atualizar status** exibe a data e a hora da última atualização. Ele acumula informações dos IVs na tarefa de correção. Para obter mais informações, consulte Campos do formulário da tarefa de correção. Quando uma tarefa é formada com base em uma vulnerabilidade específica, essa vulnerabilidade é listada no formulário da tarefa de correção.

Se você abrir um item vulnerável associado, todas as entradas de tarefa de correção associadas serão exibidas na guia da lista relacionada **Tarefa** de correção.

Adicionar usuários ao grupo da Resposta a vulnerabilidades

Quando o recurso Fechar/Adiar é usado para adiar ou fechar um item vulnerável sem exigir uma verificação, o grupo Resposta a vulnerabilidades é notificado para aprovar ou rejeitar a solicitação. Você pode atribuir os usuários apropriados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Abra o grupo Resposta a vulnerabilidades.
3. Clique na lista relacionada **Membros do grupo** e clique em **Editar**.
4. Selecione um ou mais nomes na lista **Coleção**.
5. Clique em **Adicionar**.
6. Clique em **Salvar**.

Informações relacionadas

Criar um usuário

Gerenciar itens vulneráveis individuais manualmente

Itens vulneráveis representam um item de configuração (IC) com uma determinada vulnerabilidade. Itens vulneráveis são importados de fontes de terceiros ou usando as informações do SAM NVD (link) para comparar entradas de vulnerabilidade com registros de software recuperados do módulo Software Gestão de ativos.

Os itens vulneráveis estão contidos em tarefas de correção definidas por regras de vulnerabilidade. Normalmente, as tarefas de correção são o local onde grupos de itens vulneráveis são atribuídos e trabalhados.

Itens vulneráveis podem ser exibidos e editados em massa no módulo **Itens vulneráveis**. Os registros de item vulnerável exibem informações da vulnerabilidade na guia **Vulnerabilidade**. Esta guia pode indicar se há explorações públicas ou ativas para ela. Além disso, mostra se ele pode ser corrigido por meio de um patch, mudança de configuração ou combinação de ambos. Se houver endereços IP encontrados durante a desduplicação, eles serão exibidos em uma lista relacionada.

Se um IC for removido do CMDB, todos os itens vulneráveis associados também serão removidos.

Quando um item vulnerável é adicionado a uma tarefa de correção, o grupo aparece na lista **Tarefas** de correção de itens vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando é criada uma tarefa que afeta um item vulnerável, a tarefa aparece na lista relacionada **Tarefas que afetam** de itens vulneráveis.

Itens vulneráveis podem ser criados manualmente. Você pode criar incidentes de segurança ou solicitações de mudança e fechá-los ou adiá-los manualmente. As regras de tarefa de correção podem ser aplicadas a itens vulneráveis criados manualmente.

As tarefas de correção e as regras de tarefa de correção foram aprimoradas para assumir a funcionalidade da tarefa. Itens vulneráveis não podem ser vinculados como uma tarefa primária.

Criar Resposta a vulnerabilidades itens vulneráveis

Vários métodos criam itens vulneráveis (VI). Normalmente, uma integração a um scanner de vulnerabilidades é instalada e configurada para importar resultados todas as noites. Há casos, como vulnerabilidades de segurança física, em que você pode preferir adicionar manualmente registros de itens vulneráveis.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_write

Por Que e Quando Desempenhar Esta Tarefa
Os IVs criados manualmente e os VIs criados automaticamente são adicionados e removidos automaticamente das tarefas de correção por regras de tarefa de correção e condições de grupo.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Selecione uma categoria para abrir a lista.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.
   Para obter informações sobre os campos de itens vulneráveis, consulte Resposta a vulnerabilidades campos de formulário de item vulnerável.
5. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.

   As regras de tarefa de correção avaliam o item vulnerável e o adicionam a uma tarefa existente ou criam uma nova tarefa. Se a avaliação falhar, o item vulnerável será adicionado à lista de **Itens vulneráveis** não agrupados.

   Quando você salva um novo item vulnerável, todas as calculadoras habilitadas são executadas.

   Nota: Somente uma calculadora por **campo de destino** pode estar ativa por vez. Quando você ativa um, todos os outros com o mesmo **campo de destino** são desativados.

6. Você pode clicar em qualquer uma das listas relacionadas para exibir informações adicionais.

   Você pode usar o Link relacionado, **Verificar vulnerabilidades** para acionar manualmente uma verificação iniciada por ServiceNow®. Para obter informações sobre como configurar um scanner de vulnerabilidades, consulte Configurar e gerenciar Qualys scanners e verificações de vulnerabilidade.

   Para uma integração de vulnerabilidade da Qualys, um scanner padrão é pré-instalado no módulo **Scanners de vulnerabilidade**. Este scanner está desativado por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marque as caixas de seleção **Ativo** e **Padrão** para ativar o scanner da Qualys para funcionar usando o link relacionado **Verificar vulnerabilidades** na tarefa de correção e nos formulários de itens vulneráveis.

As seguintes opções de edição e correção ficam disponíveis na barra de cabeçalho:

- Atualizar: salva atualizações no formulário.
- Criar incidente de segurança: cria um incidente de segurança.
- Fechar: fecha o item. Se todos os itens do grupo forem encerrados, a tarefa de correção será encerrada automaticamente.
- Exceção de solicitação: envia uma solicitação para adiar um item.
- Resolver: resolve o item.
- Excluir: remove o item vulnerável.

Informações relacionadas

Editar itens vulneráveis em massa no Resposta a vulnerabilidades

Adiar um item vulnerável

Se você determinar que o problema associado a um item vulnerável (VIT) é de baixo risco e pode ser adiado imediatamente sem análise adicional, você pode usar o recurso **Adiar**.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho agendado é executado todos os dias, verificando se há itens vulneráveis adiados que atingiram a data de reabertura. No dia em que o adiamento do IV estiver definido para expirar, o registro será reaberto.

A partir da Resposta a vulnerabilidades v20.0, antes de reabrir um VI adiado, o trabalho agendado `Verificar item vulnerável e adiamento de expiração de grupos` verifica se alguma regra de exceção é aplicável em um VI adiado e atualiza os campos **Motivo** e **Até** de acordo com a regra de exceção. O estado do IV permanece Adiado até a data de vencimento mais recente.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item vulnerável.
3. Clique **em Solicitar exceção**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 18.0 de Resposta a vulnerabilidades (VR), se um item vulnerável adiado for fechado e reaberto por um scanner antes que a janela de exceção expire, o estado do VIT será revertido para o estado adiado, respeitando a janela de exceção ativa. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema sn_vul.auto_defer_vit_in_active_exception_window como verdadeiro. Além disso, a data adiada Até persiste mesmo depois que o item vulnerável é fechado ou a exceção expira. A função necessária é sn_vul.manage_exception_configuration para leitura e gravação. Depois que o registro for enviado, se as notificações por e-mail estiverem definidas, os membros do grupo Resposta a vulnerabilidades receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como Aberto e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Falso positivo ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Clique em **Enviar**.
   O grupo está marcado como **Em revisão**. Um link relacionado a **Reabrir** é exibido. A data e o motivo da reabertura aparecem nas anotações de trabalho na guia **Aprovações de mudança de estado**.

Solicitar uma extensão para um item vulnerável adiado

Solicite uma extensão para um item vulnerável adiado antes que ele atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item vulnerável adiado.
3. Selecione **Solicitar extensão**.

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável é Adiado.

4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

   Nota:
   - A solicitação passa por dois níveis de aprovação.
   - Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Atualizar Resposta a vulnerabilidades itens vulneráveis
O link relacionado **Atualizar status** é usado para que itens vulneráveis sejam inspecionados para ver se há itens vulneráveis adicionais que pertençam a uma tarefa de correção. Use-o se uma atualização for garantida fora do trabalho agendado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write ou, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

O link relacionado **Atualizar status** só pode ser editado no formulário da tarefa de correção nos estados **Aberto** ou **Sob investigação**, usando um grupo de filtros ou em que o tipo de filtro é condição. Esta inspeção é feita independentemente do status da caixa de seleção **Atualizar itens vulneráveis** automaticamente.

A partir da v22.0 de Resposta a vulnerabilidades, o botão **Atualizar status** está disponível na exibição de registro para tarefas de correção em Vulnerability Manager Workspace e Espaço de correção de problemas de TI.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra qualquer registro nos estados **Aberto** ou **Sob investigação**.
3. Clique no link **Atualizar status**.
   Novos itens vulneráveis aparecem na guia **Itens vulneráveis**.

Identificar e escalar problemas de segurança em software de terceiros

Você pode exibir vulnerabilidades de software retornadas de entradas de terceiros para determinar a correção. Use essas informações para corresponder as entradas de software vulnerável a um modelo de descoberta de Software Gestão de ativos.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Bibliotecas** > **Terceiro**.
   Uma lista de software vulnerável baixado é mostrada.
2. Clique em um registro de software para exibir informações de vulnerabilidade.
3. Clique nas seguintes listas relacionadas para obter mais informações para identificar vulnerabilidades.

Lista relacionada	Descrição
Itens vulneráveis	Lista todos os itens vulneráveis, que consistem em emparelhamentos de um item de configuração e software potencialmente vulneráveis. Para obter mais informações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
	sobre um emparelhamento, clique no ícone de informações (ícone). **Nota:** Se o software for removido, todos os itens vulneráveis associados serão encerrados e removidos da lista relacionada de **itens vulneráveis**.
Entradas de Vulnerabilidade	Lista as entradas de vulnerabilidade do registro de software selecionado. Clique em um registro para exibir seus detalhes.

Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Identificar e escalar problemas de segurança usando o NVD

Quando os registros do identificador de vulnerabilidade e exposição comum (CVE-ID) são baixados do banco de dados nacional de vulnerabilidades (NVD), eles são comparados ao software na rede da sua empresa conforme identificado pelo modelo de descoberta de ativos de software. Quando um CVE-ID corresponde a um software vulnerável ou item de configuração em sua rede, um item vulnerável é criado. Você usa as informações no registro CVE-ID para decidir se deve escalar o item vulnerável para correção.

Antes de Iniciar

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Bibliotecas** > **NVD**.
   Uma lista de CVE-IDs que foram baixados do NVD é mostrada. As atualizações do NVD podem ser realizadas sob demanda e por execuções programadas dos registros do NIST National Vulnerability Database Integration, localizados em **Todos** > **Administração** > **Integrações**.
2. Clique em um registro CVE para exibir as seguintes informações:
   - um resumo do CVE-ID.
   - uma referência a uma entrada de Enumeração de Pontos Fracos Comuns (CWE), se aplicável.
   - a pontuação de vulnerabilidade do CVE-ID no Common Vulnerability Scoring System (CVSS). Para obter mais informações sobre o CVSS, consulte o site do Banco de dados nacional de vulnerabilidades .
3. Clique nas listas relacionadas para obter mais informações sobre vulnerabilidades.

   Referências de vulnerabilidade

   Nome, descrição e URL da vulnerabilidade fornecida e onde ela é referenciada.

   Explorações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes.

Pontos fracos

Lista de pontos fracos do CWE.

4. Clique nas seguintes listas relacionadas para obter mais informações para identificar vulnerabilidades.

Lista relacionada	Descrição
Itens vulneráveis	Lista todos os itens vulneráveis, que consistem em emparelhamentos de um item de configuração e software potencialmente vulneráveis. Para obter mais informações sobre um emparelhamento, clique no ícone de informações (ícone). **Nota:** Se o software for removido, todos os itens vulneráveis associados serão encerrados e removidos da lista relacionada de **itens vulneráveis**.
Entradas de Vulnerabilidade	Lista as entradas de vulnerabilidade do registro de software selecionado. Clique em um registro para exibir seus detalhes.

Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Identificar e escalar problemas de segurança usando o CWE

Exiba a biblioteca de registros de Enumeração de pontos fracos comuns (CWE) do Banco de dados nacional de vulnerabilidades (NVD) para entender como eles se relacionam com os registros de Vulnerabilidade e exposição comuns (CVE). Em seguida, use essas informações para corresponder as entradas de software vulnerável a um modelo de descoberta de Software Gestão de ativos.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Bibliotecas** > **CWE**.
   Uma lista de software vulnerável baixado é mostrada.
2. Clique em um registro de software CWE para exibir informações de vulnerabilidade.
3. Clique nas seguintes listas relacionadas para obter mais informações para identificar vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Itens vulneráveis	Lista todos os itens vulneráveis, que consistem em emparelhamentos de um item de configuração e software potencialmente vulneráveis. Para obter mais informações sobre um emparelhamento, clique no ícone de informações (ícone). **Nota:** Se o software for removido, todos os itens vulneráveis associados serão encerrados e removidos da lista relacionada de **itens vulneráveis**.
Entradas de Vulnerabilidade	Lista as entradas de vulnerabilidade do registro de software selecionado. Clique em um registro para exibir seus detalhes.

Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Exibir o status da meta de correção de um Resposta a vulnerabilidades item vulnerável

Quando um item vulnerável quase atingiu (ou passou) sua data de meta de correção, conforme definido por uma regra de meta de correção, o registro do item vulnerável é atualizado com um status. Essas informações podem ajudar o analista a monitorar proativamente as próximas atividades de correção.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [somente leitura]

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho agendado chamado **Avaliar metas de correção** é executado uma vez por dia para comparar a data atual com a data de correção do item vulnerável especificada na regra de meta de correção associada. Quando a data atual estiver dentro do número de dias anteriores ao vencimento da correção, um status de correção será adicionado ao registro do item vulnerável.

Para obter mais informações sobre regras de destino de correção, consulte Resposta a vulnerabilidades regras de destino de correção.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Itens vulneráveis**.
2. Clique no item vulnerável que você deseja revisar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a data de correção do item vulnerável estiver dentro do intervalo das condições definidas na regra de meta de correção, a guia **Status** da meta de correção ficará visível.

3. Clique na guia **Status da meta de correção**.
4. Clique no registro de status da meta de correção para revisá-lo.

> **Nota:** Para exibir o número de itens vulneráveis que estão se aproximando da meta, em curso e meta passada, consulte Usando os painéis padrão Resposta a vulnerabilidades.

Informações relacionadas

Criar ou editar Resposta a vulnerabilidades regras de destino de correção

Como trabalhar com ICs incompatíveis

Como Gerente e analista de vulnerabilidade, você pode exibir e reclassificar itens de configuração (ICs) incompatíveis, reconciliar itens descobertos incompatíveis, reaplicar regras de pesquisa de IC nos itens descobertos selecionados e desduplicar ICs existentes.

Exibir e reclassificar itens de configuração incompatíveis

Os itens de configuração (ICs) que não são encontrados em Configuration Management Database (CMDB) são colocados em uma lista visível de itens descobertos. Esta lista oferece uma maneira conveniente de reclassificar ICs não correspondentes.

Antes de Iniciar

Função necessária:
sn_vul.read (mínimo para exibir ICs incompatíveis)

e

itil ou ativo (para reclassificar)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

Como Analista de vulnerabilidade, você pode exibir ICs incompatíveis.

A ação de reclassificação está disponível somente em ICs de classe *sn_sec_cmn_unmatched_ci*, quando você tem as funções itil ou de ativo. Depois que um IC é reclassificado, ele não pode ser reclassificado usando a IU. Você pode reclassificar, no formulário de IC ou na exibição de lista de ICs, alterando o valor da **classe**. Para obter mais informações, consulte Reclassificar um IC .

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **CMDB** > **Itens Descobertos**.
2. Para revisar, clique em cada item.
3. Para fazer correções nas informações nos campos de formulário de **Item descoberto**, edite nesta página e clique com o botão direito do mouse em **Salvar**.
   Todos os dados adicionados ou deixados nesses campos são transferidos para o **item de configuração** resultante quando ele é reclassificado.
4. Se tudo estiver correto, clique em **Reclassificar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na lista de seleção, selecione um **Nome de classe** e clique em **Enviar**.
   A **classe** de **item descoberto** é atualizada, o campo **Estado** é alterado para Reclassificado e todos os dados estão no CMDB.

Reconciliar itens descobertos sem correspondência

Crie um trabalho agendado para reconciliar itens descobertos incompatíveis.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Um item vulnerável (VI) consiste em uma vulnerabilidade e um item de configuração (IC). Quando um VI é criado, o IC adicionado a ele no momento da criação pode estar desatualizado. As informações de IC incompatível não serão reconciliadas se as informações no CMDB mudarem. Para reconciliar, aplique regras de pesquisa de item de configuração (IC) nos itens que estão em um estado incompatível quando o CMDB é atualizado com os ICs mais recentes.

Você pode executar uma demanda de trabalho agendada para reaplicar a regra de correspondência de IC para os itens descobertos em um estado incompatível. Se o IC mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. As detecções afetadas e os itens vulneráveis também são atualizados. Para obter detalhes, consulte Mudanças de IC para itens descobertos.

Procedimento

1. Navegar até **Todos** > **Operações de segurança > Reconciliar itens descobertos incompatíveis**.
2. Na página Trabalhos em segundo plano, clique em **Criar trabalho de reconciliação**.
3. No formulário, preencha os campos.

Nota: Você só pode editar o campo **Parâmetros**.

Formulário de trabalho em segundo plano

Campo	Descrição
Número	Número de trabalho exclusivo.
Criado por	Usuário que criou o trabalho.
Parâmetros	Parâmetros para reconciliar os itens descobertos incompatíveis: ◦ limite: número máximo de itens descobertos a serem reconciliados. Se você não inserir um valor, 10.000 itens descobertos serão reconciliados. ◦ firstDiscovereditem: primeiro item descoberto que deve ser reconciliado. Se você não inserir um valor, o processo de reconciliação será iniciado a partir do primeiro item descoberto.
Estado	Estado atual do trabalho em segundo plano.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição do estado	Descrição do estado atual do trabalho em segundo plano.
Tipo de trabalho	Tipo de trabalho. O valor é **Reconciliar itens descobertos incompatíveis**.
Iniciada em	Hora em que o trabalho foi iniciado.
Finalizado às	Hora em que o trabalho foi concluído.
Duração do trabalho	Tempo total necessário para concluir o trabalho.
Subestado	Subestado do estado selecionado.
Anotações	Número de registros que foram processados.

4. Clique em **Enviar**.

Nota:

- Para interromper a execução do trabalho, clique em **Cancelar**.
- Você não pode reconciliar ICs incompatíveis ou reaplicar regras de pesquisa de IC enquanto estiver importando hosts ou itens vulneráveis.

Reaplicar regras de pesquisa de IC em itens descobertos selecionados

Reaplicar as regras de pesquisa de item de configuração (IC) nos itens descobertos selecionados nas ações de seleção da exibição de lista de itens descobertos. Se o IC mudar depois que você reaplicar as regras, os itens descobertos serão atualizados com o novo IC e as detecções afetadas. Itens vulneráveis também são atualizados.

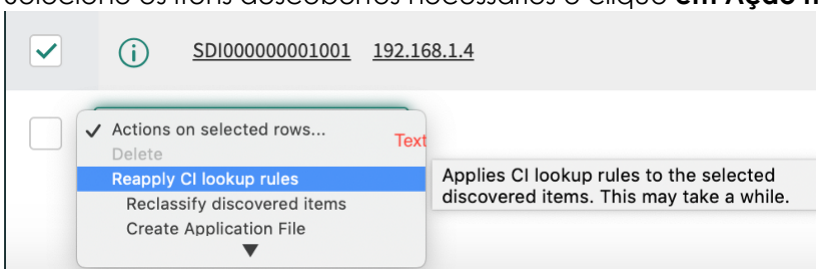
Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para obter mais informações, consulte Mudanças de IC para itens descobertos.

Para obter mais informações sobre os conceitos de correspondência de IC e o CMDB, pesquisa de item descoberto, identificação baseada em regras e outras informações detalhadas sobre como funciona a correspondência de IC, consulte o artigo Correspondência de IC na Resposta a vulnerabilidades [KB0998706] na Base de conhecimento HI.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **CMDB** > **Itens Descobertos**.
2. Selecione os itens descobertos necessários e clique **em Ação nas linhas selecionadas**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista, selecione **Reaplicar regras de pesquisa de IC**.

   As regras são reaplicadas nesses itens descobertos.

4. Clique em **Exibir status** na mensagem.

   O status é exibido no formulário de trabalho em segundo plano.

   Nota: No campo **Anotações**, os `itens descobertos não puderam ser processados porque o atributo de exceção` com um valor diferente de zero indica que há um erro ou uma exceção ao reaplicar uma regra de pesquisa de IC. Verifique os logs do sistema para obter mais detalhes.

Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Resposta a vulnerabilidades regras de pesquisa de IC

Tome medidas para ajudar a evitar registros duplicados ou órfãos resultantes da correspondência (itens de configuração (ICs) no CMDB.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência no CMDB pode resultar em tempos de processamento demorados. O teste completo e a depuração de scripts de processamento nas regras ajudam a aliviar o potencial de problemas posteriores no processo.

Como evitar registros duplicados ou órfãos

- Use pequenos subconjuntos de dados que são específicos para a regra de pesquisa de IC que está sendo testada.
  - Defina todas as Regras de pesquisa de IC, exceto a que está sendo testada, como Inativas.
  - Analise os ICs importados para garantir que você esteja observando o comportamento esperado e que a correspondência esteja ocorrendo corretamente.
- Revisar ICs correspondentes
  - Examine a contagem de ICs correspondentes versus não correspondentes. Certifique-se de que a porcentagem seja aceitável. Não olhe apenas para a primeira página, provavelmente é a primeira inserida.
  - Pesquise manualmente alguns ICs.
  - Verifique se há problemas de nomeação ou de campo (como pesquisar um domínio específico).

    Se parecer apropriado, adicione regras de correspondência adicionais.
- Revisar ICs incompatíveis
  - Navegue até a tabela ICs incompatíveis.
  - Agrupar por classe de item de configuração.
  - Revise todas as classes que não parecem corretas (certificados, cartões de rede, imagens).
    - Descobrir por que eles não corresponderam ao IC correto?
    - A classe deve ser excluída?
    - A classe deve ser elevada a uma classe relacionada?

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Revise os estados do IC, como **Descontinuado**.
- Remover dados de teste
  - Depois de começar a observar o comportamento correto ou esperado na correspondência de IC, reinicie.
  - Reinicie: Excluindo os dados usados para testar: (consulte a seção **Excluindo dados de tabelas**)
    - Itens Descobertos
    - Itens vulneráveis
    - Tarefas de correção
  - Reexecução manual de todas as regras de correspondência de IC.

Para obter mais informações sobre Regras de pesquisa de IC e Qualys, consulte o artigo KB0750656 .

Para obter mais informações sobre Regras de pesquisa de IC e Rapid7, consulte KB0818096 .

Excluindo dados de tabelas

Às vezes, você importou dados e percebeu que algo está errado. Se algo estiver errado em um ambiente de desenvolvimento ou desempenho, você poderá recriar a partir de um ambiente melhor, mas isso nem sempre é uma opção.

Nota: A execução dessas ações requer ServiceNow experiência.

Existem quatro opções para excluir dados de tabelas:

- Usando **Excluir todos os registros** na **configuração da tabela**.
- Configure o **limpador de tabela** navegando até **Limpezas automáticas** (sys_auto_flush.list) e criando um novo registro **de limpeza automática**.
- Truncar gs.truncateTable usando um script em segundo plano.

  O uso de *truncateTable* requer a desativação do registro para caixa de seleção de reversão nos scripts em segundo plano. Caso contrário, uma cópia da tabela e das tabelas em cascata relacionadas será criada, demorará muito e provavelmente falhará.

  Nota: Nunca use *truncateTable* em um ambiente de produção. Consulte o representante de suporte antes de executar grandes exclusões em ambientes compartilhados ou de produção.

Desduplicação de itens de configuração existentes

Sempre que os itens de configuração (ICs) são atualizados por meio de uma tarefa de desduplicação, os itens descobertos (DIs) que estão relacionados a esses ICs também são atualizados. Os itens vulneráveis (IVs) e as detecções também são atualizados com o IC.

Para obter mais informações, consulte Mudanças de IC para itens descobertos.

Informações relacionadas

Como corrigir uma tarefa de desduplicação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resolver tarefas de correção

A flexibilidade inerente ao Resposta a vulnerabilidades permite que você corrija vulnerabilidades da maneira que for mais adequada à sua organização de segurança.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Depois de receber a notificação de que uma solicitação de mudança foi resolvida, mova o estado da tarefa de correção para Resolvido e aguarde a próxima verificação. Novas verificações são acionadas automaticamente pela programação de importação de terceiros configurada no Assistente de configuração.

Nota:

Se a sincronização de estado estiver ativada, as tarefas de correção serão movidas automaticamente para o estado Resolvido depois que uma solicitação de mudança associada a uma tarefa de correção (VUL) for implementada e estiver no estado Revisão. Consulte Gestão de mudanças para Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuído a mim**.
2. Clique em um registro que esteja no estado Aberto.

   O estado Aberto indica que o registro ainda não foi trabalhado. O formulário exibe:

   - Informações da tarefa de correção
   - Detalhes da configuração do grupo
   - Anotações
   - Itens vulneráveis associados
   - ANS de tarefas
   - Solicitações de mudança
3. Execute sua análise do grupo.
4. Quando você estiver pronto para começar a trabalhar no registro, escolha uma das seguintes opções.

Opção	Descrição
Se o item vulnerável representar um risco para o seu ambiente de TI, crie um registro CHG e escale o problema para a equipe de Gestão de mudanças .	Atribua o grupo ao grupo ou indivíduo apropriado e clique em **Criar mudança**.
Se o item vulnerável representar um possível risco de segurança para sua organização, crie um registro de incidente de segurança e escale o problema para a equipe Security Incident Response.	Clique **em Criar incidente de segurança**. Este botão é exibido somente quando Security Incident Response está ativado. Um cálculo de impacto nos negócios é aplicado, o incidente é atribuído e o incidente de segurança é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de criar uma solicitação de mudança, o registro apropriado aparece na lista relacionada **Solicitações de mudança** no formulário Grupo de vulnerabilidade.

5. Se você determinar que o problema é de baixo risco e pode ser adiado, clique em **Solicitar exceção**.
   Para obter mais informações sobre como adiar uma tarefa de correção, consulte Adiar uma tarefa de correção.
6. Se você determinar que o problema pode ser encerrado imediatamente sem análise adicional, clique em **Fechar**.
   Para obter mais informações sobre como encerrar uma tarefa de correção, consulte Fechar uma tarefa de correção. A partir da v23.0 de Resposta a vulnerabilidades, o botão **Fechar** foi removido para uma tarefa de correção.

   Um trabalho agendado de integração de terceiros atualiza e verifica automaticamente os registros em um intervalo definido. Os itens vulneráveis são verificados na próxima data e hora programadas. Como alternativa, você pode iniciar manualmente uma verificação de vulnerabilidades usando o link relacionado **Verificar vulnerabilidades**.

   Se a verificação encontrar novamente a vulnerabilidade no item de configuração e não marcá-la como Corrigida, o item vulnerável retornará ao estado Sob investigação. Entre em contato com Operações de TI para reabrir a solicitação de mudança.

   Se a verificação não encontrar a vulnerabilidade e retornar que o item vulnerável foi marcado como Corrigido, o item vulnerável passará para o estado Fechado-Corrigido e será fechado durante a importação.

   Somente quando todos os itens vulneráveis em uma tarefa estão no estado Fechado-Corrigido, a tarefa de correção é fechada automaticamente. As tarefas de correção com itens vulneráveis em estados Encerrados diferentes de Fixo devem ser encerradas manualmente.

Adiar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção (VUL) é de baixa prioridade e pode ser adiado imediatamente sem análise adicional, você pode usar o recurso **Solicitar exceção**.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você pode adiar uma tarefa de correção de um registro de tarefa de correção nos espaços Resposta a vulnerabilidades. Depois de enviar a solicitação, ela é enviada para aprovação. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Um trabalho agendado é executado todos os dias, verificando se há tarefas de correção adiadas que atingiram a data de reabertura. No dia em que o adiamento da tarefa estiver definido para expirar, a tarefa será reaberta.

Nota: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção , a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados Encerrado ou Adiado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra um registro.
3. Clique **em Solicitar exceção**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada. Depois que o registro for enviado, se as notificações por e-mail estiverem definidas, os membros do grupo Resposta a vulnerabilidades receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, a tarefa de correção é definida novamente como **Aberta** e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Falso positivo ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Clique em **Enviar**.
   O grupo está marcado como Em revisão. Um link relacionado a **Reabrir** é exibido. A data e o motivo da reabertura aparecem nas anotações de trabalho na guia **Aprovações de mudança de estado**.

Solicitar uma extensão para uma tarefa de correção adiada

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento adiada. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Com a aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis devem estar no estado adiado e seus dados atuais até precedem a data atualizada até. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Fechar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção pode ser encerrado imediatamente sem análise adicional, poderá usar o recurso **Fechar**. A partir da v23.0 de Resposta a vulnerabilidades, o botão **Fechar** foi removido para uma tarefa de correção e o fechamento de uma tarefa de correção é orientado pelo scanner.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nos espaços Resposta a vulnerabilidades, uma tarefa de correção passa pelos mesmos estados que uma tarefa de correção anterior tinha nas versões anteriores do Resposta a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades. Quando todos os itens vulneráveis (VITs) em uma tarefa de correção são encerrados, a tarefa de correção faz a transição para o estado Inativo.

Importante: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção , a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados `Encerrado` ou `Adiado`.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Selecione o botão **Fechar/Adiar**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Estado	Selecione um estado. As opções são: ◦ Adiado ◦ Encerrado
Até	Disponível somente no pop-up **Adiar** estado. Selecione a data em que o estado **Adiado** expira e a tarefa de correção é reativada. Depois que o registro for enviado, se as notificações por e-mail estiverem definidas, os membros do grupo Resposta a vulnerabilidades receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como **Aberto** e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para encerrar o problema.
Informação adicional	Insira outras informações relevantes.

4. Selecione **Enviar**.
   A tarefa de correção é marcada como **Encerrada**.

Identificação de itens vulneráveis duplicados de vários scanners

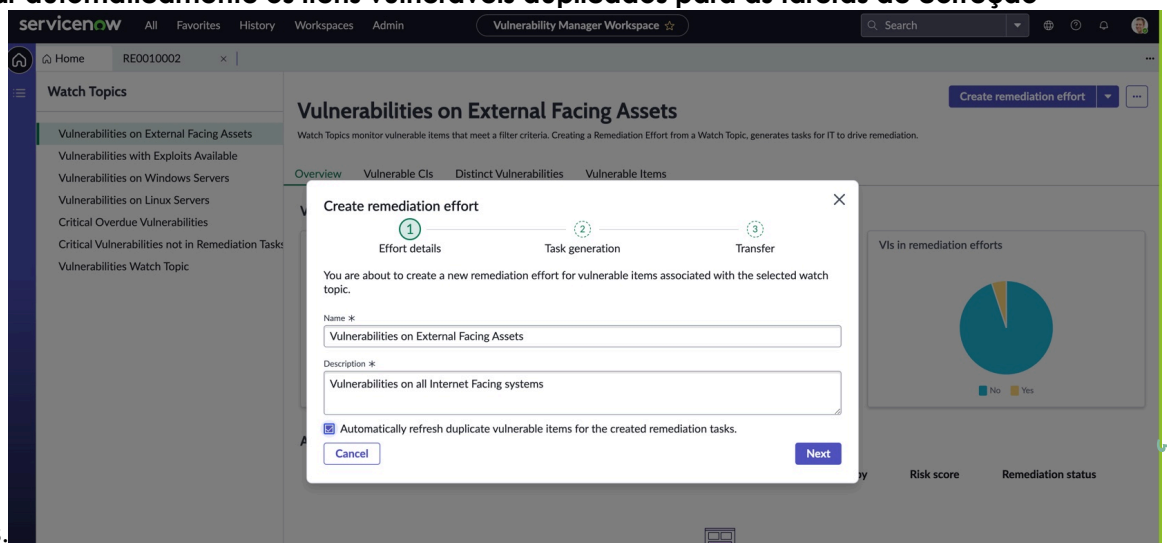
Se você estiver usando vários scanners no mesmo ativo para detectar vulnerabilidades, vários itens vulneráveis (IVs) poderão ser criados. Você pode identificar esses IVs duplicados para garantir que as vulnerabilidades duplicadas não sejam atribuídas aos responsáveis pela correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta resolução só será possível se as mesmas vulnerabilidades, como as mesmas CVEs (Common Vulnerability and Exposures, vulnerabilidades e exposições comuns), forem detectadas. A combinação de vulnerabilidades depende dos scanners usados. Por exemplo, a Qualys e a Tenable têm seu próprio tipo de vulnerabilidade, ou seja, entradas de terceiros (TPEs), e outros scanners, como o Microsoft Defender for Endpoint, detectam vulnerabilidades com base em CVEs.

A partir da v 17.1, ao criar um esforço de correção, você pode atualizar automaticamente os itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar a opção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.



Mostrar IVs duplicados: identifica itens vulneráveis duplicados relatados por vários scanners no sistema. Você pode marcar o VI duplicado como Resolvido. Para obter mais informações, consulte Resolver automaticamente vulnerabilidades duplicadas. Entradas duplicadas são mostradas somente quando a combinação de vulnerabilidades é criada usando CVEs. Para obter mais informações, consulte Tarefa de correção da Resposta a vulnerabilidades e estados de itens vulneráveis.

Possíveis duplicatas são identificadas para as seguintes combinações de vulnerabilidade:

Combinação de scanner	Tipo de vulnerabilidade
Verificador 1 e Verificador 2	CVE
Verificador 1 e Verificador 2	CVE e TPE

Resolver automaticamente vulnerabilidades duplicadas

A partir de Resposta a vulnerabilidades (VR) v17.1, você pode resolver automaticamente quaisquer vulnerabilidades duplicadas em um ativo.

Quando um ativo é verificado com vários scanners, há uma chance de identificar a mesma vulnerabilidade como duplicatas por diferentes scanners. Por exemplo, se os scanners da Qualys e da Microsoft identificarem a mesma vulnerabilidade, você poderá optar por resolver automaticamente a vulnerabilidade duplicada.

Cenário de amostra

O VR cria um registro, VI1, para a vulnerabilidade 1 do scanner do Microsoft Defender for Endpoint. Um segundo registro, VI2, é criado a partir do scanner Qualys para a mesma vulnerabilidade. A equipe de correção aplica os patches que podem resolver os registros

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

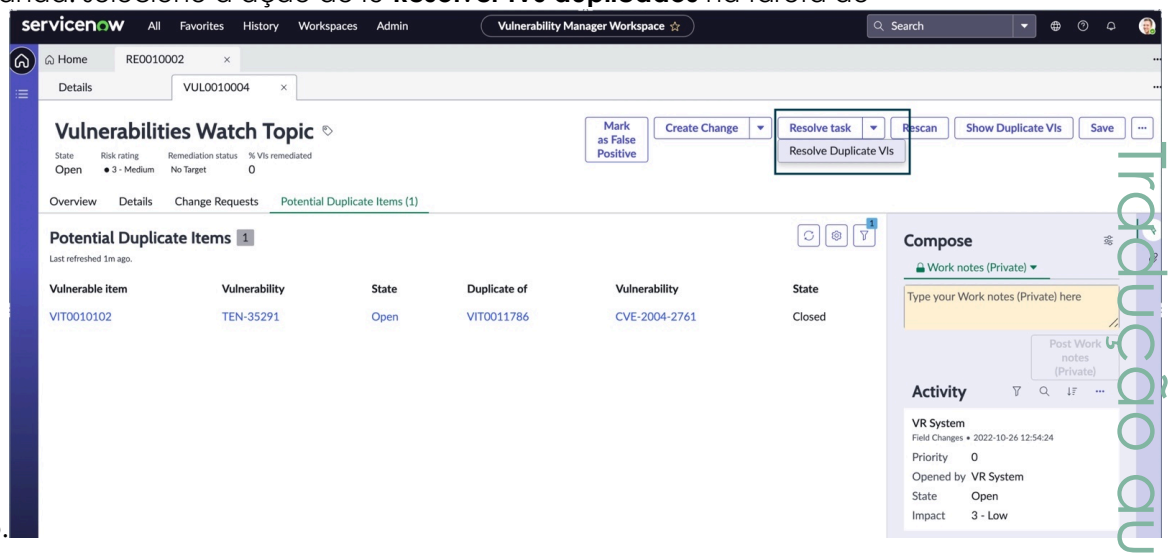
VI1 e VI2. Se você configurar a programação de verificação da Qualys além de um dia, nesse momento o Microsoft Defender fornecerá as informações de vulnerabilidade fixa e o VR fechará o registro VI1 como Encerrado/Corrigido.

Neste cenário, o registro de VI2 ainda está no estado Aberto e o VR aguarda os resultados da verificação da Qualys. Nessa situação, os registros de VI do segundo scanner permanecem no estado Aberto mesmo se o patch for aplicado e o VI for confirmado como corrigido pelo outro scanner.

Para resolver essa situação, considere resolver o registro de vulnerabilidade duplicado com base na condição de que a vulnerabilidade seja fechada pelo primeiro scanner.

Resolva vulnerabilidades das seguintes maneiras:

- Sob demanda: selecione a ação de IU **Resolver IVs duplicados** na tarefa de correção.



- Automatizado: habilite a propriedade do sistema `sn_vul.auto_resolve_duplicate_vit` para resolver automaticamente itens vulneráveis duplicados. O trabalho diário programado "Atualizar e resolver VITs duplicados na tarefa de correção" atualiza automaticamente os itens duplicados.

Os IVs duplicados são então marcados como resolvidos.

Nota: O registro do item de vulnerabilidade resolvido será reaberto se o scanner o identificar como **Não corrigido**.

Criar e editar um grupo de classificação

Crie grupos para que as regras subjacentes deste grupo possam classificar os registros da tabela com base nas condições. As regras podem ser usadas para selecionar qualquer campo na tabela correspondente.

Antes de Iniciar

Função necessária: sn_vul.manage_classification_rule

Procedimento

1. Navegue até a tabela Propriedades do sistema.
2. Na propriedade do sistema *sn_sec_cmn.classificationTables*, adicione o nome da tabela para a qual você deseja criar o grupo de classificação.
3. Crie uma nova regra de negócio adicionando o seguinte snippet de código à regra de negócio na tabela definida no grupo:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
varclassificationCalc = new
sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','sn_vu
classCalc.calculate();
```

Nota: As regras de negócio são fornecidas para executar a classificação durante a ingestão das tabelas Itens descobertos e Entrada de vulnerabilidade. Para outras tabelas, para ter as regras de classificação na ingestão, você deve adicionar as regras de negócio.

4. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de classificação**.
5. No menu de contexto Grupos de classificação, clique em **Novo**.
6. No formulário, preencha os campos.

Formulário Grupo de classificação de vulnerabilidade

Campo	Descrição
Nome	Nome do novo grupo de classificação.
Ativo	Opção para ativar o grupo.
Descrição	Descrição do novo grupo de classificação.
Tabela	Tabela com base na qual as regras são executadas. **Nota:** O sistema de base da Resposta a vulnerabilidades inclui grupos de classificação para itens descobertos e vulnerabilidades.

Criar e editar uma regra de classificação

Crie regras para classificar automaticamente as vulnerabilidades de entrada para as equipes corretas para correção.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Por Que e Quando Desempenhar Esta Tarefa
Quando criadas, essas regras classificam as vulnerabilidades como pertencentes a uma plataforma ou a uma aplicação. Você pode configurar essas regras para substituir o valor de um campo específico na entrada de vulnerabilidade.
Use essas regras para mover o cálculo ascendente para a tabela Entrada de vulnerabilidades de terceiros para habilitar a reutilização de conteúdo.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de classificação**.
2. Para exibir um grupo de classificação, clique nesse grupo.
3. No menu de contexto Regras de classificação, clique em **Novo**.
4. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de classificação de vulnerabilidade

Campo	Descrição
Nome	Nome da nova regra de classificação.
Ativo	Opção para ativar a regra.
Descrição	Descrição da nova regra de classificação.
Ordem de execução	Ordem na qual a regra deve ser executada.
Exibição avançada	Opção para exibir campos adicionais nas seções com guias.
Quando esta condição for atendida	
Tipo de condição	Tipo de condição para a regra. Estas são as opções: ◦ **Filtro**: condições básicas de filtro para determinar se a regra deve ser usada ou não. ◦ Grupo de**filtros**: conjunto de várias condições que são usadas juntas. A regra é avaliada com base nas condições definidas no grupo de filtros. ◦ **Script**: condição de script usada para determinar quando esta regra deve ser aplicada. Este campo aparece somente quando a opção **Exibição avançada** está selecionada.
Condição	Condição para a regra. Defina condições com base na coluna selecionada na coluna de entrada de vulnerabilidade necessária. Você pode adicionar várias condições para refinar a regra. Este campo aparece somente quando **Filtro** é selecionado no campo **Tipo de condição**. **Nota:** Ao definir várias condições ou modelos, você pode selecionar somente a partir de uma tabela primária e secundária. Você não pode selecionar duas ou mais tabelas secundárias.
Grupo de filtros	Grupo de filtros. O grupo é definido quando um conjunto de condições é usado repetidamente em vários locais. Clique na pesquisa usando o ícone de lista (Ícone de) para selecionar o grupo de filtros. Para obter mais informações, consulte Criação e definição de grupos de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	filtros em Operações de segurança. Este campo aparece somente quando **Grupo de filtros** é selecionado no campo **Tipo de condição**.
Script	Script que é avaliado para determinar quando aplicar esta regra. Você pode escrever seu código e definir a resposta como verdadeira ou falsa. Este campo aparece somente quando **Script** é selecionado no campo **Tipo de condição**
Definir estes valores	
Classificação	Classificação da regra. Para selecionar uma opção, clique no ícone da ampola (ícone da). A lista exibe as opções para Plataforma e Aplicação. Como alternativa, você pode inserir sua própria classificação que não está na lista.
Tipo de classificação	Tipo de classificação. Este campo mostra a lista filtrada de tipos de classificação com base no valor selecionado para o campo **Classificação**.
Tipo de valor	Tipo do valor que é atribuído usando esta regra. Estas são as opções: ◦ **Modelo**: selecionar um modelo. Você pode usar um modelo necessário. ◦ **Script**: selecione um script pré-existente ou grave seu próprio script personalizado. Este campo aparece somente quando a opção **Exibição avançada** está selecionada.
Modelo	Outra condição para a regra além dos campos **Classificação** e **Tipo** de classificação. Selecione uma combinação de campos e valores que você deseja definir quando a regra for avaliada. Este campo aparece somente quando o **modelo** é selecionado no campo **Tipo de valor**.
Valor do script	Script para definir valores no registro atual. Este campo define quais valores definir nos campos nas entradas de vulnerabilidade. Este campo aparece somente quando **Script** é selecionado no campo **Tipo de valor**.

5. Para criar a nova regra, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Use regras de classificação de VR para adicionar a lógica a tabelas ascendentes, como Vulnerabilidade e Itens descobertos, e calculá-la. Você pode reutilizar a saída várias vezes, melhorando assim o desempenho de regras, como regras de atribuição. Por exemplo, classifique a entrada de terceiros (TPE) como Java e reutilize a saída nas regras de atribuição várias vezes. Exemplo de regra de atribuição:

```
VI.TPE.Classfication Type
          | IS | Java
```

Aplicar uma regra a uma vulnerabilidade existente

Ao alterar uma regra de classificação, execute novamente todas as regras ativas em todas as entradas de vulnerabilidade. Você também pode adaptar as vulnerabilidades existentes, aplicando as regras de classificação recém-criadas às vulnerabilidades existentes.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Regras de classificação de vulnerabilidade**.
2. Para selecionar uma regra, marque a caixa de seleção ao lado da regra.
3. Clique em **Aplicar mudanças**.
4. Clique **em Reaplicar**.

Desativar ou excluir uma regra de classificação

Desative ou exclua uma regra de classificação se ela não for mais necessária ou relevante.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Por Que e Quando Desempenhar Esta Tarefa
Quando uma regra de classificação é desativada ou excluída, os dados que foram preenchidos nos campos **Classification** e **Classification_type** por essa regra excluída permanecem em suas respectivas tabelas.

Se você quiser limpar esses dados, crie uma regra com valores vazios nos campos **Classification** e **Classification_type** e reaplique o grupo. Depois que a nova regra for reaplicada, as mudanças serão refletidas em todos os registros aos quais a regra é aplicável, com base nas condições da regra.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Regras de classificação de vulnerabilidade**.
2. Para selecionar a regra que você deseja excluir, clique na caixa de seleção ao lado da regra.
3. Para excluir a regra, siga um destes procedimentos:
   - Na lista Ação em linhas selecionadas, clique em **Excluir**.
   - Selecione a regra e clique no botão **Excluir**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Aplicar mudanças**.

> **Nota:** Se você não clicar neste botão, a regra continuará a residir no sistema. As vulnerabilidades referenciadas pela regra continuam a fazer referência a elas.

Criar uma regra de exclusão

Crie uma regra para filtrar ou impedir que as detecções sejam convertidas em itens vulneráveis (VITs) durante a ingestão.

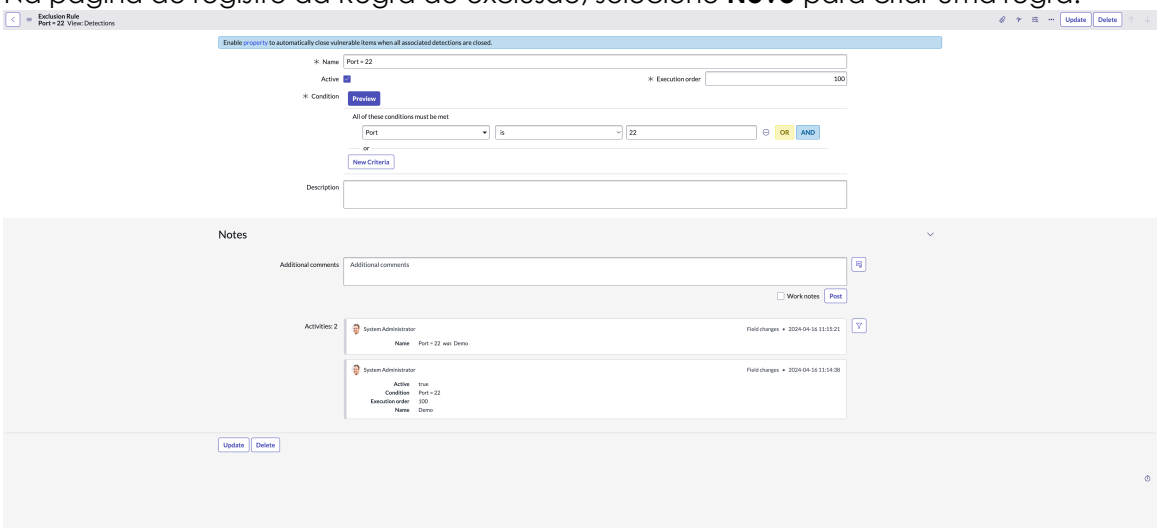
Antes de Iniciar

Função necessária: administrador de vulnerabilidade

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Regras de exclusão**.
2. Na página de registro da Regra de exclusão, selecione **Novo** para criar uma regra.



Uma mensagem dizendo "Habilitar propriedade para fechar automaticamente itens vulneráveis quando todas as detecções associadas forem fechadas" é exibida. Por padrão, a propriedade está inativa. Para habilitar, selecione o link da propriedade e insira o valor como Verdadeiro no campo **Valor**.

3. No formulário, preencha os campos.

Formulário Regra de exclusão

Campo	Descrição
Nome	Nome da regra de exclusão.
Ativo	Opção para ativar a regra de exclusão.
Ordem de execução	Ordem exclusiva para cada regra de exclusão.
Condição	Condições de filtro para as detecções que podem ser definidas durante o processamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Você não pode selecionar Regra de exclusão ou Condições do campo de item de vulnerabilidade.
Descrição	Descrição da regra de exclusão.

4. Selecione **Enviar**.
   A atividade é registrada no sistema.

Nota: Depois que uma regra de exclusão é criada, ela entra em vigor nas detecções a partir da ingestão subsequente.

Gestão de mudanças tarefas para Resposta a vulnerabilidades

A partir de tarefas de correção (RTs), crie solicitações de mudança, associe RTs a solicitações de mudança existentes ou divida tarefas de correção em novas tarefas com subconjuntos de itens vulneráveis (VI).

Crie e gerencie solicitações de mudança diretamente de uma tarefa de correção se um processo manual e controlado de qualquer tipo for necessário para modificação ou remoção de itens de configuração (ICs) compatíveis no seu CMDB. Criar e gerenciar solicitações de mudança diretamente de um registro ajudam a investigar e resolver vulnerabilidades rapidamente.

Consulte Gestão de mudanças para Resposta a vulnerabilidades para obter uma visão geral de como a gestão de mudanças funciona com a aplicação Resposta a vulnerabilidades e os requisitos do sistema.

Consulte os tópicos a seguir para saber como criar solicitações de mudança, associar tarefas de correção a solicitações de mudança existentes e dividir tarefas de correção. Consulte Sincronização de estado entre solicitações de mudança e tarefas de correção para obter informações sobre como os campos de estado nas solicitações de mudança (CHG) resolvem automaticamente as tarefas de correção.

Criar uma solicitação de mudança a partir de uma tarefa de correção

Como responsável pela correção de TI, crie uma solicitação de mudança (CHG) diretamente de uma tarefa de correção (VUL) para todos os itens vulneráveis do grupo. Crie uma solicitação de mudança com informações pré-preenchidas que incluem a solução preferencial para agilizar sua investigação de vulnerabilidades que exigem intervenção manual.

Antes de Iniciar

Funções necessárias: para criar uma solicitação de mudança: qualquer usuário com a função itil. A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a um usuário.

Função necessária: para aprovação de solicitações de mudança: usuários com funções itil, admin, sn_change_write, change_manager.

Por Que e Quando Desempenhar Esta Tarefa

Para obter informações sobre como criar uma solicitação de mudança nos espaços Resposta a vulnerabilidades, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

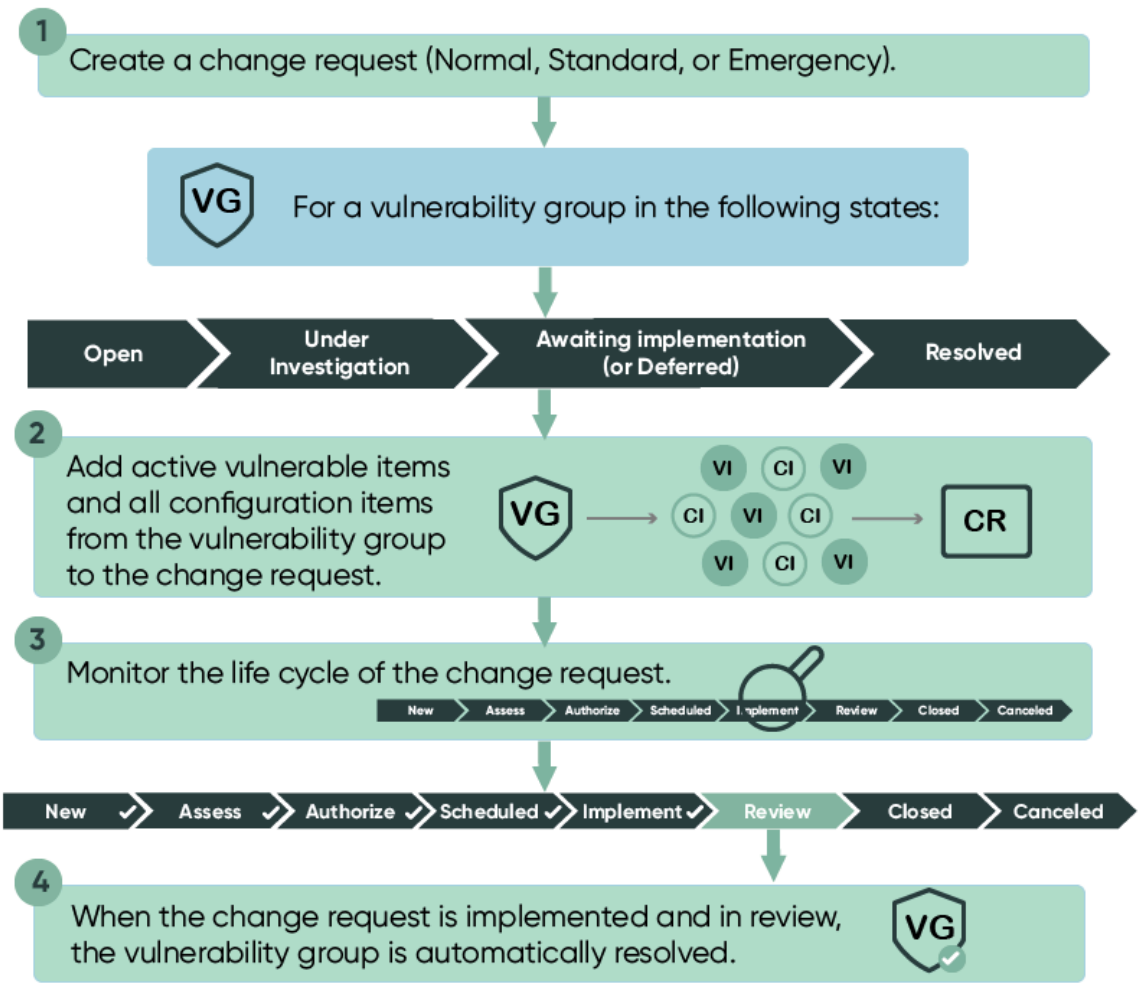
Para criar uma solicitação de mudança a partir do ambiente clássico, siga as etapas listadas abaixo.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente de uma tarefa de correção. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente de uma tarefa de correção:

- Padrão. Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento ou instrução de trabalho especificado.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de serem implementadas, revisadas e encerradas.
- Emergência. Uma mudança para resolver um incidente grave.

A imagem a seguir ilustra o fluxo básico para criar uma solicitação de mudança a partir de uma VUL (tarefa de correção). As etapas detalhadas para este fluxo seguem a imagem.

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Nas versões anteriores do Resposta a vulnerabilidades, as tarefas de correção eram chamadas de grupos de vulnerabilidades (VGs). Nas imagens a seguir, VG= tarefa de correção ou um registro VUL.



Nota: Pontos principais sobre como criar novas solicitações de mudança:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode criar novas solicitações de mudança para qualquer tarefa de correção (VUL) em um estado diferente de `Encerrado`.
- Verifique se você tem um aprovador para solicitações de mudança diferente do padrão (pré-aprovado) que você cria ou associa a uma VUL. Isso agiliza a movimentação da VUL para a resolução. Para obter mais informações sobre como adicionar usuários, consulte Adicionar usuários ao grupo da Resposta a vulnerabilidades.
- Antes que uma tarefa de correção possa ser resolvida, todas as tarefas em pelo menos um CHG associado ao VUL devem ser concluídas para que a solicitação de mudança possa ser implementada e movida para o estado `Revisão`.

Procedimento

1. Para criar uma solicitação de mudança completa a partir de um registro de tarefa de correção existente, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuído aos Meus grupos**.
   A lista de tarefas de correção atribuídas ao seu grupo de atribuição é exibida.
2. Opcional: Navegar até **Todos** > **Resposta a vulnerabilidades** > **Visão Geral da Correção** para exibir o painel Visão geral de correção e localizar uma VUL atribuída a você ou ao seu grupo de atribuição.
3. Como alternativa, na coluna Número, clique em uma tarefa de correção para abrir o registro e exibir os detalhes.
   O registro é exibido.
4. Com o registro VUL exibido para o qual você deseja criar a solicitação de mudança, no canto superior direito do registro, clique em **Criar mudança**.
   O formulário Criar solicitação de mudança é exibido.
5. Preencha os campos.

   a. Na lista de seleção do campo Aplica-se a, escolha uma para continuar.

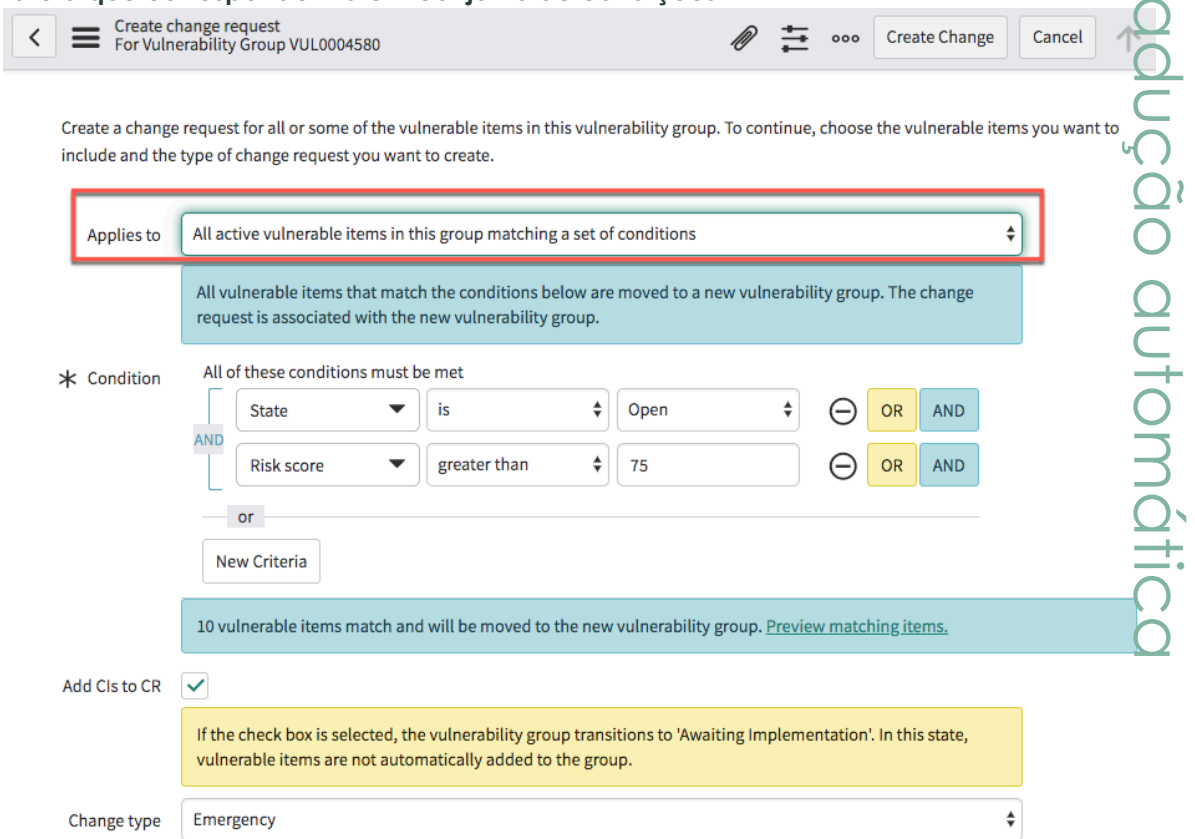
Opção	Descrição
Todos os itens vulneráveis ativos neste grupo	Se selecionado, todos os itens vulneráveis ativos desta tarefa de correção com um estado diferente de Encerrado serão adicionados automaticamente à solicitação de mudança depois que você clicar em **Criar mudança**.
Todos os itens vulneráveis neste grupo que correspondem a um conjunto de condições	Se selecionado, o Construtor de condições será exibido conforme mostrado na segunda figura abaixo. Insira critérios de filtro para identificar os itens vulneráveis que você deseja para a nova solicitação de mudança. Um exemplo de filtro pode incluir somente itens vulneráveis que correspondam a critérios de pesquisa específicos: **O estado é Em aberto** e a **pontuação de risco** é **maior que 75**. Depois de inserir suas condições, uma mensagem será exibida com o número de IVs que correspondem aos seus critéri-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	os (10). Um link (**Visualizar itens correspondentes**) para visualizar os itens correspondentes é exibido. Se nenhum item corresponder às condições do filtro, uma mensagem será exibida abaixo do Construtor de condições instruindo você a ajustar o filtro. Depois de clicar em **Criar mudança**, todos os itens vulneráveis que correspondem a este filtro de condição são movidos para uma nova tarefa de correção. Esta solicitação de mudança está associada à nova tarefa de correção.

Criar formulário de solicitação de mudança para itens vulneráveis em uma tarefa que correspondem a um conjunto de condições



b. Opcional: Se exibido no formulário, clique no link **Visualizar itens correspondentes** para obter uma lista dos IVs que correspondem aos seus critérios de filtro.
A visualização da Lista de tarefas de correção é exibida. Você pode selecionar itens nesta lista de visualização e executar ações de IU neles. No entanto, essas ações também são executadas no VUL. Por exemplo, se você excluir um VI da lista de visualização, esse VI também será excluído do VUL.

c. Depois de concluir a visualização, feche a janela do navegador para retornar o formulário de solicitação de mudança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Para a caixa de seleção Adicionar ICs ao CR, escolha um para continuar.

Opção	Descrição
Caixa de seleção Adicionar ICs ao CR marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (IC) que pertencem aos itens vulneráveis ativos nesta tarefa de correção serão adicionados a esta solicitação de mudança. A VUL passa automaticamente para o estado `Aguardando implementação`.
Caixa de seleção Adicionar ICs ao CR desmarcada	Desmarque a caixa de seleção se não quiser que os ICs dos itens vulneráveis ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. Quando desabilitado, o estado da solicitação de mudança não é sincronizado com o VUL e o VUL permanece em seu estado atual.

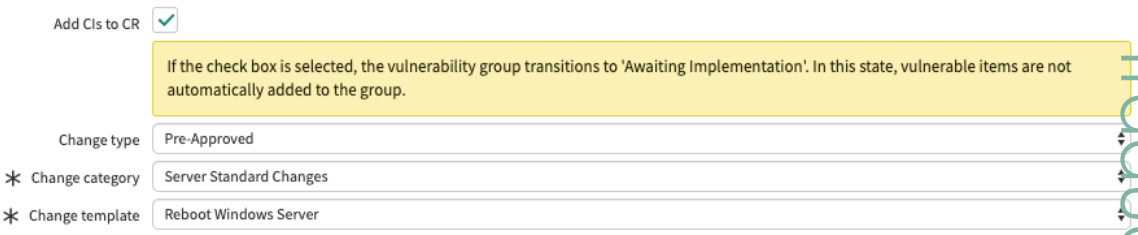
e. Na lista de seleção do campo Tipo de mudança, escolha um para continuar.

Tipo de mudança	Descrição
Emergência	Uma mudança para resolver um incidente grave.
Normal	Um tipo de mudança que é usado para implementar qualquer mudança em um serviço que não seja uma mudança padrão ou de emergência.
Padrão	Uma solicitação de mudança pré-autorizada de baixo risco que é implementada com frequência. As solicitações de mudança padrão aprovadas podem ser predefinidas em um catálogo de modelos para tornar mais eficiente o acesso e a solicitação de uma mudança padrão. Se selecionado, dois campos serão exibidos, conforme mostrado na figura a seguir. Selecione um de cada lista de seleção para preencher estes campos: ▪ Categoria de mudança: selecione uma categoria para a mudança no catálogo existente, por exemplo, `Hardware`, `Mudanças padrão do servidor`, `Software`. Neste exemplo, `Patching Standard Changes` está selecionado. ▪ Modelo de mudança: selecione um modelo disponível para solicitações de mudança com tarefas de suporte predefi-

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de mudança	Descrição
	nidas do seu catálogo. Neste exemplo, o modelo `Ciclo de patch mensal da Microsoft` está selecionado. Para obter mais informações sobre categorias, modelos e tipos de mudança de solicitação de mudança do ITSM, consulte Tipos de mudança .

O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Gestão de mudanças. Por exemplo, se você alterar o nome das solicitações de mudança padrão no ITSM de `Padrão` para `Pré-aprovado`, o novo nome será exibido automaticamente na lista de seleção Tipo de mudança em Criar solicitação de mudança de, conforme mostrado na figura a seguir.



Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações da VUL. Se necessário, esses valores de campo podem ser editados. Por exemplo, revise os valores nos campos na figura a seguir:

Data de término planejada

Esta data (`2019-10-10`) é o mesmo valor exibido no campo Data de meta de correção do VUL. Este valor é derivado da data da meta de correção mais antiga dos itens vulneráveis que pertencem ao VUL. Se você estiver criando uma solicitação de mudança para um problema crítico que requer uma data de correção anterior, talvez prefira editar este valor e o valor no campo Prioridade.

Justificativa

Este campo exibe o número de ICs adicionados ao CHG. Se você quiser adicionar informações adicionais, talvez prefira editar este texto. Por exemplo, você pode preferir adicionar uma anotação neste campo sobre o filtro usado para criar a nova VUL, por exemplo, `Pontuação de risco maior que 75`. Este texto pode ajudá-lo a localizar sua nova solicitação de mudança e grupo de vulnerabilidades.

Plano de implementação

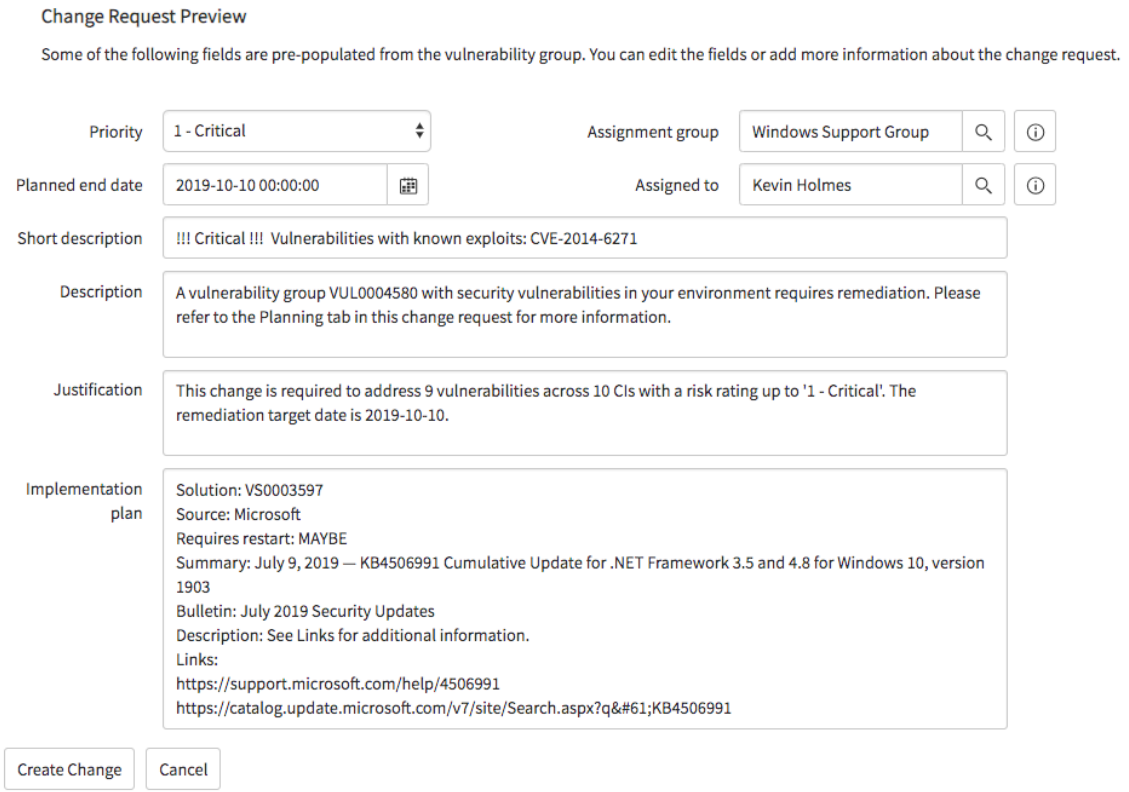
Este campo exibe a solução preferencial para a vulnerabilidade.

Grupo de atribuição e Atribuído a

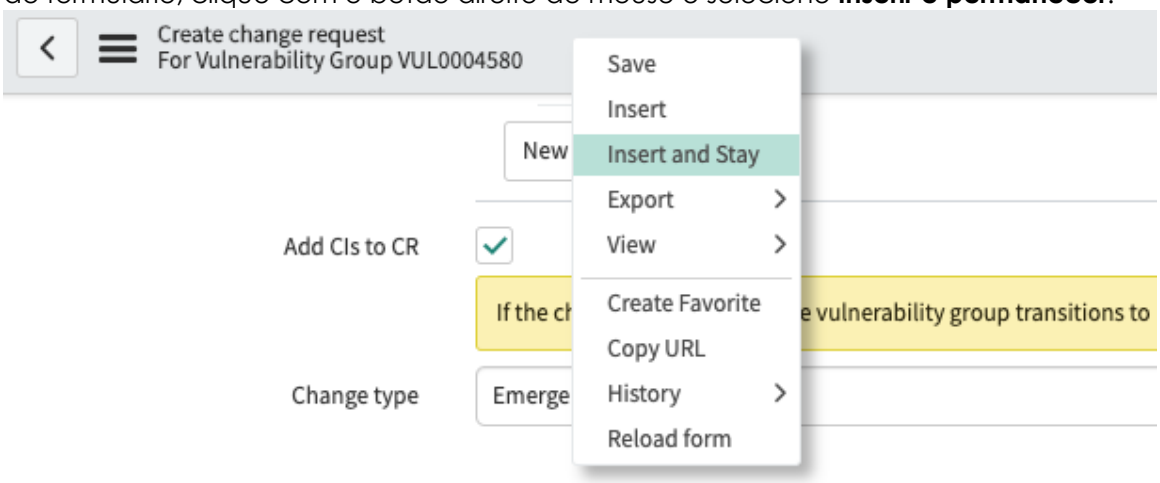
Edite esses campos para mudar o grupo de atribuição ou reatribua esta solicitação de mudança a um usuário em um de seus grupos de atribuição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Continue a visualizar e editar os campos conforme necessário.
7. Para salvar suas mudanças e permanecer nesta página, na faixa cinza na parte superior do formulário, clique com o botão direito do mouse e selecione **Inserir e permanecer**.



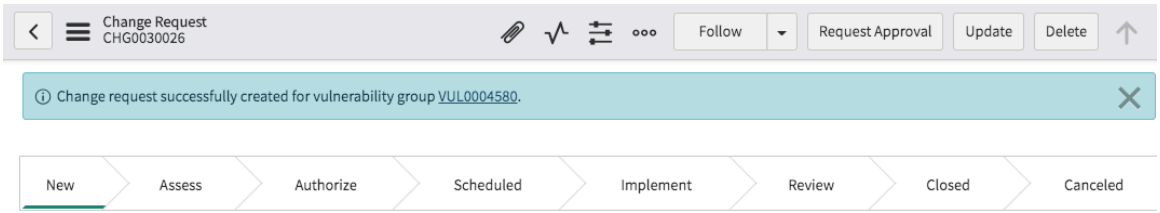
8. Depois de concluir as edições, escolha uma para continuar.

Opção	Descrição
Criar Mudança	Sua solicitação de mudança é criada e a nova solicitação de mudança é exibida no estado `Novo`. Na parte superior, são exibidas mensagens que indicam que a solicitação de mudança foi criada com sucesso com o número de itens vulneráveis que fo-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ram adicionados, conforme mostrado na figura a seguir. Se a sincronização de estado estiver habilitada e a VUL ainda não estiver em `Sob investigação`, a VUL será movida automaticamente para `Sob investigação` e uma anotação de trabalho será publicada.
Cancelar	A solicitação de mudança não é criada e o VUL é exibido.



Nota:

Para uma tarefa de correção no estado `Aberto` com os campos Grupo de atribuição e Atribuído a não atribuídos (vazios), o usuário conectado no momento é atribuído automaticamente à tarefa depois que você clica em **Criar mudança**. Além disso, a caixa de seleção Adicionar ICs ao CR deve estar marcada. Na parte superior da VUL, uma mensagem de confirmação azul é exibida indicando esta atribuição.

O que Fazer Depois

Monitore a solicitação de mudança e as tarefas de mudança para verificar se elas foram concluídas e se a solicitação de mudança foi implementada. Depois que este CHG for implementado e movido para o estado `Revisão`, se a sincronização de estado estiver habilitada, a VUL será movida automaticamente para `Resolvido`. Para obter mais informações sobre sincronização de estado, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Associar uma tarefa de correção a uma solicitação de mudança existente

Como proprietário de correção de TI, evite criar solicitações de mudança duplicadas (CHG) enquanto trabalha para resolver suas tarefas de correção associando uma tarefa de correção (VUL) a uma solicitação de mudança que já está disponível em sua instância.

Antes de Iniciar

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: qualquer usuário com a função itil. A função sn_vul.remediation_owner também é atribuída automaticamente a um usuário quando a função itil é atribuída.

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre como associar uma tarefa de correção a uma solicitação de mudança existente, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

Tradução automática

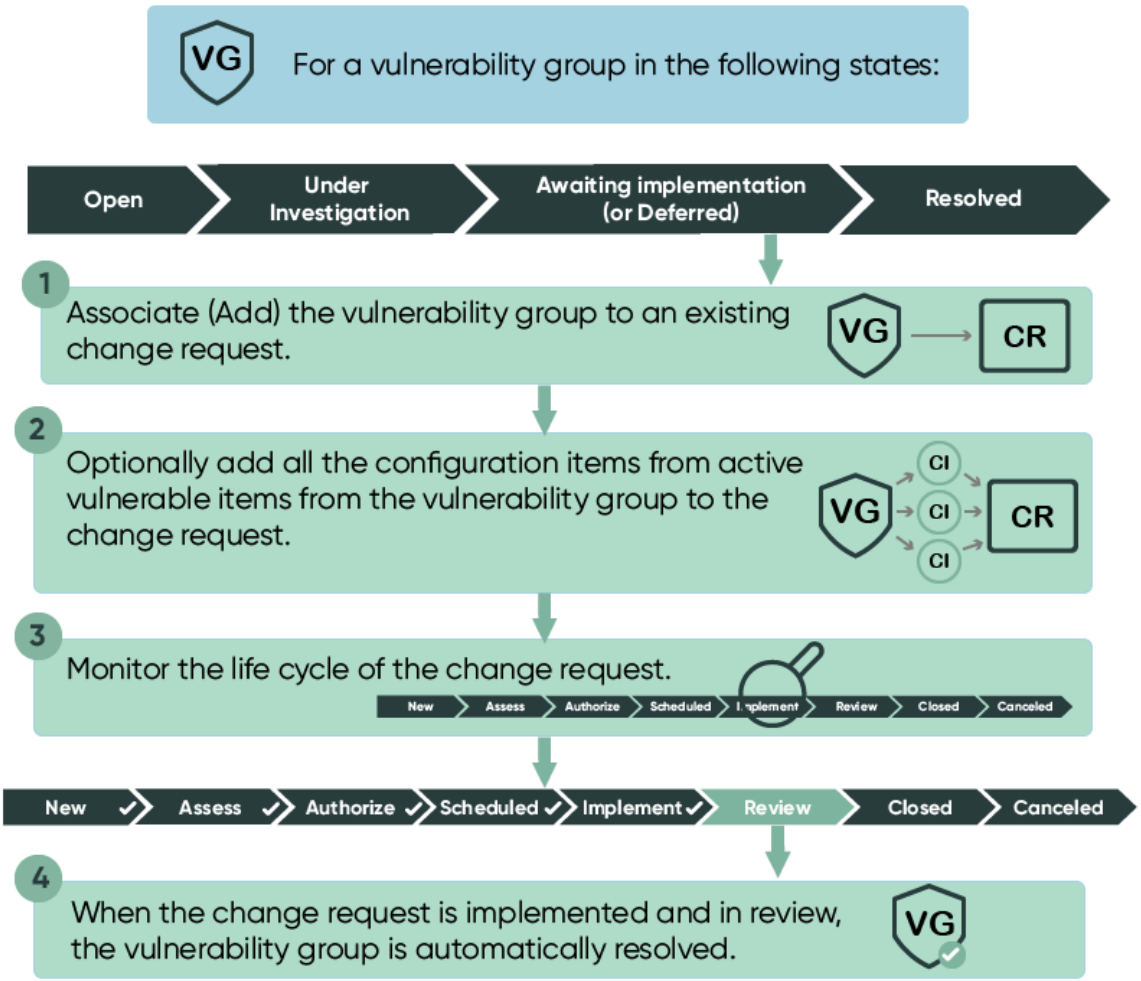
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Nas versões anteriores do Resposta a vulnerabilidades, as tarefas de correção eram chamadas de grupos de vulnerabilidades (VG). Nas imagens a seguir, VG= tarefa de correção ou um registro VUL.

Para obter mais informações sobre como associar uma tarefa de correção a uma solicitação de mudança existente, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

Como proprietário de correção, você pode associar tarefas de correção atribuídas a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros da tarefa de correção. A imagem a seguir ilustra o fluxo básico para associar uma solicitação de mudança a um VUL (VG) existente. As etapas detalhadas para este fluxo seguem a imagem.

Fluxo de trabalho para associar uma tarefa de correção a uma solicitação de mudança existente



Nota: Você pode associar uma solicitação de mudança existente a uma VUL em qualquer estado (Aberto, Sob investigação, Aguardando implementação, Encerrado e Adiado). Quando você associa uma solicitação de mudança a uma VUL existente, somente os IVs ativos são adicionados à solicitação de mudança.

Antes de começar, para evitar a criação de solicitações de mudança duplicadas, talvez você prefira exibir todas as solicitações de mudança existentes já associadas a uma VUL. Para rastrear facilmente o número de solicitações de mudança relacionadas a uma VUL específica, consulte a coluna de contagem de CR na lista Tarefas de correção. Se não for

Tradução automática

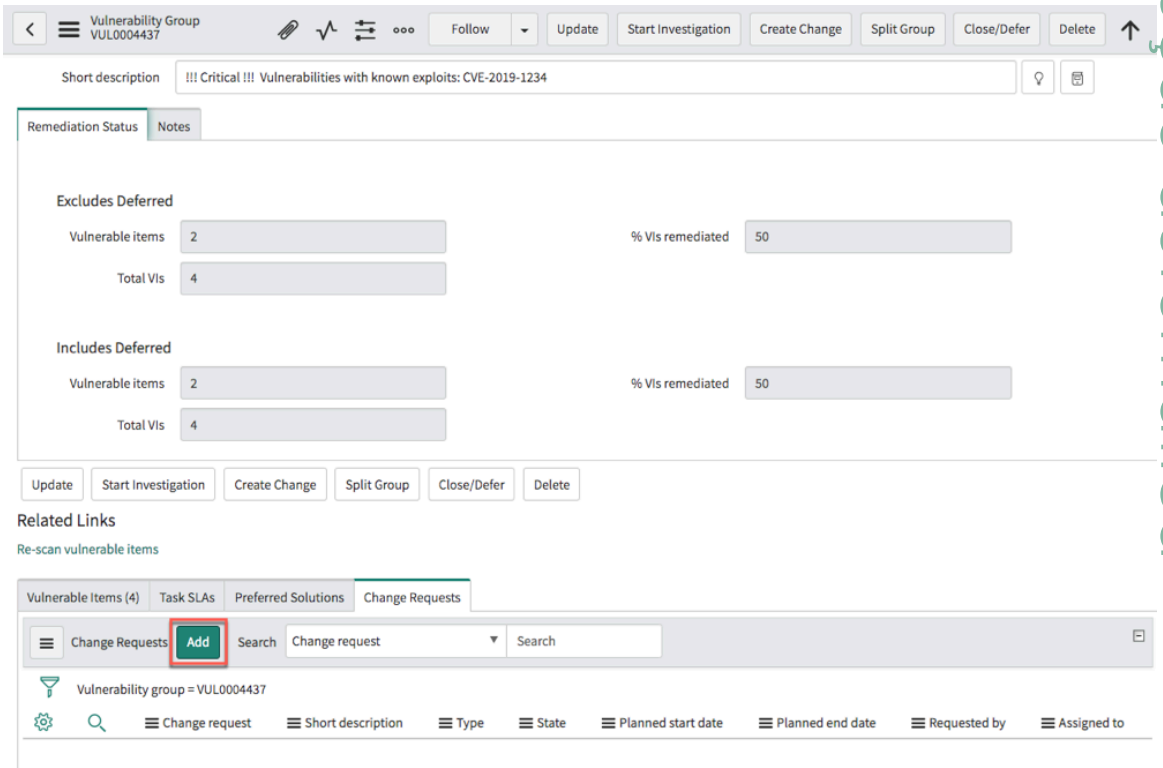
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

exibido, clique no ícone de configurações (ícone de) no canto superior direito. Mova a coluna de contagem de CR de Disponível para Selecionada e clique em **OK**.

Para preencher automaticamente a nova coluna, para clientes com dados existentes nesta tabela, execute o trabalho agendado: `Preencher nova coluna de contagem de CR`.

Procedimento

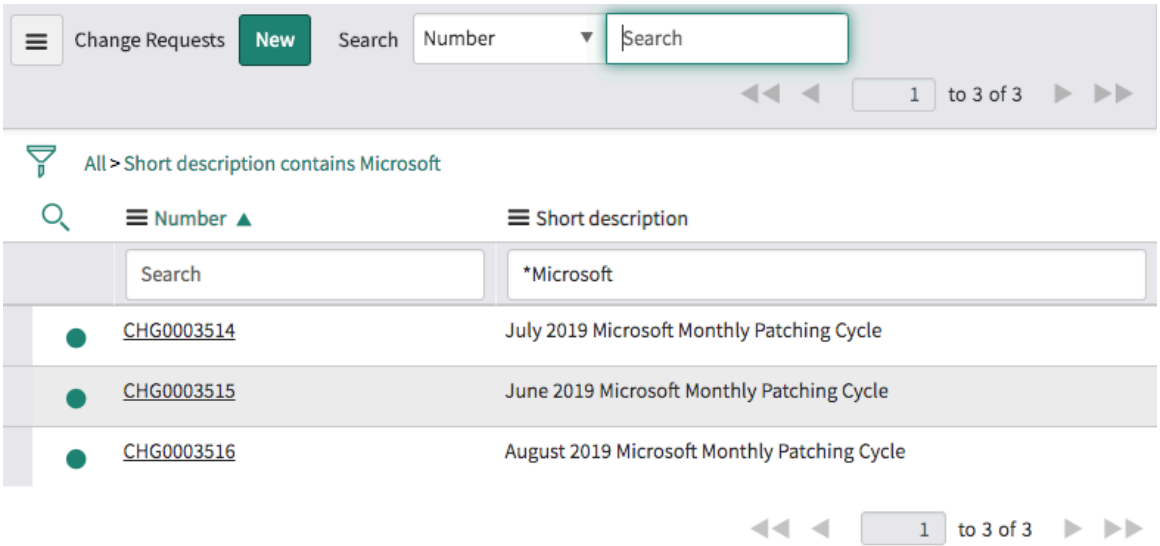
1. Para associar uma tarefa de correção a uma solicitação de mudança existente, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Localize a tarefa de correção com a qual você está trabalhando.
3. Opcional: Navegar até **Todos** > **Resposta a vulnerabilidades** > **Visão Geral da Correção** para exibir o painel Visão geral de correção e localizar uma VUL atribuída a você ou ao seu grupo de atribuição.
4. Na coluna Número, clique em um registro VUL para abri-lo.
   O registro VUL é exibido.
5. Com o registro aberto exibido, se ainda não estiver exibido, role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas à VUL são exibidas junto com o botão **Adicionar**. Na figura a seguir, não há solicitações de mudança já associadas a esta VUL.



6. Para associar a VUL a um CHG existente, clique em **Adicionar**.
   O formulário Adicionar solicitação de mudança existente à tarefa de correção é exibido.
7. No formulário, clique no ícone de pesquisa.
   Uma exibição de lista de solicitações de mudança existentes é exibida em uma nova janela, conforme mostrado na figura a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Selecione um item na lista exibida ou, como alternativa, clique no filtro ( ) e insira condições para limitar os resultados da pesquisa.
9. Para a caixa de seleção Adicionar ICs ao CR, escolha um para continuar.

Nota: Esta caixa de seleção é exibida somente para solicitações de mudança existentes no estado `Novo`.

Opção	Descrição
Caixa de seleção Adicionar ICs ao CR marcada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (IC) que pertencem aos itens vulneráveis ativos nesta tarefa de correção serão adicionados a esta solicitação de mudança. Quando selecionado, o estado da solicitação de mudança é sincronizado com o VUL. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.
Caixa de seleção Adicionar ICs ao CR desmarcada	Desmarque a caixa de seleção se não quiser que os ICs dos itens vulneráveis ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. Quando desabilitado, o estado da solicitação de mudança não é sincronizado com o VUL e o VUL permanece em seu estado atual.

10. Com o número da solicitação de mudança que você deseja exibir no campo Pesquisar solicitação de mudança, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A VUL é exibida. Na parte superior do registro, a mensagem de confirmação azul é exibida indicando que a solicitação de mudança selecionada foi associada com sucesso à VUL.

Nota: Para uma VUL no estado `Aberto` com os campos Grupo de atribuição e Atribuído a não atribuídos (vazios), o usuário conectado no momento é atribuído automaticamente à VUL depois que você clica em **Adicionar**. Além disso, a caixa de seleção Adicionar ICs ao CR deve estar marcada. Na parte superior da VUL, uma mensagem de confirmação azul é exibida indicando que o usuário atual está atribuído.

O que Fazer Depois

Revise o registro VUL. Na coluna Solicitação de mudança na lista relacionada Solicitações de mudança, clique no link do novo CHG para exibir o registro de CR. No registro CHG aberto, você pode monitorar o estado da solicitação de mudança. Os itens de configuração (IC) afetados e as tarefas de correção são exibidos nas listas relacionadas a ICs afetados e tarefas de correção.

Dividir uma tarefa de correção

Como proprietário de correção de TI, a partir de uma tarefa de correção existente (VUL), identifique um subconjunto de itens vulneráveis (VI) que você deseja mover para um novo grupo.

Antes de Iniciar

Nota:

Os casos de uso para dividir IVs de VULs existentes em novas tarefas de correção podem incluir os seguintes exemplos:

- Quando você deseja criar uma solicitação de mudança ou solicitações de mudança para uma tarefa dividida.
- Quando você reatribui um grupo dividido a outro usuário em seu grupo de atribuição.
- Quando você solicita um adiamento ou uma exceção para uma tarefa de divisão, porque você sabe que algumas vulnerabilidades em itens de configuração (IC) específicos não podem ser corrigidas em um determinado intervalo de tempo.

Função necessária: qualquer usuário com a função itil para dividir uma VUL.

Nota: A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a um usuário.

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre como dividir tarefas de correção nos espaços Resposta a vulnerabilidades, consulte Dividir uma tarefa de correção no Espaço de correção de problemas de TI.

Para dividir uma tarefa de correção no ambiente clássico ou para versões do Resposta a vulnerabilidades.

Você pode dividir as tarefas de correção existentes com mais de um item vulnerável que esteja nos estados `Aberto`, Sob investigação ou Aguardando implementação. Ao criar uma nova VUL com itens vulneráveis que correspondem a critérios específicos, você pode trabalhar com um grupo específico de itens vulneráveis sem afetar a tarefa de correção original.

Tradução automática

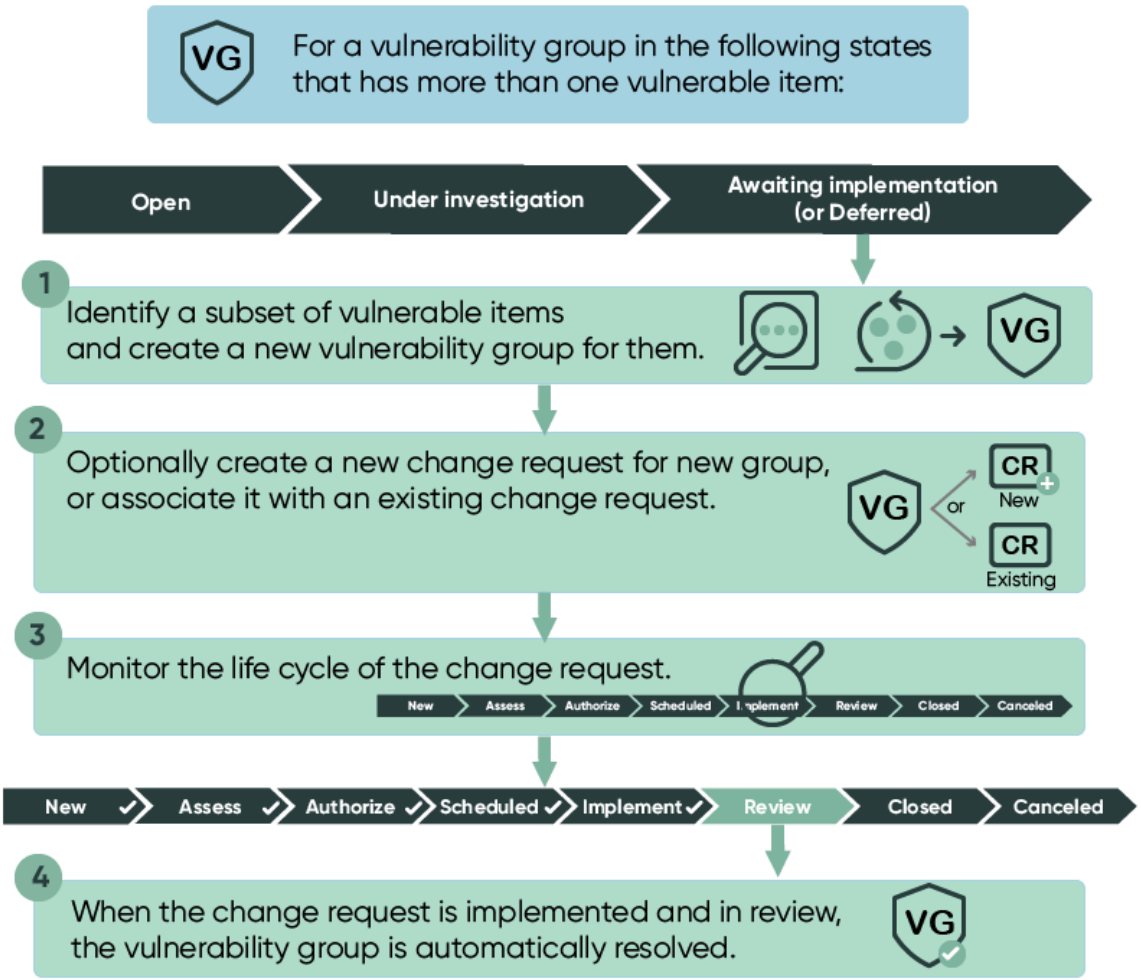
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando você especifica as condições dos itens vulneráveis que deseja mover para uma nova tarefa de correção com o Construtor de condições, somente os IVs ativos que correspondem aos seus critérios são movidos para o novo grupo.

Você não é obrigado a criar solicitações de mudança (CHG) ao dividir uma VUL. Você tem a opção de dividir uma VUL ao mesmo tempo em que cria uma solicitação de mudança ou pode dividir uma VUL sem criar uma solicitação de mudança. A imagem a seguir ilustra o fluxo básico para dividir um grupo de vulnerabilidades. As etapas detalhadas para este fluxo seguem a imagem.

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Nas versões anteriores do Resposta a vulnerabilidades, as tarefas de correção eram chamadas de grupos de vulnerabilidades (VG). Nas imagens a seguir, VG= tarefa de correção ou um registro VUL.

Fluxo de trabalho para dividir uma tarefa de correção

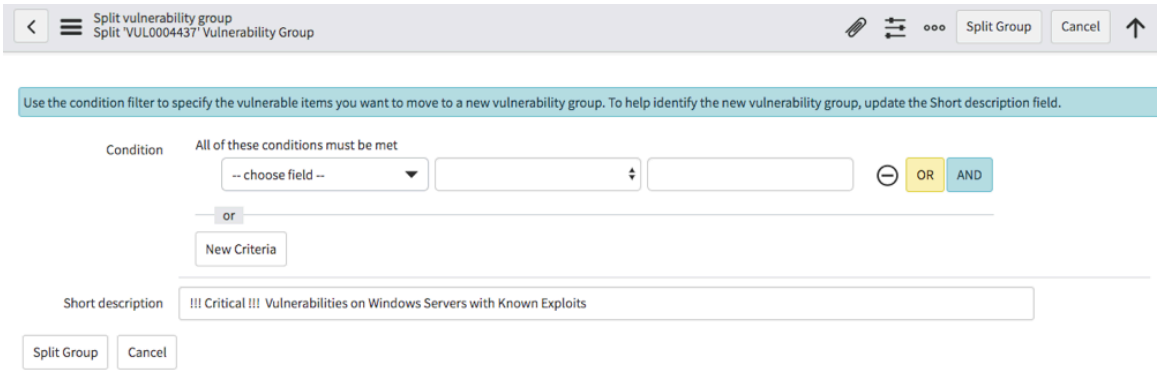


Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Atribuído aos Meus grupos**.
   A lista de tarefas de correção é exibida.
2. Na coluna Número, clique em um registro para abri-lo.
   O registro é exibido.
3. No canto superior direito da VUL, clique em **Dividir tarefa**.
   O formulário Dividir tarefa de correção é exibido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

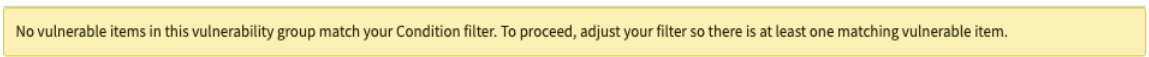


4. Com o filtro de condição exibido, especifique as condições dos itens vulneráveis que você deseja mover para uma nova tarefa.
   Por exemplo, talvez você prefira filtrar somente itens vulneráveis que correspondam às seguintes condições:
   - Em estados `Abertos`.
   - Pontuações de risco superiores a `80`.
   - Itens de configuração que contêm "`WINSV`".
   - Localizado em San Diego.

   Por exemplo, para condições, você pode inserir:
   - Estado - é - Aberto
   - Pontuação de risco - é maior que ou é - 80
   - Item de configuração . Nome - contém - WINSV
   - Item de configuração . Local - é - San Diego

   Se os itens vulneráveis corresponderem ao seu filtro depois de inserir as condições, será exibida uma mensagem com o número de itens vulneráveis correspondentes.

   Nota: Se for exibida uma mensagem informando que nenhum item vulnerável corresponde ao seu filtro, ajuste as condições para que pelo menos um item vulnerável corresponda aos seus critérios de filtro.

5. Opcional: Ajuste o filtro conforme necessário.
6. Opcional: Para ajudá-lo a identificar a nova VUL depois que ela for criada, talvez você prefira atualizar o campo Descrição resumida.
   Se editado, use o campo de descrição resumida como critério de pesquisa para a nova VUL para ajudá-lo a localizá-la depois que ela for criada, por exemplo,`LOCATED IN SAN DIEGO`.
7. Opcional: Para visualizar detalhes sobre os itens vulneráveis que correspondem aos seus critérios de filtro, siga estas etapas antes de clicar em **Dividir tarefa** para criar a nova VUL. Esses detalhes incluem solicitações de mudança existentes que já estão associadas a este subconjunto e VULs a esses itens vulneráveis. Exibir essas informações na visualização pode impedir a criação de VULs duplicadas.

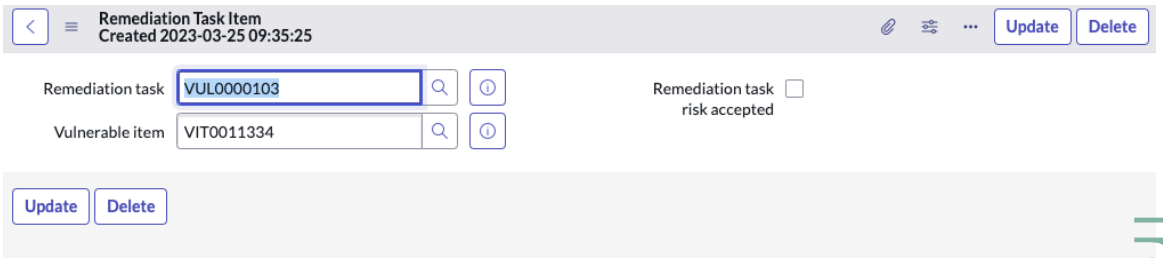
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na mensagem de confirmação azul do formulário Dividir tarefa de correção, clique em **Visualizar itens correspondentes**.
A lista de Itens da tarefa de correção é exibida em uma nova janela no navegador com uma lista de itens vulneráveis que correspondem às suas condições.

b. Na coluna Número, clique em um item para abrir o registro.

c. No registro exibido, à direita do grupo de vulnerabilidades ou dos campos de item de vulnerabilidade, clique no ícone de informações do item vulnerável para exibir os registros.



d. Na caixa de diálogo exibida, clique em **Abrir registro**.
As informações sobre a data da meta de correção são exibidas. Na seção Listas relacionadas, clique em uma lista relacionada para exibir mais informações sobre o VI.

8. Quando você estiver pronto para criar a nova VUL com os VIs que atendem às suas condições, feche a janela de visualização para retornar ao formulário de tarefa de divisão na outra janela e, na parte superior do formulário, clique em **Dividir tarefa**.

Nota:

Para menos de 200 IVs, a operação de divisão é feita de forma síncrona.

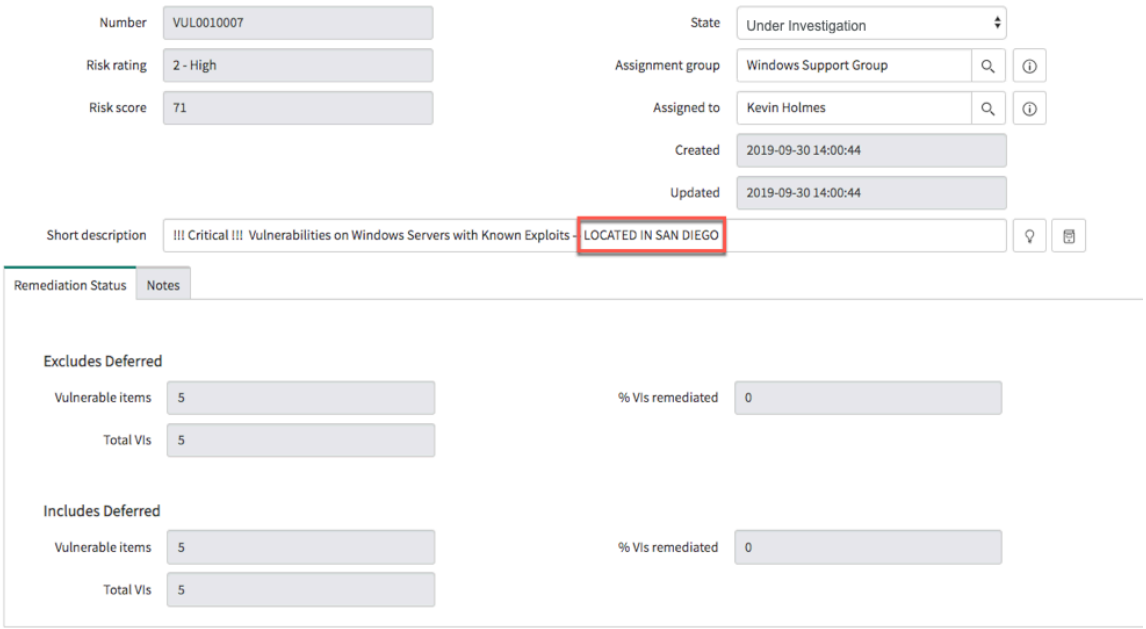
Para mais de 200 VIs, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os IVs apareçam no novo grupo.

Uma mensagem de confirmação é exibida mostrando todos os IVs ativos que foram movidos para o novo grupo. O novo número da tarefa de correção também é exibido. Se ainda não estiver em Sob investigação, a VUL será movida para Sob investigação. Verifique o campo Descrição resumida do texto que você inseriu para a nova VUL em (`LOCATED IN SAN DIEGO`).

Os cálculos de acúmulo no novo grupo são realizados para calcular sua nova pontuação de risco, data de meta de correção e outros valores de campo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os itens vulneráveis, soluções preferenciais e solicitações de mudança são exibidos nas Listas relacionadas na parte inferior do registro. Processe e monitore esta nova tarefa como você faria com qualquer tarefa de correção.

9. Opcional: Role até a lista relacionada **Anotações** e clique para selecioná-la.
   Confirme se o número de itens vulneráveis da tarefa de correção original foi movido para o novo grupo no fluxo de atividades.
10. Opcional: Na nova VUL, para selecionar e dividir os IVs da lista relacionada Itens vulneráveis mais uma vez, role até a parte inferior do registro do grupo de vulnerabilidades e, com os VIs que você deseja mover selecionados na coluna Item vulnerável dos Itens vulneráveis relacionados lista, na lista de seleção Ações em linhas selecionadas, selecione **Dividir tarefa**.
    O formulário Dividir tarefa de correção é exibido.
11. Para dividir o grupo novamente e mover os itens selecionados para um novo grupo, clique em **Dividir tarefa**.
    Os IVs selecionados são movidos para outra tarefa de correção, a mensagem de confirmação é exibida e o novo grupo é exibido.
12. Escolha um para continuar sua investigação ou correção.

Opção	Descrição
Criar Incidente de segurança	Crie um incidente de segurança.
Criar Mudança	Crie uma solicitação de mudança para esta tarefa de correção.
Dividir tarefa	Se o novo grupo tiver mais de um VI, divida esta tarefa de correção novamente para criar outro subconjunto de itens vulneráveis.
Aguardando Implementação	Se exibido, mova a tarefa do estado Sob investigação para o estado Aguardando implementação.
Fechar ou Solicitar Exceção	Feche ou adie a tarefa de correção. Uma caixa de diálogo de confirmação é exibida com os seguintes campos obrigatórios:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	◦ Estado ◦ Motivo ◦ Informação adicional Preencha os campos para fechar ou adiar o grupo e clique em **Enviar**.
Excluir	Exclua esta tarefa de correção.
Estado	Mova o registro para outro estado exibido na lista de seleção e clique em **Atualizar** para salvar as mudanças no registro. **Nota:** Você pode mover manualmente a nova VUL pelos estados de seu ciclo de vida. No entanto, se a sincronização de estado estiver habilitada e o sistema registrar que uma solicitação de mudança associada ao VUL mudou seu estado, ou você adicionar um CHG ou removê-lo do VUL, a sincronização de estado poderá substituir sua intervenção manual. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.
Grupo de atribuição	Reatribua a VUL a um grupo de atribuição e clique em **Atualizar** para salvar suas mudanças no registro.
Atribuído a	Atribua a VUL a você ou a um usuário específico em outro grupo de atribuição e clique em **Atualizar** para salvar as mudanças no registro.

O que Fazer Depois

Monitore o estado da nova VUL para agilizar sua resolução.

Sincronização de estado entre solicitações de mudança e tarefas de correção

Há um relacionamento sincronizado entre os campos de estado das tarefas de correção (VULs) e os campos de estado das solicitações de mudança (CHG) no produto Resposta a vulnerabilidades. Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também move o estado de todas as tarefas de correção relacionadas automaticamente.

Visão geral

O registro da tarefa de correção é chamado de VUL nas seções a seguir. Nas versões anteriores do Resposta a vulnerabilidades, as tarefas de correção eram chamadas de grupos de vulnerabilidades (VG). Nas imagens a seguir, VG= tarefa de correção ou um registro VUL.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A sincronização de estado é habilitada por uma propriedade do sistema (sn_vul.cr_state_synch) por padrão em sua instância quando você baixa a aplicação Resposta a vulnerabilidades.

Quando a sincronização de estado está habilitada, o campo Estado CHG muda o campo Estado da tarefa de correção automaticamente nos seguintes casos:

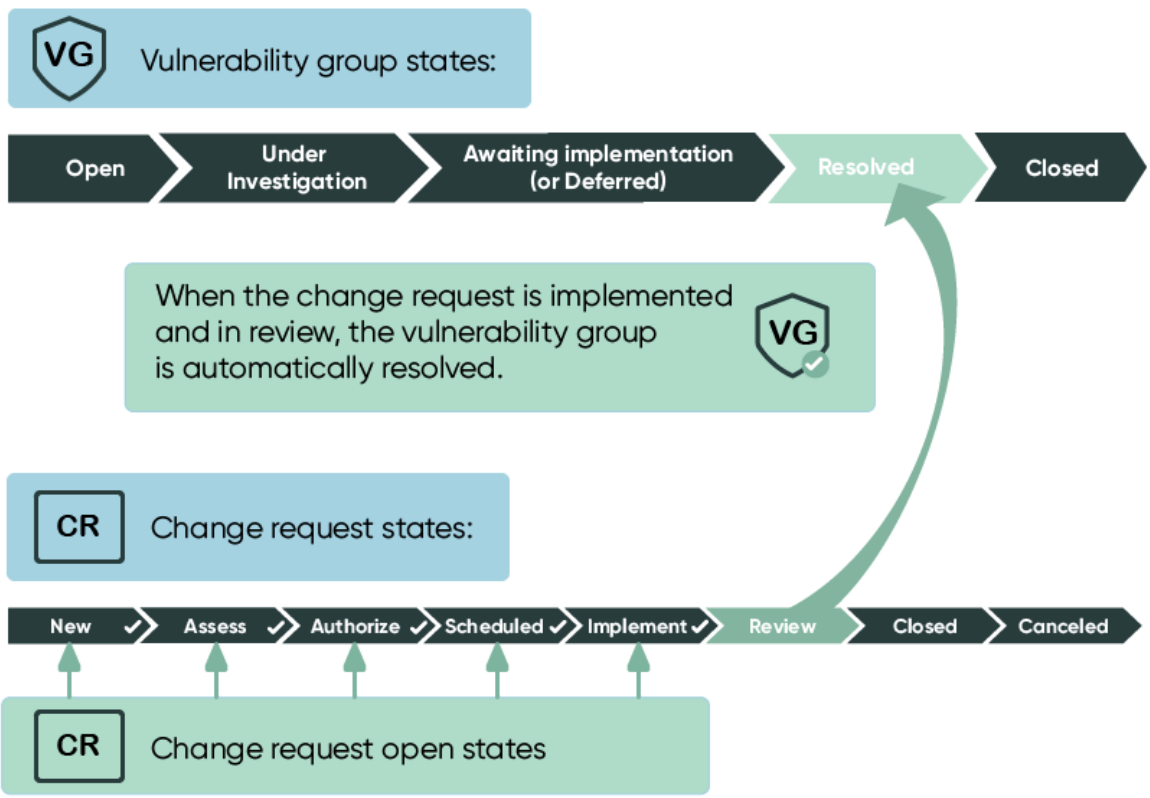
- Quando um novo CHG for criado para uma tarefa de correção (VUL), se não estiver em `Aguardando implementação`, o estado do VUL avançará para `Aguardando implementação`.
- Quando um CHG existente estiver associado a uma VUL, se não estiver em `Aguardando implementação`, o estado da VUL avançará para `Aguardando implementação`.
- Depois que as tarefas em um CHG são concluídas (`Implementado`) e o CHG é movido para o estado `Revisão`, a VUL avança para `Resolvido`.

Para obter mais informações e exemplos de sincronização de estado, consulte as seções a seguir.

Nota: Você ainda pode mover CHGs e VULs manualmente pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou de estado, você adiciona um CHG ou o remove de uma VUL, o estado A sincronização pode potencialmente substituir sua intervenção manual. No entanto, os estados das solicitações de mudança não movem automaticamente a VUL dos estados `Encerrado` ou `Adiado`.

Sincronização de estado de encaminhamento

A imagem a seguir ilustra como os estados CHG movem automaticamente os estados VUL em um ciclo de vida avançado, ou seja, de `Aberto` para `Resolvido`.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar novas solicitações de mudança para qualquer tarefa de correção em um estado diferente de `Encerrado`. A sincronização de estado move automaticamente a VUL bidirecionalmente pelos estados `Aberto`, `Sob investigação`, `Aguardando implementação`e `Resolvido`. Este movimento é baseado em determinados valores do campo de estado na solicitação de mudança. A sincronização de estado entre a solicitação de mudança e a tarefa de correção é invocada automaticamente, a menos que a caixa de seleção (`Adicionar ICs ao CR`) seja exibida em um formulário e você opte por desmarcar a caixa de seleção.

A VUL não avança para `Resolvido` quando um CHG está em seus estados abertos. Qualquer CHG em estados anteriores a `Revisão` em seu ciclo de vida, como `Novo`, `Avaliar`, `Autorizar`, `Programado` ou `Implementar`, conforme mostrado na figura anterior, são considerados estados abertos para o CHG. Estados abertos não movem o campo de estado no VUL, porque as investigações ou tarefas no CHG não foram concluídas. A sincronização de estado é invocada quando um CHG é criado para a VUL ou associado a ela ou o estado de um relacionamento existente muda no CHG. Os estados de CHG concluídos são `Revisão` e `Encerrado`com sucesso . Quando um CHG é encerrado com sucesso, seus códigos encerrados são: Bem- `sucedido`ou `Bem-sucedido com problemas`. Nesse caso, o VUL avança para `Resolvido`.

Sincronização de estado reverso

Como um CHG é processado durante seu ciclo de vida, ele pode ser cancelado em algum momento. Nesse caso, se o CHG for `Cancelado`ou `Encerrado` (com um código de encerramento `Malsucedido`), o VUL voltará automaticamente para `Sob investigação`. A VUL retorna para `Sob investigação`porque não há nenhum plano ativo para corrigir a vulnerabilidade.

Se uma VUL estiver em um estado `Resolvido` e você criar um novo CHG ou associá-lo a um CHG existente em um dos estados abertos iniciais, o VUL fará a transição automaticamente de volta para `Aguardando implementação`. A VUL retorna para este estado, pois agora há mais trabalho atribuído ao CHG.

VULs com mais de um CHG

Se uma VUL em `Aguardando Implementação` tiver mais de um CHG associado a ela, a sincronização de estado será baseada no status do CHG no estado mais antigo de seu ciclo de vida. Por exemplo, uma VUL tem quatro CHGs associados a ela, CHG1, CHG2, CHG3 e CHG4, conforme mostrado na tabela a seguir.

Número CHG	Estado CHG
1	Implementar
2	Cancelado
3	Encerrado (código de encerramento `malsucedido`)
4	Encerrado (código de encerramento bem- `sucedido`)

A sincronização de estado entre o CHG e a VUL, neste caso, é baseada no CHG1, que está no estado mais antigo dos quatro CHGs, (`Implementar`). Nesse caso, a VUL permanece em `Aguardando implementação`.

Em outro exemplo, se uma VUL estiver no estado `Resolvido` e tiver um CHG existente que foi implementado e estiver no estado `Revisão`, e um novo CHG for criado, o VUL voltará de `Resolvido` para `Aguardando Implementação`. A sincronização de estado é baseada no CHG no estado `Novo`, que é o CHG no estado mais antigo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número CHG	Estado CHG
1	Revisão
2	Novo

Além disso, quando as VULs têm mais de um CHG, o estado da VUL muda automaticamente nos seguintes casos:

- Quando um CHG avança para `Revisão`, se todos os outros CHGs associados ao VUL estiverem nos estados `Revisão` ou `Encerrado` (com um código de encerramento bem-sucedido), o VUL fará a transição automaticamente para `Resolvido`. Todos os outros CHGs relacionados que são cancelados ou encerrados sem sucesso são ignorados.
- Quando um CHG passa para `Cancelado` ou`Encerrado` (código de fechamento de `Malsucedido`), se todos os outros CHGs associados ao VUL estiverem no mesmo estado, o VUL fará a transição automaticamente de volta para `Sob investigação` .

Para obter mais informações sobre os estados da tarefa de correção e o que você pode fazer em cada estado, consulte Resposta a vulnerabilidades tarefa de correção e estados de itens vulneráveis.

Avalie sua exposição a software vulnerável

Você pode fornecer as informações do fornecedor e do produto no módulo Avaliação de exposição para avaliar a exposição de dia zero (dia atual) de seus ativos a software vulnerável usando a aplicação Gestão de ativos de software do ITSM (SAM) Foundation.

Importante: Você pode executar a avaliação de exposição por software e vulnerabilidades e exposições comuns (CVE) para aproveitar os recursos adicionais no espaço de avaliação de vulnerabilidade. Para obter mais informações, consulte Explorar o espaço de avaliação de vulnerabilidade.

Antes de Iniciar

Função necessária: administrador de vulnerabilidades (sn_vulnerability_write)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tenha as seguintes informações disponíveis sobre o software vulnerável que você deseja avaliar:

- Fornecedor
- Versão
- Produto
- Edição

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre requisitos do sistema, consulte Configurar a avaliação de exposição de vulnerabilidade.

Exiba o módulo de avaliação de exposição de software e crie e edite registros de avaliação de exposição sob demanda para software vulnerável em sua instância Now Platform®.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você gerencia as atividades de resposta a vulnerabilidades para uma grande operação responsável por muitos ativos. O Centro de Operações de Segurança (SOC) em sua operação entra em contato com você sobre uma versão do software que eles aprenderam como vulnerável. Você descobre que uma verificação de seus ativos foi concluída recentemente e não encontrou esta vulnerabilidade. A equipe de SOC descobriu essa vulnerabilidade por meio de uma fonte confiável fora do Banco de dados nacional de vulnerabilidades (NVD), Enumeração de pontos fracos comuns (CWE) ou de outras bibliotecas de terceiros em sua instância. t ainda adicionou o plug-in para ele.

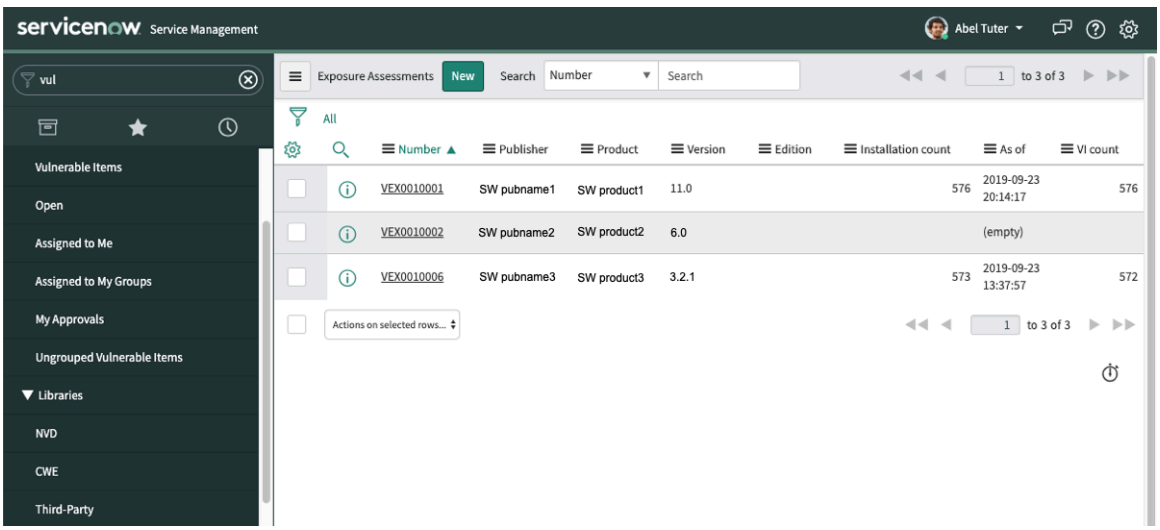
Você está confiante de que os dados desta vulnerabilidade serão atualizados no NVD e importados em breve para que o scanner possa detectar esta vulnerabilidade na próxima verificação, mas como você está preocupado com o escopo de sua possível exposição, você deseja determinar hoje se você tem ativos em sua rede que têm este software instalado.

A partir da v23.0 de Resposta a vulnerabilidades, se você tiver a assinatura Pro ou Enterprise, será redirecionado para a página **Avaliação de exposição** nos espaços com base na sua função ao selecionar o link **Avaliação de exposição** no menu **Todos**. Para obter mais informações, consulte Configurar a avaliação de exposição de vulnerabilidade.

Tradução automática

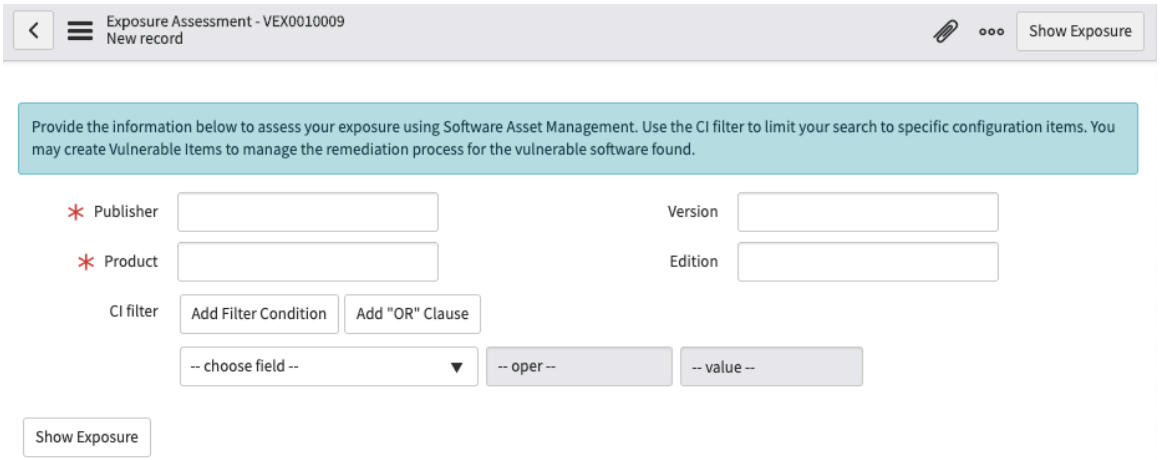
Procedimento

1. Para criar uma nova avaliação de exposição, navegue até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Avaliação de Exposição**.
   A lista Avaliações de exposição é exibida.



2. Selecione **Novo**.
   O formulário Avaliação de exposição é exibido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



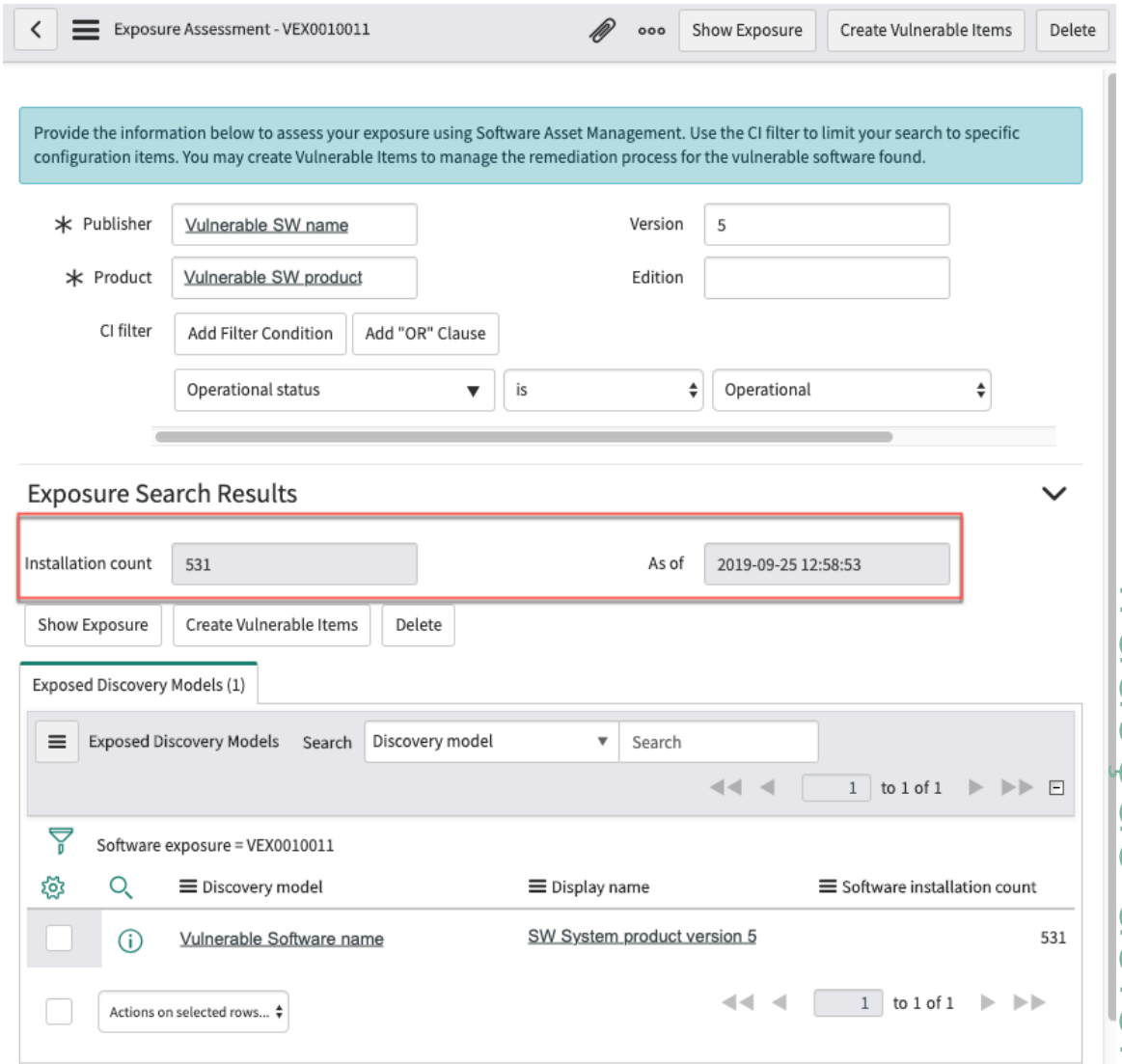
3. Preencha o formulário.

Campo	Descrição
Fornecedor	Nome do fornecedor do software.
(Opcional) Versão	Insira o número da versão para ajudá-lo a restringir a pesquisa em seus ativos.
Produto	Nome do produto de software.
(Opcional) Edição	Insira a edição para ajudá-lo a restringir a pesquisa em seus ativos.
Filtro de IC	Use as listas de seleção do filtro Item de configuração (IC) para limitar sua pesquisa a itens de configuração específicos (ativos). Por exemplo, você pode enviar uma consulta somente para ativos ativos que podem ter este software instalado: `O status operacional é Operacional`

4. Selecione **Mostrar exposição**.
O registro de avaliação de exposição com seu modelo de descoberta e a contagem de instalação de software em seus ativos a partir da data específica são exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Escolha um para continuar.

Opção	Descrição
Mostrar Exposição	Adicione condições de filtro de IC adicionais e selecione **Mostrar exposição** para refinar ainda mais os resultados da pesquisa.
Criar Itens vulneráveis	Crie itens vulneráveis para os itens de configuração a partir dos resultados da pesquisa. Se os itens vulneráveis forem criados com sucesso, uma tarefa de correção será criada para todos os itens vulneráveis e exibida no registro de avaliação de exposição.
Excluir	Exclua este registro e retorne à lista Avaliações de exposição. Uma caixa de diálogo de confirmação é exibida.

6. Opcional: Crie um item vulnerável para o resultado da pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Depois de criar itens vulneráveis, você não poderá alterar os critérios de pesquisa para este registro de exposição.

7. Como alternativa, revise as condições do filtro e refine ainda mais os resultados da pesquisa.
8. Para criar itens vulneráveis, siga estas etapas:

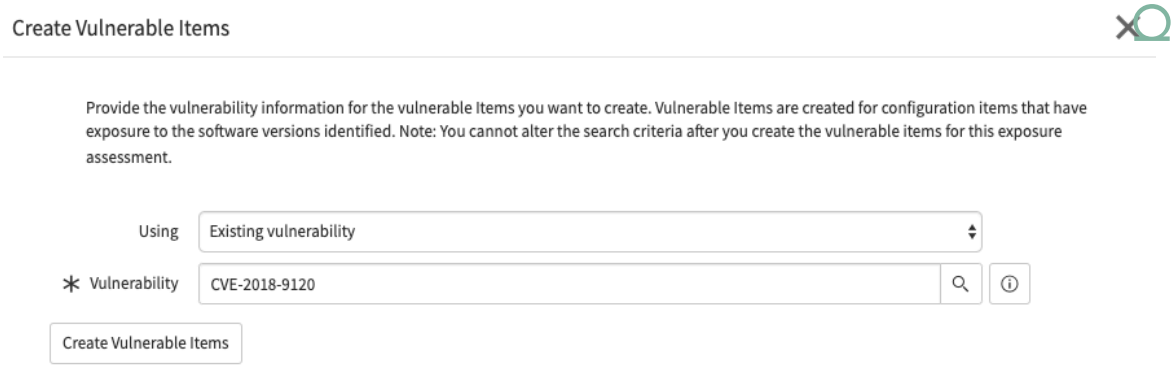
   a. Selecione **Criar itens vulneráveis**.
   A caixa de diálogo Criar itens vulneráveis é exibida.

   b. Preencha os campos.

Campo	Descrição
Usando	Na lista de seleção, escolha um para continuar. ▪ **Vulnerabilidade existente**. À direita do campo Vulnerabilidade, clique no ícone de pesquisa. Na lista exibida, selecione o CVE-ID ou insira os critérios de pesquisa para localizar o CVE-ID existente, por exemplo, CVE 2018-9120. **Nota:** Pode ser um CVE-ID de um banco de dados de vulnerabilidades diferente do NVD. ▪ **Nova vulnerabilidade**. Insira o CVE-ID da sua nova vulnerabilidade no formato xxxx-xxxx, xxxx-xxxxx ou xxxx-xxxxxx.
Resumo da vulnerabilidade (somente para vulnerabilidade nova)	Insira um resumo para a nova vulnerabilidade, por exemplo, `Um invasor pode executar o script no navegador de um usuário desavisado`.

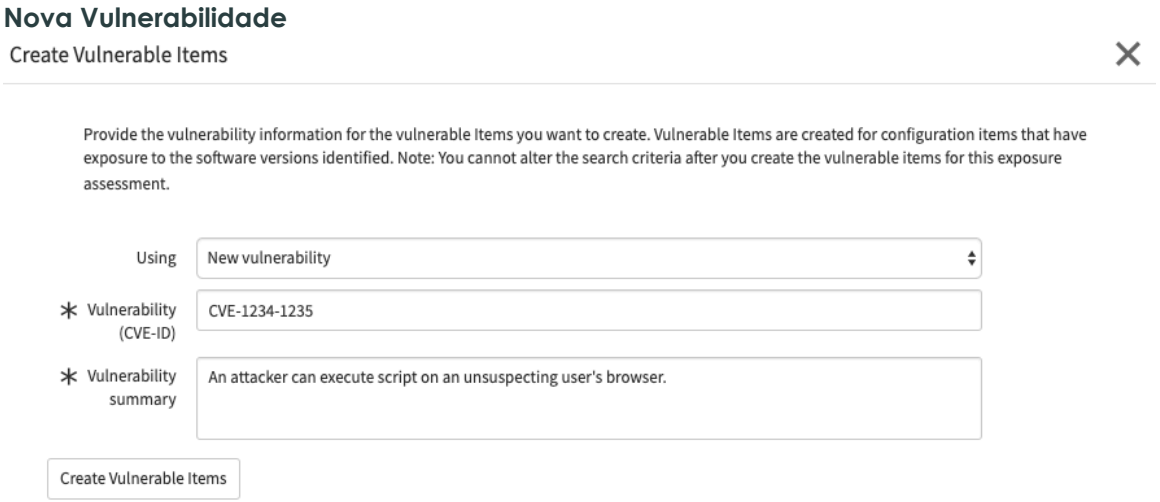
As imagens a seguir mostram exemplos do formulário preenchido para uma vulnerabilidade existente e uma nova vulnerabilidade.

Vulnerabilidade Existente



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



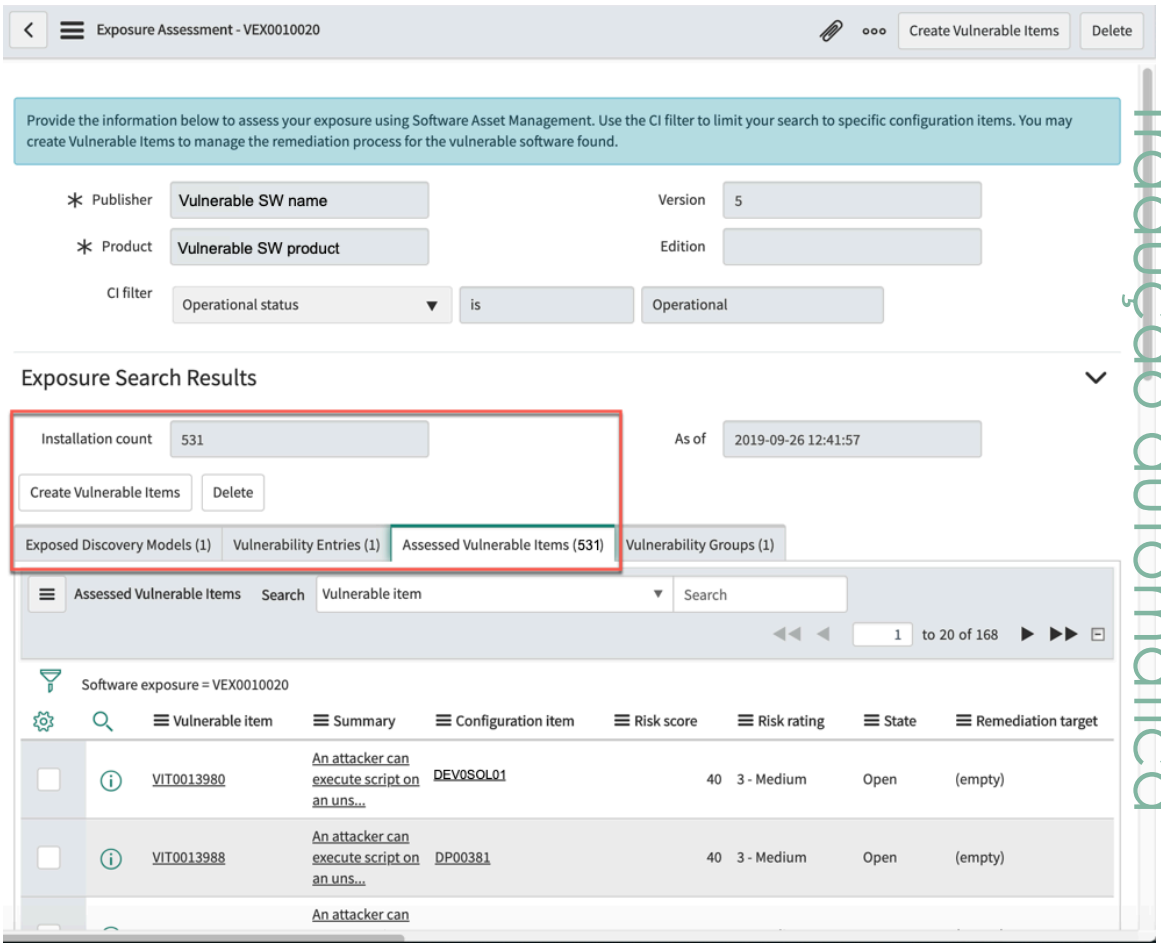
c. Selecione **Criar itens vulneráveis**.
O registro de avaliação de exposição é exibido com uma mensagem de status que indica que itens vulneráveis estão sendo criados.

d. Após alguns segundos, na parte superior do formulário, clique com o botão direito do mouse na faixa cinza para recarregar a página.
Os novos itens vulneráveis são exibidos conforme mostrado na figura a seguir na guia Itens vulneráveis avaliados (531). A nova tarefa de correção criada para esses itens vulneráveis é exibida na guia Tarefa de correção (1).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para este exemplo, uma tarefa de correção é criada de acordo com as regras e condições do grupo da regra de tarefa de correção chamada Vulnerabilidade. Esta regra de grupo é a regra de tarefa de correção padrão que é instalada com o produto Resposta a vulnerabilidades em sua instância Now Platform®. Neste exemplo, as condições desta regra de grupo colocaram todos os itens vulneráveis em uma única tarefa de correção. Se você preferir criar mais de uma tarefa de correção para os itens vulneráveis que correspondem aos resultados da pesquisa de avaliação de exposição, talvez prefira configurar regras de tarefa de correção adicionais. Criar mais tarefas de correção pode ajudar a evitar a criação de tarefas de correção com um grande número de itens vulneráveis. Para obter mais informações sobre regras de tarefa de correção, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral e Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção.



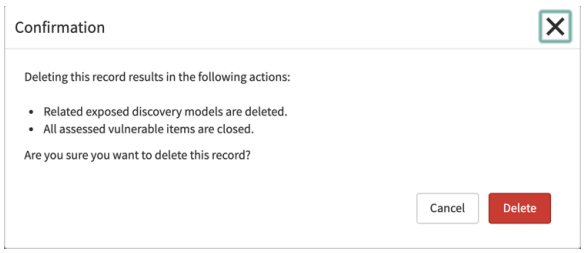
9. Escolha um para continuar.

Opção	Descrição
Tarefas de correção	Com a guia Tarefas de correção selecionada, na coluna numérica, clique para abrir o registro e revisar e atribuir a tarefa de correção. Para obter mais informações sobre grupos de atribuição, consulte Criando grupos .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Itens de vulnerabilidade avaliados	Com a guia Itens vulneráveis avaliados selecionada, na coluna Itens vulneráveis, clique para abrir os registros e revisar e atribuir itens vulneráveis individuais.
Excluir	Exclua o registro de avaliação de exposição. Uma caixa de diálogo de confirmação é exibida. **Nota:** Se você excluir o registro de exposição depois de criar itens de vulnerabilidade, todos os itens vulneráveis criados para este registro que não estejam relacionados a outro registro de exposição serão movidos automaticamente para o estado `Fechado`. O motivo do fechamento é `Cancelado`.



O que Fazer Depois

Responda a quaisquer ameaças de dia zero (dia atual) com base em sua avaliação de exposição. Para obter mais informações sobre tarefas de correção e gestão de mudanças para Resposta a vulnerabilidades, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral e Gestão de mudanças para Resposta a vulnerabilidades.

Exibição de recomendações de atribuição

Um grupo de atribuição geralmente é alocado a um item vulnerável usando regras de atribuição. Essas regras são configuradas pelo administrador de vulnerabilidades para alocar os grupos de atribuição corretos que se baseiam nos dados recebidos de scanners de terceiros.

Para obter mais informações, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Se um grupo de atribuição correspondente não estiver disponível ou estiver incorreto, você poderá usar Recomendações de atribuição de vulnerabilidade para exibir grupos de atribuição alternativos.

Use Recomendações de atribuição de vulnerabilidade para realizar as seguintes ações:

- Solicitar recomendações do grupo de atribuição para um item vulnerável.
- Solicitar recomendações do grupo de atribuição para vários itens vulneráveis.
- Solicitar recomendações do grupo de atribuição para uma tarefa de correção.

Solicitar recomendações do grupo de atribuição para um item vulnerável

Solicitar Recomendações de atribuição de vulnerabilidade para que você possa exibir as recomendações do grupo de atribuição. Você pode solicitar recomendações se um grupo de atribuição correspondente não estiver disponível ou estiver incorreto para um item vulnerável (VI).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** e abrir um VI.
   O item deve estar no estado Aberto, Adiado, Sob investigação ou Aguardando implementação.
2. Clique no ícone de recomendação (ícone de) ao lado do campo **Grupo** de atribuição para obter sugestões de atribuição para esse VI.
3. Na caixa de diálogo Recomendações do grupo de atribuição, selecione uma recomendação baseada na pontuação de confiança.
   A pontuação de confiança prevê a relevância da correspondência para o VI. Para obter mais informações, consulte Soluções de aprendizado de máquina para Resposta a vulnerabilidades.
4. Clique **em Atribuir**.

Resultados
O grupo selecionado aparece no campo **Grupo de atribuição** e o Tipo de atribuição muda para Recomendação.

Solicitar recomendações do grupo de atribuição para vários itens vulneráveis

Use Recomendações de atribuição de vulnerabilidade para exibir as recomendações do grupo de atribuição para vários itens vulneráveis (VIs) usando uma edição em massa. Quando vários IVs são selecionados, uma previsão é realizada em uma amostra aleatória dos IVs selecionados.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
As recomendações e suas pontuações de confiança podem diferir um pouco entre as invocações, com base nas amostras coletadas dos IVs selecionados. A pontuação de confiança avalia se o sistema está confiante de que o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade. Use a propriedade do sistema `Assign_recommendation_batchsize` para definir o tamanho do lote ao solicitar Recomendações de atribuição de vulnerabilidade para tarefas de correção (VULs) e VIs usando a opção de edição em massa. O valor padrão desta propriedade do sistema é definido para o desempenho de previsão ideal.

Nota: Se você aumentar o valor padrão, o tempo de resposta para Recomendações de atribuição de vulnerabilidade nesses casos poderá mudar.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Item Vulnerável** e selecione vários IVs.
   Os itens devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Itens vulneráveis em massa

Campo	Descrição
Seleção de registro	Registros a serem selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição a ser definido para os itens vulneráveis selecionados. Para exibir os grupos de atribuição recomendados, clique no ícone de recomendação (ícone de) ao lado do campo. Selecione uma recomendação baseada na pontuação de confiança e clique em **Atribuir**.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.

Resultados
O grupo selecionado aparece no campo **Grupo de atribuição** e o Tipo de atribuição muda para Recomendação para todos os IVs selecionados.

Solicitar recomendações do grupo de atribuição para uma tarefa de correção

Use Recomendações de atribuição de vulnerabilidade para exibir recomendações de grupo de atribuição para uma tarefa de correção (VUL).

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
Use a propriedade do sistema `assign_recommendation_batchsize` para definir o tamanho do lote ao solicitar Recomendações de atribuição de vulnerabilidade para VULs e itens vulneráveis (VIs) usando a opção de edição em massa. O valor padrão desta propriedade do sistema é definido para o desempenho de previsão ideal.

Nota: Se você aumentar o valor padrão, o tempo de resposta para Recomendações de atribuição de vulnerabilidade nesses casos poderá mudar.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** e selecione uma VUL.
   O grupo deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique no ícone de recomendação (ícone de) ao lado do campo **Grupo** de atribuição para as recomendações de grupo de atribuição da VUL selecionada.
   A caixa de diálogo Recomendações de grupo de atribuição exibe os grupos de atribuição recomendados com a pontuação média de confiança para todos os IVs nesse grupo.
3. Selecione uma recomendação na lista Grupo de atribuição com base na pontuação de confiança.
   A pontuação de confiança prevê a relevância da correspondência para a VUL selecionada.
4. Clique **em Atribuir**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O grupo selecionado aparece no campo **Grupo de atribuição**.

5. Salve a tarefa de correção com as informações atualizadas.

Resultados
Todos os IVs com o mesmo grupo de atribuição da VUL são atribuídos ao grupo de atribuição selecionado. O Tipo de atribuição muda para Recomendação para a VUL, bem como todos os IVs modificados.

Como solicitar e aprovar uma exceção

Você pode solicitar o adiamento da correção de um item vulnerável ou tarefa de correção por um período especificado. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Você pode solicitar exceções nos espaços Resposta a vulnerabilidades. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

- Solicitar uma exceção para um item vulnerável
- Solicitar uma exceção para uma tarefa de correção
- Solicitar uma exceção em massa

Você também pode solicitar exceções às políticas usando GRC: Gestão de políticas e conformidade:

- Solicitar uma exceção usando GRC: Gestão de políticas e conformidade
- Solicitar uma exceção em massa usando GRC: Gestão de políticas e conformidade

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Solicitar uma exceção para um item vulnerável

Solicite uma exceção para um item vulnerável (VI) que não pode ser corrigido imediatamente. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Importante: Você pode solicitar exceções no Gerenciador de vulnerabilidades e nos Espaços de correção de TI. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros do Vulnerability Manager Workspace e Solicitar uma exceção no Espaço de correção de problemas de TI.

Você também pode solicitar exceções para IVs no ambiente clássico.

Nota:

A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Todos**.
2. Selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No formulário Item vulnerável, clique em **Solicitar exceção**.
4. Se Resposta a vulnerabilidades for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado Aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 18.0 de Resposta a vulnerabilidades (VR), se um item vulnerável tiver sido adiado para correção usando o recurso de gestão de exceções, caso ele seja reaberto pelo scanner, a data de adiamento definida na vulnerabilidade ainda persistirá. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema *sn_vul.auto_defer_vit_in_active_exception_win* como verdadeiro. Além disso, a data adiada **Até** persiste mesmo depois que o item vulnerável é fechado ou a exceção expira. A função necessária é sn_vul.manage_exception_configuration para leitura e gravação.
Motivo	Motivo da solicitação. As opções são: ◦ Risco aceito ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Redução do controle no local ◦ Outro Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser atualizado pelo responsável pela correção.

5. Envie a solicitação de exceção clicando em **Solicitar aprovação**.

Resultados
O estado do item vulnerável muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma exceção para uma tarefa de correção

Solicite uma exceção para adiar uma tarefa de correção por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Importante:

Você pode solicitar as exceções no Gerenciador de vulnerabilidades e nos Espaços de correção de TI. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções para tarefas de correção no ambiente clássico.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** > **Todos**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No registro da tarefa de correção (VUL), selecione **Solicitar exceção**.
4. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Solicitar uma exceção em massa

Use a opção de edição em massa para solicitar uma exceção para vários itens vulneráveis (VITs) em vez de selecionar cada item manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst

Por Que e Quando Desempenhar Esta Tarefa

Quando vários VITs são selecionados, uma tarefa de correção (VUL) é formada com esses itens. Consulte Editar itens vulneráveis em massa no Resposta a vulnerabilidades para obter mais informações sobre como editar vários VITs.

Importante: Você pode solicitar uma exceção para:

- um VIT de Vulnerability Manager Workspace e Espaço de correção de problemas de TI. Para obter mais informações, consulte Solicitar uma exceção no Espaço de correção de problemas de TI.
- vários VITs do Vulnerability Manager Workspace. Para obter mais informações, consulte Solicitar exceção em massa no Espaço do gerenciador de vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Todos** e selecione os itens para os quais você deseja solicitar uma exceção.
   Os itens selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros que você selecionou para uma edição em massa.
Estado	Estado do item vulnerável. Selecione o estado Adiado para solicitar uma exceção para os itens selecionados.
Motivo	Subestado para o estado que você selecionou.
Descrição resumida	Nome da tarefa de correção que você está criando.
Até	Data de término que você especifica para sua solicitação de exceção.
Informação adicional	Detalhes adicionais que você deseja mencionar para informar o aprovador sobre os motivos da sua solicitação.
Solução preferencial	Solução que é direcionada para corrigir todos os itens vulneráveis que você selecionou para uma edição em massa.
Grupo de atribuição	Grupo de atribuição para o VI. Você pode selecionar um grupo manualmente ou usar as Recomendações de atribuição se esse recurso estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma tarefa de correção é criada contendo os IVs selecionados. Esta tarefa de correção foi enviada para aprovação.

Tradução automática

Solicitar uma exceção usando GRC: Gestão de políticas e conformidade

Solicite exceções de política usando a capacidade de gestão de exceções de política GRCGestão de políticas e conformidade na aplicação [] de dentro de Resposta a vulnerabilidades.

Antes de Iniciar

Antes de poder usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Gestão de políticas e conformidade do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção. O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.
3. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

4. Clique em **Enviar**.
   Para obter mais informações sobre a integração de exceção à política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Solicitar uma exceção em massa usando GRC: Gestão de políticas e conformidade

Selecione um grupo de itens vulneráveis e envie uma exceção em massa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Antes de poder usar a integração de exceção de política para solicitar exceções em massa, você deve baixar a aplicação GRC: Gestão de políticas e conformidade do ServiceNow Store.

Nota: Para usar este recurso, você deve atualizar GRC: Gestão de políticas e conformidade antes de atualizar Resposta a vulnerabilidades. Se você já tiver atualizado Resposta a vulnerabilidades antes de GRC: Gestão de políticas e conformidadee quiser usar este recurso, deverá executar os procedimentos de upgrade novamente na ordem correta.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções no ambiente clássico em Resposta a vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Todos** e selecione os itens para os quais você deseja solicitar uma exceção.
   Os itens selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros que você selecionou para uma edição em massa.
Estado	Estado do item vulnerável. Selecione o estado Adiado para solicitar uma exceção para os itens selecionados.
Descrição resumida	Nome da tarefa que você está criando.
Solução preferencial	Solução que você está direcionando para corrigir todos os itens vulneráveis selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição para o VI. Você pode selecionar um grupo manualmente ou usar as Recomendações de atribuição se esse recurso estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma tarefa de correção é criada com os itens vulneráveis selecionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em GRC: Gestão de políticas e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

6. Clique em **Enviar**.
Para obter mais informações sobre a integração de exceção à política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Aprovar ou rejeitar uma solicitação de exceção no Resposta a vulnerabilidades

Aprove ou rejeite as solicitações de exceção para itens vulneráveis ou tarefas de correção que não podem ser corrigidas imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Importante:

Você pode aprovar ou rejeitar as solicitações de exceção no Vulnerability Manager Workspace. Para obter mais informações, consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Antes de Iniciar
Função necessária: sn_vul.exception_approver
Você também pode aprovar solicitações de exceção no ambiente clássico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Como trabalhar com uma regra de exceção

Você pode solicitar uma exceção para vulnerabilidades, itens vulneráveis (IVs) ou itens de configuração (ICs) que não podem ser corrigidos ou adiados imediatamente. Ao automatizar o processo de adiamento de VI, você pode adiar os IVs correspondentes com base na regra quando o sistema os identifica.

Você pode executar as seguintes tarefas para uma regra de exceção:

- Criar uma regra de exceção
- Aprovar uma solicitação de regra de exceção
- Ativação de uma regra de exceção
- Reabrir uma regra de exceção
- Atualizar uma regra de exceção aprovada
- Excluir uma regra de exceção

Nota:

A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Criar uma regra de exceção

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica para um grupo de itens vulneráveis (IVs), como uma regra com uma condição que se baseia na gravidade da vulnerabilidade desses IVs. Com esta regra, você pode adiar IVs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A regra é aplicada a partir da data "Válido de" até a data "Válido até". A tarefa de correção (VUL) é criada quando a regra é aprovada. O método de agrupamento para esta VUL é conhecido como regras de exceção. A VUL é criada no estado Adiado. Você não pode fechar, reabrir ou excluir esta VUL. IVs novos e reabertos são adiados e adicionados a esta VUL a partir da data "Válido a partir de" até que o grupo expire na data "Válido até".

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Na página de registro Novo regra de exceção, clique em **Novo** para criar uma regra.
3. No formulário, preencha os campos.

Formulário Regra de exceção

Campo	Descrição
Nome	Nome da regra de exceção.
Válido de	Data a partir da qual esta regra está ativa para adiar os IVs.
Válido até	Data a partir da qual a tarefa de correção para de aceitar novos IVs.
Motivo	Motivo para criar esta regra de exceção.
Grupo de atribuição	Grupo ao qual a tarefa de correção criada para rastrear os IVs adiados está atribuída.
Informação adicional	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condição de filtro para os IVs que podem ser definidos durante o processamento dos IVs.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.
Fase do fluxo de trabalho	Status de aprovação atual da regra de exceção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	Estado da regra de exceção.
Ordem de execução	Ordem exclusiva para cada regra de exceção.
Adiado até	Data até quando as VULs e VIs são adiadas. Nesta data, a VUL criada é fechada, todos os IVs são movidos para fora do grupo e as regras do grupo são reaplicadas.

4. Adicione o grupo de atribuição ao criar a regra.
5. Envie o formulário para aprovação.
   O status da solicitação muda para Em revisão. Até que você envie a regra de exceção, ela permanecerá no estado Rascunho.

Aprovar uma solicitação de regra de exceção

Avalie as solicitações de regra de exceção dos usuários para que você possa aprovar ou rejeitar essas solicitações.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Os membros do grupo de usuários de nível 1 do aprovador de exceção podem aprovar as solicitações de regra de exceção de nível 1. Da mesma forma, os membros do grupo de usuários de nível 2 do aprovador de exceção podem aprovar as solicitações de regra de exceção de nível 2. Ambos os grupos de usuários herdam a função de aprovador de exceção por padrão.

Nota:

Se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação com e explique por que você aprovou ou rejeitou a solicitação.
   Depois que uma regra de exceção é aprovada, uma tarefa de correção (RT) é criada no estado Adiado por padrão. A partir da data "Válido a partir de", esta regra é executada em todos os IVs criados e também naqueles que são movidos do estado Fechado para o estado Aberto. IVs que correspondem às condições definidas são adicionados ao RT e adiados pelo período especificado.

Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativação de uma regra de exceção

Uma regra é ativada na data "Válida a partir de". Após a ativação, ele automatiza o processo de exceção para itens vulneráveis (IVs).

A regra de exceção segue este ciclo de vida:

1. Os novos itens vulneráveis (VIs) que você cria ou reabre e que atendem à condição especificada são adiados. Se você habilitar a opção Executar em dados existentes ao executar a regra de exceção pela primeira vez, todos os IVs ativos e não adiados que corresponderem à condição da regra de exceção serão movidos para a tarefa de correção (RT) recém-criada e seu estado será alterado para Adiado.
2. Se um VI recém-criado corresponder à condição da regra de exceção, ele será movido para o RT adiado que está associado à regra e a regra do grupo não será executada nele.
3. Na data "Válido a partir de", os IVs existentes serão adicionados se você habilitar a opção Executar em dados existentes.
4. O RT para de aceitar novos IVs quando a regra expira na data "Válido até". O RT permanece até a data "Adiado até".
5. A regra de exceção expira na data "Válido até".

Solicitar uma extensão para uma regra de exceção

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ◦ Risco aceito ◦ Aguardando janela de manutenção

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Correção indisponível ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção e itens vulneráveis associados. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.
- A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Reabrir uma regra de exceção

Reabra uma regra de exceção que foi rejeitada, mas você deseja reenviar. A reabertura da regra a move para o estado Rascunho.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode atualizar e reenviar a regra para aprovação.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Encontre a regra que deseja reabrir e clique em **Reabrir**.
3. Atualize o formulário e reenvie-o para aprovação.

Atualizar uma regra de exceção aprovada

Cancele uma regra aprovada para poder atualizá-la. Por exemplo, antes de poder modificar quaisquer datas ou adicionar uma condição a uma regra aprovada, você deve cancelá-la para que a tarefa de correção (VUL) seja excluída e os itens vulneráveis (IVs) sejam movidos para o estado Aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
As regras de grupo são reaplicadas a esses IVs. Envie a regra depois de fazer as mudanças para que ela passe pelo processo de aprovação mais uma vez.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja cancelar e clique em **Cancelar**.
3. Na caixa de diálogo Cancelar regra, clique em **Cancelar regra**.
   A regra retorna para o estado Rascunho e a VUL associada é excluída. Os IVs relacionados são reabertos e as regras de grupo são aplicadas aos IVs individuais.

Excluir uma regra de exceção

Exclua uma regra de exceção que não é mais necessária. Por exemplo, você pode excluir uma regra se não quiser adiar um item vulnerável (VI) durante a ingestão.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A exclusão de uma regra cancela a tarefa de correção associada (VUL). Os IVs relacionados são reabertos e as regras de grupo são aplicadas aos IVs individuais.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo Excluir regra, clique em **Excluir regra** para excluir a regra selecionada.
   A tarefa de correção associada também é excluída. Os IVs relacionados são reabertos e as regras de grupo são aplicadas aos IVs individuais.

Marcar e aprovar um falso-positivo

Itens vulneráveis (VIs) e tarefas de correção (VULs) podem ser marcados como falso-positivos. Aprovadores com acesso de gravação podem aprovar essas solicitações de outros usuários.

- Marcar como falso-positivo
- Edição em massa para falso-positivo
- Aprovar ou rejeitar um falso-positivo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho de falso-positivo, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando um VI ou tarefa de correção é marcado como falso-positivo, o solicitante recebe um e-mail de confirmação. Simultaneamente, o aprovador recebe um e-mail informando que um VI ou tarefa de correção foi marcado como falso-positivo.

A partir da v21.0 de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Marcar como falso-positivo

Marque um item vulnerável (VI) ou tarefa de correção (VUL) como falso-positivo se o aviso fornecido pelo scanner não for realmente um problema. Por exemplo, se um item de configuração foi desativado, mas o scanner ainda está levantando um problema relacionado a ele, marque-o como um falso-positivo.

Antes de Iniciar

Função necessária: responsável pela correção
Você pode solicitar falsos positivos nos espaços Resposta a vulnerabilidades. Consulte Solicitar um falso-positivo no Espaço de correção de problemas de TI.

Você também pode solicitar falsos positivos no ambiente clássico:

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis (ou Tarefas de correção)** > **Todos**.
2. Abra o VI ou VUL que você deseja marcar como falso-positivo e clique em **Marcar como falso-positivo**.
   O VI ou VUL deve estar em um estado **Aberto**.
3. No formulário Falso-positivo, insira os detalhes em **Informações adicionais** e clique em **Solicitar aprovação**.
   A solicitação é enviada para aprovação e o Estado do VI ou VUL muda para **Em revisão**.

Edição em massa para falso-positivo

Use a edição em massa para marcar vários itens vulneráveis (VITs) como falso-positivos. Se vários VITs forem selecionados, uma tarefa de correção será formada com esses itens.

Importante: Como administrador ou analista, você pode usar o recurso de edição em massa no Espaço do gerenciador de vulnerabilidades para marcar vários VITs como falso-positivos. Para obter mais informações, consulte Edição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária: responsável pela correção
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Você também pode solicitar falsos positivos no ambiente clássico:

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Itens vulneráveis** > **Todos** e selecione os itens que você deseja marcar como falso-positivos.
   Os itens selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros a serem selecionados para edição em massa.
Estado	Estado dos itens vulneráveis. Selecione Encerrado para marcar como falso-positivo.
Motivo	Subestado do estado selecionado. Se você selecionou Fechado como o Estado, selecione Falso-positivo aqui para marcar como falso-positivo.
Cancelar atribuição	Envie uma solicitação para limpar os campos Atribuído a e Grupo de atribuição.
Solução preferencial	Solução direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição para o VI. Selecione manualmente ou usando Recomendações de atribuição, se estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma nova tarefa de correção é criada contendo os IVs selecionados e essa tarefa é enviada para aprovação.

Aprovar ou rejeitar um falso-positivo

Como aprovador de falso-positivo, você pode aprovar ou rejeitar solicitações de falso-positivo de outros usuários.

Importante:

Você pode aprovar ou rejeitar as solicitações de falso-positivo no Vulnerability Manager Workspace. Para obter mais informações, consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.false_positive_approver ou sn_vul.app_false_positive_aprovador

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Nota: Um falso-positivo pode ter limite de tempo. Somente o aprovador pode definir a data de término.

Soluções de análise e emissão de relatórios para Resposta a vulnerabilidades

O monitoramento da correção de vulnerabilidades envolve a exibição de tendências, o gerenciamento de riscos e o monitoramento de grupos de atribuição. Você pode revisar problemas de alto risco, cargas de trabalho do grupo de atribuição, adiamentos e vulnerabilidades recorrentes. Resposta a vulnerabilidades oferece ferramentas, relatórios e procedimentos para tornar esse processo mais produtivo e eficiente.

Visualizações de dados nos espaços Resposta a vulnerabilidades

Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Os analistas de vulnerabilidade também podem usar painéis padrão Resposta a vulnerabilidades em **Todos** > **Resposta a vulnerabilidades** > **Visão geral**.

Importante:

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e Painéis no espaço de correção de TI.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Resposta a vulnerabilidades processo de correção

A maior parte da correção de vulnerabilidades é feita a partir do registro da tarefa de correção nos espaços Resposta a vulnerabilidades. Nas tarefas de correção (RTs) no estado Sob investigação, você pode executar várias tarefas.

- Criar solicitações de mudança.
- Adicione anotações de trabalho e descrições de vulnerabilidades na tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adie a tarefa de correção e os itens vulneráveis nela contidos para uma data posterior.
- Feche a tarefa de correção.
- Rastreie novas obrigações de conformidade regulatória, que geralmente são sensíveis ao tempo.

- Faça login na sua instância Resposta a vulnerabilidades.
- Revise os painéis e relatórios da Gestão de vulnerabilidades e de terceiros para localizar áreas com problemas. Por exemplo, exiba painéis que mostram o envelhecimento da tarefa de correção (RT) por estados ou itens vulneráveis (VIs) de alto risco após a data de meta de correção.
- Revise o estado das tarefas de correção, em ordem de risco.
- Revise a priorização das tarefas ajustando as calculadoras de pontuação de risco se a pontuação de risco não estiver sendo calculada corretamente ou adiando VIs ou RTs, conforme necessário. Consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade ou Adiar uma tarefa de correção para obter mais informações sobre essas opções.
- Revise os itens vulneráveis adiados prestes a reabrir e tome outras medidas conforme necessário. Se você quiser iniciar e rastrear atividades de mudança em seus ativos, tarefas de correção e itens vulneráveis correspondentes, para obter mais informações, consulte Gestão de mudanças para Resposta a vulnerabilidadespara ações adicionais.
- Analise o feedback das Operações de TI.

  Depois de receber a notificação de que uma solicitação de mudança foi resolvida, aguarde a próxima verificação. As verificações são acionadas automaticamente pela programação de importação de terceiros configurada no Assistente de configuração.

- Após uma verificação, se o estado for Fixo, os itens vulneráveis serão fechados automaticamente durante a importação. O grupo é encerrado quando todos os itens vulneráveis do grupo são corrigidos.
- Após a verificação, se o estado não for Fixo, o VI será movido automaticamente de volta para Sob investigação.

- Itens vulneráveis definidos como "Resolvidos" em sua instância, mas não transicionados para "Fechados/Corrigidos" pelas execuções de integração de terceiros, serão reabertos se forem detectados durante novas verificações.

  Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como "Resolvidos", mas que não foram transicionados para "Encerrado/Corrigido" pelas verificações subsequentes, esses IVs voltarão para "Aberto" quando a última data encontrada for posterior a Data de resolução.

  Para Rapid7 detecções, uma opção agora está disponível na página de configuração Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como "Resolvidos", mas não transicionados para "Fechados/Corrigidos" pelas verificações subsequentes, retornam para "Aberto" após o número de dias inserido.

Solução de gestão de vulnerabilidade Progresso da implantação

As métricas de implantação abrangentes para tarefas de correção e entradas de vulnerabilidade estão incluídas em Solução de gestão de vulnerabilidade em **Status** de correção em vulnerabilidades, itens vulneráveis. Identifique facilmente qual tarefa de correção ou vulnerabilidade está atrasando o andamento da resolução. Detalhe

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

como a vulnerabilidade é identificada ou quais aspectos dos ativos afetados podem estar causando o problema de correção. Atualize o status de suas métricas usando o link relacionado **Atualizar status** nos formulários de vulnerabilidade, soluções e tarefa de correção.

Usando os painéis padrão Resposta a vulnerabilidades

O Resposta a vulnerabilidades painel de visão geral (Gestão de vulnerabilidades) fornece uma visão executiva das vulnerabilidades e itens vulneráveis, ajudando o Administrador de vulnerabilidade a identificar rapidamente as áreas de preocupação. O Resposta a vulnerabilidades painel de correção (Correção de vulnerabilidade) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Visualizações de dados nos espaços Resposta a vulnerabilidades

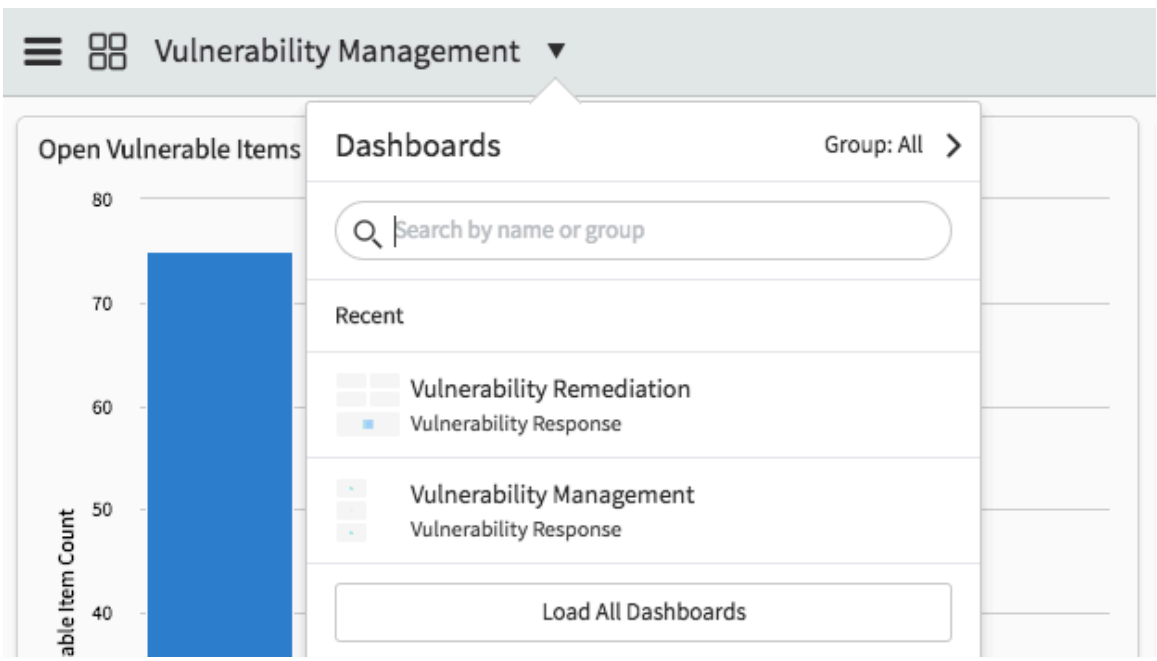
Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços, Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Os analistas de vulnerabilidade também podem usar painéis Resposta a vulnerabilidades padrão.

Funções necessárias: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e usuários com sn_vul.vulnerability_read (ou que herdam a função sn_vul.vulnerability_read) e pa_viewer.

Os painéis Resposta a vulnerabilidades padrão no ambiente legado

Esses relatórios são incluídos como parte da aplicação Performance Analytics para Resposta a vulnerabilidades e não exigem uma assinatura separada. Para abrir um, selecione a lista de seleção para expandi-la e escolha um painel. Como alternativa, insira o nome de um painel no campo de pesquisa.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Quando o pacote de conteúdo Resposta a vulnerabilidadesPerformance Analytics para a aplicação [] é instalado e ativado, o painel Gestão de vulnerabilidades (PA) é exibido automaticamente no módulo Visão geral. Este painel contém relatórios que cobrem todas as fases do ciclo de vida da gestão de vulnerabilidades.

Para obter informações sobre os relatórios incluídos no Pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades, consulte Painel Gestão de vulnerabilidades [PA].

Para obter informações sobre o painel do CISO e os relatórios de cobertura de verificação, consulte Painel do CISO de gestão de vulnerabilidades.

Painel de gestão de vulnerabilidades

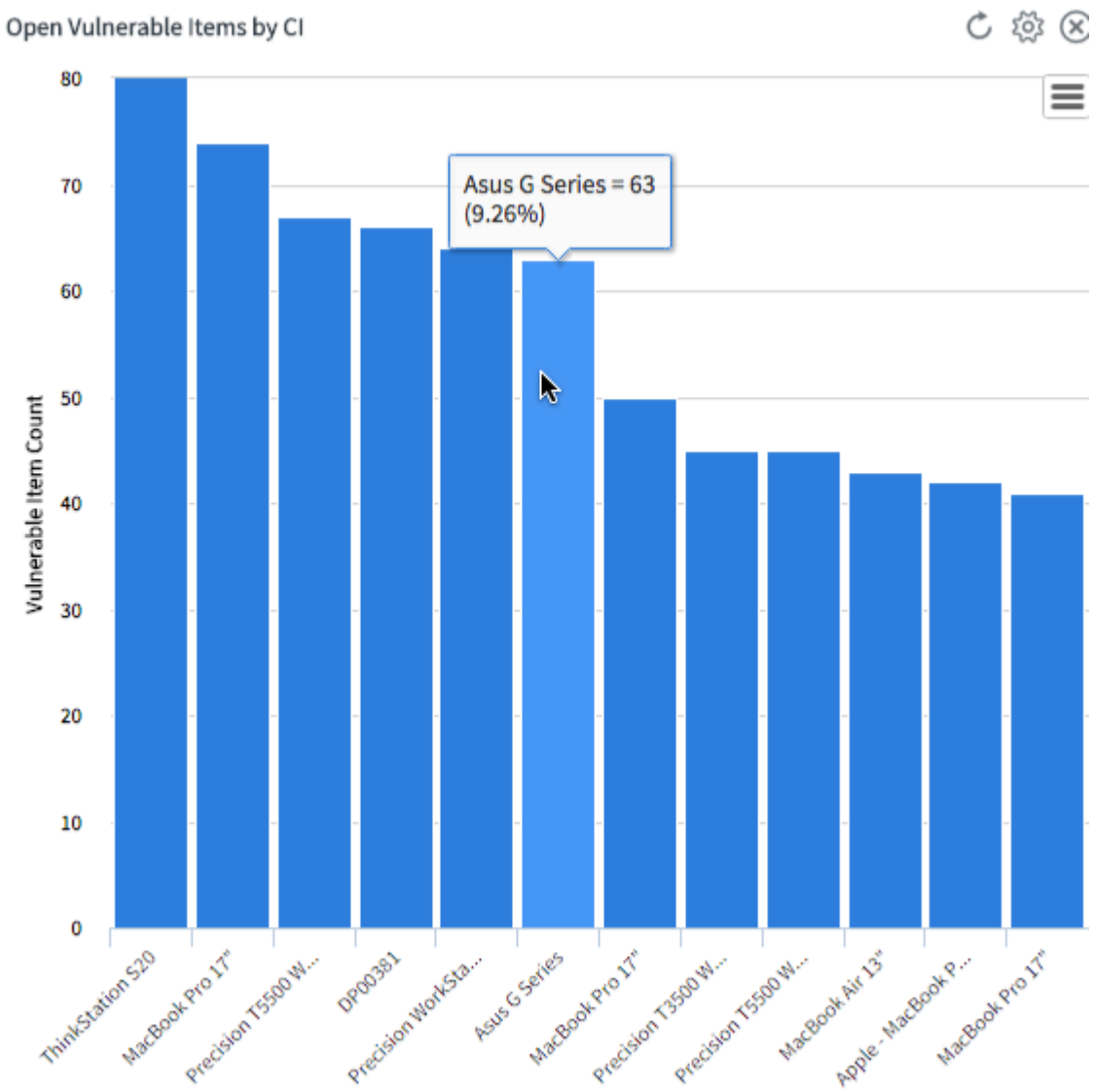
Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Nota:

Se forem necessários painéis personalizados, consulte Criar e usar painéis para obter mais informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Itens vulneráveis abertos por IC	Barra	Exibe o número de itens vulneráveis em aberto registrados para cada item de configuração (IC), do maior para o menor.
Itens vulneráveis por status da meta de correção	Barra	Exibe o número de itens vulneráveis que estão se aproximando da meta, em curso e após a meta. **Nota:** Itens no estado Adiado, Resolvido ou Encerrado não são incluídos.
Itens vulneráveis adiados que expiram esta semana	Gráfico	Exibe o número de itens vulneráveis adiados programados para serem reativados em sete dias.
Itens vulneráveis abertos por vulnerabilidade	Barra	Exibe o número de itens vulneráveis em aberto para cada vulnerabilidade, do maior para o menor.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Vulnerabilidades por modelo	Barra	Exibe o número de itens vulneráveis registrados para cada modelo (classe de IC), do mais para o menos.
Vulnerabilidades por semana	Tendência	Exibe o número de entradas de vulnerabilidade registradas a cada semana.
Modelos mais vulneráveis	Donut	Exibe modelos (classes de IC) com os itens mais vulneráveis.
Vulnerabilidades por fornecedor	Barra	Exibe o número de itens vulneráveis registrados para cada fornecedor, do mais para o menos.
Vulnerabilidades por impacto	Barra	Exibe o número de entradas de vulnerabilidade para tipos de rede afetados.
Fornecedores mais vulneráveis	Donut	Exibe os fornecedores com os itens mais vulneráveis.
ICs mais vulneráveis	Donut	Exibe ICs com os itens mais vulneráveis.
Vulnerabilidades por pontuação	Barra	Exibe o número de entradas de vulnerabilidade por pontuação de vulnerabilidade.
Itens vulneráveis reabertos	Lista	Lista os itens vulneráveis reabertos e sua idade.
ICs mais vulneráveis por classe	Donut	Exibe ICs com os itens mais vulneráveis.
Idade do Item Vulnerável	Lista	Lista o número de dias desde que os itens vulneráveis foram abertos pela última vez.
ICs com vulnerabilidade por data	Lista	Lista os itens de configuração que foram verificados nos últimos 30 dias.
ICs não verificados	Lista	Lista os itens de configuração que nunca foram verificados quanto a vulnerabilidades.

Painel de correção de vulnerabilidade

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

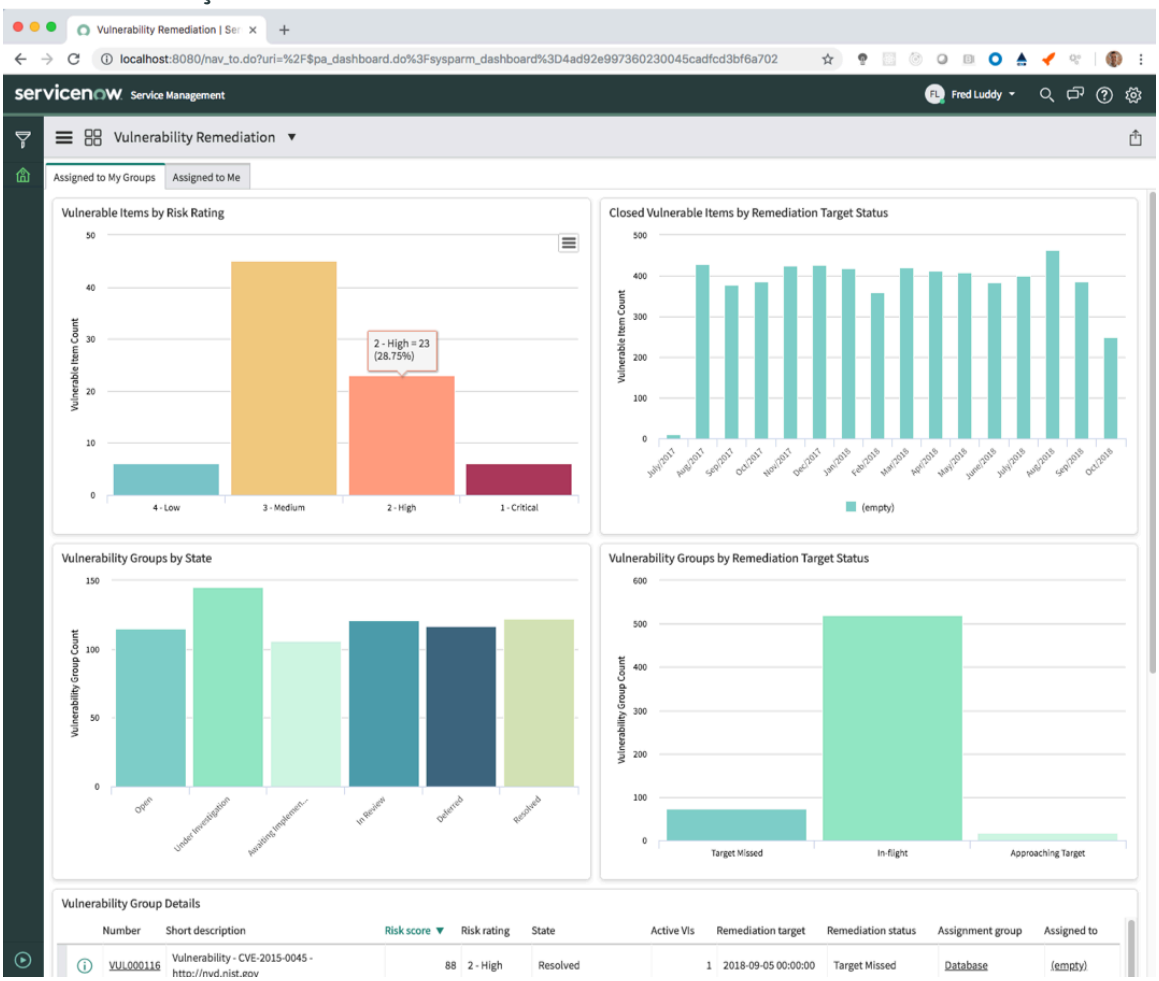
Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

O painel Correção de vulnerabilidades contém as seguintes guias: **Atribuído aos Meus grupos**, **Atribuído a mim**e **Solicitado por mim**. As guias Atribuído aos Meus grupos e Atribuído a mim mostram os mesmos relatórios. A primeira guia é relatada pelos grupos de atribuição aos quais você pertence e a última por itens vulneráveis ou tarefas de correção atribuídas a você. A guia Solicitado por mim relata os falsos positivos e as exceções que você solicitou.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel de correção de vulnerabilidade



Relatórios

Atribuído aos Meus grupos e Atribuído a mim

Nome	Visual	Descrição
Itens vulneráveis por classificação de risco	Barra de barra	Número de itens vulneráveis ativos, agrupados por classificação de risco no período selecionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuído aos Meus grupos e Atribuído a mim

Nome	Visual	Descrição
Itens vulneráveis encerrados por status da meta de correção	Barra de barra	Número de itens vulneráveis encerrados, agrupados por status da meta de correção no período selecionado.
Tarefas de correção por estado	Barra de barra	Número de tarefas de correção (RTs) ativas agrupadas por estado.
Tarefas de correção por status do meta de correção	Barra de barra	Número de RTs ativos agrupados por status de meta de correção. Este relatório exclui itens vulneráveis adiados.
Detalhes da tarefa de correção	Lista	Detalhes do registro da tarefa de correção em uma lista.

Solicitado por mim

Nome	Visual	Descrição
Status solicitações de falso-positivo e de exceção	Barra de barra	Número de solicitações ativas suas.
Tarefas de correção de falso-positivo e adiadas expirando	Barra de barra	Número de tarefas de correção (RTs) adiadas e com falso-positivo, agrupadas por data Até.

Painel de aprovações de vulnerabilidade

O painel Aprovações de vulnerabilidade contém os seguintes relatórios para aprovadores de exceção e falso-positivos.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Nome	Visual	Descrição
Solicitações de falso-positivo e exceção por idade com minha aprovação pendente	Barra de barra	Número de aprovações pendentes para você, agrupadas por data de criação.
Minha aprovação, exceção rejeitada e solicitações de falso-positivo	Barra de barra	Número de solicitações de aprovação aprovadas ou rejeitadas, agrupadas por estado de aprovação.
Todas as Tarefas de correção por classificação de risco com aprovação pendente	Barra de barra	Número de tarefas de correção com aprovação pendente, agrupadas por classificação de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Visual	Descrição
Todas as solicitações de aprovação pendentes e com falso-positivo agrupadas por motivo	Barra de barra	Número de solicitações de aprovação pendentes agrupadas por motivo.

Soluções Análise da plataforma e relatórios para Gestão de vulnerabilidades

Soluções Análise da plataforma e relatórios contêm conteúdo Performance Analytics e Emissão de relatórios pré-empacotado para uso com outros produtos Now Platform. Esta solução de análise e emissão de relatórios permite que você rastreie o volume, o desempenho e o andamento das vulnerabilidades, desde a análise inicial e detecção até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado.

O pacote de conteúdo Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com a aplicação Resposta a vulnerabilidades. Ele está disponível no ServiceNow Store como uma assinatura separada.

Performance Analytics para Resposta a vulnerabilidades contém dois painéis:

- Painel de gestão de vulnerabilidades (PA)
- Painel do diretor de segurança da informação (CISO) da Gestão de vulnerabilidades

Funções necessárias, instalação e exibição dos painéis

As seguintes funções e tarefas estão associadas a esta Solução:

- Now Platform administrador (admin): instale e ative esta solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Para instalar esta aplicação, consulte Instalação e configuração da aplicação Performance Analytics para Vulnerability Response [PA].

Nota: Configure e teste Soluções de análise e emissão de relatórios em uma instância de não produção antes de habilitá-las na produção.

As Soluções de análise e relatório fornecem todos os registros de configuração necessários para analisar as aplicações padrão. Personalize esses registros para uso em seu ambiente de produção. Para obter mais informações, consulte Configuração de soluções de análise e emissão de relatórios .

Para exibir o painel de Gestão de vulnerabilidades (PA), navegue até **Resposta a vulnerabilidades** > **Visão geral** > **.**

Para exibir o painel CISO da Gestão de vulnerabilidades, navegue até **Resposta a vulnerabilidades** > **Painel do CISO** > **.**

Termos principais

Análise de desempenho (PA)

Solução que cria painéis de gestão, relatórios sobre KPIs e métricas e responde a perguntas de negócios importantes para ajudar a aumentar a qualidade e reduzir custos.

Item vulnerável (VI)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma vulnerabilidade de segurança relatada por um scanner de vulnerabilidade de terceiros que está presente em um item de configuração (IC).

Tarefa de correção

As tarefas de correção são criadas e atribuídas automaticamente a equipes de TI com base no grupo associado aos itens vulneráveis em um esforço de correção. As equipes de TI e os responsáveis pela correção exibem as tarefas de correção no Espaço de correção de TI. Consulte Resposta a vulnerabilidades Espaços para obter mais informações

.

Indicador de PA

Define uma medida de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional, por exemplo, Itens vulneráveis críticos atrasados não adiados.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, VI ativo.

Exibir visualizações de dados em tempo real

Para ver o que está acontecendo hoje com os itens mais críticos na sua aplicação Resposta a vulnerabilidades, você pode exibir determinados relatórios no painel Gestão de vulnerabilidades (PA) em tempo real. A exibição desses relatórios em tempo real ajuda a gerenciar seus itens vulneráveis (IVs) mais importantes e a corrigi-los rapidamente. Você pode exibir os seguintes relatórios em tempo real:

- Guia Visão geral - Itens vulneráveis por grupo de atribuição
- Guia ICs vulneráveis
  - Itens de configuração (ICs) vulneráveis sem proprietários
  - ICs desativados ou roubados com IVs ativos
- Guia Exceções
  - Itens vulneráveis adiados por motivo
  - Solicitações de adiamento prestes a expirar
  - Itens vulneráveis adiados por gerente de CIO
- Guia Correção - Itens vulneráveis não atribuídos

Para obter mais informações, consulte Exibir relatórios da Análise de desempenho para Resposta a vulnerabilidades [PA] em tempo real.

Informações relacionadas

Soluções de análise e relatório

Painel Gestão de vulnerabilidade do CISO

Com o painel do Gestão de vulnerabilidade CISO, exiba dados como KPIs (principais métricas de desempenho) para correção de vulnerabilidades, veja os riscos mais altos, verifique a cobertura da verificação e saiba como reduzir riscos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias de Now Platform

- sn_vul.vulnerability_ciso para exibir o painel.
- sn_vul.ciso_write para editar o painel.

Ativação do painel do CISO

Para ativar o painel do CISO, você deve instalar o Performance Analytics para Resposta a vulnerabilidades e ativar o trabalho correspondente do Performance Analytics. Para obter mais informações, consulte Soluções de análise e emissão de relatórios para Resposta a vulnerabilidades.

Casos de uso

Usuário	Uso do painel
Diretores de segurança da informação (CISOs)	Os diretores de segurança da informação (CISOs) podem usar o painel do CISO para obter informações sobre o programa de gestão de vulnerabilidades de suas organizações. O painel fornece dados para ajudá-los a identificar dados rapidamente como eles podem usar para reduzir as vulnerabilidades de seus ambientes.

Como usar o painel do CISO

Usuários executivos, como os diretores de segurança da informação (CISOs) em sua organização, podem visualizar o painel do CISO para a Resposta a vulnerabilidades para entender a eficácia do programa de gestão de vulnerabilidades. Você pode exibir o painel do CISO navegando até **Resposta a vulnerabilidades** > **Painel do CISO**. Use os filtros de nível superior para filtrar relatórios por Classificação de risco, Faixa etária ou Voltado para a Internet. Alguns relatórios exibem dados de tendências ao longo de um período de tempo. Você pode exibir regularmente as tendências das métricas importantes, analisar o risco geral à segurança dos negócios e identificar as áreas que precisam ser aprimoradas.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e Painéis no espaço de correção de TI.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Executando os trabalhos agendados

Execute os trabalhos agendados nesta ordem para atualizar os dados nos relatórios:

1. Atualizar tabelas do painel
2. [PA VR] Painel do CISO

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos agendados para o painel do CISO

Nome do trabalho programado	Descrição
Atualizar tabelas do painel	Trabalho agendado diariamente que você deve executar antes do trabalho do Painel CISO [PA VR] para que você possa coletar os dados do CISO. Ao executar este trabalho agendado, você atualiza os relatórios de cobertura de verificação. As informações atualizadas incluem os itens de configuração (ICs) operacionais verificados nos últimos 90 dias, suas classes e o número total de ICs operacionais que correspondem a essas classes. A execução deste trabalho agendado também atualiza os relatórios na guia **Ações recomendadas**. **Nota:** Os ICs operacionais se referem aos ICs que têm um status operacional como `Operacional`.
[PA VR] Painel do CISO	Depois que o trabalho programado Atualizar tabelas do painel for concluído, execute-o para preencher todos os relatórios na guia **Visão geral do CISO**.

Guias do painel do CISO

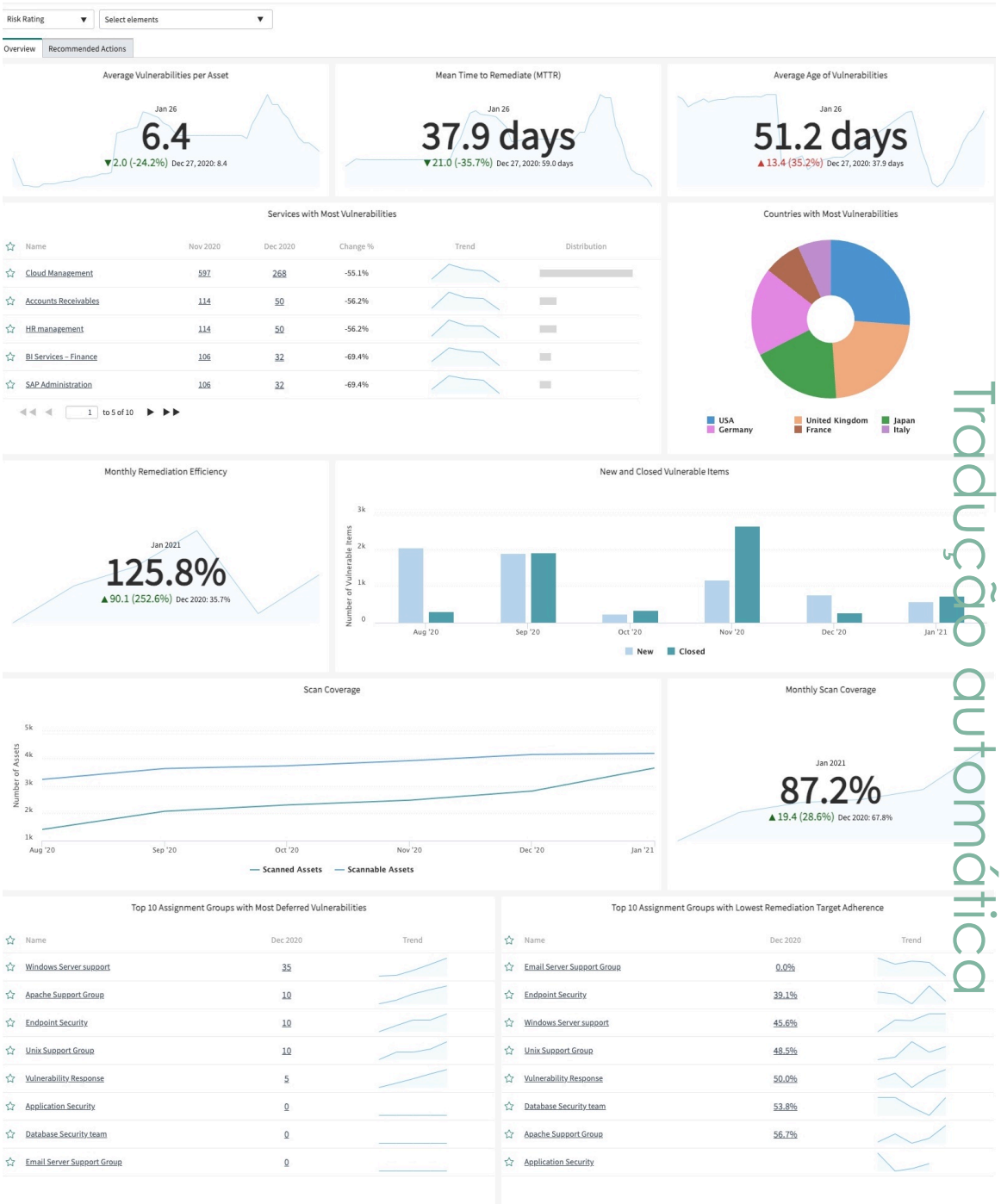
Este painel fornece informações sobre os riscos presentes na Gestão de vulnerabilidades. Você pode exibir vulnerabilidades e seus dados relacionados por região, idade, serviços e outros detalhamentos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão Geral

A guia Visão geral contém relatórios que fornecem uma visão geral da postura de segurança da sua organização.



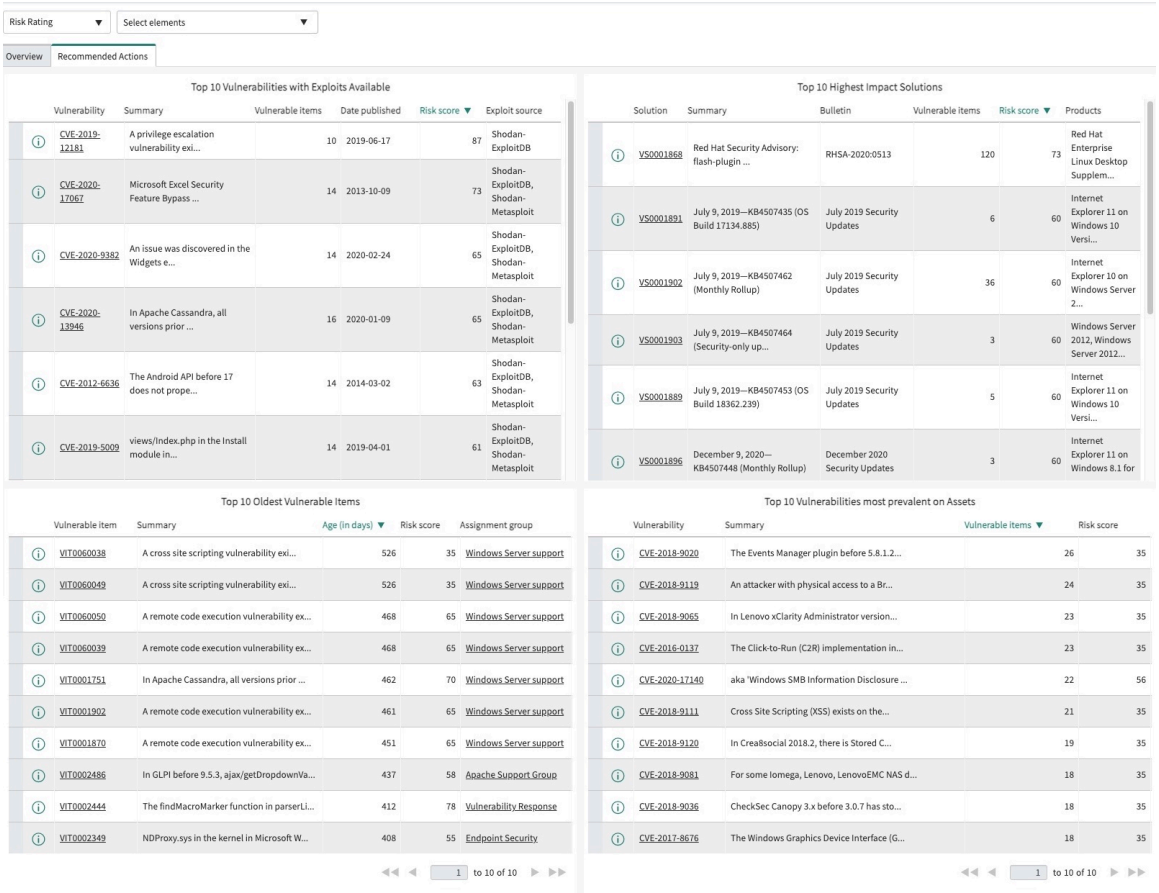
Nota: O filtro de nível superior só pode ser usado para alguns relatórios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Ações recomendadas

A guia Ações recomendadas contém relatórios que fornecem informações sobre vulnerabilidades exploráveis, obsoletas e comuns. Ele também contém soluções que recomendam ações para reduzir os riscos. Execute o trabalho agendado **Atualizar tabelas do painel do CISO** para atualizar os relatórios nesta guia.



Indicadores

Para exibir os indicadores, navegue até **Análise de desempenho** > **Indicadores**.

1. Na página Indicadores, pesquise o nome do indicador necessário na coluna Nome.
2. Clique no nome do indicador para abrir o registro e exibir seus detalhes.

Os indicadores do painel do CISO não coletam registros por padrão. Você pode optar por coletar registros marcando a caixa de seleção Coletar registros.

Duração total de itens vulneráveis encerrados

A duração total de IVs encerrados é medida diariamente em Dias. O objetivo deste indicador é minimizar a pontuação.

Ativos verificáveis

Os ativos verificados são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Serviços com mais vulnerabilidades

Os serviços com a maioria das vulnerabilidades são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades médias por ativo

[[Itens vulneráveis ativos]] / [[Itens de configuração vulneráveis ativos]

Itens vulneráveis encerrados

Os itens vulneráveis encerrados são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Tempo médio de correção dos itens vulneráveis

[[Soma da duração de itens vulneráveis encerrados]]/[[Itens vulneráveis encerrados]]

Cobertura de verificação atual

Calcula a cobertura da verificação atual como porcentagem.

Ativos verificados

Os ativos verificados são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Itens vulneráveis encerrados (meta atingida)

Itens vulneráveis encerrados (meta atingida) são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Percentual de itens vulneráveis encerrados que cumpriram a meta

[[Itens vulneráveis encerrados (Meta atingida) / SOMA por mês]] / [[Itens vulneráveis encerrados / SOMA por mês]] *100

Itens vulneráveis ativos

Os itens vulneráveis ativos são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Idade média dos itens vulneráveis

A idade média dos IVs ativos é medida diariamente em unidades Dias. O objetivo deste indicador é minimizar a pontuação.

Itens de configuração vulneráveis ativos

Os ICs vulneráveis ativos são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Eficiência de correção mensal

[Número de itens vulneráveis encerrados durante um mês] / [Número de itens vulneráveis novos ou reabertos no mesmo mês]

Novos itens vulneráveis

Os novos itens vulneráveis são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Itens vulneráveis adiados

Os IVs adiados são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Detalhamentos

- Grupo de atribuição: aplica-se a alguns relatórios de IV.
- Classificação de risco: aplica-se a relatórios de IV.
- Faixa etária: aplica-se a relatórios de VI.
- Encerrado por idade: aplica-se a relatórios de IVs encerrados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Voltado para a Internet: indica se o IC pertence à classe de hardware e é voltado para a Internet.
- Região: o parâmetro de IC do CMDB usado é Local. Este local indica o país de origem do item de configuração.

Visualizações de dados

Nome	Tipo	Descrição
Vulnerabilidades médias por ativo	Pontuação	Número médio de itens vulneráveis ativos para cada item de configuração.
Tempo médio para correção (MTTR)	Pontuação	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução. **Nota:** O valor de Idade fechada é calculado quando os dados são coletados. O valor é a diferença entre a data da Última abertura e a data e hora do trabalho de coleta.
Idade média das vulnerabilidades	Pontuação	Idade média dos itens vulneráveis ativos em dias.
Serviços com mais vulnerabilidades	Lista e linha Ícone	Média mensal de itens vulneráveis ativos para serviços na empresa. **Nota:** Para obter informações sobre como definir as classificações de serviço que você deseja exibir nos relatórios da Resposta a vulnerabilidades e nas listas relacionadas, consulte a guia Serviços no painel Gestão de vulnerabilidades [PA].
Países com mais vulnerabilidades	Donut	10 principais países com o maior número de itens vulneráveis.
Eficiência de correção mensal	Pontuação	Percentual de itens vulneráveis encerrados dividido por novos itens vulneráveis no mês atual.
Itens vulneráveis novos e encerrados	Barra de barra	Número de novos itens vulneráveis importados e número de itens vulneráveis encerrados em um mês.
Cobertura de verificação	Linha de linha	Número de ativos verificados em comparação com o número total de ativos verificáveis, mostrado ao longo do tempo. As classes de IC incluídas no widget são especificadas no módulo Configuração de cobertura de verificação. Para obter informações sobre como configurar o módulo Cobertura de verificação, consulte Configuração dos relatórios de cobertura de verificação.
Cobertura de verificação mensal	Pontuação	Percentual de ativos verificados dividido pelo número total de ativos verificáveis no mês atual.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		Para obter informações sobre como configurar o módulo Cobertura de verificação, consulte Configuração dos relatórios de Cobertura de verificação
10 principais grupos de atribuição com vulnerabilidades mais adiadas	Lista e linha Ícone	10 principais grupos de atribuição com o maior número de itens vulneráveis adiados, adiados com base na média mensal.
10 principais grupos de atribuição com menor adesão à meta de correção	Lista e linha Ícone	10 principais grupos de atribuição cujos itens vulneráveis têm a menor adesão às metas de correção.

Ações recomendadas

Nome	Tipo	Tabela de origem	Descrição
10 principais vulnerabilidades com explorações disponíveis	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Vulnerabilidades ativas com explorações disponíveis para todos os fornecedores de inteligência contra ameaças que usam a estrutura de exploração de VR.
10 principais soluções de maior impacto	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Soluções ou patches preferenciais com as pontuações de risco mais altas para itens vulneráveis ativos. Este relatório usa os recursos da Gestão de soluções de vulnerabilidade (VSM), que correlaciona patches da Microsoft e da Red Hat a vulnerabilidades no ambiente. O VSM ajuda a identificar a solução preferencial para vulnerabilidades.
10 principais itens vulneráveis mais antigos	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Itens vulneráveis ativos com a maior idade. Resolva esses itens para reduzir a idade média da vulnerabilidade na guia Visão geral.
10 principais vulnerabilidades mais comuns em ativos	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Itens vulneráveis ativos disponíveis para o maior número de ativos.

Configurar os relatórios de cobertura de verificação

Permita que os usuários executem relatórios de cobertura de verificação no painel do CISO. Com esses relatórios, os usuários podem ver qual é a cobertura de verificação da organização durante um período de tempo.

Antes de Iniciar

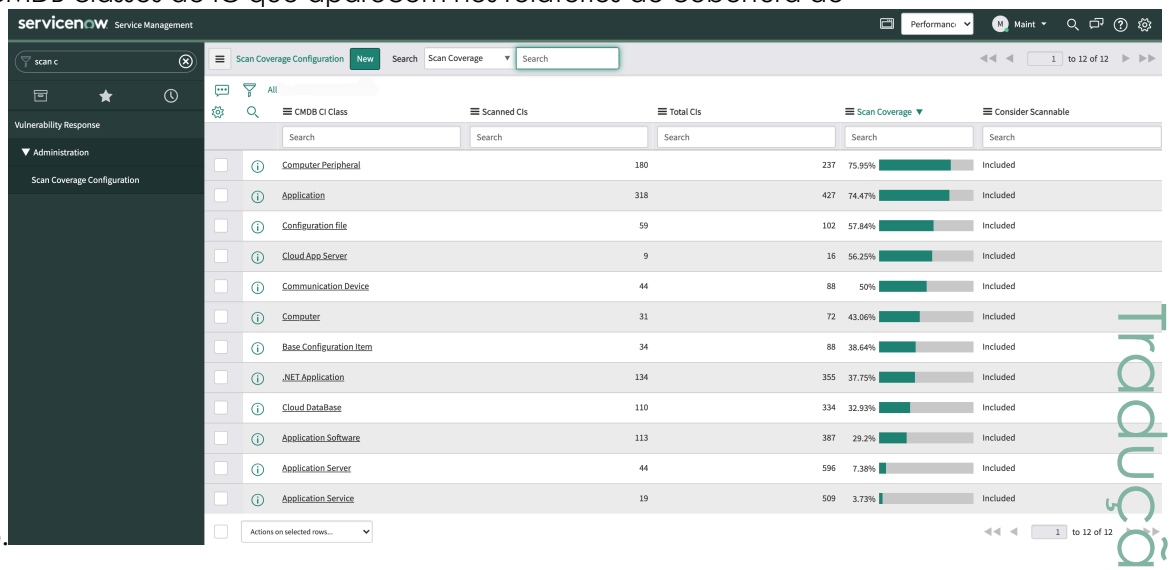
Função necessária: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A cobertura de verificação mostra o número de ativos que estão sendo verificados pelos scanners de vulnerabilidade para as várias classes nos últimos 90 dias. Esses ativos são comparados ao número de ativos verificáveis no Configuration Management Database (CMDB). Por padrão, o módulo Configuração de cobertura de verificação inclui CMDB classes de IC, às quais pelo menos um ativo verificado foi correspondido. Você pode adicionar uma classe de IC de CMDB ao relatório Cobertura de verificação que é exibido no painel do CISO. Você pode incluir ou excluir CMDB classes de IC que aparecem nos relatórios de cobertura de verificação.



Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Configuração de cobertura de verificação**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Configuração de cobertura de verificação

Campo	Descrição
Classe de IC do CMDB	Classe de IC que deve ser adicionada ao relatório de cobertura de verificação no painel do CISO. **Nota:** Se uma classe de IC já existir no módulo Configuração de cobertura de verificação, ela não será incluída nesta lista.
Considerar verificável	Opção para definir se a classe de IC deve ser incluída ou não. Inclua uma classe de IC se quiser que seus dados sejam adicionados aos relatórios de cobertura de verificação. Se excluído, os dados dessa classe de IC não serão adicionados.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar os indicadores do PA para o painel do CISO

Monitore os indicadores CISO automatizados e formulados para que você possa gerenciar os dados de vulnerabilidade em sua instância.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades tem indicadores automatizados e formulados.

Termos principais

Indicador

Define uma medida de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional. Um exemplo é um item vulnerável ativo.

Fonte do indicador

Conjuntos de dados que consistem em registros filtrados de uma tabela ou exibição de banco de dados para maior eficiência. Um exemplo é VI.Ativo (voltado para a Internet).

Detalhamentos

Os Detalhamentos filtram e agrupam pontuações do indicador usando atributos qualitativos, como Prioridade, Categoria e Grupo de atribuição.

Trabalhos agendados

Trabalhos agendados são executados para preencher os dados de origem do indicador. O trabalho agendado diário do painel do CISO [PA VR] está desabilitado por padrão. Você deve ativá-lo para coletar pontuações do indicador para o painel do CISO.

Procedimento

1. Navegar até **Todos** > **Análise de desempenho** > **Indicadores** e escolha uma das seguintes opções:
   - Indicadores Automatizados
   - Indicadores de Fórmula

   Para obter mais informações sobre indicadores, consulte Indicadores do Performance Analytics .
2. Na página Indicadores, pesquise o nome do indicador necessário na coluna Nome.
3. Clique no nome do indicador para abrir o registro e exibir seus detalhes.

   Os indicadores do painel do CISO não coletam registros por padrão. Você pode optar por coletar registros marcando a caixa de seleção **Coletar registros**.

   Nota: Ativar a coleta de registros em um indicador pode causar problemas de desempenho, como consumir muito mais tempo e memória necessários para executar o trabalho de coleta de dados.

   O número máximo de linhas que você pode buscar para uma origem de indicador é 1.000.000.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel de Integridade da Resposta a vulnerabilidades do SecOps

O painel de Integridade da Resposta a vulnerabilidades é uma ferramenta projetada para capacitar as organizações com informações abrangentes sobre a implementação e o uso de suas aplicações da Resposta a vulnerabilidades.

A avaliação geral de integridade é determinada pela agregação de vários fatores críticos em configuração, implementação, integração, desempenho, dados e processo. Exiba o painel agregado de cada categoria para as seguintes aplicações:

- Resposta a vulnerabilidades
- Resposta a vulnerabilidades de aplicações
- Resposta a vulnerabilidades do contêiner
- Conformidade de configuração

Instalando o painel de integridade da Resposta a vulnerabilidades do SecOps

Para instalar e configurar as aplicações SecOps Vulnerability Response Health Dashboard for Resposta a vulnerabilidades na sua instância da Now Platform, navegue até ServiceNow® Store e ative o plug-in SecOps Health Analytics (sn_sec_analytics).

Funções necessárias de Now Platform

Funções necessárias: sn_sec_analytics.admin, sn_sec_analytics.read

Trabalho agendado

Para exibir o trabalho agendado, navegue até **Todos** > **Scheduler do Sistema** > **Trabalhos agendados** > **Coletar métricas do painel de integridade**. O trabalho programado "Coletar métricas do painel de integridade" é executado diariamente às 00:00 horas. Ele gera os dados para o painel de Integridade da Resposta a vulnerabilidades do SecOps. Você também pode optar por executar o trabalho agendado manualmente.

Casos de uso

Para obter exemplos de como as pessoas em sua organização usariam este painel, consulte estes casos de uso.

Usuário	Uso do painel
Administrador de vulnerabilidade	Ajuda a entender a pontuação de integridade das aplicações Resposta a vulnerabilidades. Também é útil destacar as áreas que precisam ser aprimoradas. O Painel de Integridade da Resposta a vulnerabilidades lida somente com a implementação e a integridade de uso. Ele não ajuda na gestão de vulnerabilidades ou ativos.
Administrador do suporte	Ajuda a identificar problemas de desempenho, personalização e configuração usando KPIs. Com base na integridade da aplicação, você pode executar uma análise extra ou fornecer uma recomendação aos usuários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
Parceiro de implementação	Ajuda a avaliar a Resposta a vulnerabilidades integridade de implementação para configurações, complementos, personalizações e integrações e fornece recomendações de melhoria para os usuários.

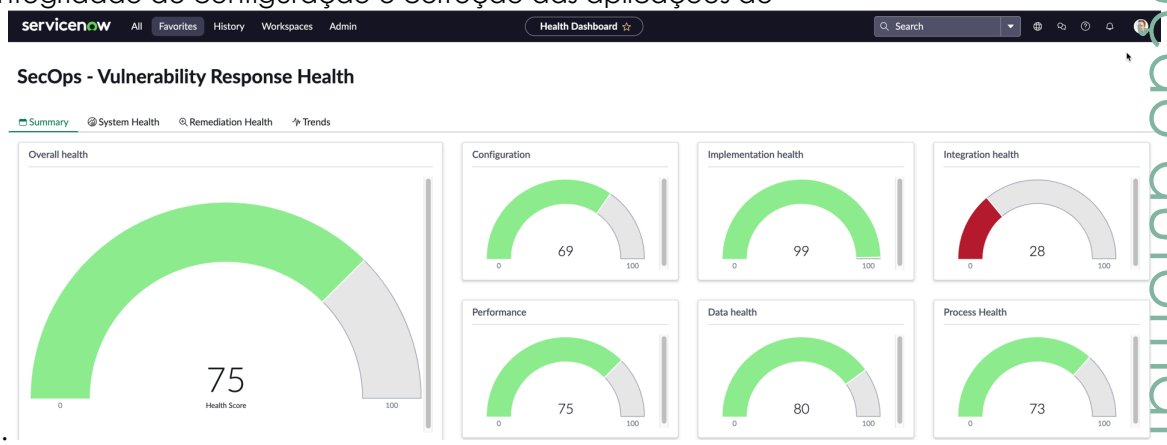
As guias do painel de integridade da Resposta a vulnerabilidades do SecOps

Para exibir o painel de Integridade da Resposta a vulnerabilidades do SecOps, navegue até **Integridade do Security Operations** > **Integridade da Resposta a vulnerabilidades**. Cada cor no painel representa o seguinte:

- Verde: seguro
- Amarelo: aviso
- Vermelho: Crítico

Guia Resumo

Este painel comunica a pontuação de integridade geral para a integridade de configuração e correção das aplicações de VR.

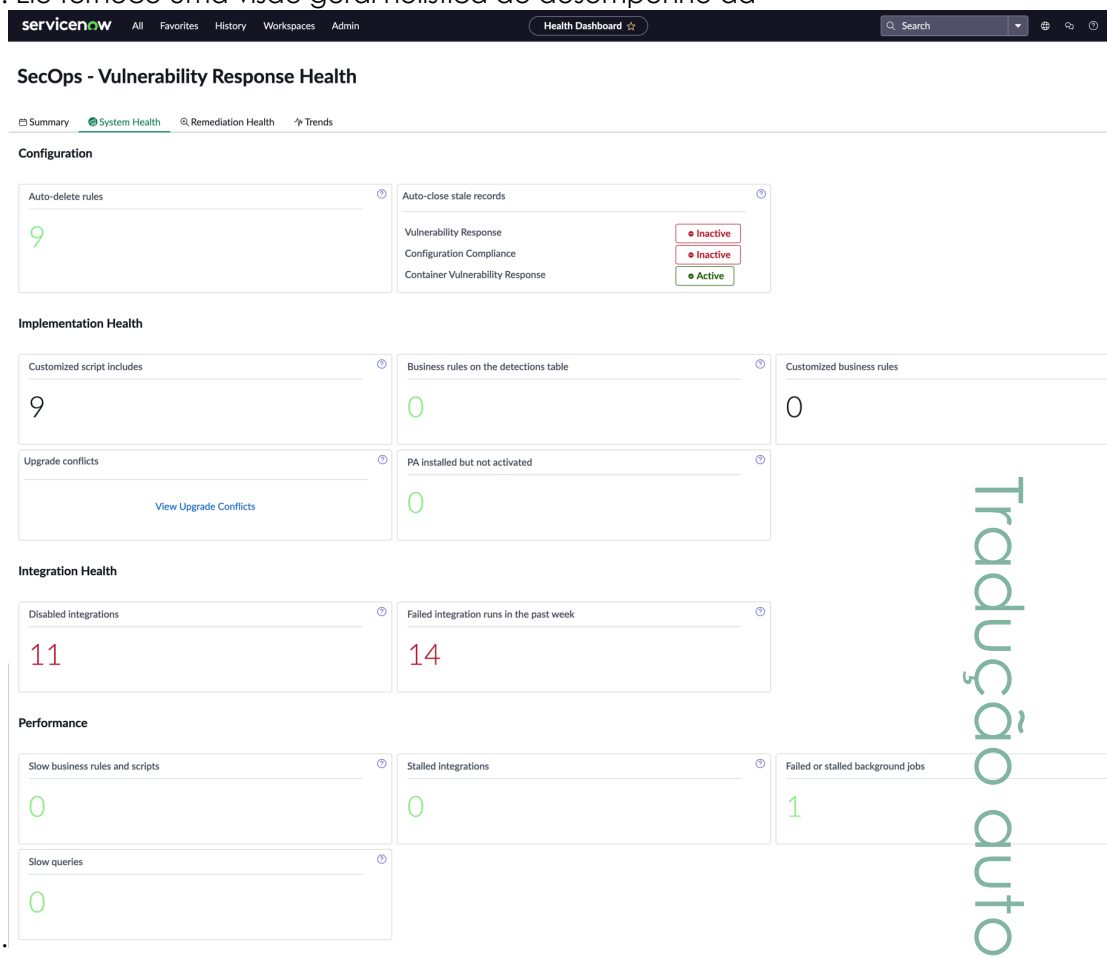


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Integridade do sistema

Este painel exibe a configuração e a integridade da integração da sua implementação. Ele fornece uma visão geral holística do desempenho da implementação.

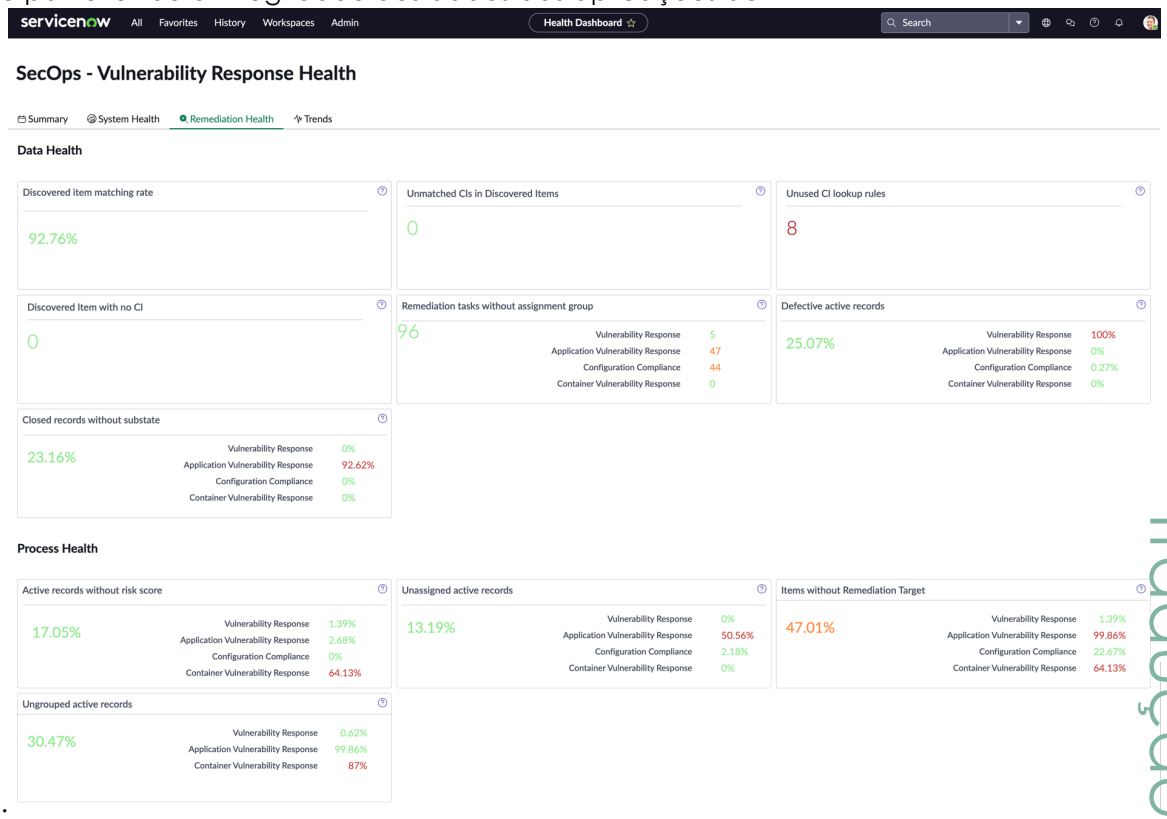


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Integridade de correção

Este painel exibe a integridade dos dados das aplicações de VR.



Guia Tendências

Este painel exibe as tendências das métricas de desempenho de ingestão de itens vulneráveis nos últimos 30 dias para as aplicações de VR.

Relatórios

Nota: Os valores de limite fazem parte do sistema de base. Você pode configurar os valores com base em seus requisitos.

Resumo

Título	Descrição
Integridade geral	Pontuação de integridade geral das aplicações de VR. Para obter mais informações, consulte os relatórios das métricas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo

Título	Descrição
Configuração	Integridade geral da configuração das aplicações de VR.
Integridade da implementação	Integridade geral de implementação das aplicações de VR.
Integridade da integração	Integridade geral de integração das aplicações de VR.
Desempenho	Pontuação geral de integridade de desempenho das aplicações de VR.
Integridade de dados	Integridade geral dos dados das aplicações de VR.
Integridade do processo	Pontuação geral de integridade do processo das aplicações de VR.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Configuração				
Regras de exclusão automática	Exibe o número de regras de exclusão automática habilitadas.	Revise e resolva as regras de exclusão automática inativas.	3	1
Fechar automaticamente registros obsoletos	Encerra automaticamente as detecções obsoletas. Para obter mais informações, consulte o tópico "Fechar automaticamente detecções obsoletas na Resposta a vulnerabilidades" em docs.servicenow.com.	Reduza o volume de detecções obsoletas. Habilite esta opção para fechar as detecções obsoletas que não são fechadas pelos scanners.	3	1
Integridade da implementação				
Inclusões de script personalizadas	Número de "inclusões de script" personalizadas.	Minimize "inclusões de script" personalizadas para facilitar os upgrades.	10	12

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Regras de negócio na tabela de detecções	Número de regras de negócio personalizadas na tabela de detecção.	Minimize as regras de negócio para facilitar os upgrades.	4	8
Regras de negócio personalizadas	Número de regras de negócio personalizadas antes da criação de registros no CMDB.	Use as regras de negócio padrão nos registros.	5	8
Conflitos de upgrade	Conflitos como regras de negócio e scripts identificados em um upgrade.	Revise e resolva os conflitos de upgrade.	10	15
PA instalado, mas não ativado	Indica se o painel do Performance Analytics não está habilitado.	Ative o painel do PA.	10	15
Integridade da integração				
Integrações desabilitadas	Número de integrações que foram desabilitadas.	Revise e habilite as integrações necessárias.	6	9
Execuções de integração com falha na última semana	Número de execuções de integração que não foram bem-sucedidas na última semana.	Revise e resolva a causa das execuções de integração com falha.	9	12
Desempenho				
Regras de negócio e scripts lentos	Regras de negócio e scripts com tempo médio de execução superior a 10 ms e contagem de execução superior a 10.000.	Revise e resolva as regras de negócio de execução lenta.	10	15

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Integrações paralisadas	Número de integrações que atingiram o tempo limite antes da conclusão.	Revise e resolva a causa das integrações paralisadas.	10	15
Trabalhos em segundo plano com falha ou parados	Trabalhos em segundo plano com falha ou com tempo esgotado na última semana.	Revise e resolva a causa dos trabalhos com falha.	5	10
Consultas lentas	Consultas cujo tempo médio de execução é maior que 10 ms e a contagem de execuções é maior que 10.000.	Revise e resolva as regras de negócio de execução lenta.	10	15

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Integridade de dados				
Taxa de correspondência de item descoberto	Número de itens descobertos correspondentes a ICs existentes.	Revise a integridade do seu CMDB e a lógica das regras de pesquisa de IC.	50	20
ICs incompatíveis em itens descobertos	Itens descobertos em estado incompatível.	Revise a integridade do seu CMDB e a lógica das regras de pesquisa de IC.	9	12
Regras de pesquisa de IC não utilizado	Regras de pesquisa de IC que não estão associadas a nenhum item descoberto.	Altere o status das regras de pesquisa de IC não utilizados para inativo.	4	6

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Item descoberto sem IC	Item descoberto sem item de configuração.	Revise e reaplique as regras de pesquisa de IC.	9	12
Registros ativos com defeito	Registros sem um item de configuração ou vulnerabilidade.	Descontinue os ICs usando a opção Gestão de ciclo de vida do IC do CMDB. **Nota:** A exclusão direta de ICs pode resultar em VITs órfãos.	40	60
Tarefas de correção sem grupo de atribuição	Tarefas de correção ativas cujo grupo de atribuição ainda não foi atribuído.	Atribua tarefas de correção a um grupo de atribuição e revise as regras de atribuição existentes.	40	60
Registros encerrados sem subestado	Registros que são encerrados sem um subestado.	Forneça informações no campo Motivo ao fechar os registros.	40	50
Integridade do processo				
Registros ativos sem pontuação de risco	Registros ativos com uma pontuação de risco de 0 ou sem pontuação de risco atribuída.	Revise e resolva as regras de risco.	40	60
Registros ativos não atribuídos	Registros sem um grupo de atribuição.	Atribua um grupo aos registros e revise as regras de atribuição existentes.	30	50
Itens sem meta de correção	Itens sem uma data de meta de correção.	Revise e resolva as regras de destino de correção. Essas	30	50

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
		regras devem incluir todos os registros.		
Registros ativos desagrupados	Registros que não estão incluídos em uma regra de tarefa de correção.	Revise as regras de tarefa de correção.	40	60

Tendências

Título	Descrição
Métricas de desempenho de ingestão de itens vulneráveis nos últimos 30 dias	Tempo médio necessário para ingerir itens vulneráveis e processar várias regras nos últimos 30 dias.

Modificando os valores de limite

Você pode modificar os valores de limite dos dados do painel de Integridade de VR do SecOps com base em suas preferências.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Integridade do Security Operations** > **Configuração** > **Métricas**.
2. Na página Dados do painel de integridade, abra o registro que você deseja modificar.
3. Atualize o registro e salve.

Painel Gestão de vulnerabilidade do (PA)

Rastreie o volume, o desempenho e o andamento das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado, por exemplo. Obtenha informações rapidamente sobre sua exposição a vulnerabilidades e quais serviços de negócio foram afetados.

Funções necessárias de Now Platform

Função necessária: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e usuários com sn_vul.vulnerability_read (ou que herdam a função sn_vul.vulnerability_read) e pa_viewer.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
Gerentes de TI, analistas de TI, responsáveis pela correção de vulnerabilidades	Ajude sua organização a lidar com o aumento de incidentes de segurança devido a vulnerabilidades exploradas, determinando com eficiência quais itens vulneráveis apresentam mais riscos. Esses painéis fornecem uma exibição gráfica da atividade de item vulnerável e ajudam a projetar planos de correção e andamento do status. Você pode se concentrar nos KPIs associados a ativos afetados críticos e vulnerabilidades de alta visibilidade.

Para exibir o painel Gestão de vulnerabilidades (PA), navegue até **Resposta a vulnerabilidades** > **Visão geral**.

Consulte relatórios que mostram dados de tendências ao longo do tempo. Relatórios com dados em tempo real estão listados abaixo. Visualize tendências de métricas importantes em uma programação regular para analisar seus processos de negócios gerais e identificar áreas de melhoria.

Para obter mais informações sobre como exibir seus relatórios de PA com pontuações em tempo real, consulte Exibir relatórios de Análise de desempenho para Resposta a vulnerabilidades [PA] em tempo real.

Tradução automática

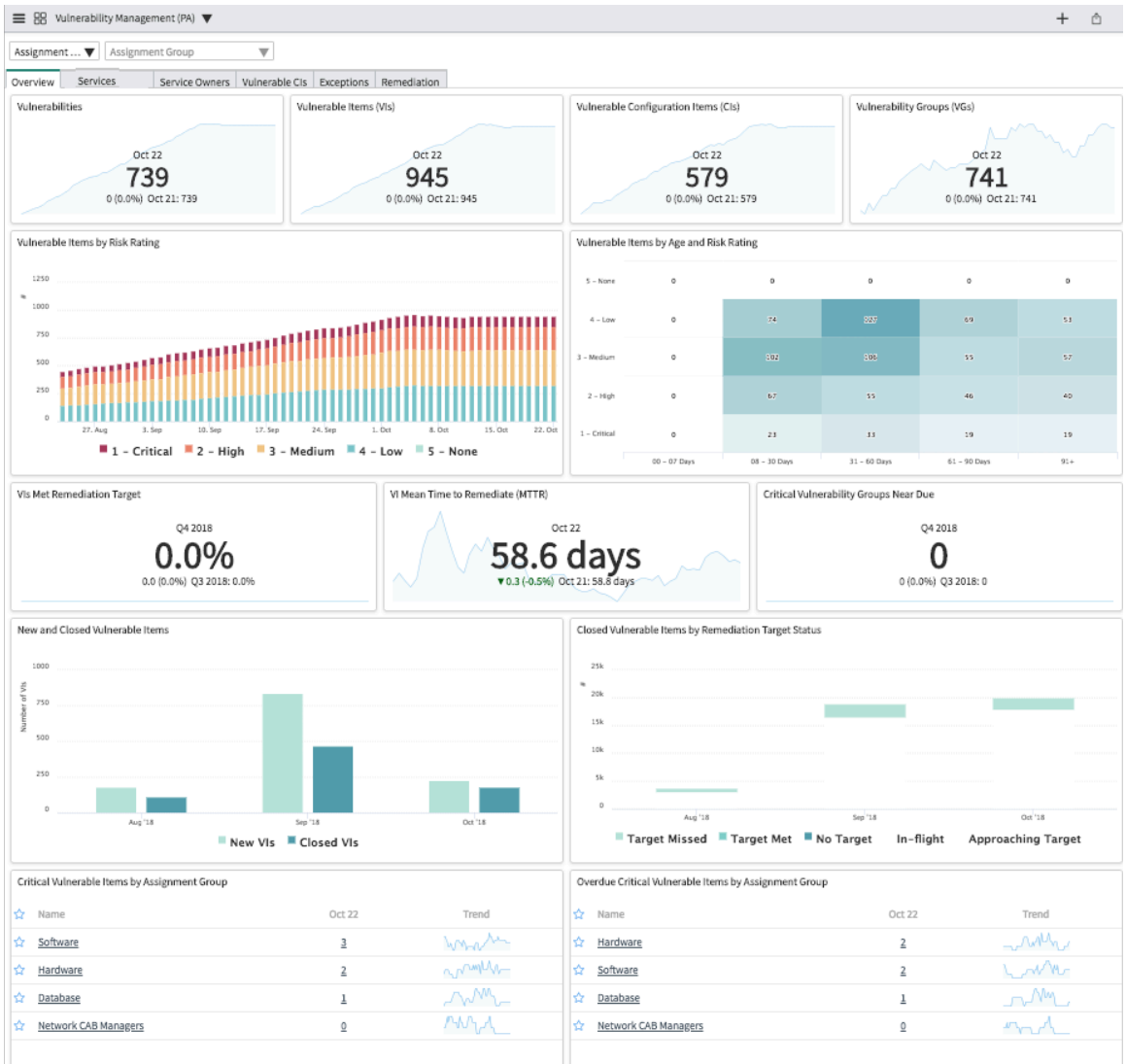
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As guias do painel da Gestão de vulnerabilidades [PA]

Guia Visão Geral

Este painel comunica os KPIs de risco e prevalência de vulnerabilidade, ativos afetados, cumprimento da meta de correção e andamento da correção.

Na guia Visão geral, você pode exibir o relatório Itens vulneráveis críticos por grupo de atribuição que é executado com base no trabalho agendado.



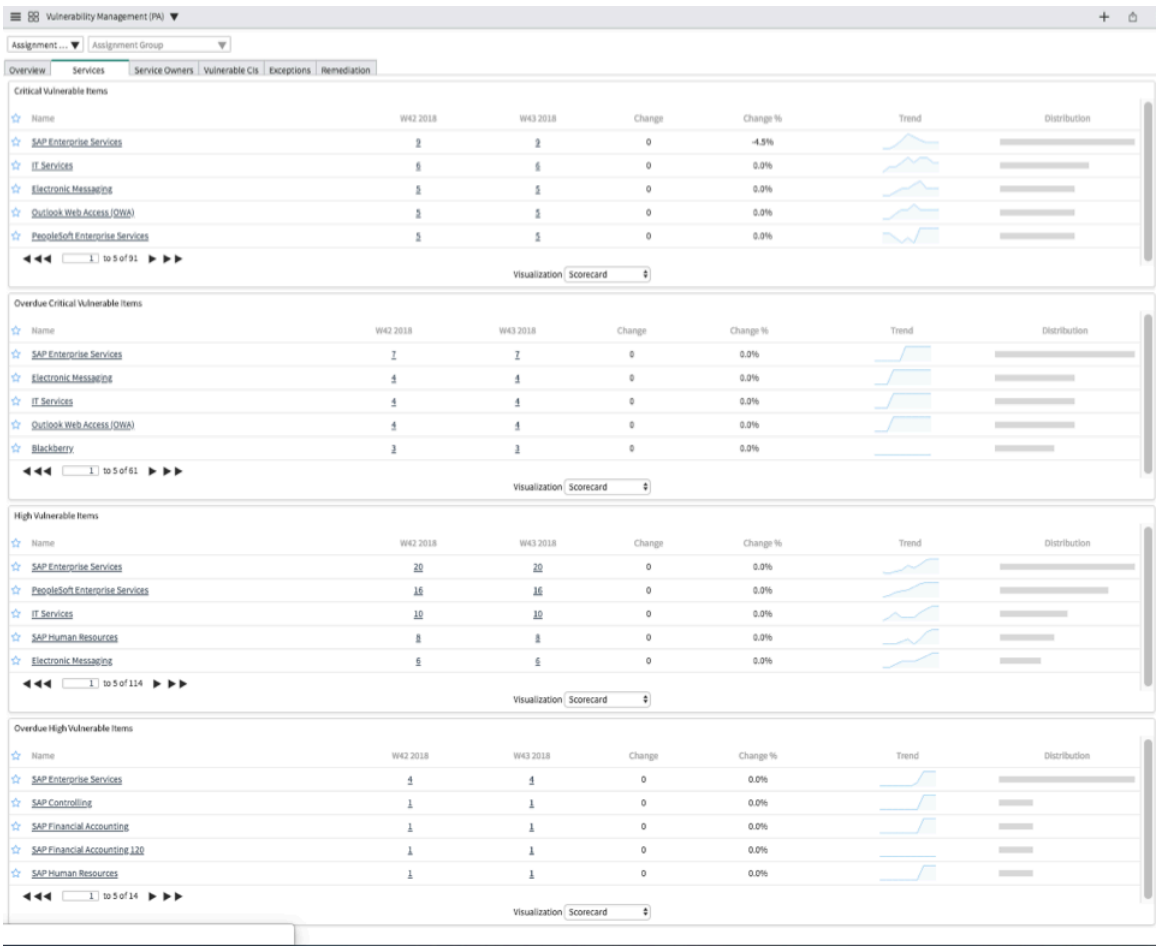
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Serviços de negócio

Este painel expõe o risco de vulnerabilidade no nível de serviço de negócios. Compartilhar essas informações em toda a organização pode ajudar os gerentes de serviço a corrigir vulnerabilidades de forma rápida e proativa e direcionar a organização para um modelo de responsabilidade compartilhada de segurança da informação.

Você pode mudar a classe de serviço para serviços técnicos ou de aplicações usando a propriedade do sistema `sn_vul.service_classifications`.

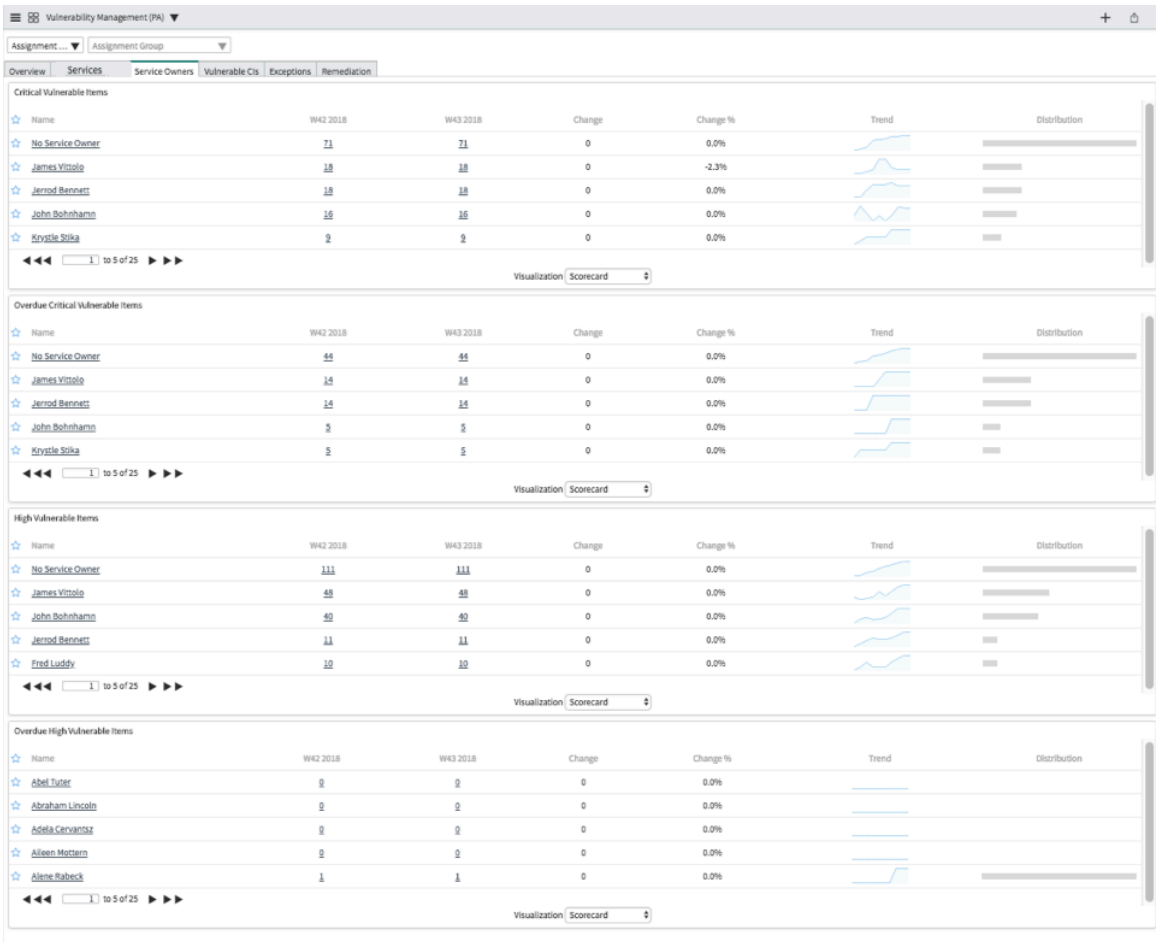


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Responsáveis pelo serviço

Este painel agrega o risco de vulnerabilidade do nível de serviço de negócio para os responsáveis pelo serviço - os executivos responsáveis por esses serviços de negócio. Ele mostra quais executivos estão assumindo o maior risco de vulnerabilidade e quais podem precisar de mais ajuda para incentivar atividades de correção imediata.



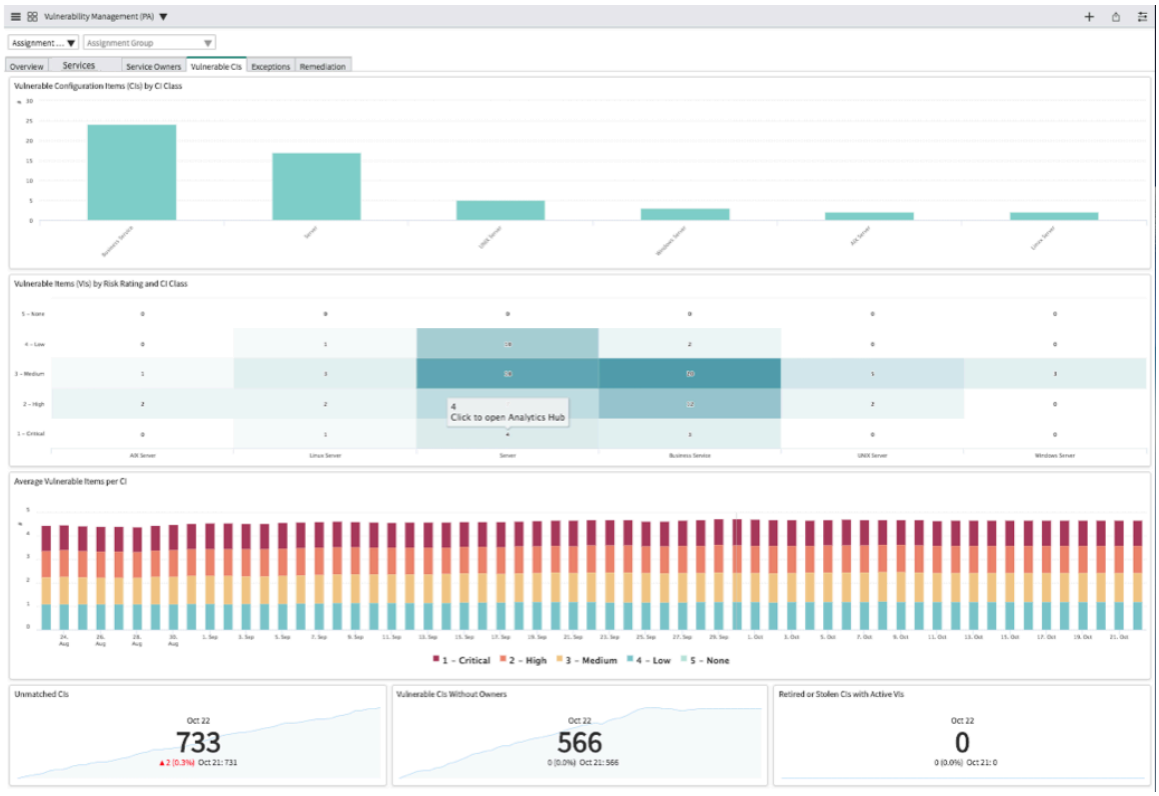
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia ICs vulneráveis

Este painel mostra o escopo e a composição de ICs com vulnerabilidades ativas e quais categorias de ICs precisam de mais atenção. Identifique ativos desativados com itens vulneráveis ativos e confirme se os ativos foram desativados. Exiba o número de ICs vulneráveis sem informações de propriedade para que você possa identificar proativamente os proprietários desses ativos antes que uma vulnerabilidade crítica afete esses sistemas.

Na guia ICs vulneráveis, você pode exibir os relatórios de ICs vulneráveis sem proprietários e ICs descontinuados ou roubados com IVs ativos em tempo real.



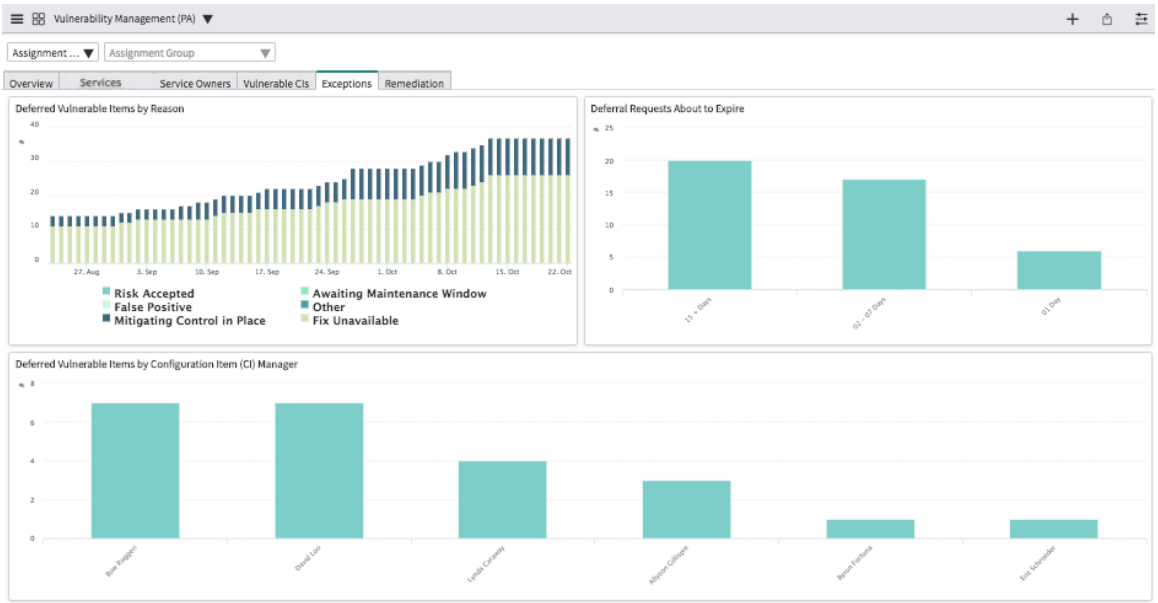
Guia Exceções

Este painel ajuda a entender onde sua organização está assumindo riscos devido a adiamentos potencialmente excessivos e a considerar as opções de correção.

Você pode exibir relatórios de itens vulneráveis adiados por motivo, solicitações de adiamento expirando, exceções para itens vulneráveis críticos por grupo de atribuição e solicitações de exceção por solicitante.

Tradução automática

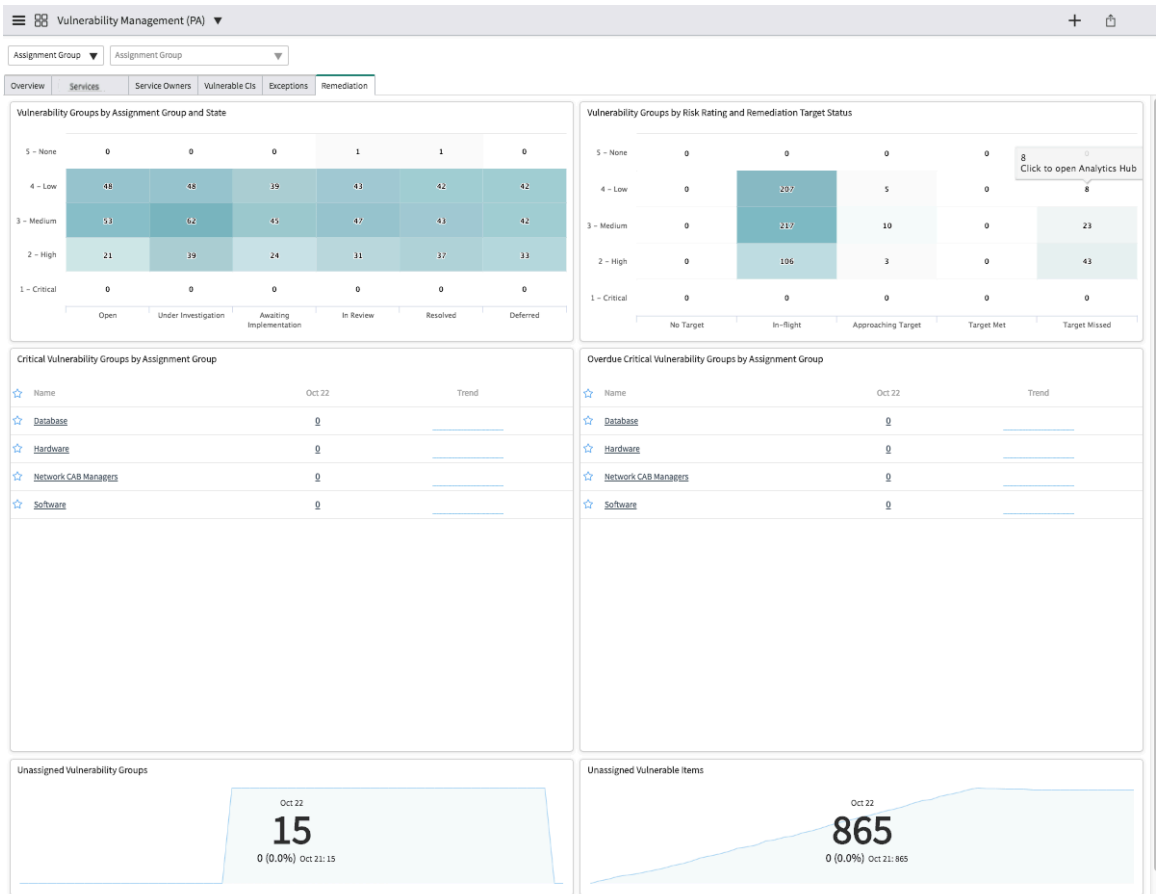
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Guia Correção

Este painel ajuda a entender o andamento de suas ações de correção e quais equipes de suporte precisam de mais assistência para concluí-las.

Na guia Correção, você pode exibir o relatório de Itens vulneráveis não atribuídos em tempo real.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Indicadores de Resposta a vulnerabilidades

Há vários indicadores usados para medir e rastrear o andamento da correção de vulnerabilidades na aplicação Resposta a vulnerabilidades.

A opção de coletar registros para os indicadores está desabilitada por padrão para a aplicação Resposta a vulnerabilidades. Esta opção está desabilitada para que determinados relatórios possam ser exibidos em tempo real. As informações de tendências usadas por esses indicadores ainda estarão disponíveis se você preferir habilitar a coleta de registros manualmente e a exibição dos registros que compõem as pontuações.

Vulnerabilidades distintas

Vulnerabilidades distintas com count_active_vi > 0. O objetivo é minimizar.

Itens vulneráveis críticos que estão atrasados mas não adiados

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Percentual de meta de correção atingida de itens vulneráveis

`([[Itens vulneráveis encerrados > Meta de correção = Meta atingida]] / [[Itens vulneráveis encerrados]]) * 100`. O objetivo é maximizar.

Itens vulneráveis não atribuídos

Todos os Itens vulneráveis ativos nos quais o Grupo de atribuição e os campos Atribuído a estão vazios. O objetivo é minimizar.

Itens vulneráveis críticos (serviços)

É a contagem na fonte de dados IVs Ativos (Serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de alta vulnerabilidade atrasados (serviços)

É a contagem na fonte de dados IVs Ativos (Serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Tarefas de correção não atribuídas

Todas as tarefas de correção ativas em que os campos Grupo de atribuição e Atribuído a estão vazios. O objetivo é minimizar.

Itens vulneráveis críticos

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Novos itens vulneráveis

É a contagem na fonte de dados VI.New, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens de configuração vulneráveis

É a contagem distinta na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Soma da duração de itens vulneráveis encerrados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É a soma na fonte de dados VI.Closed, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Tarefas de correção não adiadas

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Tempo médio de correção do item vulnerável

```
[[Soma da duração de itens vulneráveis encerrados]]/[[Itens vulneráveis encerrados]]
```

Itens vulneráveis críticos atrasados (serviços)

É a contagem na fonte de dados IVs Ativos (Serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de configuração desativados

É a contagem distinta na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Solicitações de adiamento

É a contagem na fonte de dados Solicitações de adiamento ativas, que está usando a tabela: sn_vul_change_approval. O objetivo é minimizar.

Itens vulneráveis por itens de configuração

É a contagem de ICs de fonte de dados com IVs ativos, que está usando a tabela: sn_vul_analytics_vi_ci_class. O objetivo é minimizar.

Itens vulneráveis encerrados

Os itens vulneráveis encerrados são medidos diariamente em unidades numéricas. O objetivo é maximizar.

Itens de configuração incompatíveis

Lista os hosts descobertos por scanners de vulnerabilidade de terceiros que não correspondem a nenhum IC existente no CMDB.

Tarefas de correção crítica que estão atrasadas mas não adiadas

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens de configuração vulneráveis sem grupo de suporte

É a contagem na fonte de dados VI.Open, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Tarefas de correção crítica sem postergação

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens vulneráveis adiados

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens de alta vulnerabilidade (serviços)

É a contagem na fonte de dados IVs Ativos (Serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de configuração distintos com itens vulneráveis ativos

É a contagem distinta em ICs de fonte de dados com IVs ativos, que está usando a tabela: sn_vul_analytics_vi_ci_class. O objetivo é minimizar.

Número médio de itens vulneráveis por item de configuração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

`[[Itens vulneráveis ativos]] / [[ICs vulneráveis]]`. O objetivo é minimizar.

Tarefas de correção

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens vulneráveis adiados

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Solicitações de adiamento (criadas)

É a contagem na fonte de dados Closed.Requests, que está usando a tabela: sn_vul_change_approval. O objetivo é minimizar.

Detalhamentos

Os seguintes nomes de detalhamento se aplicam aos indicadores no painel:

- Idade
- Momento do fechamento
- Grupo de atribuição
- Classe do IC
- Gerenciador de IA
- Idade do Adiamento
- Motivo do Adiamento
- Solicitantes da exceção
- Explorar Vetor de Ataque
- Explorar Itens Existentes
- Explorar Nível de Habilidade
- Regra de meta de correção
- Status da meta de correção
- Status da meta de correção (Encerrado)
- Pontuação de risco
- Serviço
- Importância do Serviço
- Responsável pelo serviço
- Gravidade
- Estado

Fonte de detalhamento

- Grupo de atribuição: aplica-se a relatórios VI ou e RT
- Exploração existente: aplica-se a relatórios de VI.
- Explorar vetor de ataque: aplica-se a relatórios de VI.
- Nível de habilidade de exploração: aplica-se a relatórios de IV.
- Status da meta de correção: aplica-se a relatórios VI e RT.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Classificação de risco: aplica-se a relatórios VI e RT.
- Estado: aplica-se a relatórios VI e RT.

Visualizações de dados

Título	Tipo	Descrição
Vulnerabilidades	Pontuação	Número de vulnerabilidades associadas a um ou mais itens vulneráveis ativos.
Itens vulneráveis (IVs)	Pontuação	Número de itens vulneráveis ativos (não encerrados).
Itens de configuração (ICs) vulneráveis	Pontuação	Número de itens de configuração (ICs) associados a um ou mais itens vulneráveis ativos.
Tarefas de correção	Pontuação	Número de tarefas de correção ativas (não encerradas).
Itens vulneráveis por classificação de risco	Barra de barra	Número de itens vulneráveis ativos, agrupados por classificação de risco no período selecionado.
Itens vulneráveis por idade e classificação de risco	Mapa térmico	Número de itens vulneráveis ativos agrupados por classificação de risco e idade (em dias).
Meta de correção atendida de IVs	Pontuação	Percentual de itens vulneráveis encerrados que atenderam às datas de meta de correção nos trimestres atual e anterior. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medidos como incrementos de 24 horas).
Tempo médio de correção (MTTR) de IVs	Pontuação	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
		Nota: O valor de Idade fechada é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e hora do trabalho de coleta.
Tarefas de correção críticas próximas ao vencimento	Pontuação	Número de tarefas de correção ativas que se aproximam da data de meta de correção. A data de meta de correção de uma tarefa de correção é definida como a data de vencimento mais próxima pertencente a um item vulnerável ativo no grupo. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medidos como incrementos de 24 horas). Este relatório exclui tarefas de correção adiadas.
Itens vulneráveis novos e encerrados	Barra de barra	Número de itens vulneráveis novos e encerrados no período selecionado. **Nota:** O valor de Idade fechada é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e hora do trabalho de coleta.
Itens vulneráveis encerrados por status da meta de correção	Barra de barra	Número de itens vulneráveis encerrados, agrupados por status da meta de correção no período selecionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
		Nota: O valor de Idade fechada é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e hora do trabalho de coleta.
Itens vulneráveis críticos por grupo de atribuição	Lista e linha Ícone	Número de itens vulneráveis ativos, com uma classificação de risco crítica, agrupados por grupo de atribuição.
Itens vulneráveis críticos e atrasados por grupo de atribuição	Lista e linha Ícone	Número de itens vulneráveis ativos com uma classificação de risco crítica e após as datas de meta de correção, agrupados por grupo de atribuição. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medidos como incrementos de 24 horas). Este relatório exclui itens vulneráveis adiados.

Serviços de negócio

Nome	Tipo	Descrição
Itens vulneráveis críticos	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de risco crítica, agrupados por serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens vulneráveis críticos	Lista, linha e barra de distribuição	Número de itens vulneráveis ativos com uma classificação de risco crítica e após as datas de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Serviços de negócio

Nome	Tipo	Descrição
que estão atrasados	Ícone de de	meta de correção, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.
Itens de alta vulnerabilidade	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de alto risco, agrupados por serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens de alta vulnerabilidade atrasados	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de risco alta e após as datas de meta de correção, agrupados por serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.

Responsáveis pelo serviço

Nome	Tipo	Descrição
Itens vulneráveis críticos	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de risco crítica, agrupados por responsável pelo serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Responsáveis pelo serviço

Nome	Tipo	Descrição
		A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens vulneráveis críticos que estão atrasados	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de risco crítica e após as datas de meta de correção, agrupados por responsável pelo serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.
Itens de alta vulnerabilidade	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de alto risco, agrupados por responsável pelo serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens de alta vulnerabilidade atrasados	Lista, linha e barra de distribuição Ícone de de	Número de itens vulneráveis ativos com uma classificação de risco alta e após as datas de meta de correção, agrupados por responsável pelo serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.

ICs Vulneráveis

Nome	Tipo	Descrição
Itens de configuração (ICs) vulneráveis por classe de IC	Barra de barra	Números de itens de configuração com vulnerabilidades ativas, agrupados por classe de IC no CMDB.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ICs Vulneráveis

Nome	Tipo	Descrição
Itens vulneráveis (VIs) pela Classe de IC	Mapa mapa de árvore	Número de IVs ativos divididos por classe de IC.
Média de Itens vulneráveis por IC	Barra de barra	Número médio de itens vulneráveis que pertencem a um item de configuração, agrupados conforme a classificação de risco.
ICS incompatíveis	Pontuação	Número de itens de configuração importados que não correspondem a nenhum IC existente no CMDB.
ICS vulneráveis sem grupo de suporte	Pontuação	Número de itens de configuração vulneráveis que não têm um grupo de suporte atribuído.
ICs desativados ou roubados com IVs ativos	Pontuação	Número de itens de configuração marcados como Descontinuados ou **Roubados** no **CMDB** que têm itens vulneráveis ativos.

Exceções

Nome	Tipo	Descrição
Itens vulneráveis adiados por motivo	Barra de barra	Número de itens vulneráveis adiados, agrupados por motivo de adiamento.
Solicitações de adiamento prestes a expirar	Barra de barra	Número de solicitações de adiamento associadas a tarefas de correção ou itens vulneráveis que estão prestes a ser reabertos para revisão. Eles são agrupados pelo número de dias restantes até a reabertura. Se as notificações por e-mail forem definidas, um e-mail será enviado.
Itens vulneráveis adiados por gerenciador de item de configuração (IC)	Barra de barra	Número de itens vulneráveis adiados agrupados pelo gerente do item de configuração associado.

Correção

Nome	Tipo	Descrição
Tarefas de correção por classificação de risco e estado	Mapa térmico	Número de tarefas de correção ativas agrupadas por classificação de risco e estado.
Tarefas de correção por classificação de risco e status da meta de correção	Mapa térmico	Número de tarefas ativas agrupadas por classificação de risco e status da meta de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Correção

Nome	Tipo	Descrição
		Este relatório exclui itens vulneráveis adiados.
Tarefas de correção críticas por grupo de atribuição	Lista e linha Ícone	Número de tarefas de correção ativas com uma classificação de risco crítica agrupadas por grupo de atribuição. Este relatório exclui tarefas de correção adiadas.
Tarefas de correção críticas em atraso por grupo de atribuição	Lista e linha Ícone	Número de tarefas de correção ativas com uma classificação de risco crítica e após as datas de meta de correção, agrupadas por grupo de atribuição. Este relatório exclui tarefas de correção adiadas.
Tarefas de correção não atribuídas	Pontuação	Número de tarefas de correção ativas sem um atribuído ou grupo de atribuição.
Itens vulneráveis não atribuídos	Pontuação	Número de itens vulneráveis ativos sem um atribuído ou grupo de atribuição.

Exibir Performance Analytics para Resposta a vulnerabilidades [PA] relatórios em tempo real

Para gerenciar seus itens vulneráveis (IVs) mais importantes e ajudá-lo a corrigi-los rapidamente, exiba relatórios sob demanda, em tempo real no painel Gestão de vulnerabilidades (PA). A aplicação Performance Analytics para Resposta a vulnerabilidades está disponível com uma assinatura separada do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Para obter mais informações sobre os relatórios de Performance Analytics para Resposta a vulnerabilidades, consulte Painel de Gestão de vulnerabilidades [PA].

Para obter mais informações sobre a configuração e a instalação da aplicação Performance Analytics para Resposta a vulnerabilidades, consulte Instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades [PA].

Se não for exibido, para exibir o painel, navegue até **Resposta a vulnerabilidades** > **Visão geral**. Na parte superior do painel, as guias de relatório são exibidas.

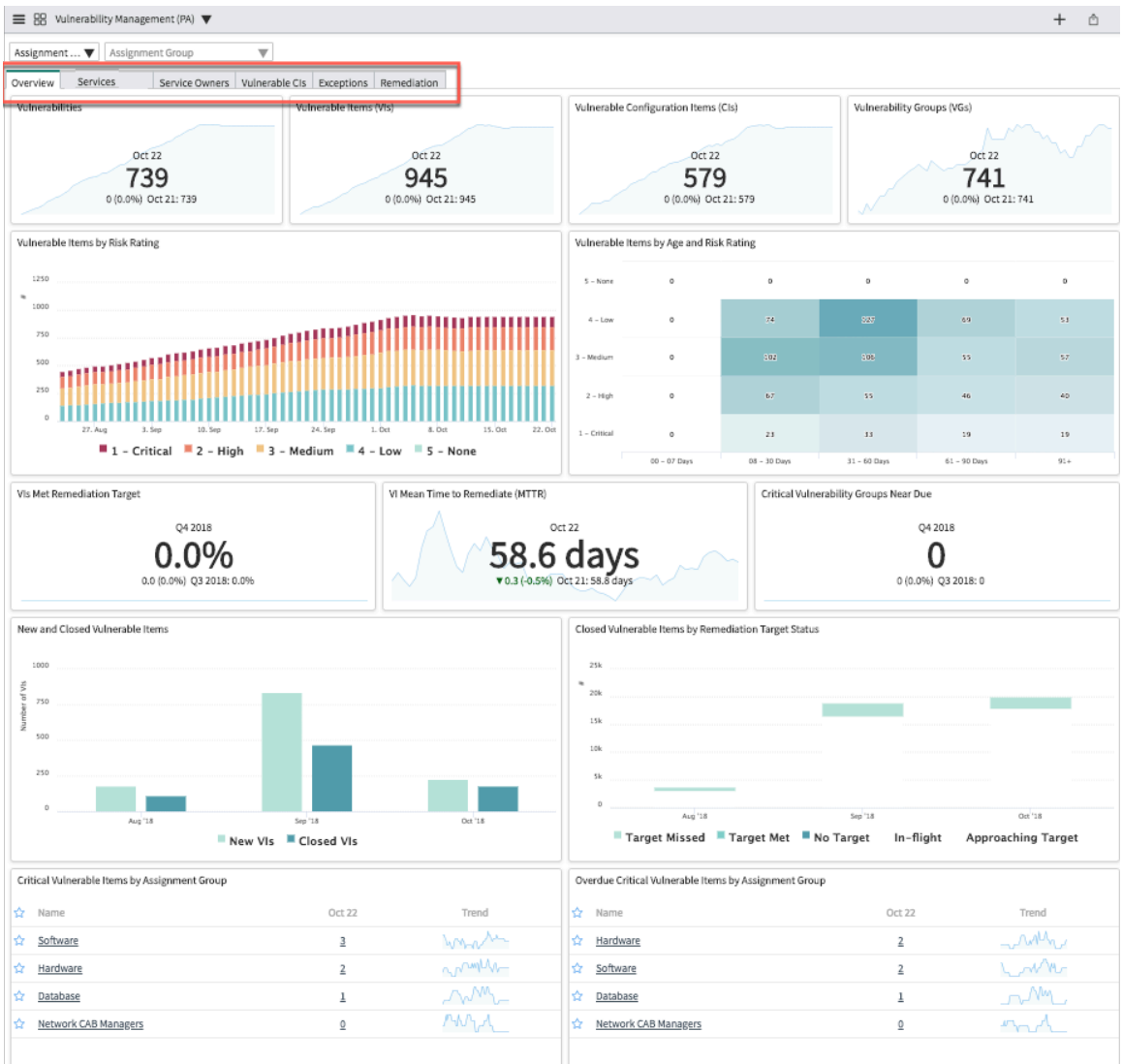
A partir da versão 19.0 do Resposta a vulnerabilidades, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e Painéis no espaço de correção de TI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Guia Visão Geral



Exiba os relatórios a seguir nas guias do painel Gestão de vulnerabilidades (PA) em tempo real.

- Guia Visão Geral
  - Itens vulneráveis críticos por grupo de atribuição
- Guia ICs vulneráveis:
  - ICs vulneráveis sem responsáveis
  - ICs desativados ou roubados com IVs ativos
- Guia Exceções:
  - Itens vulneráveis adiados por motivo
  - Solicitações de adiamento prestes a expirar
  - Itens vulneráveis adiados por gerente de CIO
- Guia Correção:
  - Itens vulneráveis não atribuídos

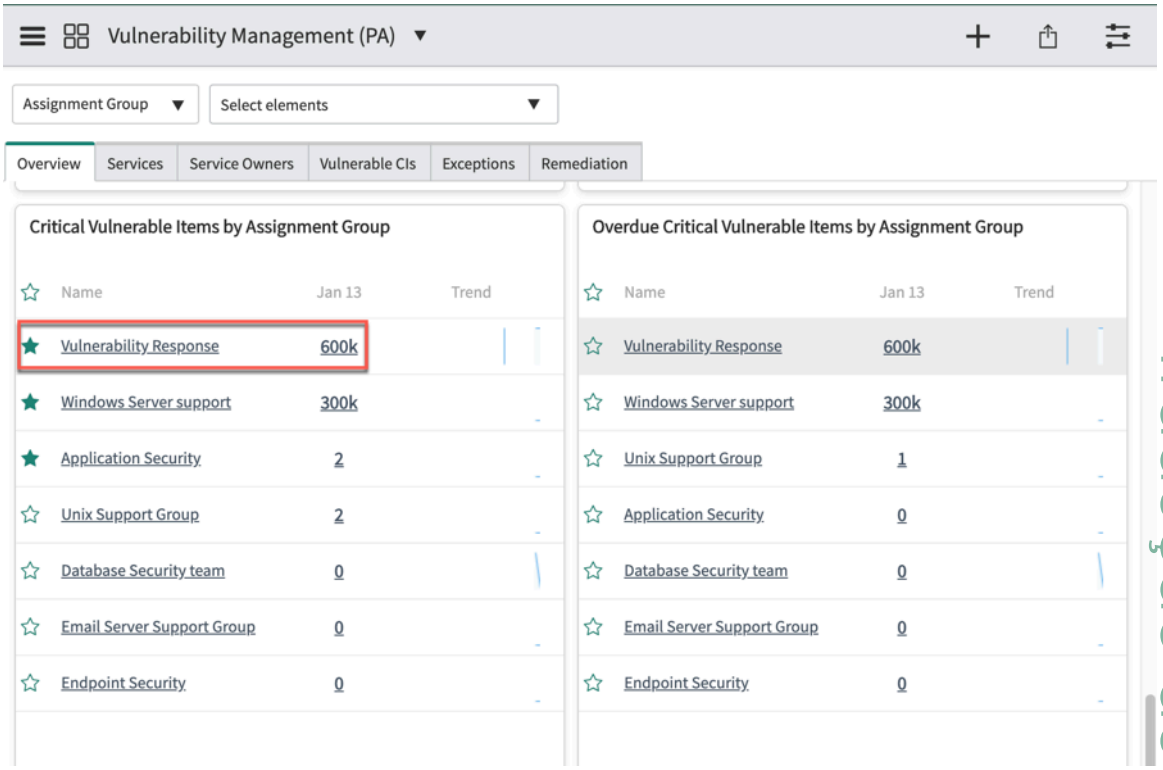
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

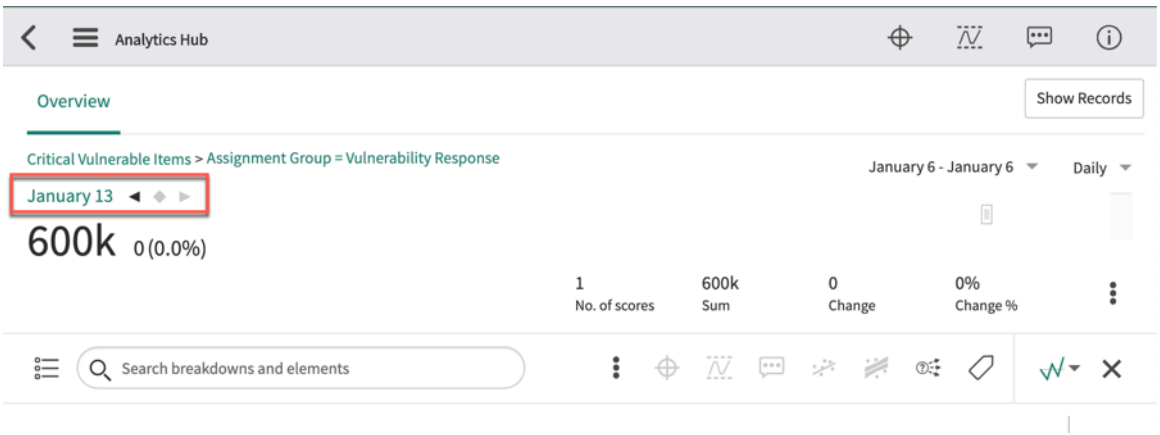
Para exibir pontuações em tempo real, com uma das guias selecionadas que contém relatórios em tempo real, siga estas etapas:

Procedimento

1. No relatório, por exemplo, Itens vulneráveis críticos por grupo de atribuição, clique em um dos links exibidos.



2. No registro exibido, clique na data.

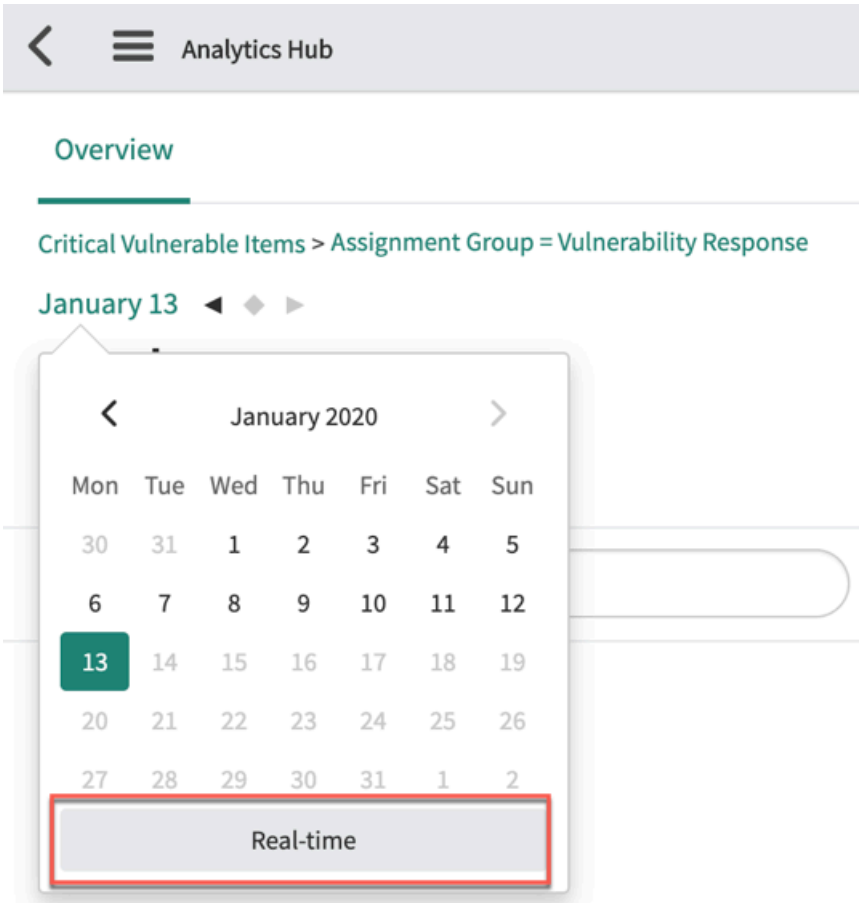


3. No calendário exibido, clique em Tempo real.

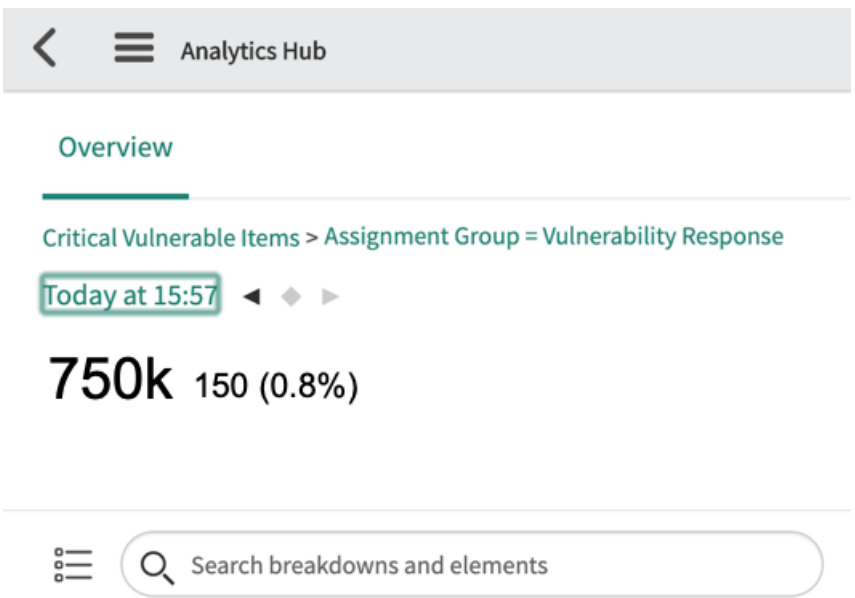
   Se um relatório não for compatível com uma pontuação em tempo real, o botão Tempo real não será exibido no calendário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Pode levar alguns minutos para que o valor seja atualizado. A data atual, os registros, o número de novos registros desde o último relatório e a mudança percentual do último relatório também são exibidos.



4. Opcional: Para exibir os registros que compõem o relatório, com o relatório em tempo real exibido, no canto superior direito, clique em **Mostrar registros**.
   Uma lista de registros que compõem a pontuação é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir os indicadores [Performance Analytics para Resposta a vulnerabilidades [PA]

Exiba indicadores Performance Analytics automatizados e formulados que representam os dados de vulnerabilidade em sua instância.

Antes de Iniciar

A opção de coletar registros para os indicadores está inativa por padrão para a aplicação Performance Analytics - Content Pack Vulnerability Response. Esta opção está desabilitada para que determinados relatórios possam ser exibidos em tempo real. As informações de tendências usadas por esses indicadores ainda estarão disponíveis se você preferir habilitar a coleta de registros manualmente e a exibição dos registros que compõem as pontuações.

Nota: Ativar a coleta de registros em um indicador pode afetar seu desempenho e aumentar consideravelmente o tempo e a memória necessários para executar o trabalho de coleta de dados.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou pa.viewer

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades tem indicadores automatizados e formulados.

Termos principais

Indicador de PA

Define uma medida de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional, por exemplo, Itens vulneráveis críticos atrasados não adiados.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, VI ativo.

Coletar registros

Quando habilitado, armazena registros na memória e fornece acesso ao Hub de análise.

Detalhamentos

Filtro de Detalhamentos e registros coletados por grupo. Os detalhamentos podem aumentar o uso da memória, especialmente à medida que o número e a diversidade aumentam.

Exclusões de detalhamento

As exclusões removem determinados detalhamentos, o que pode reduzir o consumo de memória.

Procedimento

1. Para indicadores automatizados, navegue até **Análise de desempenho** > **Indicadores** > **Indicadores Automatizados**.
2. Para indicadores formulados, navegue até **Análise de desempenho** > **Indicadores de Fórmula**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter informações detalhadas sobre indicadores, consulte Indicadores de Análise de desempenho .

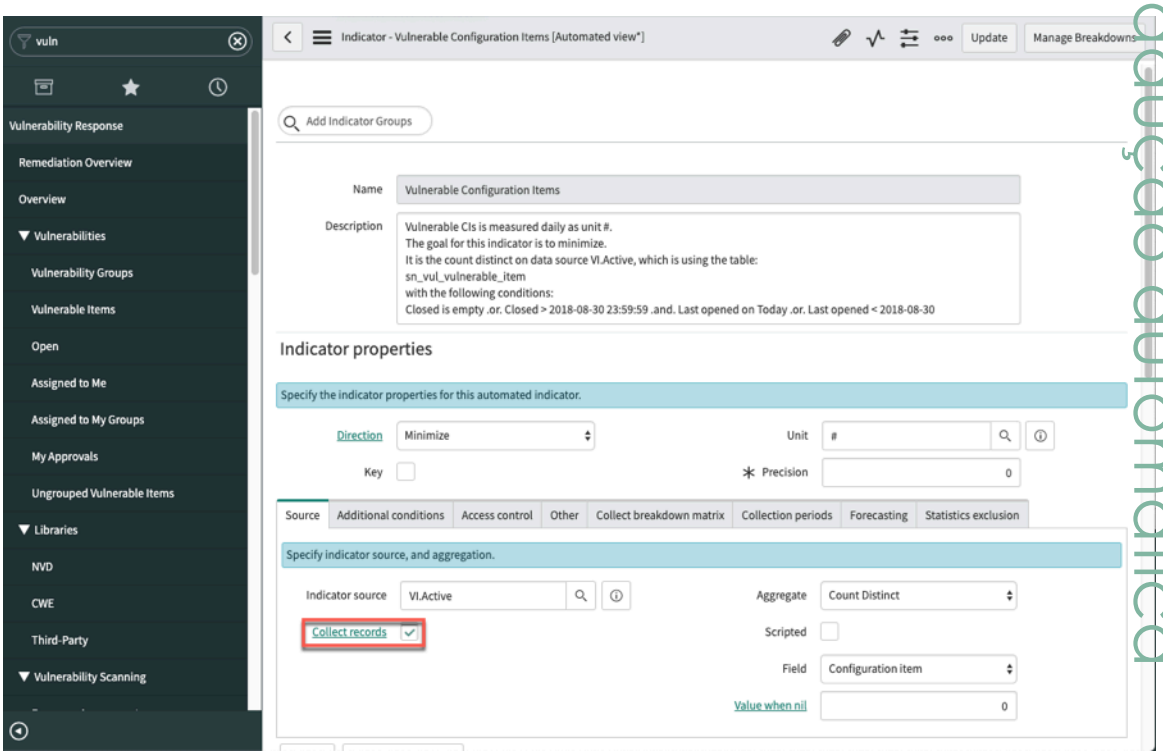
3. Em qualquer um dos casos, pesquise em **Aplicação** > **Análise de desempenho**.

> **Nota:** Se não estiver na exibição padrão, adicione a coluna **Aplicação** usando o ícone de) no canto superior esquerdo da página. A coluna Aplicação é exibida no menu suspenso Pesquisar.

4. Opcional: Para habilitar Coletar registros em um indicador do Performance Analytics para Resposta a vulnerabilidades, siga estas etapas:

   a. Com a lista de indicadores automatizados exibida, na coluna Nome, clique no indicador para o qual você deseja habilitar a coleta de registros.
   O registro do indicador é exibido.

   b. Na seção Propriedades do indicador com a guia Origem selecionada, marque a caixa de seleção Coletar registros.



   c. Escolha um para continuar.

Opção	Descrição
Atualizar	Salve suas edições e retorne à lista de Indicadores.
Gerenciar Detalhamentos	Reative detalhamentos de segundo nível para os indicadores listados ou edite detalhamentos para outros indicadores.

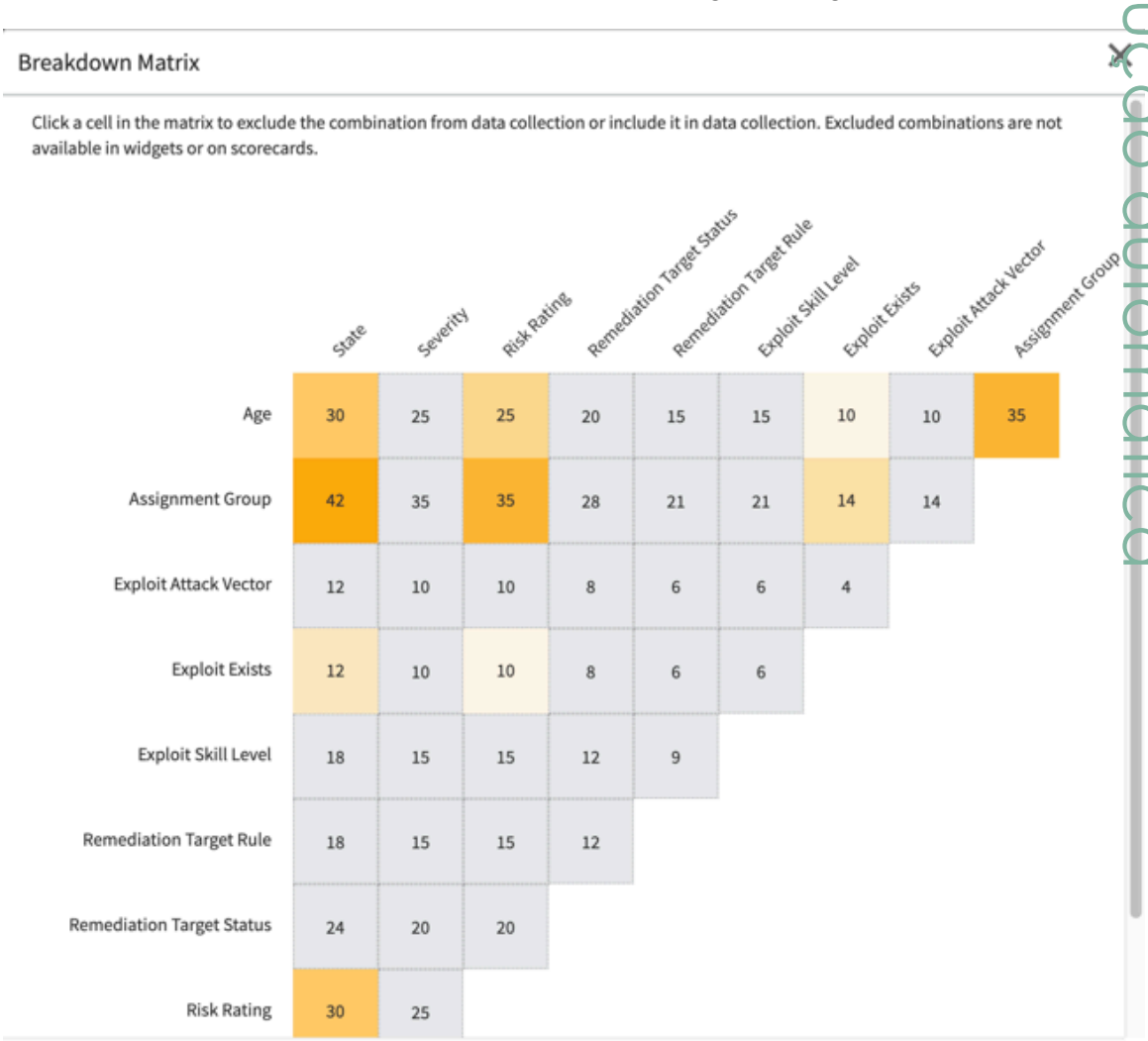
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Nota: Se você optar por reativar os detalhamentos de segundo nível, poderá aumentar significativamente o consumo de memória e tornar mais lento o trabalho de coleta de dados. Por padrão, as exclusões de detalhamento de segundo nível foram aplicadas aos seguintes indicadores: ▪ Itens de configuração vulneráveis ▪ ICs descontinuados ▪ IVs adiados	(Optional) Para obter mais informações sobre detalhamentos do Performance Analytics, consulte Detalhamentos do Performance Analytics .

d. Clique **em Gerenciar Detalhamentos**.

e. No formulário exibido, clique em **Configurar matriz de detalhamento**.
O formulário Matriz de detalhamento é exibido. As combinações excluídas são selecionadas e exibidas com cores, conforme mostrado na figura a seguir.



f. Para remover a exclusão e reativar uma combinação excluída, clique em uma célula selecionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

g. No canto superior direito do formulário, clique em **Fechar** para retornar ao formulário Gerenciar Detalhamento.

h. Clique na seta de retorno para retornar ao registro do indicador.

i. Clique em **Atualizar** para salvar suas edições e retornar à lista de Indicadores.

Resposta a vulnerabilidades informações de referência

Os tópicos a seguir fornecem links, informações de referência, solução de problemas e artigos de conhecimento, além de dados de campo nos formulários e registros encontrados em Resposta a vulnerabilidades.

Abaixo estão listados alguns links para outros recursos que podem ser úteis, começando com um link para os links da base de conhecimento para suporte e solução de problemas do artigo VR/CC na Base de conhecimento HI.

- Links da base de conhecimento para suporte e solução de problemas de VR/CC
- Para obter mais informações sobre aplicações e compatibilidade, consulte KB0856498 Mudanças no esquema de versão e matriz de compatibilidade da Resposta a vulnerabilidades .
- Vídeos das Operações de segurança
- Desenvolver treinamento
- Desenvolver documentação
- Trabalhe com um especialista em implementação para alcançar os resultados de negócios desejados com a Central de sucesso do cliente .
- Faça um curso do Vulnerability Response para adquirir conhecimento e obter ROI mais rapidamente. Para se inscrever, consulte Treinamento e certificação da ServiceNow .
- Localizar componentes instalados com uma aplicação
- Orquestração de resposta a vulnerabilidades
- Dicas para escrever integrações
- Fazer ou responder a perguntas na comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Check-list de implementação da aplicação Resposta a vulnerabilidades

Esta check-list lista as etapas necessárias para uma implementação básica da aplicação Resposta a vulnerabilidades em sua instância Now Platform®. Quando você concluir essas tarefas, o sistema de base estará pronto para operação e verificação.

Antes de Iniciar

Funções necessárias: administrador para baixar e ativar aplicações e atribuir funções, sn_vul.vulnerability_admin para configurar Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Considere criar e imprimir um PDF desta check-list para que você possa marcar as tarefas conforme as conclui.
2. Para gerar um PDF, clique no ícone Salvar como **PDF** (ícone) na parte superior do tópico e clique em Tópico selecionado.

Resposta a vulnerabilidades tarefas básicas de check-list de implementação para administrador

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você obteve direitos e baixou (**instalar**) as seguintes aplicações da ServiceNow® Store na sua instância Now Platform : ◦ Resposta a vulnerabilidades ◦ Resposta a vulnerabilidades Integração com o banco de dados nacional de vulnerabilidades do NIST ◦ Qualys Integração para Operações de segurança **a.** Para verificar se as aplicações estão disponíveis em sua instância, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e pesquise [sn_vul], [sn_vul_nvd] e [sn_vul_qualys]. **b.** Se você não conseguir localizar as aplicações, consulte para obter mais informações sobre como obter direitos e baixar as aplicações.
☐	Como um usuário com a função de administrador, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação de aplicação de integração** e ative (**Instale**) a aplicação Resposta a vulnerabilidades junto com suas dependências na sua instância Now Platform. **Nota:** Durante a instalação da aplicação Resposta a vulnerabilidades, você tem a opção de instalar dados de demonstração. Os dados de demonstração serão necessários se você quiser executar testes automatizados para confirmar que sua instância funciona após a instalação. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção para evitar corrupção e indisponibilidade de dados. Se forem criados dados de demonstração ou contas de demonstração, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção. O Assistente de configuração para Resposta a vulnerabilidades é instalado automaticamente junto com a aplicação. O Assistente de configuração é necessário para configurar a aplicação Resposta a vulnerabilidades. Além disso, ele é usado para instalar e configurar a aplicação Qualys Integration for Security Operations usada neste exemplo, bem como outras aplicações que oferecem suporte e são compatíveis com Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações sobre como instalar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades.
☐	Como um usuário com a função de administrador, no Assistente de configuração, navegue até **Todos** > **Grupos e usuários da Resposta a vulnerabilidades** e atribua usuários com as funções de persona Resposta a vulnerabilidades necessárias. **a.** No Assistente de configuração, exiba os usuários existentes e as funções já atribuídas clicando no link **do módulo Administração de usuários**. **b.** Na lista, clique em um nome de usuário para abrir o registro e clique na lista relacionada **Funções**. Todas as funções atribuídas a este usuário são exibidas. **c.** Navegar de volta para **Grupos e usuários da Resposta a vulnerabilidades** no Assistente de configuração e siga os avisos para atribuir a função sn_vul.vulnerability_admin. **Nota:** A função sn_vul.vulnerability_admin é necessária para continuar com a configuração. Como alternativa, você pode continuar com a configuração como um usuário com a função de administrador. (Opcional) Você também pode atribuir as funções de Gerente de item de configuração (IC) [sn_vul.ci_manager] e de Aprovador de exceção [sn_vul.exception_approver], mas essas personas não são necessárias para as tarefas de configuração restantes. Para obter mais informações sobre como atribuir as funções de persona usando o Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre usuários e atribuição de funções a usuários e grupos, consulte Administração de usuários .
☐	**a.** Navegar até **Todos** > **Administração** > **Integrações** e verifique se a **Integração do CWE Abrangente 2000** está ativada e execute o trabalho agendado para importar dados. **b.** Como um usuário com a função de administrador, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** e ative (**Instalar**) a aplicação Integração de resposta a vulnerabilidades com NVD. Execute as integrações de NVD e CWE como parte da configuração inicial de Resposta a vulnerabilidades e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros e Configure e execute o trabalho agendado para atualizar registros de CWE para obter mais

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	informações sobre como instalar, configurar e exibir as bibliotecas do NVD e do CWE.
☐	Como um usuário com a função de administrador, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação de aplicação de integração** e ative a aplicação Qualys Integration for Security Operations. Antes de instalar e executar um produto de scanner de terceiros como Qualys que tenha uma biblioteca, você deve primeiro instalar e executar as integrações de NVD e CWE para ingerir dados de vulnerabilidade. Para obter mais informações, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.
☐	(Opcional) Como um usuário com a função de administrador, se você instalou dados de demonstração com a aplicação Resposta a vulnerabilidades, poderá executar o pacote de testes Resposta a vulnerabilidades ATF para verificar se as aplicações foram instaladas com sucesso. **Nota:** Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção para evitar corrupção e indisponibilidade de dados. Para obter mais informações, consulte Executar o pacote de testes Automated Test Framework (ATF) para Resposta a vulnerabilidades. Para obter mais informações sobre testes automatizados, consulte Automated Test Framework (ATF) .

3. Continue com a configuração das aplicações iniciando na seção Configurações da Resposta a vulnerabilidades.

   A revisão dessas configurações ajuda a entender como Resposta a vulnerabilidades funciona conforme você continua a configurar seu ambiente. Para a integração de scanner usada neste exemplo, é necessário editar as configurações.

   Os conceitos usados neste exemplo de configuração para o produto Qualys se aplicam a outras aplicações de scanner.

   Suas Qualys credenciais são necessárias para configurar a aplicação. Verifique se você tem nomes de contas, senhas e outras informações de serviço exigidas pelos produtos Qualys para que você tenha acesso a eles.

   Funções necessárias: sn_vul.vulnerability_admin ou, alternativamente, admin.

Resposta a vulnerabilidades tarefas básicas de check-list de implementação para administrador de vulnerabilidades

Tarefa	Descrição
☐	Revise as Regras de atribuição de vulnerabilidade. As regras de atribuição atribuem automaticamente itens vulneráveis (VIs) ao grupo de atribuição apropriado. Para obter mais informações,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Para obter mais informações sobre como configurar Resposta a vulnerabilidades usando o Assistente de configuração, consulte Configuração de Resposta a vulnerabilidades usando o Assistente de configuração.
☐	Revise as regras de tarefa de correção. As regras de tarefa de correção agrupam automaticamente os itens vulneráveis (IVs) conforme são importados com base em determinadas condições. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral.
☐	Revise as calculadoras de risco. Calculadoras de risco pontuam itens vulneráveis para priorização. Você pode configurar calculadoras para incorporar características do item de configuração (IC), explorar a disponibilidade e a gravidade da vulnerabilidade relatada pelo seu fornecedor de avaliação de vulnerabilidade (scanner). Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
☐	Revise as Regras de destino de correção. As Regras de destino de correção definem linhas do tempo de correção para IVs e tarefas de correção. Para obter mais informações, consulte Resposta a vulnerabilidades regras de destino de correção.
☐	Na seção Configuração de integração, revise as configurações da aplicação Qualys e defina e programe suas importações de dados. **a.** Clique **em Integrações de scanner**. **b.** Na página Aplicações instaladas, clique em **Editar**. **c.** Insira suas credenciais e clique em **Avançar**. **d.** Leia as descrições da Configuração da base de conhecimento. **e.** Revise a página Configuração de detecção de host para configurações de importação, regras de pesquisa de IC e cronogramas de importação. **f.** Quando estiver satisfeito com as configurações nesta página, clique em **Executar agora** para importar dados. Clique no link **Exibir detalhes** exibido para exibir o status de execução da integração de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	g. (Opcional) Continue a editar as definições de configuração. **h.** Clique em **Concluir** para concluir a instalação e a configuração no Assistente de configuração. Para obter mais informações sobre como configurar a aplicação Qualys, consulte Configurar o Qualys Vulnerability Integration usando o Assistente de configuração.

O que Fazer Depois

Parabéns! Você instalou com sucesso a aplicação Resposta a vulnerabilidades e a configurou junto com uma aplicação de scanner usando o Assistente de configuração. O sistema de base agora está pronto para operação.

Para baixar, instalar e configurar outras aplicações para Resposta a vulnerabilidades, siga as mesmas etapas e conceitos que você concluiu para a check-list anterior. Consulte os tópicos específicos fornecidos para cada aplicação para obter mais informações.

Para obter mais informações sobre as aplicações compatíveis disponíveis que estão disponíveis para você em ServiceNow Store para Resposta a vulnerabilidades, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

Para obter mais informações sobre como usar Resposta a vulnerabilidades, consulte Explorar a aplicação Resposta a vulnerabilidades.

Resposta a vulnerabilidades estados da tarefa de correção

As integrações de terceiros importam dados de detecção de itens vulneráveis que criam novos itens de vulnerabilidade (VITs) ou atualizam os VITs existentes. Os estados de detecção atualizam os estados de VIT, desde que sejam Abertos ou Fechados.

Para obter mais informações sobre como o estado de uma detecção afeta o estado de um VIT, consulte Detecções, tarefas de correção e estados de itens vulneráveis.

Com Gestão de mudanças para Resposta a vulnerabilidades, há um relacionamento sincronizado entre os campos de estado das tarefas de correção e os campos de estado das solicitações de mudança (CHG) no produto Resposta a vulnerabilidades. Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também move o estado de todas as tarefas de correção relacionadas automaticamente. Depois que uma solicitação de mudança é implementada, a tarefa de correção é resolvida automaticamente. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Nota: A partir da v23.0 de Resposta a vulnerabilidades:

- o fluxo de trabalho **de aprovação do estado da tarefa de correção** foi descontinuado e substituído pelo fluxo de aprovação do estado da tarefa de correção no Flow Designer.
- o botão **Fechar** foi removido para uma tarefa de correção e o fechamento de uma tarefa de correção é orientado pelo scanner.

A tabela a seguir lista os estados da tarefa de correção e as ações que você pode executar em uma tarefa de correção no respectivo estado:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
Aberto	Estado após a criação. A partir deste estado, você pode: Mostrar IVs duplicados Identifique IVs duplicados relatados por vários scanners no sistema. Você pode marcar o VI duplicado como Resolvido ou Encerrado. Entradas duplicadas são mostradas somente quando a combinação de vulnerabilidades é criada usando Vulnerabilidades e exposições comuns (CVE). Para obter mais informações, consulte Resposta a vulnerabilidades tarefa de correção e estados de itens vulneráveis. Iniciar Investigação Atribua esta tarefa de correção a uma pessoa ou grupo para começar a investigar. Marcar como falso positivo Marque um item ou grupo como falso-positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas na verdade não há vulnerabilidade. Exceção de Solicitação Solicite uma exceção, uma data de reabertura (Até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item ou grupo até a data em que uma exceção é solicitada. Resolver Marque como Resolvido para mover o item ou grupo para um estado resolvido. Criar Mudança Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. Dividir tarefa de correção Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Dividir uma tarefa de correção no Espaço de correção de problemas de TI. Adiar Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. Excluir

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	Confirmar a exclusão. Remove o grupo.
Sob Investigação	Acionado pelo botão **Iniciar investigação**. A partir deste estado, você pode: Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Criar Mudança Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. Dividir tarefa Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Dividir uma tarefa de correção. Criar uma solicitação de mudança Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção. Aguardando Implementação Muda o estado para Aguardando implementação. Este estado indica que as tarefas de correção foram encaminhadas para fora de um Resposta a vulnerabilidades. Adiar Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. Excluir Confirmar a exclusão. Remove a tarefa de correção.
Adiado	Acionado pelo botão **Solicitar exceção**. Como parte do fluxo de trabalho de aprovação, o estado Adiado é Em revisão e não pode ser fechado até ser aprovado. A partir deste estado, você pode: Criar Mudança Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. Dividir tarefa Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir um grupo de vulnerabilidades. Os itens selecionados são movidos automaticamente para um novo VG. Consulte Dividir uma tarefa de correção. Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Reabrir Faça a transição de volta para um estado Aberto. Excluir Confirmar a exclusão. Remove a tarefa de correção. As informações de adiamento aparecem na guia **Fechar/Adiar**. Na data de adiamento, o grupo é reaberto para correção.
Aguardando Implementação	Acionado pelo botão **Aguardando implementação**. A partir deste estado, você pode: Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Criar Mudança Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. Dividir tarefa Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir um grupo de vulnerabilidades. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Dividir uma tarefa de correção. Criar uma solicitação de mudança Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	Adiar Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. Resolver Adicionar anotações. O estado se torna Resolvido. As anotações aparecem na guia **Resolução**. Excluir Confirmar a exclusão. Remove a tarefa de correção.
Resolvido	Acionado a partir do botão **Resolver**. A partir deste estado, você pode: Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Criar Mudança Crie uma solicitação de mudança ou associe um grupo de vulnerabilidades a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. Reabrir Faça a transição de volta para um estado Aberto. Excluir Confirmar a exclusão. Remove a tarefa de correção. As anotações aparecem na guia **Anotações**. As informações de resolução aparecem na guia **Resolução**.
Encerrado	Acionado pelo scanner. A partir deste estado, você pode: Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Reabrir Faça a transição de volta para um estado Aberto. Excluir Confirmar a exclusão. Remove a tarefa de correção. As informações de fechamento aparecem na guia **Fechar/Adiar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O proprietário de correção só pode marcar um item vulnerável ou tarefa de correção como resolvido. Com base na confirmação do scanner, este item resolvido ou tarefa de correção pode ser marcado como Encerrado ou reaberto.
- O botão **Excluir** está disponível para o administrador quando há vários itens vulneráveis criados manualmente e eles precisam ser encerrados ou excluídos.
- Se você determinar que os itens são de baixo risco, aguardando uma janela de mudança ou um patch, você poderá alterar a tarefa de correção para o estado Adiarvermelho por um período de tempo definido. Você pode solicitar uma exceção usando a opção **Solicitar exceção**.

  Nota: Quando as tarefas de correção são adiadas ou encerradas, você pode especificar resoluções para definir melhor os motivos para isso.

- Quando um VIT é reaberto, manual ou automaticamente, acontece o seguinte:
  - O estado do VIT muda para Aberto. O estado da tarefa de correção original não é atualizado.
  - O VIT é reavaliado e colocado em uma tarefa de correção nova ou existente que se baseia nas Regras de tarefa de correção ativas.

  Isso preserva o histórico e permite correções adicionais.

- Quando uma tarefa de correção é criada (automaticamente ou manualmente) ou dividida, os campos **Estado**, **Motivo**e **Até** são avaliados. No caso da ação de divisão, esses campos são avaliados para as tarefas de correção antigas e novas. Quando um VIT é atualizado, os campos **Estado**, **Motivo**e **Até** de todas as tarefas de correção associadas são avaliados.
  - Se todos os VITs em uma tarefa de correção forem adiados e tiverem o mesmo motivo, o estado da tarefa de correção será alterado para **Adiado** e o motivo dos VITs será atribuído à tarefa de correção. Se os VITs diferirem no motivo, o motivo da tarefa de correção será alterado para **Nenhum**.
  - A data **Até** mais próxima de todos os VITs é atualizada no campo **Até** da tarefa de correção.
  - Se você reabrir qualquer VIT, o estado da tarefa de correção será alterado para **Aberto**.

  Esta avaliação é feita pelo trabalho agendado *`Rollup vulnerability item values to vulnerability and group`*, que é executado a cada 15 minutos.

Detecções, tarefas de correção e estados de itens vulneráveis

As integrações de terceiros recuperam os dados de detecção de itens vulneráveis. As detecções são ocorrências distintas de vulnerabilidades conforme relatadas pelos scanners.

Os dados de detecção são emparelhados com itens vulneráveis (VIs, VITs) e o estado de IV é atualizado com base no estado das detecções. Se um IV não for encontrado, um novo será criado. As detecções são abertas ou fechadas somente pelos dados encontrados diretamente por um scanner.

Se todas as detecções de um item vulnerável forem encerradas, esse item vulnerável será encerrado. No registro VI, o estado é Encerrado/Corrigido. Quando todos os IVs são encerrados para uma tarefa de correção, a tarefa de correção é encerrada. Caso contrário, o fluxo de estado permanecerá o mesmo.

IVs encerrados com um subestado fixo ou obsoleto serão reabertos se uma nova detecção for criada e os VIs puderem ser correspondidos com a nova vulnerabilidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 20.0 de Resposta a vulnerabilidades, se uma detecção for obsoleta e o IV associado estiver no estado Encerrado, o estado do VI não fará a transição para Encerrado - Obsoleto. Isso evita que o VI seja reaberto quando uma nova detecção for identificada, para que você possa evitar passar por todo o processo de aprovação e solicitação de falso-positivo. Para reverter esse comportamento, desmarque a caixa de seleção **Ignorar detecções obsoletas para IVs encerrados** no formulário Configuração de fechamento automático. Para obter mais informações, consulte Fechar automaticamente detecções obsoletas no Resposta a vulnerabilidades.

De acordo com a inclusão de script, *DetectionBase*, método *_shouldReOpenVI()*, se o VI foi encerrado anteriormente com um subestado de Fixo, Obsoleto ou IC desativado, ele será reaberto e a detecção será mapeada para o VIT existente.

Por exemplo, digamos que a data de encerramento de um VI seja posterior à última data encontrada de uma detecção. Você esperaria que esses registros de IV permanecessem fechados. No entanto, se você vir que um VI encerrado anteriormente foi reaberto, isso significa que o VI foi encerrado por uma detecção anterior e a vulnerabilidade foi encontrada novamente em uma verificação posterior. Quando é encontrada uma nova detecção que corresponde ao VIT encerrado que tem a mesma vulnerabilidade no item de configuração do VI, o VI é reaberto.

Tarefas de correção e estados de itens vulneráveis

As tarefas de correção e os estados de itens vulneráveis podem afetar um ao outro. Na maioria das vezes, um estado de tarefa de correção atualiza o estado do item vulnerável, com o estado da tarefa de precedência mais alta usado para atualizar os itens vulneráveis no grupo.

A precedência de estado é a seguinte.

Adiado > **Resolvido** > **Aguardando implementação** > **Sob investigação** > **Aberto**

- Quando um grupo de itens vulneráveis está em uma tarefa de correção e não é alterado em um nível individual, eles têm o mesmo estado que a tarefa de correção.
- Quando a tarefa de correção passa do estado Aberto para Aguardando implementação, todos os IVs na tarefa de correção são movidos para o estado Aguardando implementação.
- Quando a tarefa de correção é adiada, o VI é adiado da mesma forma. A partir da versão 16.5, você pode rastrear o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou uma tarefa de correção foi adiado. O trabalho agendado, *set deferral counts*, é executado diariamente para publicar contagens dos registros que foram adiados mais de uma vez na coluna Contagem de adiamento nos módulos de vários adiamentos para VR, AVR e CVR. Todas as contagens de IVs associadas a uma tarefa de correção serão coletadas e publicadas se uma tarefa de correção for adiada mais de uma vez.

  Itens vulneráveis atualizados somente por tarefas de correção

  Os itens correspondem ao estado da tarefa de correção, se não tiverem sido atualizados individualmente, com estas exceções:

  - Se o estado da tarefa de correção mudar para Encerrado e sua resolução para Cancelado ou Corrigido com exceção, o item não será afetado e assumirá o estado de qualquer outra tarefa de correção que o contenha. Se o item vulnerável não estiver em nenhuma outra tarefa de correção, ele será revertido para o estado Aberto.
  - Se o estado do item vulnerável for Encerrado/Corrigido (atualizado por uma verificação ou importação), quando a tarefa de correção mudar de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estado, o item vulnerável permanecerá no estado Encerrado/Corrigido. Esta condição é verdadeira, independentemente do estado em que a tarefa de correção está.

Itens vulneráveis em estados definidos individualmente

Itens vulneráveis, em um estado atualizado no item, como os itens encerrados ou adiados individualmente, não correspondem ao estado da tarefa de correção automaticamente. Em vez disso, ele compara seu estado a todos os grupos associados para encontrar o estado com a precedência mais alta a ser aplicada.

Nota: O estado Fechado/Corrigido é um caso especial. Para os itens vulneráveis que estão definidos com o estado Encerrado/Corrigido, se todos os itens vulneráveis em uma tarefa de correção estiverem definidos como Encerrado/Corrigido - como quando um scanner descobre que todas as vulnerabilidades foram corrigidas - a tarefa de correção será marcada automaticamente como Fechado/Fixo.

As tarefas de correção contêm campos de atribuição vazios

Se o estado dos IVs em uma tarefa de correção mudar de Resolvido para Aberto, o estado da tarefa de correção também será atualizado de Resolvido para Sob investigação.

No entanto, se os campos **Atribuído a** e **Grupo de atribuição** na tarefa de correção estiverem vazios, a tarefa de correção permanecerá no estado Resolvido e não passará para Sob investigação.

O grupo de atribuição dos itens vulneráveis nem sempre é atualizado quando a tarefa de correção é atualizada

Se o grupo de atribuição de um VI no estado Aberto for atualizado manualmente, ele não será atualizado novamente quando o grupo de atribuição da sua tarefa de correção for atualizado. Essas informações não são substituídas porque o grupo de atribuição do VI foi atualizado intencionalmente e pode fazer parte de outra tarefa de correção.

Estado da tarefa de correção para itens vulneráveis (IVs) em vários grupos

Quando um VI está em várias tarefas de correção (grupo nas tabelas a seguir) e seu próprio estado não foi definido, o estado do grupo de precedência mais alta determina o estado desse VI, conforme mostrado na tabela a seguir.

Exemplos de estados de item vulnerável

Estado de tarefas de correção	Estado de item vulnerável
Grupo A: **Aberto** > **Sob Investigação** Grupo B: **Aberto**	**Sob Investigação** Quando o Grupo A está Sob investigação e o Grupo B está Aberto, o IV muda para Sob investigação. Após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.
Grupo A: **sob investigação** Grupo B: **Aberto** > **Sob Investigação**	**Sob Investigação** Quando o Grupo B está Sob Investigação e o Grupo A está Sob Investigação, o VI permanece como Sob Investigação. Após a pesquisa, entre

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplos de estados de item vulnerável

Estado de tarefas de correção	Estado de item vulnerável
	o Grupo A e o Grupo B, eles têm o estado com a mesma precedência.
Grupo A: **sob investigação** Grupo B: **Sob Investigação** > **Aguardando Implementação**	**Aguardando Implementação** Quando o Grupo B está Aguardando Implementação e o Grupo A está Sob Investigação, o VI muda para Aguardando Implementação. Após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com a precedência mais alta.
Grupo A: **Sob Investigação** > **Adiado** Grupo B: **Aguardando Implementação**	**Adiado** Quando o Grupo A é Adiado e o Grupo B está Aguardando Implementação, o VI muda para Adiado. Após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.

Casos especiais de item vulnerável em vários grupos

Estado da tarefa de correção	Estado do item vulnerável
Grupo A: **Sob Investigação** Grupo B: **Aguardando Implementação** > **Encerrado (fixo ou cancelado)**	**Sob Investigação** Quando o grupo B é encerrado/corrigido ou encerrado/cancelado e o grupo A está sob investigação, o VI muda de Aguardando implementação (anteriormente a precedência mais alta) para Sob investigação (atualmente a precedência mais alta).
Grupo A: qualquer estado Grupo B: qualquer estado	Se o status de origem do item vulnerável for Fixo (atualizado por uma verificação ou importação), quando o grupo mudar de estado, o item vulnerável mudará seu estado para Encerrado/Corrigido. Esta condição é verdadeira, independentemente dos estados em que os outros grupos associados estão. A pesquisa de item vulnerável para o estado do grupo não ocorre.

Quando um estado de VI é definido individualmente, seu estado é considerado ao avaliar a precedência, como em qualquer outra tarefa de correção. Quando um IV pertence a mais de uma tarefa de correção, a tabela a seguir lista as atualizações feitas.

Estado de item vulnerável definido individualmente casos especiais

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado do grupo A: **Sob Investigação**	**Aguardando Implementação**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado de item vulnerável definido individualmente casos especiais

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado do grupo B: **Sob Investigação** > **Aguardando Implementação** Estado de VI original: **Sob Investigação** > **(definido no IV)**	Quando o Grupo B é movido para Aguardando Implementação e o Grupo A permanece Sob Investigação, o VI muda para Aguardando Implementação (a precedência mais alta).
Grupo A: **Sob Investigação** Grupo B: **Sob Investigação** > **Aguardando Implementação** Estado de VI original: **Adiado** > **(definido no IV)**	**Adiado** Quando o Grupo B é movido para Aguardando Implementação e o Grupo A permanece Sob Investigação, o IV permanece no estado Adiado (a precedência mais alta).

A tabela a seguir mostra que quando duas tarefas de correção com itens vulneráveis comuns são adiadas, o estado é adiado até que a data mais recente seja atingida.

Casos especiais de estado adiado de item vulnerável

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado do grupo A: **Em revisão (até 10 de abril)** Estado do grupo B: **Sob Investigação** > **Em revisão (até 30 de abril)** Estado de VI original: **Em revisão (até 10 de abril)** > **(definido no IV)**	**Adiado (até 30 de abril)** Quando o Grupo B é movido para Adiado (até Abr-30) e o Grupo A permanece Adiado (até Abr-10), o VI muda do estado Adiado (até Abr-05) para o estado Adiado (até Abr-30).
Grupo A: **Em revisão (até 15 de julho)** Grupo B: **Sob Investigação** > **Em revisão (até 10 de julho** Estado de VI original: **Adiado** > **(até 15 de julho)**	**Adiado (até 15 de julho)** Quando o Grupo B é movido para Adiado (até jul-10) e o Grupo A permanece Adiado (Jul-15), o IV permanece em Adiado (até jul-15).

Tradução automática

Configurações adicionais para Separação de domínios

Para uma execução e resultados precisos, as seguintes precauções e configurações são necessárias para Domain Separation em Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidadese Conformidade de configurações.

Não modifique as lógicas e os processos de negócios no domínio global para evitar problemas para que todas as mudanças mais recentes sejam atualizadas para cada upgrade. Duplique todas as lógicas e processos de negócios em cada domínio separadamente e verifique se eles estão inativos no domínio global. Caso contrário, as lógicas e os processos de negócios no domínio global terão precedência sobre o domínio secundário. Suponha que você tenha criado uma regra de risco em um domínio secundário e o domínio global também tenha uma regra de risco semelhante. A regra do domínio global terá precedência sobre a regra do domínio secundário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reavaliação de calculadoras e regras

Antes da v20.0, quando você reaplica calculadoras ou regras, o sinalizador de `reexecução` é definido como verdadeiro e uma regra de negócio é acionada para executar um trabalho de programação que reaplica as calculadoras e regras. A partir da v20.0, você não precisa depender do sinalizador de `reexecução`. Quando você clica no botão **Reaplicar calculadora**, é acionado um trabalho em segundo plano que reaplica as calculadoras e as regras. Isso permite que você crie calculadoras e regras para todos os domínios.

Configurações para calculadoras de acúmulo

Em um domínio, somente uma calculadora de acúmulo deve estar ativa para uma tabela. Por exemplo, considere a tabela Tarefa de correção, *sn_vul_vulnerability* com a calculadora de acúmulo, **Acúmulo da tarefa** de correção no domínio global. Se você duplicar esta calculadora de acúmulo alterando os pesos da mesma tabela no mesmo domínio, haverá discrepâncias nos cálculos de acúmulo. Portanto, certifique-se de ativar apenas uma calculadora de acúmulo se houver duas ou mais calculadoras de acúmulo para uma tabela no mesmo domínio.

Campos de formulário de Itens Descobertos

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) no Configuration Management Database (CMDB) quando são importados usando as Regras de pesquisa de IC. Registros de ICs incompatíveis são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros e incluídos nos itens descobertos. No entanto, para ativos de nuvem que não estão presentes em CMDB CI, o registro é criado na classe de recurso de nuvem.

Campos de itens descobertos

As informações nesses registros são ingeridas dos registros de terceiros e classificadas durante a importação.

Campo	Descrição
Número	Identificador atribuído ao registro.
Item de Configuração	Item de configuração importado da integração de origem de terceiros. A partir da v12.0, o item de configuração é o IC mais recente da lista de ICs após a filtragem dos desativados.
Classe	Classe atribuída ao IC durante a importação por Resposta a vulnerabilidades.
Origem	Origem importada da integração de origem de terceiros.
Regra de correspondência de IC	A regra de correspondência de IC usada para criar o item.
V18.0: tipo correspondente para DI	Tipo correspondente usado para criar o item descoberto. As opções são: • Criado por VR • Criado por IRE

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• Correspondido por pesquisa de IC • Correspondido por IRE Essas informações só estão disponíveis para dados preenchidos para Resposta a vulnerabilidades v18.0 e posterior. Em dados existentes, esta coluna não contém nenhum valor. **Nota:** Se você reaplicar as regras de pesquisa de IC, alguns ICs em DIs poderão ser atualizados, resultando no preenchimento desta coluna.
Outros ICs correspondentes	Lista dos outros itens de configuração que correspondem à regra de pesquisa de IC.
Estado	Estado do IC determinado durante a importação. As opções são: • **Correspondido**: um item de configuração correspondente foi encontrado no CMDB. • **Incompatível**: nenhuma correspondência foi encontrada no CMDB. Um registro de espaço reservado é criado.
Criação	Data em que o registro de item descoberto foi criado.
Atualizado em	Data em que o registro do item descoberto foi atualizado.
Atualizado por	Usuário que atualizou os dados.
Marcador de host	Marcadores de host atribuídos a este item descoberto durante a importação. Você pode ter até 31 marcadores de host por item descoberto.
Nome de domínio totalmente qualificado	Dados associados a este IC encontrados no CMDB.
Endereço MAC	Dados associados a este IC encontrados no CMDB.
Sistema operacional	Sistema operacional associado a este IC.
NetBIOS	NetBIOS importado da integração de origem de terceiros.
Endereço IP	Dados associados a este IC encontrados no CMDB.
Dados de origem	Dados mais recentes associados a este IC da origem.
V16: dados de origem inicial	Dados iniciais associados a este IC da origem.
V16: reavaliar IC	Recebe dados do scanner. Se houver dados atualizados, o valor será definido como verdadeiro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os valores dos dados de origem são recalculados de acordo com os dados de origem mais recentes. Quando os dados atualizados são recuperados do scanner, os dados de origem são atualizados. O valor de dados de origem existente é movido para o campo de dados de origem inicial. Para reavaliar os itens descobertos, ative o trabalho agendado `Reaplicar regras de pesquisa de IC nos itens descobertos alterados`.
Agente existe	Indica `verdadeiro`se o agente estiver instalado no ativo. Se os valores `hostUID` e `UUID` na coluna Dados de origem estiverem vazios, este valor será preenchido como `verdadeiro`. **Nota:** Este campo aparece a partir da v19.0 de Resposta a vulnerabilidades.

A partir da v23.0 de Resposta a vulnerabilidades, a coluna **% (IC) de conformidade** do resultado de testes mostra a porcentagem de resultados de testes que estão em conformidade com o IC correspondente. Para obter esse valor, você deve definir o `calcTRComplianceForCI` como `verdadeiro` no trabalho agendado **Atualizar métricas de correção**.

Nota: O valor do **percentual de conformidade (IC) do resultado de testes** é preenchido somente para os itens descobertos que têm um valor não vazio nas colunas Data da última **verificação de Conformidade de configuração ou Datada última verificação de conformidade não infraestrutural**.

A partir da versão 18.0 de Resposta a vulnerabilidades, Qualys, Tenable para Resposta a vulnerabilidades e Rapid7, os scanners podem receber os seguintes metadados adicionais para ativos em nuvem.

Campo	Descrição
Provedor de serviços em nuvem	Nome do provedor de serviços em nuvem que oferece serviços de computação em nuvem. Por exemplo, Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).
Região da nuvem	Local onde o recurso foi hospedado.
Conta de nuvem	Conta fornecida por provedores de serviços em nuvem, como AWS, GCPe assim por diante, para acessar serviços de computação em nuvem.
Tipo de recurso de nuvem	Tipos de ativos presentes na nuvem, como máquina do Amazon Elastic Compute Cloud (EC2), AWS buckets S3 e assim por diante.
ID do recurso	Identificador exclusivo atribuído a um recurso em um ambiente de computação em nuvem. Este ID é usado para identificar e gerenciar o recurso.
Nome do recurso	Nome definido pelo usuário usado para identificar e gerenciar um recurso em um ambiente de computação em nuvem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Imagem	A imagem da máquina virtual ou uma imagem do servidor é uma máquina virtual pré-configurada que contém um sistema operacional, aplicações e outros softwares. Por exemplo, Amazon Machine Image.

Uma nova regra de pesquisa de IC, "ID de recurso de nuvem", foi introduzida para corresponder aos ICs de nuvem com base nos metadados de nuvem.

Resposta a vulnerabilidades campos de formulário de vulnerabilidade

As vulnerabilidades são criadas automaticamente quando os registros são baixados do Banco de dados nacional de vulnerabilidades (NVD), Enumeração de pontos fracos comuns (CWE) ou integrações de terceiros e armazenados em **Bibliotecas** em Resposta a vulnerabilidades.

Campos de entrada do NVD

Os campos importados nesta tabela são somente leitura. Itens vulneráveis (IVs), Software vulnerável e Referências de vulnerabilidade são associados automaticamente e as entradas podem ser adicionadas manualmente.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Pontuação de risco	(Oculto quando não há IVs associados à vulnerabilidade) **Pontuação de risco** quantificado que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco do registro da solução.**
Pontuação de risco	(Oculto quando não há IVs associados à vulnerabilidade) Valor calculado de risco que o item vulnerável representa para o seu ambiente. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro de solução.** Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Criar um Resposta a vulnerabilidades mapa de severidade.
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Explorar nível de habilidade	Nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Explorar vetor de ataque	Vetor de ataque mais vulnerável das explorações para esta vulnerabilidade. Disponível quando o SAM NVD está habilitado.
IVs ativos	(Oculto quando não há IVs associados à vulnerabilidade) Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Fechado. Se não houver IVs ativos para esta vulnerabilidade, a **Classificação** de **risco e a Pontuação** de risco não serão exibidas.
Entrada de CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns em que esta vulnerabilidade se encaixa melhor.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Informações sobre ameaças (a partir da Resposta a vulnerabilidades versão 20.0)	Inteligência contra ameaças fornecida por Qualys. Com esses dados, você pode entender os motivos, metas e comportamentos de ataque de um agente da ameaça.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados do CVSS v3 importados, não disponíveis antes de 2015.
Solução preferencial	(Oculto quando não há IVs associados à vulnerabilidade) Solução de substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais elevada na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído em importações subsequentes. A definição deste valor manualmente deve ser feita no item vulnerável.
Exploração CISA (Esta guia está disponível somente quando a aplicação CISA está instalada.)	
Data de vencimento da CISA	Prazo para resolver a vulnerabilidade.
Data de inclusão	Data em que a vulnerabilidade foi adicionada ao catálogo CISA.
Produto	Produto no qual a vulnerabilidade foi identificada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Fornecedor/ projeto	Fornecedor associado à vulnerabilidade identificada.
Ransomware conhecido A partir da v21.0 de Resposta a vulnerabilidades.	Selecionado quando o campo **Conhecido por ser usado em campanhas de ransomware** é ingerido do catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA. O sinalizador é definido no nível de Vulnerabilidades e exposições comuns (CVE) e acumulado para a entrada de terceiros (TPE).
Status da Correção (Oculto quando não há IVs associados à vulnerabilidade)	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Percentual de VIs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
Percentual de VIs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Antes da v13.0: forçar importação de vulnerabilidade de software **Nota:** Removido em v13.0	(Obsoleto) Recalcula o mapeamento do produto com Gestão de ativos de software do ITSM com base nas informações do NVD. Atualiza a biblioteca de software vulnerável.
Atualizar status	Exibe a data e a hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação e classificação de risco • Métricas como VIs ativos, VIs totais da seção Status de correção
Listas relacionadas	
Itens vulneráveis	(Oculto quando não há IVs associados à vulnerabilidade)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
Explorações	Explorações associadas a esta vulnerabilidade.
Soluções	(Oculto quando não há IVs associados à vulnerabilidade) Todas as Solução de gestão de vulnerabilidade soluções de integração associadas a esta vulnerabilidade.
Pontos fracos	Dados de **vulnerabilidade** importados associados a vulnerabilidades e exposições comuns (CVE).
Software Vulnerável	(Oculto quando o software está associado ao CVE) Dados importados de Enumeração de plataforma comum (CPE) associados à vulnerabilidade.
Kits de Malware de Vulnerabilidade	Malware importado de várias origens de scanner para uma vulnerabilidade.

Campos de entrada de vulnerabilidade do CWE

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
CWE-Identificador	Identificador desta entrada de vulnerabilidade. Este identificador é usado para categorias e pontos fracos e é exclusivo entre os dois conjuntos de dados.
Nome	Nome descritivo atribuído a este CWE-ID.
Probabilidade de exploração	A probabilidade de o ponto fraco ser explorado, em uma escala qualitativa. Um dos seguintes: • Baixo • Médio • Alto(a)
10 principais posições da OWASP	A posição numérica desta vulnerabilidade na lista das 10 principais da OWASP.
SANS para 25 posições	A posição numérica desta vulnerabilidade na lista das 25 principais da SAN.
Classe	Tipo de fraqueza
Status	Um dos seguintes: • Incompleto • Rascunho

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• Estável • Preterido • Obsoleto • Instável
Subtração	Um dos seguintes: • Variante • Classe • Base • Composto
Atualizado em	Última vez em que o registro foi atualizado na instância.
Áreas funcionais	Lista de áreas funcionais afetadas. Por exemplo, **Processamento de arquivo**. Preenchido somente para pontos fracos do 24/862.
Recursos afetados	Lista de recursos afetados. Por exemplo, **Arquivo** ou **Diretório**. Preenchido somente para pontos fracos 51/863.
URL	Artigo da base de conhecimento associado a esta vulnerabilidade.
Descrição	Descrição da vulnerabilidade.
Execução de integração	A execução de integração em que este CWE foi importado.
Seções	
Detalhes adicionais	Descrições do conceito de software que explicam melhor o ponto fraco. Inclui: • Descrição estendida • Detalhes do plano de fundo • Anotações
Métodos de detecção	Detalhes sobre como você pode detectar esse ponto fraco em uma aplicação.
Modos de introdução	As fases em que o ponto fraco é introduzido, por exemplo, **Implementação**, **Arquitetura e design**e assim por diante.
Exemplos demonstrativos	Exemplos de código da fraqueza com as descrições que os acompanham.
Mitigações potenciais	Detalhes sobre como evitar o ponto fraco, incluindo em qual fase do ciclo de vida da aplicação ele ocorre e a eficácia da mitigação.
Listas relacionadas	
Relacionamentos	CWEs associados a esta vulnerabilidade. Lista os relacionamentos entre este CWE e outros. Pode incluir primário/secundário, segue/precede, exigidopor/requer (para fraquezas compostas), CanAlsoBe, PeerOf, MemberOf .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Exemplos observados	Alguns CVEs que são representativos desta fraqueza.
Consequências Comuns	Consequências de uma exploração bem-sucedida, em termos de escopo e impacto. Por exemplo: Escopo: confidencialidade Impacto: ler dados da aplicação
Associações	Associações do CWE com esta vulnerabilidade.
Plataformas aplicáveis	Plataformas associadas a esta vulnerabilidade.
Entradas de vulnerabilidade da aplicação	Outras entradas de vulnerabilidade da aplicação associadas a uma.
Referências externas	Informações sobre a vulnerabilidade de fontes externas.

Campos de entrada de vulnerabilidade de terceiros

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Versão 16.0: CVEs	Várias vulnerabilidades e exposições comuns (CVEs) associadas a esta vulnerabilidade de terceiros.
Origem	Origem da vulnerabilidade - seja um scanner ou teste físico.
Pontuação de risco	**Pontuação de risco** quantificado que separa os itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco**do registro da solução
Pontuação de risco	Valor calculado de risco que o item vulnerável representa para o seu ambiente, com base na pontuação de risco. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro de solução.** Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	mapas de severidade, consulte Criar um Resposta a vulnerabilidades mapa de severidade.
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Explorar nível de habilidade	Nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Explorar vetor de ataque	Vetor de ataque mais vulnerável das explorações para esta vulnerabilidade.
IVs ativos	Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Fechado.
Categoria	Classificação fornecida pela integração de terceiros. Ajuda na atribuição.
Tipo de correção	Tipos de ações de correção. • Patch • Mudança de configuração • Mudança de Configuração e Patch • Contramedida
Entrada de CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns em que esta vulnerabilidade se encaixa melhor.
PCI	Quando a caixa de seleção está marcada, a vulnerabilidade é sinalizada quanto a risco significativo de exposição de informações de pagamento.
Gravidade de PCI	Nível de risco de exposição de informações de pagamento. [Somente Qualys.]
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados do CVSS v3 importados, não disponíveis antes de 2015.
Ameaça	Descrição da ameaça desta vulnerabilidade.
Solução preferencial	Solução de substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais elevada na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído em importações subsequentes. A definição deste valor manualmente deve ser feita no item vulnerável.
Anotações de correção	Descrição da solução de correção extraída do fornecedor.
Status da Correção	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Percentual de VIs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
Percentual de VIs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Atualizar status	Exibe a data e a hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação e classificação de risco • Métricas como VIs ativos, VIs totais da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
CVEs	Registro de Enumeração de vulnerabilidade comum (CVE) associado a esta vulnerabilidade.
Categorias	Categorias associadas a esta vulnerabilidade.
Explorações	Explorações associadas a esta vulnerabilidade.
Kits de Malware de Vulnerabilidade	Kits de malware associados a esta vulnerabilidade.
Soluções (Rapid7)	Informações da solução das integrações da solução Rapid7. Exibido quando disponível.
Estruturas de Exploração	Explorar estruturas associadas a esta vulnerabilidade.
Soluções	Solução de gestão de vulnerabilidade soluções associadas a esta vulnerabilidade.
Exploração CISA	
CISA existe	Existe uma exploração CISA para a tabela Entrada de vulnerabilidades de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Data de vencimento da CISA	Prazo para resolver a vulnerabilidade.

Campos do formulário da tarefa de correção

Usando tarefas de correção, o analista pode monitorar o andamento e conduzir o processo de mediação com mais eficiência.

Os campos importados nesta tabela são somente leitura.

Campos da tarefa de correção

Campo	Descrição
Número	O número do item vulnerável (VI) gerado automaticamente para este registro.
Pontuação de risco	Acúmulo de pontuações de risco de item vulnerável separadas em intervalos: Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco do registro da solução.**
Pontuação de risco	Acúmulo das pontuações de risco de todos os itens vulneráveis associados a esta tarefa de correção. Valor de risco que os itens vulneráveis, coletivamente, representam para o seu ambiente. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro de solução.**
Meta de correção	Data em que os itens vulneráveis devem ser corrigidos, desde a primeira identificação. Para obter mais informações sobre metas de correção, consulte Resposta a vulnerabilidades regras de destino de correção.
Status da Correção	Status da correção da tarefa. É determinado pelo item vulnerável com a data de vencimento mais próxima. Para grupos abertos, os estados incluem: • Em andamento • Perto da meta • Meta não atingida Para grupos fechados, os estados incluem: • Nenhuma Meta • Meta atingida • Meta não atingida

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

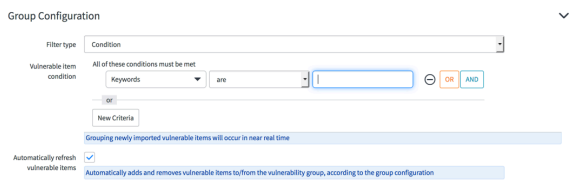
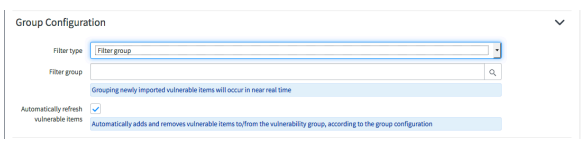
Campos da tarefa de correção

Campo	Descrição
	Para datas de meta de correção calculadas, se a tarefa estiver fechada, o status geral de correção de todos os itens vulneráveis encerrados será mostrado na tarefa. Eles determinam se a tarefa atendeu à data ou não. O status de correção de uma tarefa encerrada será **Sem meta** se nenhum de seus itens encerrados tiver uma data de meta de correção. É **meta** não atingida se algum de seus itens encerrados perdeu a data prevista. Será **Meta** atingida se pelo menos um IV encerrado tiver atingido sua meta e nenhum dos outros tiver falhado.
Estado	Status de andamento da tarefa. Os estados incluem: • Aberto • Sob Investigação • Aguardando Implementação • Adiado • Em Revisão • Resolvido • Encerrado Para obter mais informações sobre os estados, consulte Resposta a vulnerabilidades tarefa de correção e estados de itens vulneráveis.
Até a data para redução de risco	Data em que os controles compensatórios aplicados à tarefa de correção expiram. **Nota:** Este campo aparece somente quando o valor está disponível.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nesta vulnerabilidade.
Criação	Data em que esta tarefa de correção foi criada.
Atualizado em	Data em que esta tarefa de correção foi atualizada pela última vez.
Vulnerabilidade	Vulnerabilidade aplicável à tarefa. (Visível quando o grupo é formado com base em uma única vulnerabilidade.)
Descrição resumida	Breve descrição desta tarefa de correção.
Em revisão (visível quando o RT está no estado Em revisão)	
Solicitados por	Indivíduo que solicitou o adiamento.
Motivo desejado	Motivo do adiamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

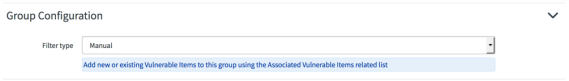
Campos da tarefa de correção

Campo	Descrição
Estado desejado	O estado solicitado do aprovador.
Subestado desejado	O motivo solicitado ao aprovador.
Adiamento(visível quando a tarefa está no estado Adiado)	
Adiado por	Indivíduo que adiou a tarefa.
Adiar expiração	Data em que o adiamento expira.
Motivo para adiar	Motivo do adiamento.
Resolução (visível quando o RT está no estado Resolvido)	
Resolvido por	Indivíduo que resolveu a tarefa de correção.
Data de resolução	Data em que a tarefa de correção foi resolvida.
Anotações de resolução	Informações adicionais.
Fechar (visível quando o RT está no estado Fechado)	
Encerrado por	Indivíduo que resolveu a tarefa de correção.
Encerrado	Data em que a tarefa de correção foi encerrada.
Anotações de encerramento	Informações adicionais.
Configuração de grupo (visível em todos os estados)	
Tipo de filtro	Tipo de filtragem usada para selecionar vulnerabilidades para o grupo: Condição  **Nota:** Atualiza uma vez por hora. Grupo de filtros  **Nota:** Atualiza uma vez por hora. Manual

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos da tarefa de correção

Campo	Descrição
	
Status da Correção	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Percentual de VIs corrigidos	Percentual concluído para correção de itens vulneráveis nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos nesta tarefa.
Total de IVs	Número total de itens vulneráveis nesta tarefa.
Percentual de VIs corrigidos	Percentual concluído para correção de itens vulneráveis nesta tarefa.
Anotações (visíveis em todos os estados)	
Descrição	Descrição do grupo ou das ações de correção.
Comentários adicionais	Informações adicionais.
Atividades	Anotações do sistema.
Links relacionados	
Examinar Itens Vulneráveis Novamente	Aciona uma nova verificação dos itens vulneráveis para determinar se eles foram corrigidos.
Status da atualização	Exibe a data e a hora da última atualização. Acumula o seguinte dos IVs na tarefa: • Estado de tarefas de correção • Pontuações de risco e classificações de risco • Data e status da meta de correção (se aplicável) • Métricas como VIs ativos, VIs totais da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis nesta tarefa.
ANS de tarefas	SLAs de plataforma associados a esta tarefa.
Soluções Preferenciais	Soluções preferenciais dos itens vulneráveis nesta tarefa.
Solicitações de mudança	Solicitações de mudança associadas a esta tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos da tarefa de correção

Campo	Descrição
Aprovações Solicitadas	(Visível quando a tarefa está no estado Em revisão.) Lista de aprovadores. Depois que o adiamento for aprovado, a tarefa de correção passará para o estado Adiado.

Campos de formulário de configuração de questionário

Você pode definir um questionário distinto para uma coleção distinta de vulnerabilidades ou tarefas de correção filtrando as vulnerabilidades ou tarefas de correção, respectivamente, na seção Configuração do questionário de VR do formulário Configurações para gestão de exceções de VR.

O formulário Configuração do questionário aparece quando você seleciona o botão **Novo** na seção Configuração do questionário de VR do formulário Configurações para Gestão de exceções de VR.

Campos de formulário de configuração de questionário

Campo	Descrição
Nome	Nome do questionário.
Regra de aprovação	Regra de aprovação para a qual o questionário é aplicável. • **Solicitação de exceção para grupos de vulnerabilidades** • **Solicitação de exceção para itens vulneráveis** • **Falso positivo para grupos de vulnerabilidades** • **Falso positivo para itens vulneráveis** • **Questionário para controles de compensação para grupos vulneráveis** para solicitações de redução de risco da tarefa de correção. • **Questionário para controles de remuneração de itens** vulneráveis para solicitações de redução de risco do item vulnerável.
Descrição	Descrição resumida da configuração do questionário.
Ordem	O questionário com a ordem mais baixa aparece durante as solicitações.
Ativo	Habilitado por padrão, o que significa que o questionário está em uso.
Tabela	Tabela para a qual a regra de aprovação é aplicável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de formulário de configuração de questionário

Campo	Descrição
	• Item vulnerável [sn_vul_vulnerable_item] para as regras de aprovação relacionadas a itens vulneráveis. • Tarefa de correção [sn_vul_vulnerability] para as regras de aprovação relacionadas a tarefas de correção.
Condição	Condição para os registros para os quais o questionário deve aparecer. Você pode aplicar a condição em todos os campos de um item vulnerável e tarefa de correção, exceto **Motivo**.
Questionário	Questionário que aparece quando um proprietário de correção está solicitando uma exceção, falso-positivo ou redução de risco.

Informações relacionadas

Configurar Gestão de exceções para Resposta a vulnerabilidades

Configurar questionário para redução de risco

Resposta a vulnerabilidades campos de formulário de item vulnerável

Itens vulneráveis são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Campos de item vulnerável

Se você habilitou a verificação de vulnerabilidades do SAM NVD, os registros serão comparados com o software em seu Configuration Management Database (CMDB) e serão encontradas correspondências com software vulnerável ou itens de configuração (ICs).

Campo	Descrição
Selecione marcador de segurança	Marcador desegurança para adicionar metadados ao registro ou identificar quem deve ter acesso a este registro de incidente de segurança. Este campo aparece somente depois que o item vulnerável foi salvo.
Número	Número de item vulnerável gerado automaticamente para este registro.
Origem	Verificador que encontrou este item vulnerável.
Pontuação de risco	**Pontuação de risco** quantificado que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Esta **classificação de risco** base não é igual à **classificação de risco do registro da solução.**
Pontuação de risco	Valor calculado de risco que o item vulnerável representa para o seu ambiente. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro de solução.** Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável.
Item de configuração	Ativo afetado.
Estado	O padrão deste campo é **Aberto**, mas você pode alterá-lo para **Sob investigação** se a vulnerabilidade estiver pronta para correção imediata.
Até a data para redução de risco	Data em que os controles compensatórios aplicados ao item vulnerável expiram. **Nota:** Este campo aparece somente quando o valor de Pontuação de risco original está disponível.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nesta vulnerabilidade.
Criação	Data em que este item vulnerável foi criado em sua instância.
Aberto pela última vez	Data em que o item vulnerável foi aberto mais recentemente em sua instância. Inicialmente, é a mesma que a data de criação do item vulnerável, no entanto, se ele foi fechado, então reaberto a Última data de abertura conterá a data e a hora da reabertura.
Atualizado em	Data da última verificação.
Vulnerabilidade	
Resumo	Descrição da vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Criar um Resposta a vulnerabilidades mapa de severidade.
Pontuação de vulnerabilidade (v3)	Pontuação do CVSS v3.
Pontuação de vulnerabilidade (v2)	Pontuação do CVSS v2.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada às vulnerabilidades associadas a este item vulnerável.
Explorar vetor de ataque	O vetor de ataque mais vulnerável das explorações das vulnerabilidades associadas a este item vulnerável.
Explorar nível de habilidade	Nível de habilidade mais baixo necessário para explorar as vulnerabilidades associadas a este item vulnerável.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Ameaça	Informações relevantes sobre a ameaça. Extraído do registro de entrada vulnerável. **Nota:** Todas as mudanças feitas aqui atualizam o registro de entrada vulnerável.
Anotações de correção	Solução relevante para a ameaça, extraída do registro de entrada vulnerável.
Etapas de Correção Disponível somente com Solução de gestão de vulnerabilidade.	
Solução preferencial	Solução preferencial importada do registro de vulnerabilidade. **Nota:** Quaisquer mudanças manuais feitas aqui não alteram o registro de vulnerabilidade e permanecem inalteradas no VI nas importações subsequentes.
Resumo	Resumo importado do registro da solução.
Detecção inicial	
Nome DNS	Nome do serviço de nome de domínio. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Nome NetBIOS	Nome do NetBIOS. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Endereço IP	Endereço IPv4 ou IPv6. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Porta	Endereço da porta
Protocolo	Nome do protocolo.
SSL	Se a criptografia SSL é usada ou não.
Detecções	
Status	Estado da detecção.
Primeiro encontrado	Data em que a origem de terceiros encontrou pela primeira vez a detecção neste ativo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Último encontrado	Data em que a origem de terceiros encontrou pela última vez a detecção neste ativo.
Nome DNS	Nome do serviço de nome de domínio. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Nome NetBIOS	Nome do NetBIOS. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Endereço IP	Endereço IPv4 ou IPv6. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Porta	Endereço da porta
Protocolo	Nome do protocolo.
SSL	Se a criptografia SSL é usada ou não.
Horas encontradas	Número de vezes que esta vulnerabilidade foi detectada neste ativo pela origem de terceiros.
Execução de integração	Execução de integração que importou a detecção.
Fechar Disponível quando o item vulnerável tiver sido corrigido e encerrado. Os itens nesta seção são somente leitura.	
Encerrado por	Quem fechou o item vulnerável.
Encerrado	Data em que o item vulnerável foi encerrado.
Anotações de encerramento	Informações incluídas no fechamento.
Momento do fechamento	Período após o qual o VI foi encerrado. Se o VI for reaberto, o valor do campo Idade encerrada será definido como zero.
Anotações	
Comentários adicionais/ Anotações de trabalho	Qualquer informação relevante. Marque a caixa de seleção para adicionar comentários adicionais. A partir da Resposta a vulnerabilidades v20.0, você pode adicionar anotações de trabalho na seção Anotações de um item vulnerável adiado.
Atividade	Aparece somente quando uma anotação de trabalho foi criada.
Links relacionados	
Calcular Pontuação de Risco	Quando as calculadoras de **gravidade de vulnerabilidade** ou de **pontuação de risco** estão habilitadas, o campo **Pontuação de risco** é atualizado.

A seguir estão as listas relacionadas a itens vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Tarefas de correção	Tarefas associadas a este item vulnerável.
Tarefas que afetam	Tarefas associadas a este item vulnerável.
Endereços IP associados	Disponível se a aplicação Integração de vulnerabilidade Qualys Vulnerability Integration estiver instalada. Endereços IP encontrados durante a desduplicação.
Serviços afetados	Serviços de negócio afetados por este item vulnerável. Mostrado quando essas informações estão disponíveis no registro do CMDB. Essas informações podem ser inseridas manualmente ou usando a aplicação ServiceNow® Mapeamento de serviços. Consulte Mapeamento de serviços para obter mais informações. Se um IC afetado associado ao item vulnerável for adicionado ou atualizado, as informações nesta lista relacionada serão atualizadas automaticamente quando o registro for salvo.
Tíquetes de Qualys	Qualys informações de integração de tíquete associadas a este item vulnerável.

Campos do formulário de solução

As soluções são criadas automaticamente quando os registros são baixados de integrações de soluções de terceiros e armazenados em **Soluções** em Resposta a vulnerabilidades.

Campos de entrada de integração de solução

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
Número	Identificador atribuído à solução.
Origem	Origem da solução.
ID da origem	Identificador de origem para esta solução.
Pontuação de risco	Separa a **pontuação de risco** do registro de solução em intervalos de Crítico a Nenhum. Para obter mais informações sobre a **classificação de risco**da solução, consulte Solução de gestão de vulnerabilidade. **Nota:** **A classificação de risco** da solução não é igual à **classificação de risco dos**registros de **item**vulnerável, **entrada de vulnerabilidade de terceiros** e **tarefa**de correção.
Pontuação de risco	Cálculo ponderado com base na **pontuação de risco** e na contagem de itens vulneráveis com esta solução como **solução preferencial**. Para obter mais informações sobre a pontuação de risco da solução, consulte Solução de gestão de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: **A pontuação de risco** do registro da solução não é igual à pontuação de risco do **item vulnerável**, **da entrada de vulnerabilidade de terceiros**e das **tarefas** de **correção**. Disponível quando o SAM NVD está habilitado, mas se não houver itens vulneráveis (VI) ativos associados a uma vulnerabilidade, a **pontuação de risco** da solução será definida como zero.
Substituição mais elevada	Indica que nenhuma solução a substitui.
Tipo de solução	Que tipo de solução é. As opções são: • Solução alternativa • Mitigação • Correção do Fornecedor • Patch • Acúmulo • Direito • Não Corrigirá • Nenhum disponível
Requer reinicialização	Reinicialização necessária. As opções são: • Sim • Não • Talvez
Data de publicação	Data em que a vulnerabilidade foi publicada por origem.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez pela origem.
Resumo	Resumo de correção da solução.
Informativo	Boletim de segurança associado à solução.
Categorias dos Produtos	Categorias de produto às quais a solução se aplica.
Produtos	Produtos aos quais a solução se aplica.
Detalhes da solução	
Descrição	Se nenhum conteúdo estiver disponível na origem da solução, você será direcionado para outra seção ou solução relevante para obter mais informações.
Links	Recursos de internet importados associados à solução.
Detalhes da Vulnerabilidade	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Anotações sobre vulnerabilidade	Resumo das vulnerabilidades corrigidas pela solução.
Status da Correção	
Metas de solução preferencial Status de correção de itens vulneráveis e seus itens de configuração (ICs) exclusivos, para os quais esta é a solução preferencial. **Nota:** Um IC exclusivo é aquele que é contado apenas uma vez, independentemente de quantos IVs ele esteja associado.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se a IVs para os quais esta solução é a preferencial. Esta contagem exclui IVs adiados.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção. Esta contagem exclui os ICs de itens vulneráveis adiados.
Total de ICs	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui os ICs de itens vulneráveis adiados.
Percentual de ICs corrigidos	Percentual concluído de ICs exclusivos corrigidos (o que significa que todos os IVs desse IC e desta solução foram corrigidos). Determinado pelo número de ICs corrigidos sobre o total de ICs exclusivos associados a itens vulneráveis com a solução preferencial. Esta contagem exclui os ICs de itens vulneráveis adiados.
Metas de solução preferencial (inclui adiadas) Status de correção de itens vulneráveis e seus ICs exclusivos, incluindo adiados, para os quais esta é a solução preferencial.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (VI). Aplica-se a IVs para os quais esta solução é a preferencial.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção.
Total de ICs	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Percentual de ICs corrigidos	Percentual concluído de ICs exclusivos corrigidos (o que significa que todos os IVs desse IC e desta solução foram corrigidos). Determinado pelo número de ICs corrigidos sobre o total de ICs exclusivos associados a itens vulneráveis com a solução preferencial. Esta contagem exclui os ICs de itens vulneráveis adiados.
Possíveis metas de solução Status de correção de itens vulneráveis e seus ICs exclusivos, com uma vulnerabilidade relacionada a esta solução.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
Possíveis metas de solução (inclui adiadas) Status de correção de itens vulneráveis e seus ICs exclusivos, incluindo adiados, com uma vulnerabilidade que pode ser corrigida por esta solução, incluindo contagens de soluções preferenciais.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção.
Anotações	
Anotações internas	Campo editável fornecido para o especialista em correção.
Links relacionados	
Atualizar status	Data e hora em que o status de correção foi atualizado pela última vez. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação e classificação de risco • Métricas da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis associados a esta solução como a solução preferencial para correção.
Vulnerabilidades de Terceiros	Vulnerabilidades de terceiros associadas a esta solução.
CVEs	Vulnerabilidades comuns de vulnerabilidade e exposição (CVE) associadas a esta solução.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tarefas de correção	Tarefas de correção que contêm itens vulneráveis relacionados com esta solução preferencial para correção.
Soluções Anteriores	Soluções anteriores que resolvem uma ou mais vulnerabilidades desta solução.
Soluções Substitutas	Soluções posteriores que resolvem todas as vulnerabilidades desta solução. Esta lista está vazia quando a caixa **de substituição mais alta** está marcada.

Configurações do fluxo de trabalho de aprovação para solicitação de cancelamento de atribuição

Você pode projetar o fluxo de trabalho de aprovação para a remoção de atribuições de itens vulneráveis (VIs, VITs), tarefas de correção, itens vulneráveis de aplicação (AVITs) e itens vulneráveis de contêiner (CVITs) para você e seu grupo.

VIT, tarefa de correção, AVIT e CVIT têm uma regra de aprovação padrão cada. Cada regra de aprovação tem uma configuração de aprovação padrão. Cada configuração de aprovação tem um nível de aprovador padrão. As regras de aprovação para VITs, tarefa de correção, AVIT e CVIT são habilitadas por padrão. Como administrador, você pode executar as seguintes ações navegando até **Todos** > **Resposta a vulnerabilidades** > **Minhas aprovações** > **Regras de aprovação** e selecionando a regra de aprovação apropriada.

- habilitar ou desabilitar uma regra de aprovação.
- criar e atualizar uma configuração de aprovação.
- defina condições para itens vulneráveis e tarefas de correção aos quais as regras de aprovação se aplicam.
- crie e atualize vários níveis de aprovador.

A tabela a seguir mostra as regras de aprovação padrão, as configurações de aprovação e os níveis do aprovador para um VIT, tarefa de correção, AVIT e CVIT que são enviados com o sistema de base.

Regras de aprovação padrão, configurações de aprovação e níveis de aprovador

Tipo	Regra de aprovação	Configuração de aprovação	Níveis de aprovação
VIT ou VI	Solicitação de mudança do campo de item vulnerável	Solicitação de mudança do campo de item vulnerável	Solicitação de cancelamento de atribuição de nível 1 para VI
Tarefa de correção	Solicitação de mudança do campo Grupo de vulnerabilidades	Solicitação de mudança de campo de vulnerabilidade	Nível 1: não atribuir solicitação para VG
AVIT	Solicitação de mudança do campo de item vulnerável da aplicação	Solicitação de mudança do campo de vulnerabilidade da aplicação	Cancelar atribuição de item de vulnerabilidade da aplicação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de aprovação padrão, configurações de aprovação e níveis de aprovador

Tipo	Regra de aprovação	Configuração de aprovação	Níveis de aprovação
CVIT	Aprovação para gestão de contêiner	Configuração padrão Cancelar atribuição de CVIT	Nível de aprovação de desatribuição de CVIT – 1

Para obter mais informações sobre como aprovar solicitações de cancelamento de atribuição, consulte Aprovar ou rejeitar uma solicitação de não atribuição no Resposta a vulnerabilidades.

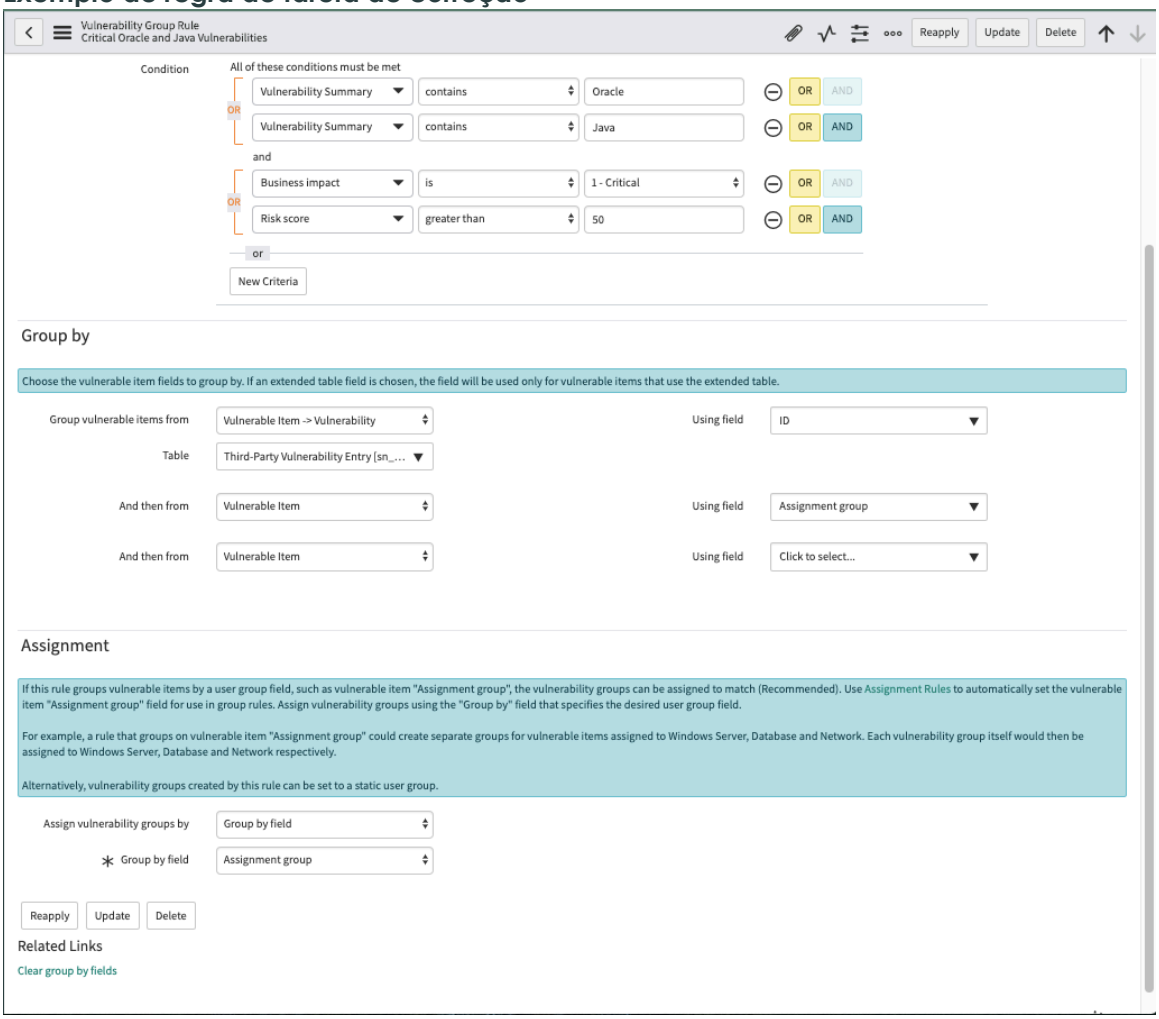
Resposta a vulnerabilidades exemplos de regra de tarefa de correção

Exemplos de regras de tarefa de correção usando vulnerabilidade e risco, ou impacto, ou item de configuração (IC).

Regra de tarefa de correção para agrupar itens vulneráveis Java e Oracle de alto risco

Este exemplo mostra um passo a passo da regra que agrupa itens vulneráveis Java e Oracle por vulnerabilidade e os atribui aos respectivos grupos de suporte.

Exemplo de regra de tarefa de correção



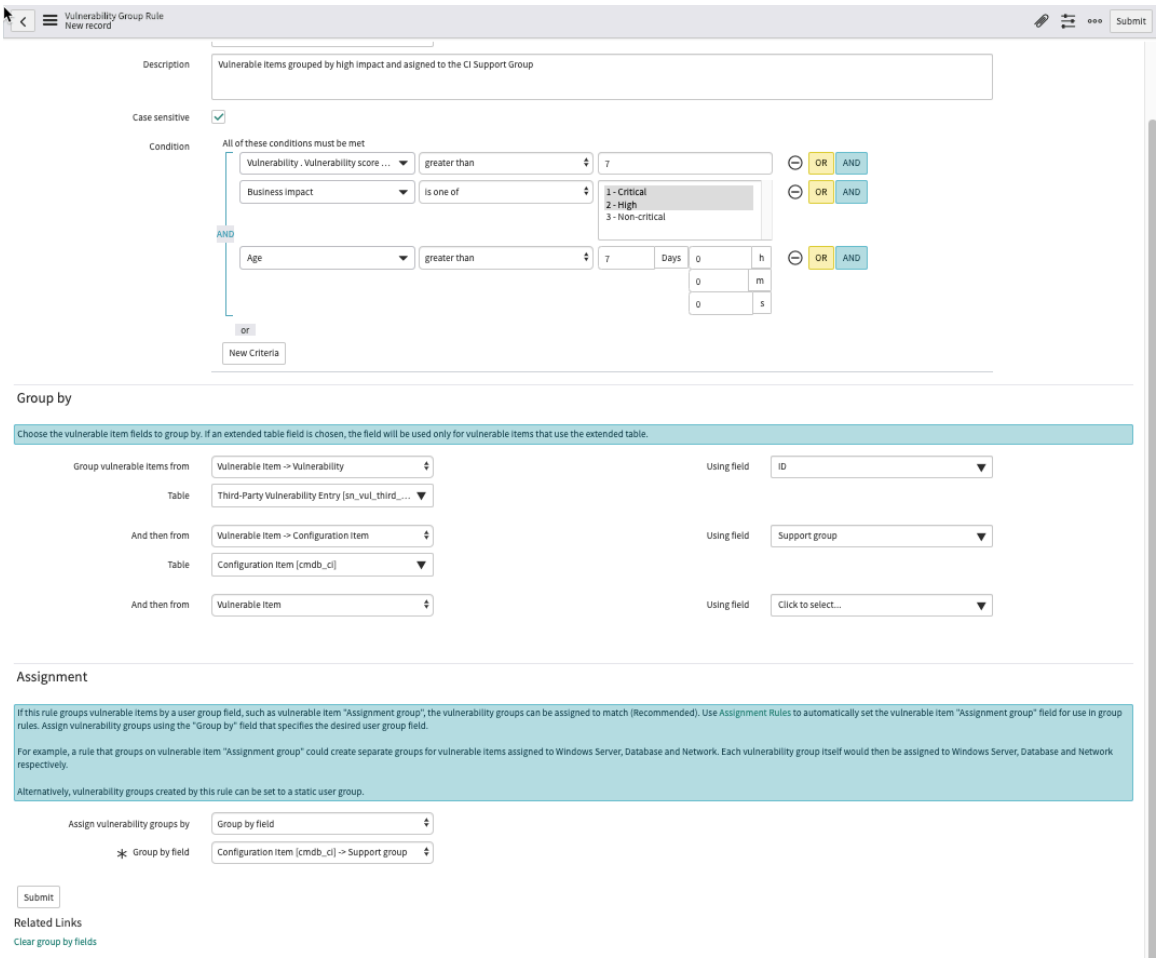
Clique com o botão direito do mouse no cabeçalho para **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regra de tarefa de correção para agrupar todos os itens vulneráveis de alto impacto por grupo de suporte de vulnerabilidade e IC

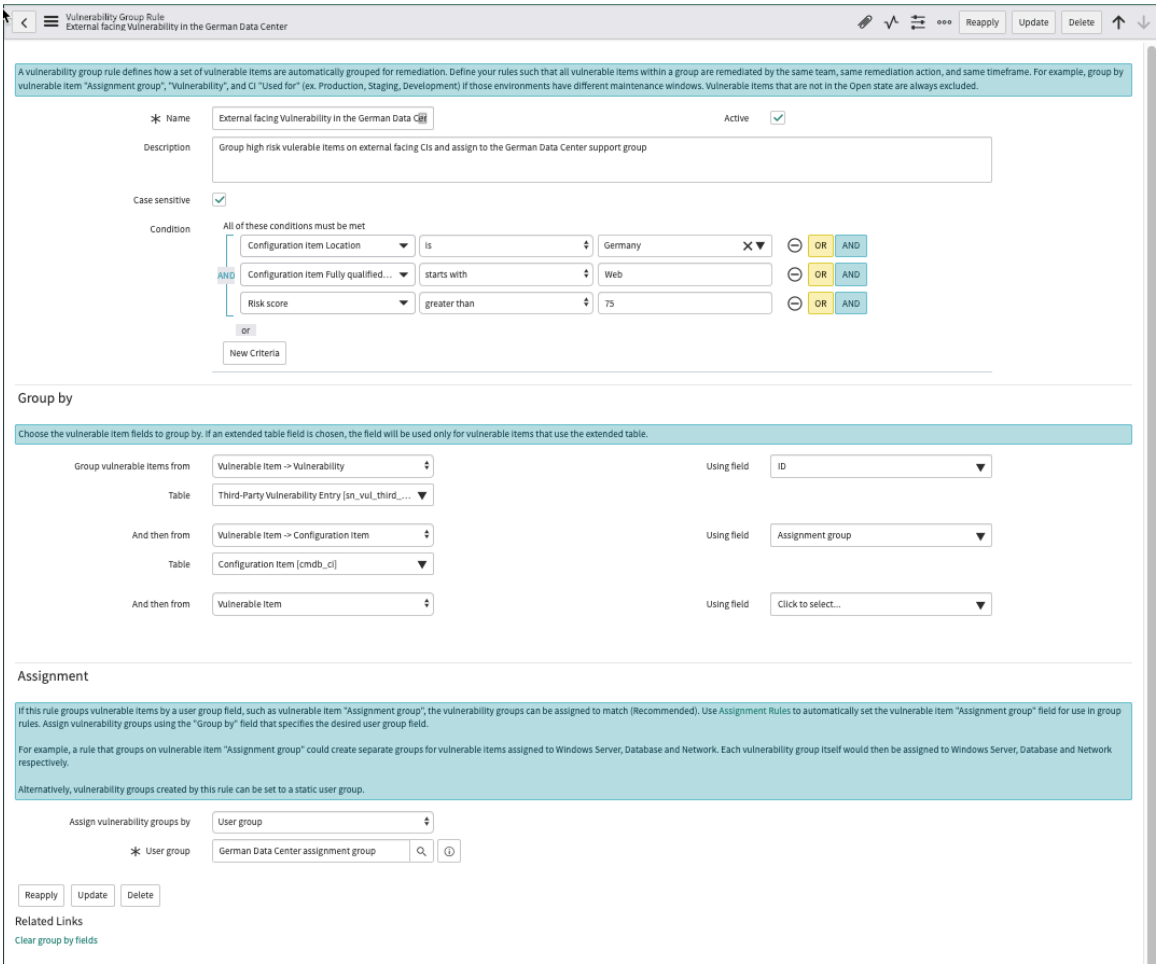
Este exemplo mostra as configurações de campo de formulário para uma regra de grupo para itens vulneráveis de alto impacto que os atribui ao grupo de suporte de IC.



Regra de tarefa de correção para agrupar todas as vulnerabilidades de alto risco em um IC externo em um datacenter alemão

Este exemplo mostra as configurações de campo de formulário para uma regra de grupo para vulnerabilidades de alto risco em ICs externos em um datacenter alemão. Eles são atribuídos ao grupo de atribuição de datacenter alemão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de cálculo de pontuação de risco para Resposta a vulnerabilidades

Você pode determinar as calculadoras de pontuação de risco para gerar pontuações de risco que usam os dados de vulnerabilidade e ativo exclusivos da sua organização.

Exemplo de determinação de pontuações de calculadoras de regra de risco

O exemplo a seguir demonstra como as pontuações das calculadoras de regra de risco são determinadas.

Suponha que uma calculadora de regra de risco esteja configurada com os campos nesta tabela:

Campo	Ponderação	Detalhamento de peso
Vulnerabilidade.Gravidade	50	Padrão: 20 1 - Crítico: 100 2 - Alto: 80 3 - Médio: 60 4 - Baixo: 40 5 - Nenhum: 20

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Ponderação	Detalhamento de peso
Exploração.Vulnerabilidade existe	50	Padrão: 50 Sim: 100 Não: 0

Além disso, suponha que os itens vulneráveis mostrados nesta tabela estejam presentes no sistema:

ID	Gravidade da vulnerabilidade	Existe exploração de vulnerabilidade
VIT00001	1 - Crítico	1 - Sim
VIT00002	2 - Alto	1 - Sim
VIT00003	3 – Médio	2 – Não
VIT00004	4 - Baixa	2 – Não
VIT00005	5 - Nenhum	2 – Não

O cálculo da pontuação de risco para os itens vulneráveis é calculado com base na fórmula:

```
Pontuação de risco = (W (gravidade) * FV (gravidade). + W (existem explorações) * FV (existem explorações)) / 100
```

em que **W** é o peso e **FV** é a porcentagem de peso do valor do campo.

A pontuação de risco resultante para esses itens vulneráveis é descrita nesta tabela:

ID	Gravidade da vulnerabilidade (50%)	Existe exploração de vulnerabilidade (50%)	Pontuação de risco resultante
VIT00001	1 - Crítico (50% x 100)	1 – Sim (50% x 100)	100
VIT00002	2 – Alto (50% x 80)	1 – Sim (50% x 100)	90
VIT00003	3 – Médio (50% x 60)	2 – Não (50% x 0)	30
VIT00004	4 – Baixo (50% x 40)	2 – Não (50% x 0)	20
VIT00005	5 - Nenhum (50% x 20)	2 – Não (50% x 0)	10

Nota: Para VIT00005, como o valor da gravidade está vazio, a ponderação padrão é aplicada.

Se a porcentagem de ponderação for alterada para um dos valores de campo, consulte esta tabela para obter os resultados:

Campo	Ponderação	Detalhamento de peso
Vulnerabilidade.Gravidade	50	• Padrão: 20 • 1 - Crítico: 100

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Ponderação	Detalhamento de peso
		• **2 - Alto: 70** *valor revisado • 3 - Médio: 60 • 4 - Baixo: 40
Exploração.Vulnerabilidade existe	50	• Padrão: 50 • Sim: 100 • Não: 0

A pontuação de risco dos itens vulneráveis após a reaplicação da calculadora é mostrada nesta tabela:

ID	Gravidade da vulnerabilidade (50%)	Existe exploração de vulnerabilidade (50%)	Pontuação de risco resultante
VIT00001	1 - Crítico (50% x 100)	1 – Sim (50% x 100)	100
VIT00002	**2 – Alto (50% x 70)** *valor revisado	1 – Sim (50% x 100)	**85** *valor revisado
VIT00003	3 – Médio (50% x 60)	2 – Não (50% x 0)	30
VIT00004	4 – Baixo (50% x 40)	2 – Não (50% x 0)	20
VIT00005	5 - Nenhum (50% x 20)	2 – Não (50% x 0)	10

Manipulação de erros para detecções

Os erros são registrados ao criar detecções ou ao criar e atualizar itens vulneráveis ao processar os anexos. Se um processo de integração de vulnerabilidades falhar, os erros serão registrados na guia "Log de integrações de vulnerabilidade".

Esses erros são registrados em log, com uma das seguintes categorias.

Campo	Descrição
Criação de VI	Erro ao criar ou atualizar a detecção.
Detecção	Erro ao criar uma detecção.

Experiência de dispositivos móveis Resposta a vulnerabilidades

Como proprietário de correção, você pode acessar a aplicação Resposta a vulnerabilidades (VR) em sua instância Now Platform® com seu dispositivo móvel Android ou iOS.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Resposta a vulnerabilidades

Para se familiarizar com os conceitos de resposta a vulnerabilidades e como este produto pode ajudar sua organização, consulte Noções básicas sobre Resposta a vulnerabilidades.

Nota: Antes de instalar o App Vulnerability Response Mobile mobile, familiarize-se com o Mobile Agent .

Visão geral

Como um usuário com a função de proprietário de correção (sn_vul.remediation_owner), o App Vulnerability Response Mobile permite que você exiba e pesquise vulnerabilidades, tarefas de correção e atribuições em sua instância Now Platform diretamente do seu dispositivo móvel Android ou iOS.

Você será notificado quando tarefas de correção (RTs) ou VIs forem atribuídas a você ou ao seu grupo de atribuição. Este aplicativo oferece ao responsável pela correção a flexibilidade de reatribuir, editar campos e iniciar a correção sem estar vinculado à área de trabalho.

Você tem acesso a vulnerabilidades, itens de vulnerabilidade, módulos e todas as soluções. Você pode executar as seguintes tarefas no seu dispositivo móvel:

- Exibir e atualizar tarefas de correção.
- Exibir solicitações de mudança.
- Reatribuir uma tarefa de correção ou item de vulnerabilidade a outro membro de um grupo de atribuição.
- Exiba notificações quando uma tarefa de correção crítica for atribuída a você ou a um de seus grupos de atribuição.
- Edite um subconjunto de campos em registros de tarefa de correção.
- Pesquise tarefas de correção que correspondam a critérios de pesquisa específicos.

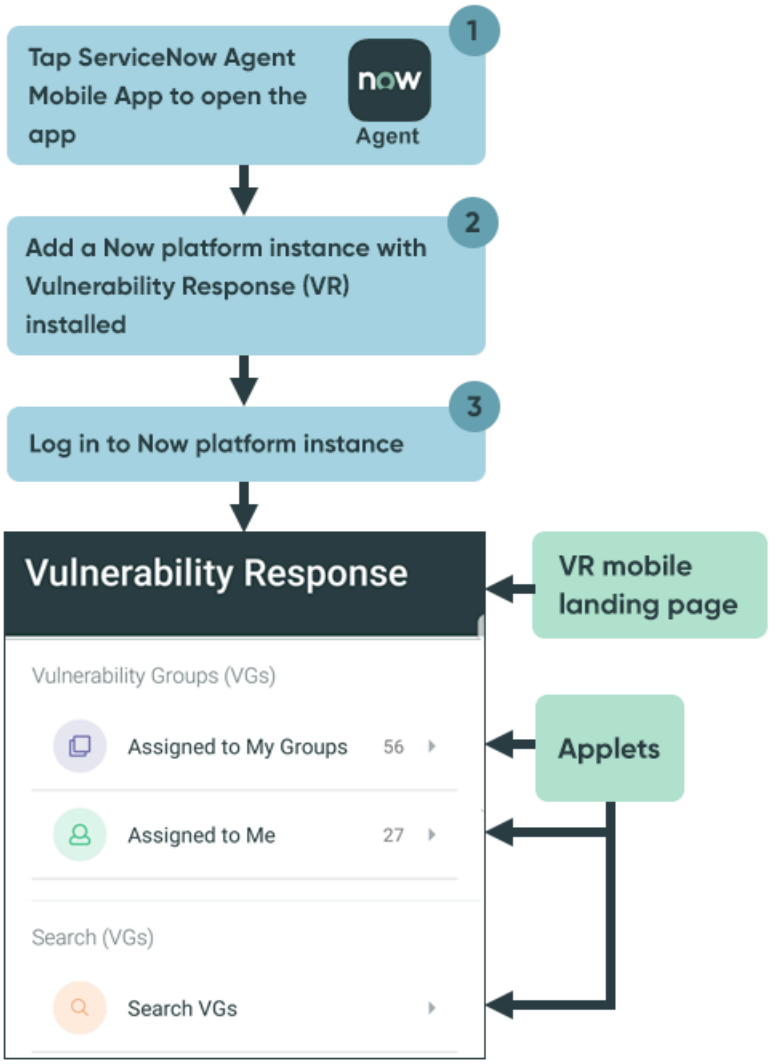
A figura a seguir ilustra como você faz login na instância Now Platform do seu dispositivo móvel e a tela inicial do App Vulnerability Response Mobile que é exibida após o login.

Para obter instruções passo a passo sobre como configurar sua instância Now Platform e instalar o App Vulnerability Response Mobile, consulte Configurar check-list para o App Vulnerability Response Mobile. Para obter instruções sobre como fazer login, consulte Faça login no App Vulnerability Response Mobile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

App Vulnerability Response Mobile



Aplicações

Aplicações são os ServiceNow componentes de software, como Security Incident Response (SIR), Resposta a vulnerabilidades (VR), Governança, risco e conformidade (GRC) e outros ServiceNow produtos que fornecem recursos e funcionalidades específicos em sua instância Now Platform. Depois de instalar as aplicações principais que têm aplicativos para celular em sua instância Now Platform, essas aplicações são exibidas como ícones na parte inferior do seu dispositivo móvel.

Ícone da Resposta a vulnerabilidades no dispositivo móvel

Pastas

Cada aplicação ServiceNow® mobile contém pastas que separam os applets por categorias. Na imagem anterior, as tarefas de correção e a pesquisa (VGs) são as pastas do App Vulnerability Response Mobile.

Applets

Applets são as diferentes opções na aplicação. Na imagem anterior, os ícones em Tarefas de correção e Pesquisa (VGs) são os applets disponíveis para o App Vulnerability Response Mobile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte os tópicos a seguir para obter mais informações sobre os applets do App Vulnerability Response Mobile.

Configurar check-list para o App Vulnerability Response Mobile

A check-list a seguir inclui as tarefas de configuração que você deve concluir na instância Now Platform® e no dispositivo móvel antes de usar o App Vulnerability Response Mobile.

Antes de Iniciar

Mais informações seguem cada etapa na coluna à direita. Tempo estimado para concluir esta tarefa: 15 a 20 minutos.

Funções necessárias: admin, sn_vul.remediation_owner

Você configurou com sucesso seu dispositivo móvel para App Vulnerability Response Mobile. A próxima etapa é fazer login no App Vulnerability Response Mobile e adicionar uma instância Now Platform ao seu dispositivo móvel.

Procedimento

1. Como opção, imprima esta check-list e use-a para orientá-lo nas tarefas necessárias para instalar o App Vulnerability Response Mobile.
2. Verifique se cada item da lista está concluído para que você possa fazer login em App Vulnerability Response Mobile e adicionar uma instância Now Platform.

Check-list para dispositivos móveis

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você tem a aplicação principal Resposta a vulnerabilidades instalada em uma instância Now Platform. Esta é a instância Now Platform que você exibe no seu dispositivo móvel. **Nota:** A aplicação principal Resposta a vulnerabilidades e a instância Now Platform devem ser da mesma versão da família. **a.** Para verificar se a aplicação principal está instalada em sua instância, navegue até Plug- **ins** e pesquise por Resposta a vulnerabilidades. **b.** Se a aplicação principal Resposta a vulnerabilidades ainda não estiver instalada, clique em **Instalar** para instalá-la. Para obter mais informações sobre como instalar a aplicação principal Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades. Para obter mais informações sobre como obter a aplicação principal Resposta a vulnerabilidades no ServiceNow Store, obter direitos, instalar aplicações principais e ativar dependências, consulte .
☐	Como um usuário com a função de administrador, verifique se você tem o App Vulnerability Response Mobile instalado na instância Now Platform que deseja exibir no seu dispositivo móvel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Nota: As instâncias App Vulnerability Response Mobile e Now Platform devem ser da mesma versão da família. As aplicações App Vulnerability Response Mobile e Resposta a vulnerabilidades devem ser compatíveis. Para obter mais informações sobre a compatibilidade da aplicação Resposta a vulnerabilidades, consulte Resposta a vulnerabilidades e matriz de compatibilidade de conformidade de configuração . Baixe e instale o App Vulnerability Response Mobile do ServiceNow Store na sua instância Now Platform. Quando você instala o App Vulnerability Response Mobile, suas dependências, com.glide.sg e com.glide.sg.agent_native_client, também são instaladas. Para verificar se essas dependências estão instaladas: **a.** Navegar até **Todos** > **Plug-ins**. **b.** Pesquise os IDs de plug-in (com.glide.sg e com.glide.sg.agent_native_client). **c.** Se eles não estiverem ativados, ative esses plug-ins. Esses plug-ins são necessários para o App Vulnerability Response Mobile. Para obter mais informações sobre como obter a aplicação App Vulnerability Response Mobile no ServiceNow Store, obter direitos, instalar aplicações e ativar dependências, consulte .
☐	Como um usuário com a função de administrador, em sua instância Now Platform, verifique se você atribuiu usuários móveis com as funções Now Platform necessárias. **a.** Para exibir as funções atribuídas a um usuário, navegue até **Todos** > **Administração** > **Usuários**. **b.** Selecione o nome de usuário seguido pela lista relacionada de funções. Todas as funções atribuídas a este usuário são exibidas. **c.** Verifique se um usuário está atribuído ou atribua um usuário com a função de biblioteca de infraestrutura de TI (itil). Usuários com a função itil podem criar, abrir, atualizar e fechar solicitações de mudança e tarefas de correção. Somente usuários com a função itil podem ter tarefas atribuídas a eles. **d.** Verifique se um usuário está atribuído ou atribua a um usuário a função de proprietário de correção (sn_vul.remediation_owner). Usuários com a função sn_vul.remediation_owner podem ler registros de vulnerabilidade e solução. Esta função é adicionada automaticamente quando você atribui a função itil. **e.** Verifique se você criou todos os grupos de atribuição necessários e atribuiu usuários móveis a esses grupos. **Nota:** Se você tiver um grande número de usuários para o aplicativo para celular, como alternativa, poderá atribuir a função sn_vul.remediation_owner a um grupo. Cada usuário adicionado ao grupo herda esta função.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações sobre regras de atribuição e grupos, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Para obter mais informações sobre usuários e atribuição de funções a usuários e grupos, consulte Administração de usuários .
☐	Como um usuário com a função de proprietário de correção (sn_vul.remediation_owner), baixe o aplicativo ServiceNow® Agent mais atual no seu dispositivo móvel. O app Agent mais atual está disponível na Apple iOS App Store e na Google Play Store.
☐	Como um usuário com a função sn_vul.remediation_owner, verifique se as notificações estão habilitadas no seu dispositivo móvel e na sua instância Now Platform. As notificações informam quando tarefas de correção críticas são atribuídas a você ou ao seu grupo de atribuição. Para ajudá-lo com a correção oportuna, depois de habilitar as notificações, clique em uma notificação no App Vulnerability Response Mobile e navegue diretamente para o registro. Para habilitar notificações em sua instância Now Platform para que sejam exibidas em seu dispositivo móvel, siga estas etapas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	a. Verifique se você baixou e instalou o App Vulnerability Response Mobile em sua instância Now Platform. **b.** Em Configurações do sistema na sua instância Now Platform, em Notificações, verifique se você habilitou o **Aplicativo para celular da ServiceNow**. Para obter mais informações sobre como definir notificações, consulte Como definir preferências de notificação no IU principal . Now Platform notificações também são exibidas na tela de mensagens do seu dispositivo móvel. Verifique se as notificações também estão habilitadas nas configurações do seu dispositivo móvel.

Faça login no App Vulnerability Response Mobile

Abra o aplicativo para celular Resposta a vulnerabilidades e adicione uma instância da Now Platform com Resposta a vulnerabilidades ao seu dispositivo móvel.

Antes de Iniciar

Verifique se você concluiu as etapas de configuração descritas em Configurar check-list para o App Vulnerability Response Mobile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 a 7 minutos.

Procedimento

1. No seu dispositivo móvel, toque no aplicativo **ServiceNow Agent**.

   Se você ainda não estiver conectado a uma instância Now Platform, a tela Instâncias será exibida.

2. Se a instância Now Platform com a aplicação principal Resposta a vulnerabilidades ainda não tiver sido adicionada ao seu dispositivo móvel, siga estas etapas para adicioná-la.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na tela Instâncias exibida, toque no ícone de).
Uma tela é exibida solicitando que você insira e salve um endereço de uma instância Now Platform.

b. Preencha os campos.

Nome do campo	Descrição
Insira o endereço da instância ou leia um código QR.	Escolha uma para continuar: ▪ Antes de `.service-now.com`, insira o nome da sua instância Now Platform, por exemplo, `vrmobilenewyorkagent`. ▪ Insira um endereço. Este endereço é o URL da instância Now Platform que você deseja exibir no seu dispositivo móvel. ▪ Verificar um código QR.
(Opcional) Insira o apelido	Insira um apelido para esta instância. Se você tiver várias instâncias adicionadas ao dispositivo, os apelidos poderão ajudá-lo a localizar rapidamente uma instância Now Platform.

c. Tocar em **Salvar e fazer login**

3. Na tela de login ServiceNow exibida, insira o Nome de usuário e a Senha da instância Now Platform que você deseja adicionar e toque em **Login**.
A tela inicial da Resposta a vulnerabilidades é exibida. Você fez login com sucesso no App Vulnerability Response Mobile !

4. Depois de fazer login, verifique se as notificações estão habilitadas no App Vulnerability Response Mobile.

a. Na tela inicial na parte inferior, toque em **Notificação**.

b. Na tela Notificações, toque em **Habilitar notificações** se não estiver habilitado.
As notificações do Now Platform são exibidas na tela Notificações no App Vulnerability Response Mobile.

5. Depois de fazer login em uma instância no seu dispositivo móvel, é a instância Now Platform padrão no dispositivo.
Se você quiser exibir outro Now Platform no dispositivo, deverá fazer logout da instância padrão. Para sair:

a. Toque no ícone **Configurações**.

b. Toque **em Logout**.
A tela Instâncias é exibida com todas as instâncias Now Platform que você adicionou ao dispositivo móvel.

c. Opcional: Toque em outra instância para fazer login nela ou, como alternativa, siga as etapas anteriores para adicionar outra instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Se a tela de instâncias do App Vulnerability Response Mobile não for exibida depois que você tocar no app **ServiceNow Agent** no seu dispositivo, verifique se o **ServiceNow Agent** é permitido como um app confiável no seu dispositivo. Para permitir o acesso como um app confiável, navegue até as configurações e gestão geral de dispositivos no seu dispositivo e toque na opção (app Truste etc.) para permitir o acesso.

Se uma mensagem de erro for exibida depois que você inserir suas credenciais na tela de login, verifique se o nome de usuário e a senha da instância Now Platform estão corretos.

Se você tiver problemas para visualizar a tela inicial, verifique sua conexão de rede.

Se você não conseguir exibir a tela Instâncias depois de tocar no aplicativo **ServiceNow Agent**, tente desinstalá-lo do seu dispositivo. Verifique se você tem a versão mais atual do app na Apple iOS App Store ou na Google Play Store e tente reinstalá-la.

Exibir, atribuir e editar tarefas de correção com o App Vulnerability Response Mobile

Exiba, atribua ou edite os campos nos registros de tarefa de correção (RT) atribuídos ao seu grupo. Navegue pelas vulnerabilidades, itens de vulnerabilidade e registros de soluções e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Antes de Iniciar

Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

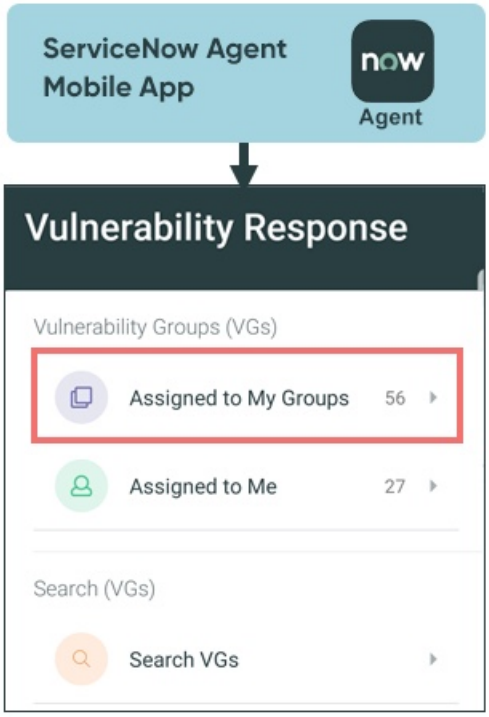
Atribua registros RT (VUL) a você mesmo ou reatribua-os a outro membro do seu grupo. Como alternativa, exiba os detalhes dos registros de tarefas de correção ativas, Itens vulneráveis (VI), vulnerabilidades do NVD e soluções antes de editar, atribuir ou corrigir. Tempo para concluir esta tarefa: 5 a 10 minutos.

Procedimento

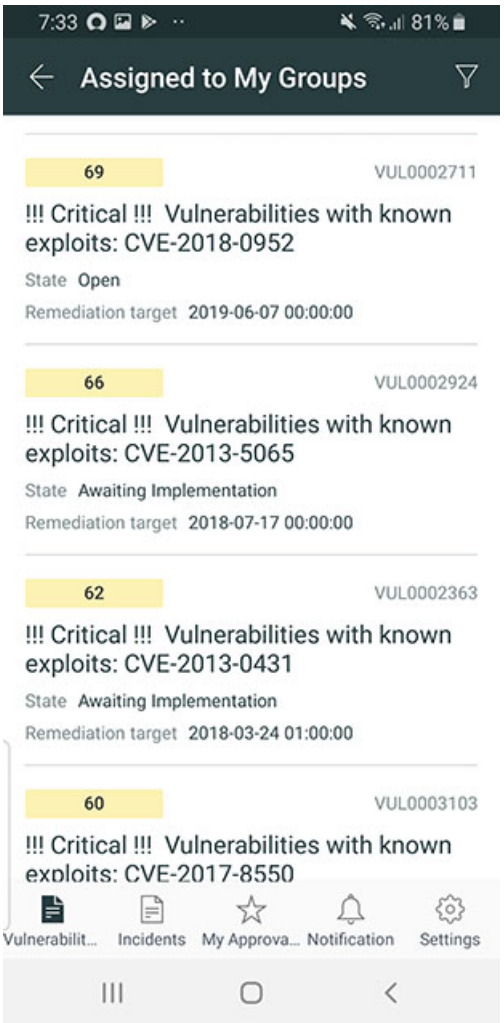
1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no App Vulnerability Response Mobile.
2. Com a tela inicial da Resposta a vulnerabilidades exibida, toque **em Atribuído a Meus grupos**.
   Se você sair de App Vulnerability Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A lista de registros em aberto atribuídos ao seu grupo é exibida.



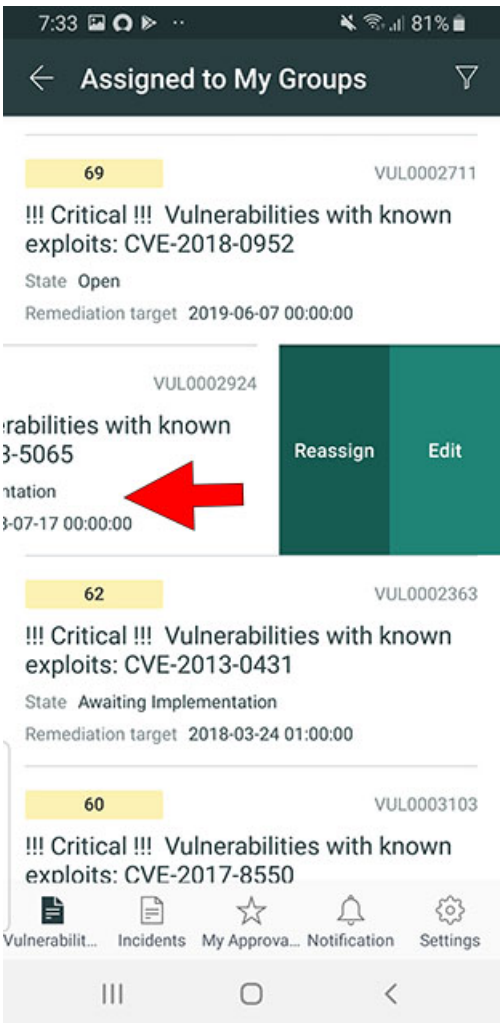
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Opcional: Consulte Pesquisar tarefas de correção com o App Vulnerability Response Mobile para pesquisar registros que correspondam a critérios específicos.

4. Como alternativa, com o ícone de filtro (Ícone de) exibido, defina filtros para limitar o número de registros na lista.
   A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições no Now Platform.

5. Para reatribuir ou editar um registro diretamente da lista, com a lista de registros abertos exibida, deslize para a esquerda em um registro para abrir o menu.



6. Escolha um no menu exibido para continuar.

Opção	Descrição
Atribuir a mim	Se o registro RT já estiver atribuído a você, esta opção não será exibida. Toque **em Atribuir a mim** para atribuir o RT a você mesmo. Seu nome é exibido no campo Atribuído a no registro. Uma mensagem é exibida confirmando a atribuição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

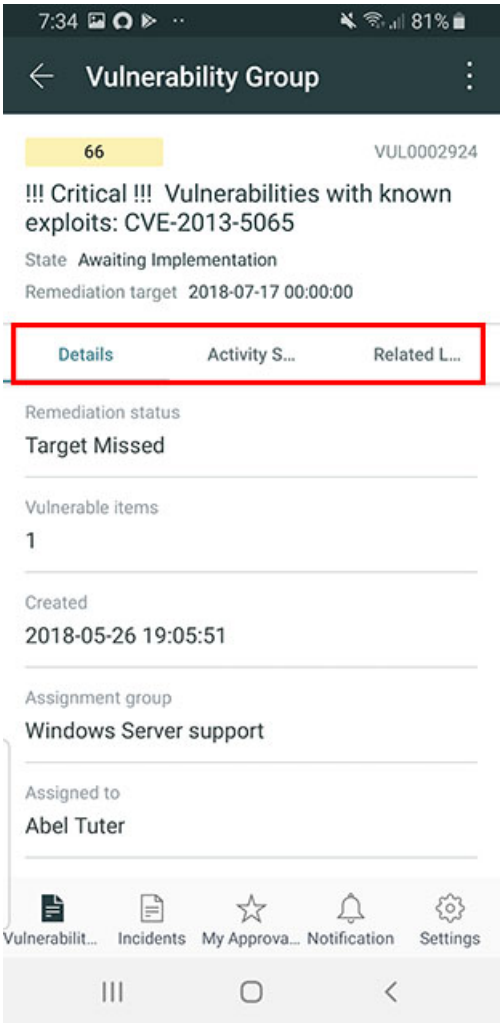
Opção	Descrição
Reatribuir	Para reatribuir o RT a um grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Na lista, toque em um grupo ou insira o texto no campo de pesquisa. Para atribuir ou reatribuir o RT a um membro de um grupo de atribuição: **a.** Toque **em Atribuído a**. **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio (ícone de) ou em **Enviar** para salvar e enviar suas mudanças.
Editar	**a.** Toque em **Editar**. **b.** Expanda os campos e selecione uma opção na lista exibida ou insira o texto no campo Pesquisar. Toque no ícone de envio (ícone de) ou em **Enviar** para salvar e enviar suas mudanças.

7. Como alternativa, para exibir os detalhes de um registro de vulnerabilidade aberto e ver mais registros associados e listas relacionadas, com a tela Atribuído aos Meus grupos exibida, toque em um registro na lista.

8. No registro de tarefa de correção em aberto exibido, escolha uma opção na tabela a seguir para exibir anotações de trabalho ou listas relacionadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos do registro RT. Toque no ícone do menu (ícone do ⋮) no canto superior direito da tela para exibir as opções disponíveis. As opções exibidas neste menu expandido variam. As ações de correção que você pode realizar em seus itens vulneráveis variam e dependem do valor exibido no campo Estado do registro. Para obter mais informações sobre o campo Estado e suas opções de correção, consulte Resposta a vulnerabilidades tarefa de correção e estados de itens vulneráveis.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ◦ Exiba a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	) para adicionar uma anotação de trabalho ou anexar um arquivo. ◦ Toque no ícone do menu (ícone do) no canto superior direito da tela para exibir as opções de correção disponíveis.
Listas relacionadas	Com a guia Listas relacionadas selecionada, exiba qualquer uma das listas relacionadas do registro RT que estão preenchidas. ◦ Toque **em Itens vulneráveis**. Toque em um registro de item vulnerável (VI) e navegue até o registro de solução preferencial. Consulte a figura que segue a tabela para obter um mapa de navegação e mais detalhes. ◦ Toque **em Solicitações de mudança**. Exiba uma lista das solicitações de mudança associadas a este registro. ◦ Quando exibido, toque no ícone do menu (ícone do) no canto superior direito de uma tela para exibir as opções de correção disponíveis.

A imagem a seguir ilustra o caminho de navegação do registro da tarefa de correção até o registro de solução preferencial para a vulnerabilidade selecionada. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caminho de navegação da tarefa de correção por meio de um registro de solução

9. Depois de revisar, editar ou corrigir, escolha um para continuar.

Opção	Descrição
Toque em um ícone na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone da Resposta a vulnerabilidades para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do App Vulnerability Response Mobile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual.

Exibir, reatribuir e editar tarefas de correção atribuídas a você com o App Vulnerability Response Mobile

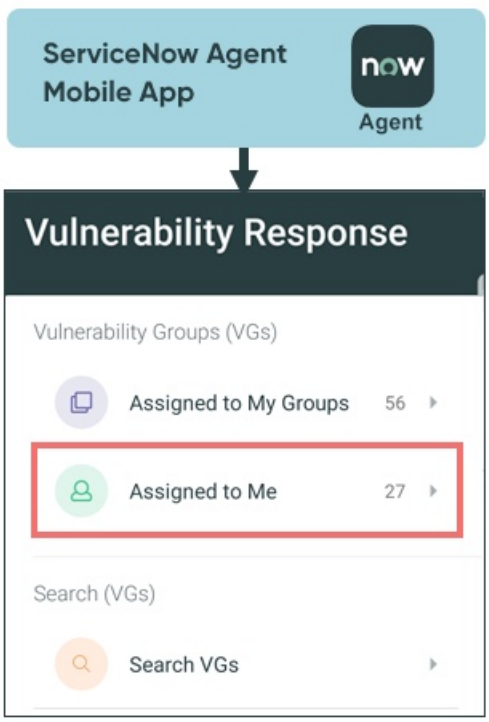
Exiba, atribua ou edite os campos nos registros de tarefas de correção atribuídos a você. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Antes de Iniciar
Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa
Reatribuir ou editar registros atribuídos a você. Exiba os detalhes dos registros de tarefas de correção ativas, registros de itens vulneráveis (VI), vulnerabilidades e soluções antes de editar, atribuir ou corrigir. Tempo para concluir esta tarefa: 5 a 10 minutos.

Procedimento

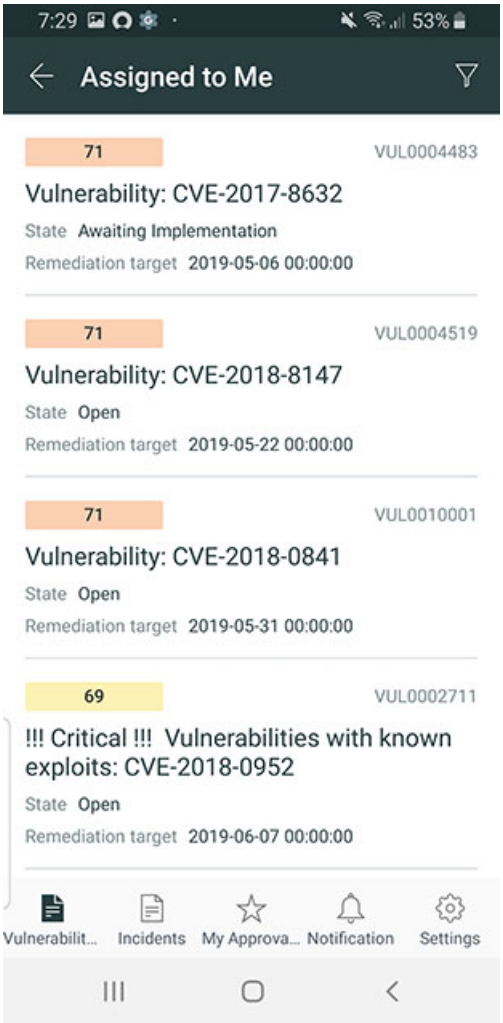
1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no App Vulnerability Response Mobile.
2. Com a tela inicial da **Resposta a vulnerabilidades** exibida, toque **em Atribuído a mim**. Se você sair de App Vulnerability Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A lista de registros de tarefa de correção atribuídos a você é exibida.

Tradução automática

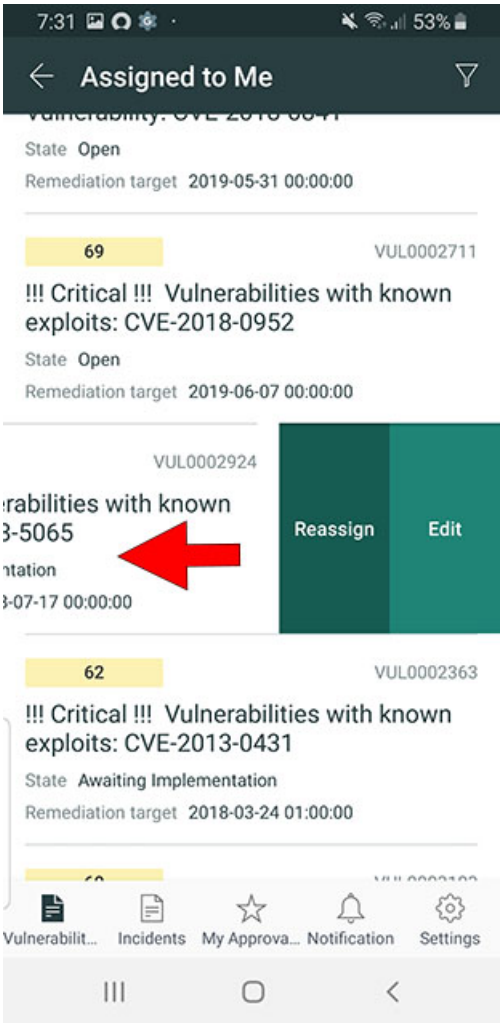
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Opcional: Consulte Pesquisar tarefas de correção com o App Vulnerability Response Mobile para pesquisar registros que correspondam a critérios específicos.
4. Como alternativa, com o ícone de filtro (Ícone de) exibido, defina filtros para limitar o número de registros na lista.
   A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições no Now Platform.
5. Para reatribuir ou editar o registro diretamente da lista, com a tela Atribuído a mim exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Escolha um para continuar.

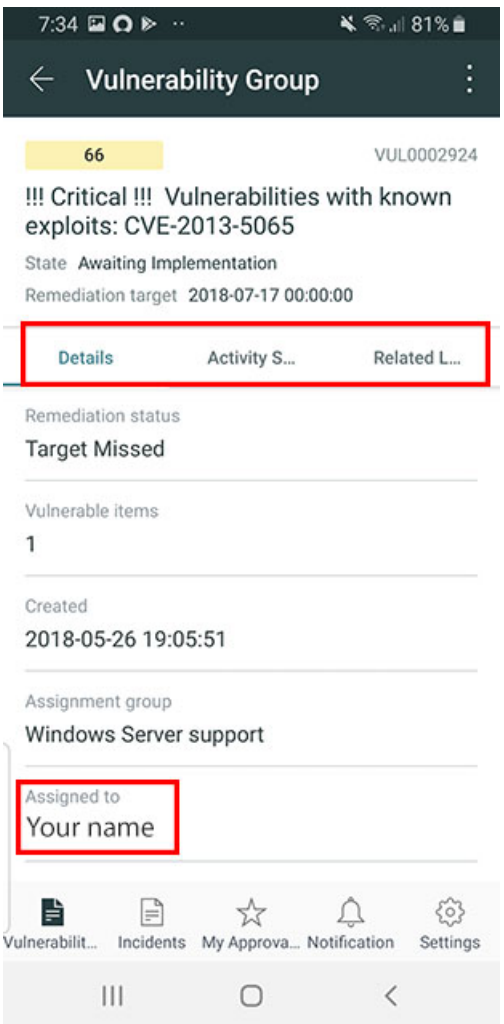
Opção	Descrição
Reatribuir	Para reatribuir a tarefa a outro grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. Para atribuir ou reatribuir o RT a um membro de um grupo de atribuição: **a.** Toque **em Atribuído a**. **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio (ícone de) ou em **Enviar** para salvar e enviar suas mudanças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Editar	**a.** Toque em **Editar**. **b.** Expanda os campos e selecione uma opção na lista exibida ou insira o texto. **c.** Toque no ícone de envio (ícone de) ou em **Enviar** para salvar e enviar suas mudanças.

7. Como alternativa, para exibir os detalhes de um registro aberto e ver mais registros associados e listas relacionadas, com a tela Atribuído a mim exibida, toque em um registro na lista.
8. No registro de tarefa de correção em aberto exibido, escolha uma opção na tabela a seguir para exibir anotações de trabalho ou listas relacionadas.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos do registro da tarefa de correção. Toque no ícone do menu (ícone do) no canto superior direito da tela para exibir as opções disponíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	As opções exibidas neste menu expandido variam. As ações de correção que você pode realizar em seus itens vulneráveis variam e dependem do valor exibido no campo Estado do registro. Para obter mais informações sobre o campo Estado e suas opções de correção, consulte Resposta a vulnerabilidades tarefa de correção e estados de itens vulneráveis.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ◦ Exiba a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de ( ) para adicionar uma anotação de trabalho ou anexar um arquivo. ◦ Toque no ícone do menu (ícone do) no canto superior direito da tela para exibir as opções de correção disponíveis.
Guia Listas relacionadas	Com a guia Lista relacionada selecionada, exiba as listas relacionadas do registro que estão preenchidas. ◦ Toque **em Solicitações de mudança**. Exiba uma lista das solicitações de mudança associadas a este registro. ◦ Toque **em Itens vulneráveis**. Toque em um registro de item vulnerável (VI) e navegue até o registro de solução preferencial. Consulte a figura que segue a tabela para obter um mapa de navegação e mais detalhes. ◦ Quando exibido, toque no ícone do menu (ícone do) no canto superior direito da tela para exibir as opções de correção disponíveis.

A imagem a seguir ilustra o caminho de navegação do registro da tarefa de correção até o registro de solução preferencial para a vulnerabilidade selecionada. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caminho de navegação de RT por meio de um registro de solução

Tradução automática

9. Escolha um para continuar.

Opção	Descrição
Toque em um ícone na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone da Resposta a vulnerabilidades para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do App Vulnerability Response Mobile. ◦ Toque em **Configurações** e escolha uma para continuar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual. Para fazer login, toque **em Logout**.

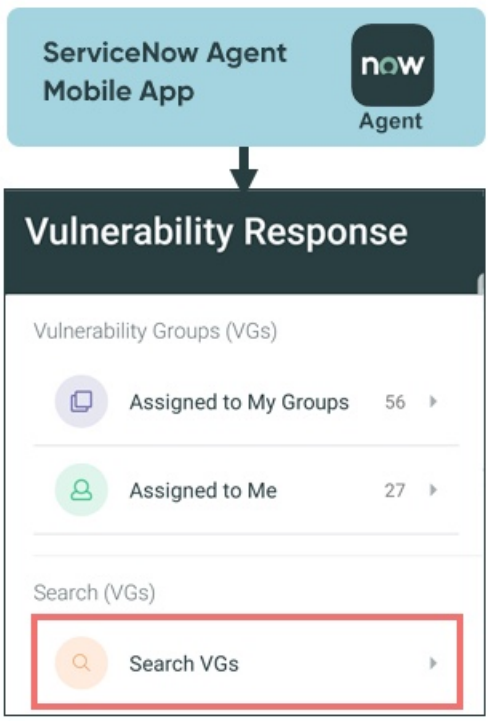
Pesquisar tarefas de correção com o App Vulnerability Response Mobile

Pesquise tarefas de correção que correspondam aos critérios de pesquisa específicos selecionados.

Antes de Iniciar
Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa
Tempo para concluir esta tarefa: 5 a 7 minutos.

Procedimento
1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no App Vulnerability Response Mobile.
2. Com a tela inicial da **Resposta a vulnerabilidades** exibida, toque **em Pesquisar RTs**.
   Se você sair de App Vulnerability Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



3. Na tela Pesquisar que é exibida, toque nos campos e preencha o formulário com os critérios de pesquisa desejados.

   Siga as instruções após a tabela para editar os critérios de pesquisa, limpar os critérios de pesquisa ou enviar uma pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar uma entrada em iOS dispositivos
Número	Toque na tela e insira um número de RT, por exemplo, (VUL0002372). Esse número é exibido no canto superior direito do registro de RT. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone de fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Insira um número de RT, por exemplo, (VUL0002372). Este número é exibido no canto superior direito do registro de RT. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Pontuação de risco	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone de fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Status da Correção	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone de fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Estado	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone de fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Motivo	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android **dispositivos**	Para adicionar uma entrada em iOS **dispositivos**
	Toque no ícone de fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Grupo de atribuição	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.
Atribuído a	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.
Descrição resumida	Toque na tela e insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs.	Na tela, insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Descrição	Toque na tela e insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs.	Na tela, insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres de texto parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela SearchRTs.

Para dispositivos Android, com a tela Pesquisar RTs exibida e todos os seus critérios inseridos, escolha um para continuar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Limpar ou modificar os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios inseridos, com a tela Pesquisar RTs exibida, toque na seta para voltar para limpar todos os campos e retornar à tela inicial da Resposta a vulnerabilidades. A pesquisa não foi enviada e os critérios de pesquisa foram limpos. Como alternativa, para editar um campo, ◦ Com a tela Pesquisar RTs exibida, toque em um campo com critérios de pesquisa para expandi-lo. ◦ Toque em um item para desmarcá-lo. Toque em Todos para selecionar todos os itens. Toque em **Todos** novamente para limpar todos os itens. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**. ◦ Toque no ícone de marca de seleção para salvar as mudanças e retornar à tela Pesquisar RTs.
Enviar uma pesquisa	Com a tela Pesquisar RTs exibida com os critérios de pesquisa inseridos, toque no ícone de envio (ícone de). Os registros da tarefa de correção que correspondem aos seus critérios de pesquisa são exibidos. Depois que a pesquisa é concluída, os critérios de pesquisa não são salvos.

4. Para dispositivos iOS, com a tela Pesquisar RTs exibida, escolha um para continuar.

Opção	Descrição
Limpar ou modificar os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios e retornar à tela inicial, toque no ícone de fechar (X). Os critérios de pesquisa inseridos não são salvos. Como alternativa, para editar um campo: **a.** Com a tela Pesquisar RTs exibida, toque em um campo com critérios de pesquisa para expandi-lo. **b.** Toque em um item da lista para desmarcá-lo ou toque em **Limpar tudo**. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**. **c.** Toque em **Concluído** para salvar as mudanças e retornar à tela Pesquisar RTs.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Enviar uma pesquisa	Com a tela Pesquisar RTs exibida com os critérios de pesquisa inseridos, toque em **Pesquisar**. Os registros de RT que correspondem aos seus critérios de pesquisa são exibidos. Depois que a pesquisa é concluída, os critérios de pesquisa não são salvos.

5. Opcional: Se a pesquisa retornar vários registros, você pode Filtrar registros com o App Vulnerability Response Mobile para refinar os resultados da pesquisa.

Filtrar registros com o App Vulnerability Response Mobile

Defina filtros adicionais para limitar o número de registros exibidos em uma tela. A filtragem de registros no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

Antes de Iniciar

Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 minutos.

Procedimento

1. Para refinar ainda mais os resultados da pesquisa ou para inserir critérios de filtro adicionais em qualquer lista de registros exibida, toque no ícone de filtro (ícone de).
2. Com a tela Filtros exibida, toque em um campo para expandi-lo.
   Um campo comum para inserir critérios de pesquisa para registros de tarefa de correção é o campo Estado.
3. Nas opções exibidas, toque na caixa de seleção ou toque em um item para o filtro.
   Para muitos dos filtros, você pode selecionar mais de uma opção.
4. Toque no ícone Voltar (ícone para trás) ou em **CONCLUÍDO** para salvar suas mudanças em um campo.
   Os critérios escolhidos são exibidos na tela Filtros. O número de registros que correspondem aos seus critérios também é exibido na parte superior da tela. Toque em **REDEFINIR** para remover todos os filtros e restaurar a configuração padrão.
5. Opcional: Repita as etapas 1 a 4 com a tela Filtros exibida para continuar definindo seus critérios de filtro.
6. Toque no ícone de interseção (ícone de) para criar condições E.
7. Como alternativa, toque no ícone de interseção (ícone de) para criar condições OU.
8. Depois de adicionar todos os critérios desejados, com a tela Filtros exibida, toque em **CONCLUÍDO**.
   Na tela, somente os registros que correspondem aos critérios de filtro são exibidos.

Informações relacionadas

Pesquisar tarefas de correção com o App Vulnerability Response Mobile

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Orquestração de resposta a vulnerabilidades

Com Orquestração de resposta a vulnerabilidades fluxos de trabalho e atividades, você pode interagir e recuperar dados de sistemas e ambientes baseados no Windows ou UNIX usando a orquestração de fluxo de trabalho. Ao aprimorar os dados, você pode encurtar o ciclo de vida de correção.

Para obter mais informações sobre como editar fluxos de trabalho ou criar fluxos de trabalho personalizados, consulte Explorando fluxos .

Orquestração de resposta a vulnerabilidades fluxos de trabalho e atividades

Vários fluxos de trabalho estão incluídos com Orquestração de resposta a vulnerabilidades. Fluxos de trabalho e atividades automatizam e agilizam seus processos. Use fluxos de trabalho e atividades para criar registros de verificação, verificar itens vulneráveis, criar registros de verificação e muito mais.

Resposta a vulnerabilidades - Verificar fluxo de trabalho de vulnerabilidade

Automatize as verificações de vulnerabilidade para um ou vários itens vulneráveis usando o fluxo de trabalho **Resposta a vulnerabilidades - Verificar vulnerabilidade** incluído no sistema de base.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Resposta a vulnerabilidades - Verificar vulnerabilidade** cria um registro de verificação para a vulnerabilidade ou grupo de vulnerabilidades a partir do qual foi invocado.

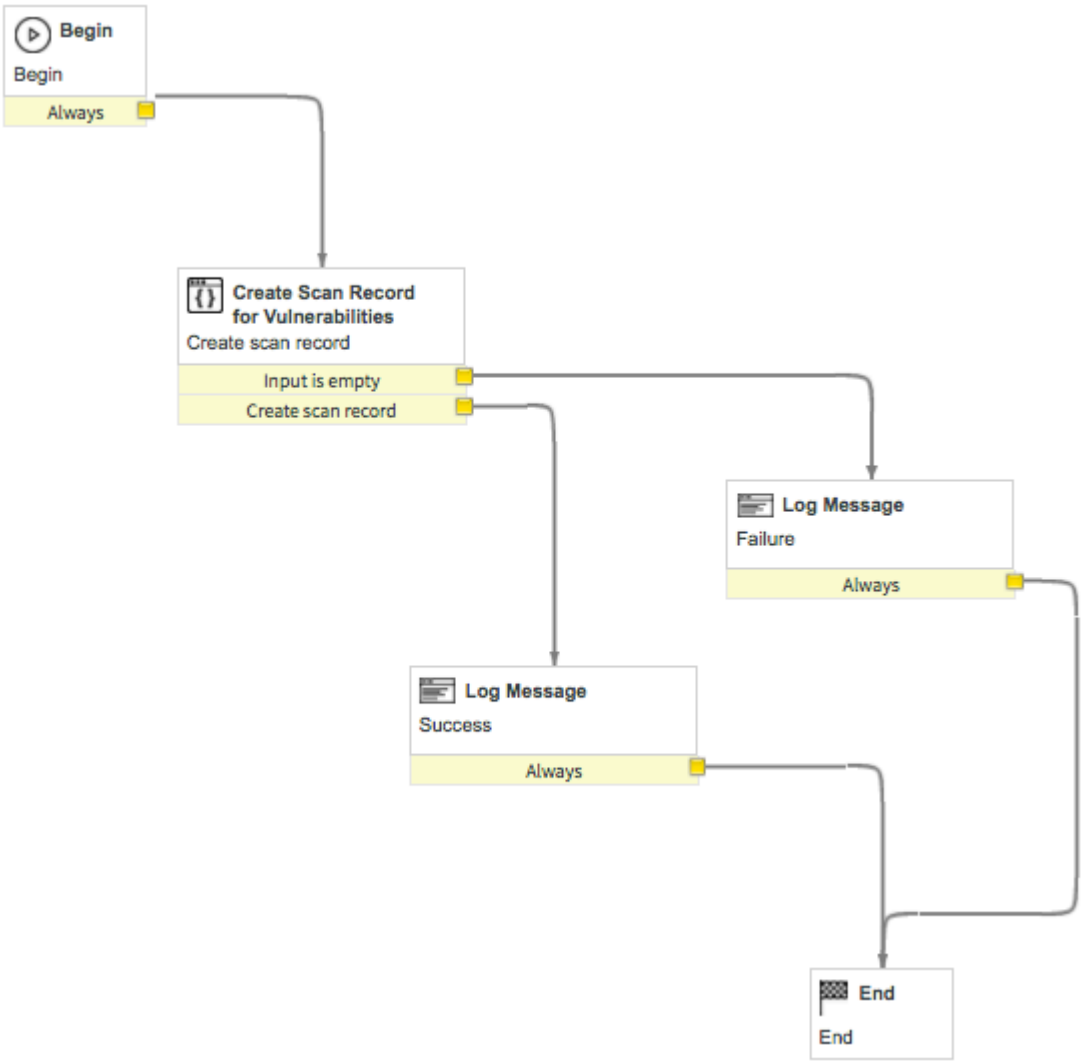
Nota:

- É uma prática recomendada verificar novamente as vulnerabilidades ou os itens vulneráveis após a correção, quando um patch de vulnerabilidade é aplicado aos registros afetados. Você pode executar a nova verificação usando o método descrito ou pode automatizar as novas verificações.
- A partir da v23.0 de Resposta a vulnerabilidades, o fluxo de trabalho **Resposta a vulnerabilidades - Verificar vulnerabilidade** foi descontinuado e substituído pelo fluxo de Nova verificação de vulnerabilidade no Flow Designer.

As atividades de fluxo de trabalho incluem Variáveis para a atividade Criar registro de verificação de vulnerabilidades

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades - Fluxo de trabalho de verificação de vulnerabilidade



Verificar fluxo de trabalho de vulnerabilidade

O **Resposta a vulnerabilidades** > **Verificar vulnerabilidade** O fluxo de trabalho verifica novamente uma tarefa de correção.

Antes de Iniciar

Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado pela verificação novamente do **grupo vulnerável** durante uma ação **Fechar/Ignorar**.

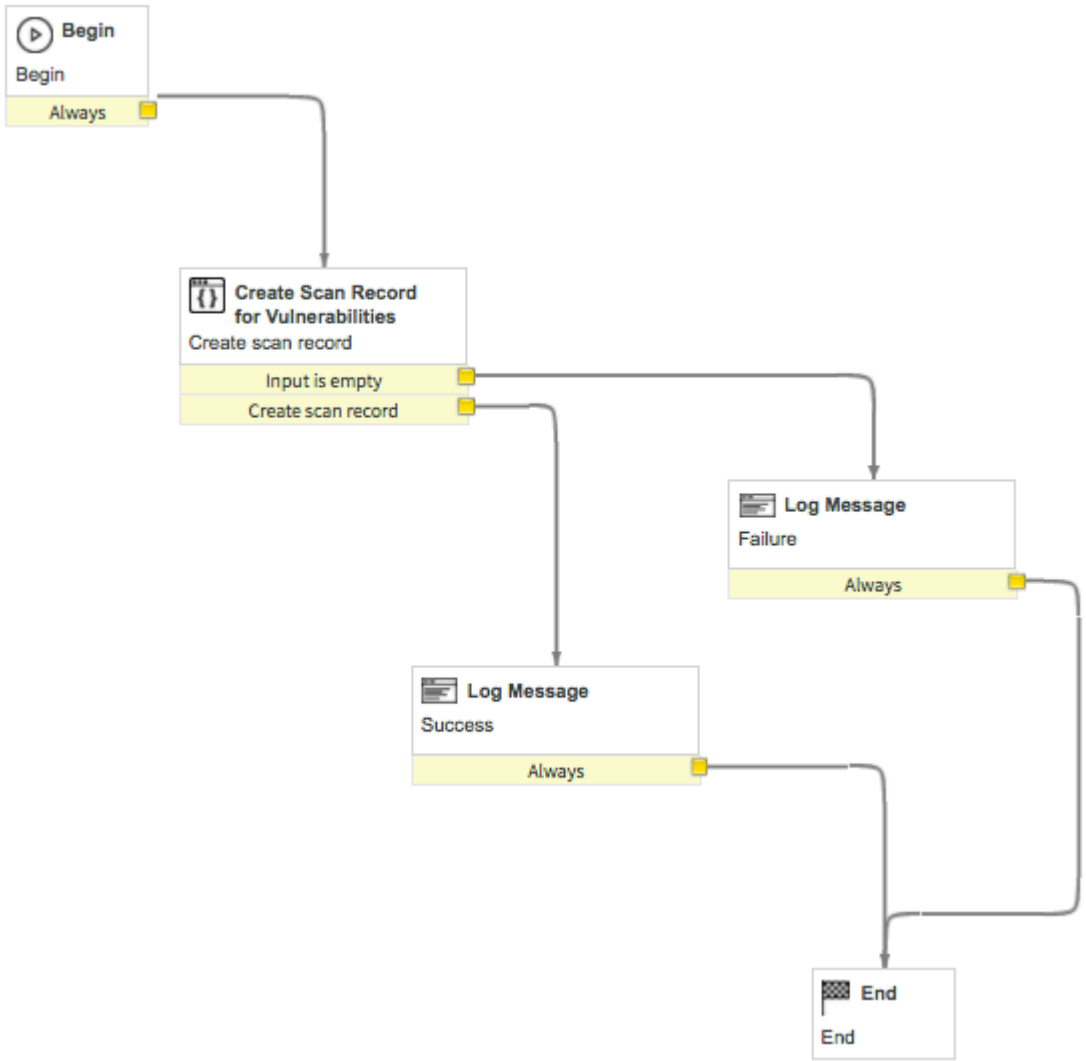
As atividades do processo de fluxo de trabalho incluem:

- Variáveis para a atividade Criar registro de verificação de vulnerabilidades
- Mensagem de Log

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho Verificar vulnerabilidade



Tradução automática

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
2. Abra um registro de tarefa (VUL).
3. Clique em **Fechar**.
4. Escolha **Encerrado** para o **Estado desejado**.
5. Escolha **Fixo** para o **Subestado**.
6. Escolha **Aguardar confirmação da próxima verificação** para **Fechar agora?**
   Para a tarefa de correção e os itens vulneráveis, o **Estado** muda para **Confirmação Pendente**, o **Subestado** muda para **Fixo**e uma nova verificação é executada.

Resposta a vulnerabilidades - Verificar fluxo de trabalho de itens vulneráveis

Automatize as verificações de vulnerabilidade para um ou vários itens vulneráveis usando o fluxo de trabalho **Resposta a vulnerabilidades - Verificar itens vulneráveis** incluído no sistema de base.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa

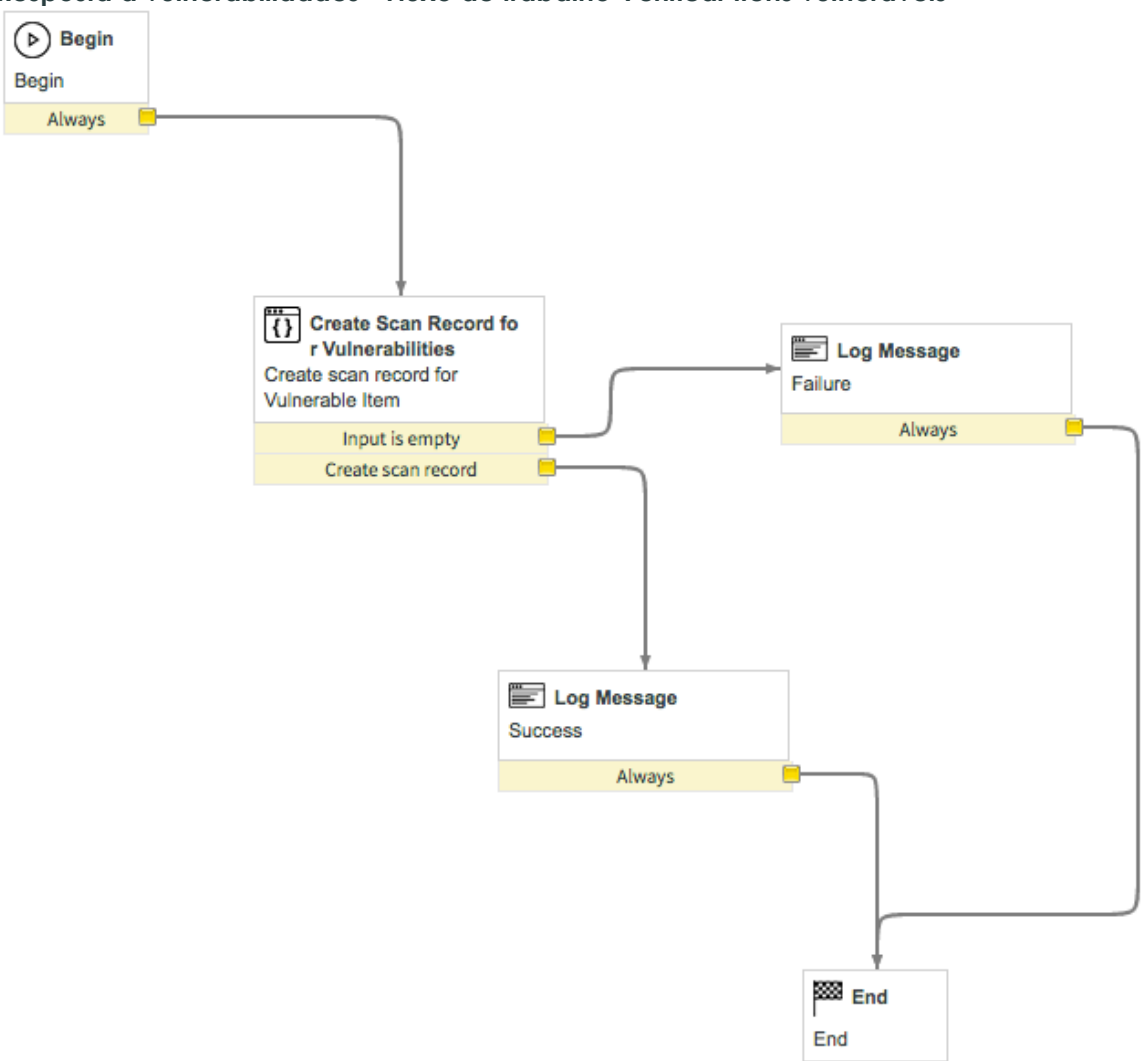
O fluxo de trabalho **Resposta a vulnerabilidades - Verificar itens vulneráveis** cria um registro de verificação para o item vulnerável ou grupo de itens a partir do qual ele foi invocado.

Nota:

- É uma prática recomendada verificar novamente as vulnerabilidades ou os itens vulneráveis após a correção quando um patch de vulnerabilidade for aplicado aos registros afetados. Você pode executar a nova verificação usando o método descrito ou pode automatizar as novas verificações.
- A partir da v23.0 de Resposta a vulnerabilidades, o fluxo de trabalho **Resposta a vulnerabilidades - Verificar itens vulneráveis** foi descontinuado e substituído pelo fluxo Verificar novamente o item vulnerável no Flow Designer.

As atividades do processo de fluxo de trabalho incluem: Variáveis para a atividade Criar registro de verificação de vulnerabilidades

Resposta a vulnerabilidades - Fluxo de trabalho Verificar itens vulneráveis



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar fluxo de trabalho de item de vulnerabilidade

O**Resposta vulnerável** > **Verificar item de vulnerabilidade** O fluxo de trabalho verifica novamente um item vulnerável.

Antes de Iniciar

Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa

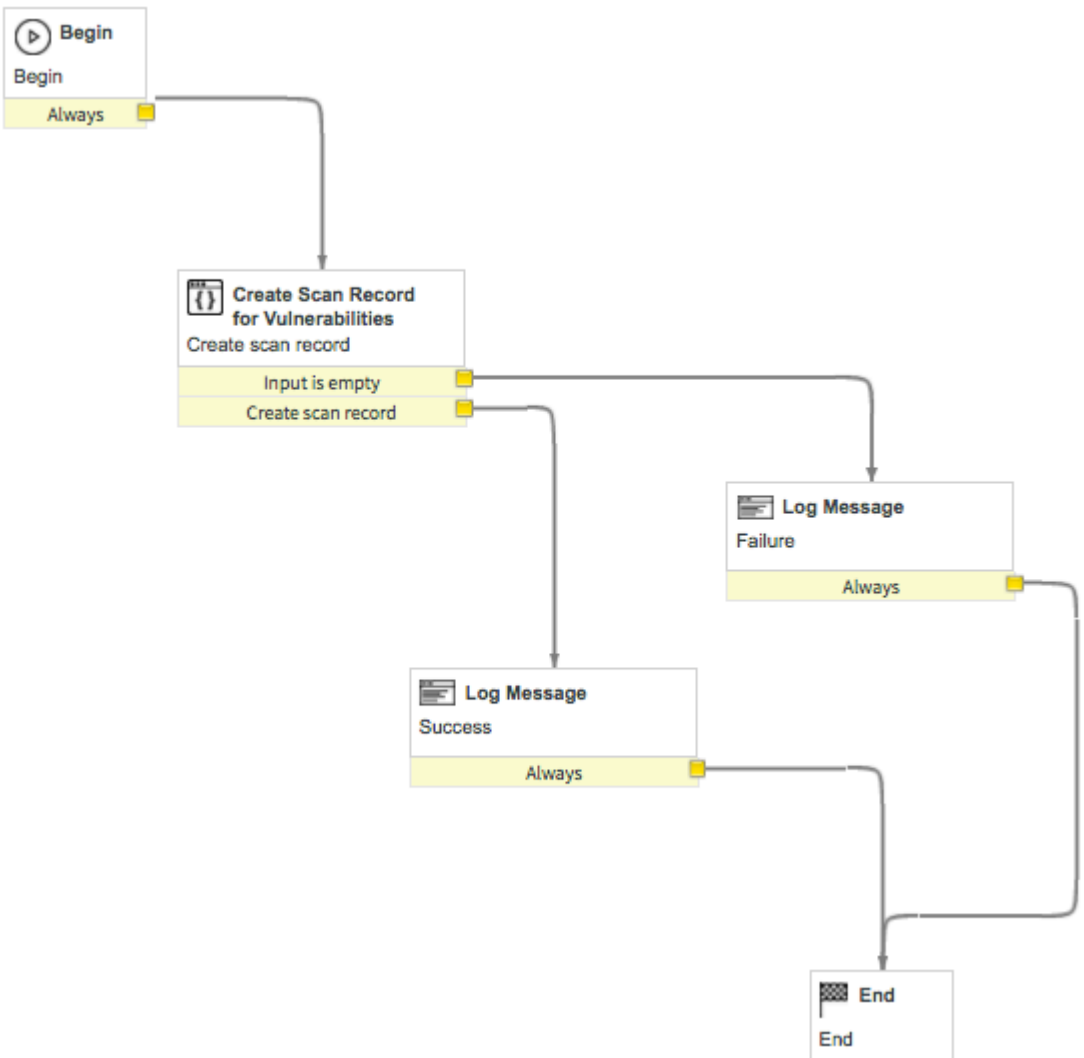
Este fluxo de trabalho é acionado pela **vulnerabilidade**de nova verificação durante uma ação **Fechar/Ignorar**.

As atividades do processo de fluxo de trabalho incluem:

Variáveis para a atividade Criar registro de verificação de vulnerabilidades

Mensagem de Log

Fluxo de trabalho Verificar vulnerabilidade



Tradução automática

Procedimento

1. Navegar até **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item de vulnerabilidade.
3. Clique **em Fechar/Ignorar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Escolha **Encerrado**para o **Estado desejado**.
5. Escolha **Fixo** para o **Subestado**.
   O **Estado** do grupo muda para **Confirmação Pendente**, o **Subestado** muda para **Fixo**e uma nova verificação é executada.

Orquestração de resposta a vulnerabilidades atividades de fluxo de trabalho

Orquestração de resposta a vulnerabilidades As atividades permitem que os usuários determinem se uma vulnerabilidade foi vista antes em outros incidentes de segurança ou em outros sistemas usando a orquestração de fluxo de trabalho.

Variáveis para a atividade Criar registro de verificação de vulnerabilidades

As verificações de vulnerabilidade para um ou vários itens vulneráveis podem ser executadas usando a atividade de fluxo de trabalho **Criar registro de verificação para vulnerabilidades** incluída no sistema de base. Quando a entrada é passada para a atividade, ela cria um registro de verificação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
taskids [cadeia de caracteres]	Uma cadeia de caracteres de sysIds separados por vírgula que define as entradas esperadas. Esse campo é obrigatório.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado da verificação [booliano]	Retorna verdadeiro se a entrada não estiver vazia. Um registro de verificação é criado para os taskIds.

Resposta a vulnerabilidades de aplicações

O recurso Resposta a vulnerabilidades de aplicações (AVR) da aplicação ServiceNow® Resposta a vulnerabilidades importa itens vulneráveis da aplicação (AVITs) e, de acordo com as regras, permite que você corrija vulnerabilidades da aplicação. Resposta a vulnerabilidades está disponível por assinatura separada.

A partir do AVR v19.0, alguns nomes de tabelas e colunas principais foram atualizados. Como resultado, você verá referências aos nomes mais antigos e mais recentes na documentação. Para obter a lista completa de termos atualizados, consulte Exibição de produto do Resposta a vulnerabilidades de aplicações.

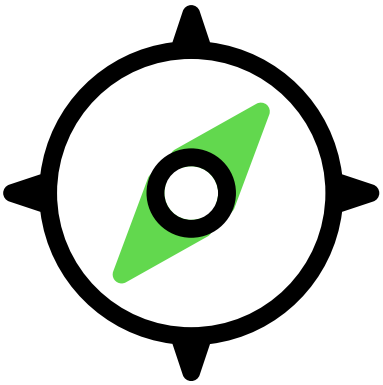
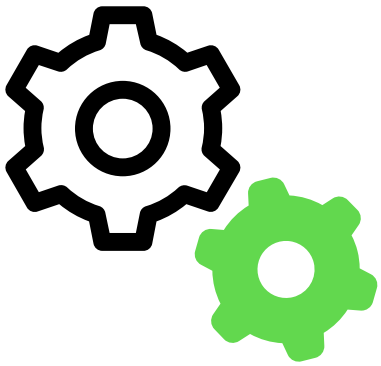
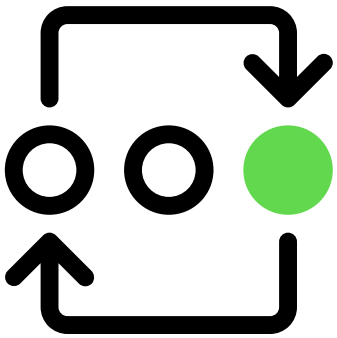
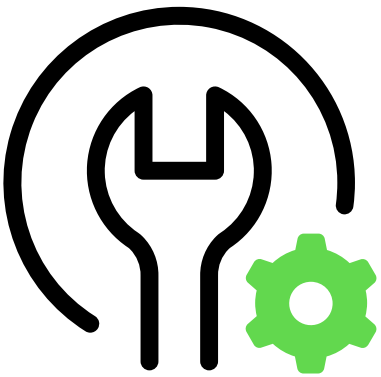
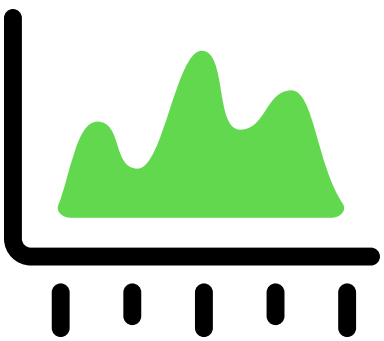
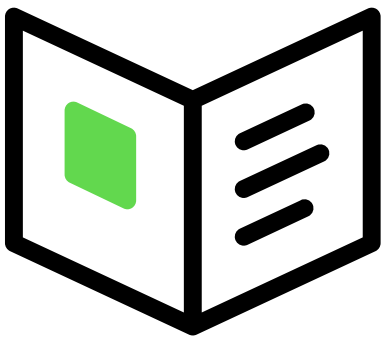
A partir da v19.0 de Resposta a vulnerabilidades, você pode ingerir dados de vulnerabilidade da Análise de composição de software (SCA) e da Lista de materiais de software (SBOM) para ajudá-lo a identificar pontos fracos em seus aplicativos de software. Para obter mais informações, consulte Exploração do Lista de materiais de software e Veracode Vulnerability Integration.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 18.0 do Resposta a vulnerabilidades, você pode monitorar e corrigir AVITs em Vulnerability Manager Workspace e Espaço de correção de problemas de TI, respectivamente. Para obter mais informações, consulte Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TIEspaço de correção de problemas de TI.

Resposta a vulnerabilidades de aplicações

Explorar  Saiba mais sobre os conceitos e recursos da Resposta a vulnerabilidades de aplicações.	**Configurar**  Configure a Resposta a vulnerabilidades da aplicação.	**Integrar**  Amplie a Resposta a vulnerabilidades de aplicações integrando com outras aplicações.
Corrigir  Saiba como corrigir vulnerabilidades de aplicações.	**Análise e Emissão de relatórios**  Exibir análise da Resposta a vulnerabilidades da aplicação	**Referência**  Veja os detalhes sobre os componentes da Resposta a vulnerabilidades da aplicação, como campos, tabelas e propriedades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorando Resposta a vulnerabilidades de aplicações

As vulnerabilidades da aplicação são vulnerabilidades em suas aplicações de software personalizadas que são verificadas durante todo o ciclo de vida de desenvolvimento da aplicação.

Visão geral de Resposta a vulnerabilidades de aplicações e versões disponíveis

Resposta a vulnerabilidades de aplicações (AVR) é a parte da aplicação Resposta a vulnerabilidades que processa as vulnerabilidades da aplicação.

Versões disponíveis

Versão de lançamento	Notas de versão
Resposta a vulnerabilidades v23.0 Resposta a vulnerabilidades v22.0 Resposta a vulnerabilidades v21.0 Resposta a vulnerabilidades v20.0 Resposta a vulnerabilidades v19.0 Resposta a vulnerabilidades v18.2	Notas de versão Resposta a vulnerabilidades de aplicações Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Como ele funciona

Os dados de vulnerabilidade são importados de fontes internas e externas, como Common Weakness Enumeration (CWE) ou integrações de terceiros. Depois que os dados são importados, eles são comparados aos dados da aplicação na sua aplicação Configuration Management Database (CMDB) e processados na aplicação Resposta a vulnerabilidades de aplicações. Se houver uma correspondência entre os dados de vulnerabilidade da aplicação importados e os dados no seu CMDB, um item vulnerável de aplicação (AVIT) será criado.

O Resposta a vulnerabilidades de aplicações inclui os seguintes recursos principais:

- Integre com scanners de terceiros compatíveis para importar dados de vulnerabilidade.
- Compare os dados relacionados à vulnerabilidade da aplicação e determine se as vulnerabilidades da aplicação foram encontradas em uma aplicação.
- Priorize, corrija e gerencie itens vulneráveis de aplicação (AVIT). Cada vulnerabilidade da aplicação representa uma entrada de vulnerabilidade no CWE ou em bibliotecas de terceiros.
- A partir da versão 18.0 de Resposta a vulnerabilidades, você pode monitorar e corrigir AVITs em Vulnerability Manager Workspace e Espaço de correção de problemas de TI, respectivamente. Para obter mais informações, consulte Vulnerability Manager Workspace e Espaço de correção de problemas de TI.
- Correlacione Resposta a vulnerabilidades de aplicações dados usando calculadoras e bibliotecas para ajudá-lo a executar as tarefas a seguir.

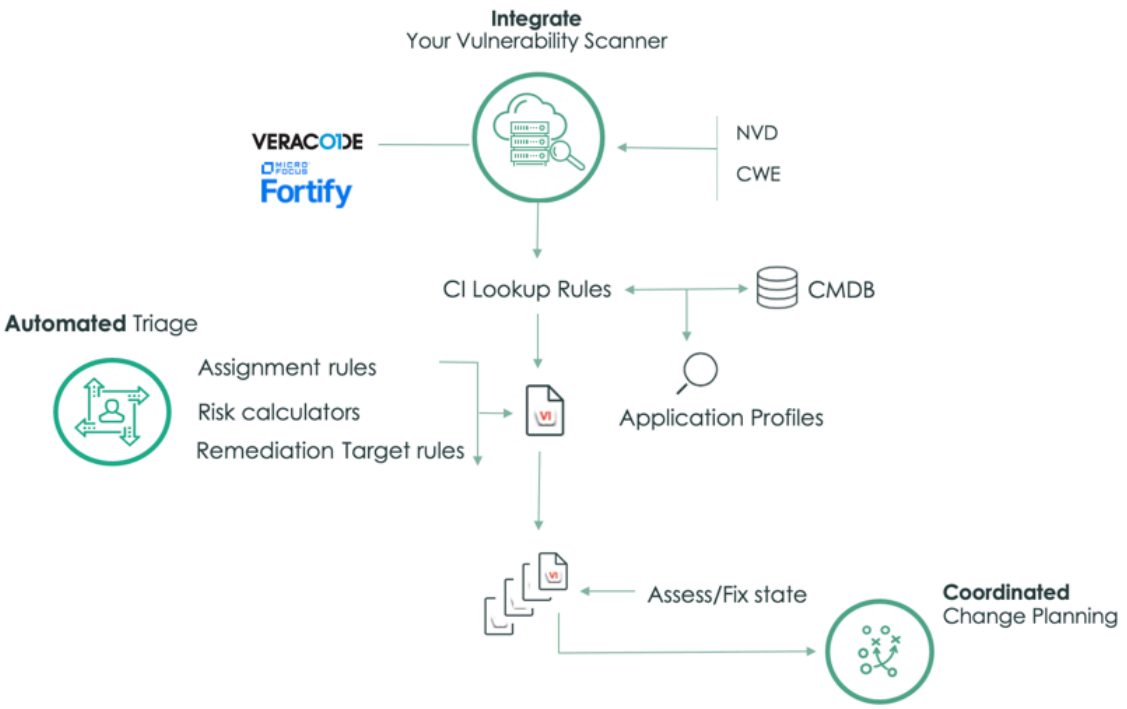
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Crie itens vulneráveis de aplicação automaticamente usando **Regras de pesquisa de IC**. Durante a importação, vulnerabilidades de terceiros são associadas a um CWE para criar um AVIT.
- Crie regras de atribuição para automatizar as atribuições de item vulnerável da aplicação.
- Use grupos de calculadoras para determinar o impacto nos negócios, especificar condições variadas usando filtros, aplicar cálculos simples ou usar um script.
- Crie regras de destino de correção que definam o intervalo de tempo esperado para corrigir itens vulneráveis da aplicação para que você possa monitorar as próximas atividades de correção.

- Relacionar uma única vulnerabilidade de terceiros a várias entradas do CWE e encontrar o CWE primário de uma vulnerabilidade para ajudá-lo a determinar o risco. Para obter mais informações sobre o **CWE primário**, consulte Campos de vulnerabilidade da aplicação.
- Use registros do CWE que são baixados do banco de dados do CWE ou importados de integrações de terceiros como referência para ajudá-lo a decidir se deve escalar uma vulnerabilidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco.

Use Resposta a vulnerabilidades de aplicações para seguir o fluxo de informações, desde a integração até a investigação e, em seguida, até a resolução.



Tipos de dados de vulnerabilidade importados

Resposta a vulnerabilidades de aplicações O é compatível com os seguintes tipos de dados de vulnerabilidade da aplicação importados.

Nota: Antes da v19.0, os dados de SAST, SCA, IAST e de teste de invasão não eram ingeridos e podem ser responsáveis pelas diferenças entre o que é mostrado em Veracode, Fortifye Invicti e o que aparece em Resposta a vulnerabilidades de aplicações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes dinâmicos de segurança da aplicação (DAST)

As verificações do DAST localizam a aplicação de vulnerabilidades enviando entradas para suas aplicações e monitorando suas respostas enquanto elas estão em execução. Essa abordagem pode imitar um ataque externo. Durante a verificação dinâmica, um serviço em execução (URL) é verificado quanto a vulnerabilidades. Os resultados de vulnerabilidade incluem um local de URL de uma vulnerabilidade descoberta.

Teste de segurança da aplicação estático (SAST)

As verificações de SAST revisam o código de origem das aplicações em repouso e ajudam a encontrar vulnerabilidades na forma como você criou seu código. A verificação do SAST ocorre em código de origem não compilado e, portanto, existe independentemente de qualquer serviço de aplicativos. Os resultados retornados incluem um arquivo e a localização do número de linha de uma vulnerabilidade descoberta.

Testes de segurança de aplicações interativos (IAST)

As verificações IAST detectam vulnerabilidades de software interagindo com o programa enquanto ele está em execução. Observação humana, testes automatizados e sensores são usados em combinação para interagir com a aplicação para localizar vulnerabilidades.

Análise de composição de software (SCA)

A partir da v19.0 de Resposta a vulnerabilidades, você pode ingerir vulnerabilidades da Análise de composição de software (SCA). Dados de vulnerabilidade de SCA para ajudar a identificar pontos fracos no software de código aberto que está sendo usado em seus aplicativos de software.

Teste de invasão

Você configura as solicitações de avaliação de teste de invasão em Resposta a vulnerabilidades de aplicações para ajudá-lo a entender onde estão os pontos fracos da sua aplicação e o que você pode fazer para corrigi-los.

Lista de materiais de software

Carregue Lista de materiais de software (SBOM) dados para identificar vulnerabilidades em seus componentes de código aberto. Para obter mais informações, consulte Exploração do Lista de materiais de software.

Casos de uso

Alguns dos seguintes casos de uso de DAST são compatíveis:

- Relacione cada vulnerabilidade dos resultados da verificação a algum tipo de cmdb_ci (classe secundária).
- Relacionar os resultados da verificação do DAST a uma aplicação existente quando houver um registro no CMDB de Descoberta ou uma integração de terceiros.
- Relacionar o resultado da verificação do DAST a uma aplicação verificada recém-inserida quando uma nova aplicação não tiver sido identificada e/ou armazenada no CMDB.
- Armazene os resultados da verificação do DAST para um CMDB ao gerenciar suas aplicações em um produto diferente de ServiceNow®.
- Armazene os resultados da verificação do DAST para um CMDB se você tiver personalizado anteriormente para outra finalidade.
- Crie uma aplicação para o repositório de código de origem manualmente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alguns dos casos de uso de SAST compatíveis são compatíveis:

- Relacione cada vulnerabilidade dos resultados da verificação a algum tipo de cmdb_ci (classe secundária).
- Crie um IC para o repositório de código de origem manualmente.
- Armazene os resultados da verificação do SAST que não têm um serviço de aplicações relacionado.

Integrações de terceiros

As integrações de terceiros compatíveis com Resposta a vulnerabilidades de aplicações estão disponíveis como aplicações separadas no ServiceNow Store. Para obter mais informações, consulte Integração do Resposta a vulnerabilidades de aplicações a outras aplicações.

Principais recursos

- Uma API compartilhada importa dados DAST, SAST, IASTe SCA e resultados de testes de invasão manuais. Consulte Teste de invasão.
- Uma API separada é usada para importar dados de SBOM. Para obter mais informações, consulte Exploração do Lista de materiais de software e Veracode Vulnerability Integration.

Regras de pesquisa de IC

: Pesquise automaticamente dados da aplicação em busca de correspondências no Configuration Management Database (CMDB).

Regras de atribuição

: Atribua automaticamente vulnerabilidades de aplicação com base em grupos de usuários, campos de grupo de usuários e scripts.

Calculadoras de Risco

: Priorize e classifique automaticamente o impacto dos AVITs usando calculadoras, com base em qualquer critério, usando filtros de condição.

Mapeamento de severidade

: Calcule automaticamente os valores iniciais dos campos nos itens vulneráveis da aplicação. As entradas de vulnerabilidade têm gravidade de origem e gravidade normalizada (com base no mapeamento de gravidade). A gravidade está vinculada à Enumeração de pontos fracos comuns (CWE).

Regras de destino de correção

: Defina o intervalo de tempo esperado para corrigir um item vulnerável da aplicação.

Emissão de relatórios

: Obtenha rapidamente informações sobre sua postura de segurança, tendências de correção e as 10 principais aplicações ou unidades de negócios com os AVITs mais críticos.

O ponto comum para ambos os tipos de verificações é a versão da aplicação. Uma versão da aplicação, que define uma cadeia de caracteres de **Nome**, é o ponto de vinculação para agrupar os resultados de vulnerabilidade verificados no lado do scanner. Dessa forma, o AVR sabe a qual versão da aplicação os resultados pertencem ao importar resultados de verificação por meio da integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma tabela secundária de item de configuração [cmdb_ci], Aplicações verificadas [sn_vul_app_scanned_application], foi criada na aplicação e no escopo Resposta a vulnerabilidades. Esta tabela armazena a abstração da versão da aplicação e fornece gráficos de serviço por meio de seus relacionamentos do CMDB. Eles podem ser exibidos em **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Aplicações** módulo. A exibição de lista de aplicações verificadas contém o **departamento** e **o grupo de suporte** adicionados durante a configuração.

Itens vulneráveis de aplicação (AVITs)

Para vulnerabilidades da aplicação, o AVR relaciona uma vulnerabilidade a uma aplicação para criar o registro de item vulnerável da aplicação (AVIT). Por causa das várias definições do que constitui uma aplicação no CMDB, Resposta a vulnerabilidades de aplicações limita as aplicações a aplicações verificadas. Aplicações verificadas são as aplicações verificadas em seu ambiente identificadas pelo AVR como **Nome** e **ID**. Os **AVITs** são baseados no resumo da verificação mais recente até que seja confirmado pelo scanner. Se um AVIT não for mais encontrado, ele permanecerá vinculado ao resumo da verificação em que foi visto pela última vez.

Os itens vulneráveis da aplicação podem ser exibidos em **Todos** > **Resposta a vulnerabilidades de aplicações** > **Vulnerabilidades** > **Itens vulneráveis** módulo.

Se uma aplicação for removida do CMDB, todos os AVITs associados serão encerrados.

Para obter informações sobre campos de formulário AVIT, consulte Campos de item vulnerável da aplicação.

Grupos de usuários e funções no Resposta a vulnerabilidades de aplicações

Frequentemente, uma equipe trabalha em conjunto para criar, gerenciar e supervisionar a gestão de vulnerabilidades da aplicação. Existem funções estratégicas, bem como funções operacionais, entre os membros da equipe. Na maioria das organizações, você pode participar de mais de uma função e geralmente compartilha funções com outras pessoas. Resposta a vulnerabilidades de aplicações usa três grupos de usuários que contêm funções granulares: gerente de App-Sec, campeão de segurança da aplicação e desenvolvedor. Consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções para obter mais informações sobre esses grupos e funções.

Resposta a vulnerabilidades de aplicações estados

Resposta a vulnerabilidades de aplicações O oferece um modelo de estado para o status dos itens vulneráveis da aplicação (AVITs) e ajuda você a determinar quando e como corrigir seus AVITs.

Um item vulnerável de aplicação tem vários estados possíveis. Consulte Estados de item vulnerável de aplicação (IVA) para obter mais informações.

Configuração da Resposta a vulnerabilidades de aplicações

Antes de executar Resposta a vulnerabilidades de aplicações em sua instância Now Platform, você deve configurá-la.

Como configurar o Resposta a vulnerabilidades de aplicações

Execute as etapas de configuração a seguir antes da configuração para garantir que a configuração esteja concluída.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se o Performance Analytics para Resposta a vulnerabilidades está instalado e ativado para ver os relatórios Resposta a vulnerabilidades de aplicações.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades [PA].
Verifique se o Veracode Vulnerability Integration está instalado, ativado e configurado. (Não execute as integrações neste ponto.)	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar a ServiceNow Integração de resposta a vulnerabilidades com Veracode.
Verifique se a integração do CWE 2000 está sendo executada em Resposta a vulnerabilidades.	Para verificar a integração, consulte Verifique se o trabalho agendado para atualizar registros do NVD está em execução.
[Opcional] Verifique se a integração do NVD está sendo executada em Resposta a vulnerabilidades.	Para verificar, consulte Verifique se o trabalho agendado para atualizar os registros do CWE está em execução.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o usuário com a função de administrador instalará a aplicação e atribuirá usuários aos seguintes grupos de usuários: Gerente de App-Sec, Campeão de segurança e Desenvolvedor. Para obter informações sobre funções de grupo, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	• O grupo de gerentes de App-Sec supervisiona a configuração e verifica os resultados esperados. **Nota:** A configuraçãoResposta a vulnerabilidades de aplicações não está disponível no recurso Assistente de configuração em Resposta a vulnerabilidades.

Função necessária: grupo de usuários do App-Sec Manager

Procedimento

1. Navegar até **Operações de segurança** > **CMDB** > **Regras de pesquisa**.
   Consulte Criar uma regra de pesquisa de IC para criar ou modificar Regras de pesquisa de IC para o seu ambiente.
2. Navegar até **Resposta a vulnerabilidades de aplicações** > **Administração**.
3. Selecione **Regras de atribuição**.
   Consulte Criar ou editar Resposta a vulnerabilidades de aplicações regras de atribuição para criar ou modificar regras de atribuição de aplicações para seu ambiente.
4. Selecione **Calculadoras de vulnerabilidade**.
   Consulte Calcular risco em Resposta a vulnerabilidades de aplicações automaticamente para criar ou modificar calculadoras de vulnerabilidade da aplicação para o seu ambiente.
5. Selecione **Regras de destino**de correção .
   Consulte Criar ou editar regras de destino de correção da aplicação para criar ou modificar metas de correção de aplicação para o seu ambiente.
6. Selecione **Mapas de gravidade normalizados**.
   Consulte Mapear a gravidade de um item vulnerável de aplicação automaticamente para criar ou modificar mapas de severidade para seu ambiente.
7. Navegue até qualquer um **Integração de vulnerabilidade da Veracode** > **Integrações** ou **Integrações de vulnerabilidade do Fortify** > **Integrações**.
8. Abra a integração da lista de aplicações Veracode ou a integração da lista de aplicações Fortify On Demand.
9. Se ainda não tiver sido executado, selecione **Executar agora**.

   Nota: As outras integrações Veracode ou Fortify estão inativas por padrão.

   Para status de execução de integração, consulte Exibir o Veracode status de execução da importação da Integração de vulnerabilidade da aplicação ou Exibir o Integrações de vulnerabilidade do Fortify status de execução de importação.
10. Depois que a integração da lista de aplicações Veracode ou Fortify on Demand tiver concluído sua execução, navegue até **Resposta a vulnerabilidades de aplicações** > **Administração** > **Aplicações**.
11. Para cada aplicação, insira um valor para **Grupo de suporte** (usado por regras de atribuição) e para **Departamento** (usado na emissão de relatórios).
    Para atualizar várias entradas, consulte Editar vários registros em uma lista usando o editor de lista para concluir a tarefa em massa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para ver a **unidade de negócios**atualizada automaticamente, atualize a página. Para obter informações sobre os campos do formulário Aplicação verificada, consulte Campos da aplicação verificados.

12. Retorne à lista de integrações e ative as outras integrações Veracode ou Fortify. Consulte Ativar Resposta a vulnerabilidades de aplicações integrações para definir suas importações de integração de dados delta.

    As integrações Veracode e Fortify são encadeadas e serão executadas consecutivamente quando ativadas.

13. Opcional: Navegar até **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de atribuição**.

    a. Opcional: Se você escolheu **Item de configuração: grupo de suporte** para **o campo Grupo de usuários** ao criar ou editar suas regras de atribuição anteriormente, os valores que você adicionou à exibição de lista Aplicações verificadas estarão disponíveis para uso agora.
    Suas regras de atribuição foram editadas.

    b. Selecione **Atualizar**.

    c. Na exibição de lista Regras de atribuição de vulnerabilidade, selecione **Aplicar mudanças** para reaplicar as regras de atribuição aos seus AVIs.

Resultados
Sua configuração Resposta a vulnerabilidades de aplicações agora está concluída.

O que Fazer Depois
Navegar até **Resposta a vulnerabilidades de aplicações** > **Visão geral** e consulte Painel de Gestão de vulnerabilidades de aplicações [PA] para obter informações sobre sua postura geral de segurança.

Verifique se o trabalho agendado para atualizar os registros do CWE está em execução

Use os registros de CWE (Common Weakness Enumeration, Enumeração de pontos fracos comuns) baixados do banco de dados do CWE como referência ao decidir se uma vulnerabilidade deve ser escalonada. Atualize os registros de fraquezas comuns do banco de dados de enumeração de fraquezas comuns em uma base programada regularmente. Você também pode atualizar o script padrão ou escrever seus próprios scripts, conforme necessário.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec
Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione o trabalho agendado **Integração abrangente do CWE 2000**.
3. Verifique se a caixa de seleção **Ativo** está marcada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> **Nota:** As configurações neste formulário são compartilhadas por Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações. Modificar as configurações de integração requer coordenação com e experiência em Resposta a vulnerabilidades e ServiceNow.

4. Se a caixa estiver selecionada, você terá concluído.

> **Nota:** Se a caixa não estiver marcada, talvez essa integração precise ser configurada em Resposta a vulnerabilidades. Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros para obter mais informações antes de selecioná-lo.

Conforme necessário, consulte Exibir bibliotecas de vulnerabilidades para ver as entradas importadas.

O campo **CWE primário** contém a entrada do CWE. Se houver mais de um CWE associado a uma vulnerabilidade, consulte Campos de vulnerabilidade da aplicação para obter informações sobre como o CWE primário é determinado.

Verifique se o trabalho agendado para atualizar registros do NVD está em execução

Identifique os repositórios que você deseja atualizar regularmente. Você pode executar um trabalho agendado para atualizar registros do Banco de dados nacional de vulnerabilidades (NVD) todas as noites ou semanas. Se ainda não estiver em execução, você poderá habilitar o trabalho

Antes de Iniciar

Funções necessárias: grupo de gerentes de App-Sec

A integração do NVD é executada como um trabalho agendado diariamente às segundas-feiras às 00:00:00, por padrão.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione o trabalho agendado do Banco de **dados nacional de vulnerabilidades do NIST**.
3. Verifique se a caixa de seleção **Ativo** está marcada.

> **Nota:** As configurações neste formulário são compartilhadas por Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações. Modificar as configurações de integração requer coordenação com e experiência em Resposta a vulnerabilidades e ServiceNow.

4. Se a caixa estiver selecionada, você terá concluído.

> **Nota:** Se a caixa não estiver marcada, talvez essa integração precise ser configurada em Resposta a vulnerabilidades. Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros para obter mais informações antes de selecioná-lo.

Conforme necessário, consulte Exibir bibliotecas de vulnerabilidades para ver as entradas importadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar Resposta a vulnerabilidades de aplicações integrações

Habilite Resposta a vulnerabilidades de aplicações integrações para executar atualizações regulares.

Antes de Iniciar

Função necessária: gerente de App-Sec

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Integrações**.
2. Selecione uma integração.
3. Marque a caixa de seleção **Ativo**.
4. Selecione **Atualizar**.
5. Repita conforme necessário para cada integração.
   Após a execução inicial, as integrações são encadeadas para fazer importações delta para execuções subsequentes.

Definir Resposta a vulnerabilidades de aplicações notificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações de falso-positivos. Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas sobre como criar notificações por e-mail, consulte Criar uma notificação por e-mail .

Resultados

A partir da v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos em Vulnerability Manager Workspace para os usuários com a função sn_vul.app_sec_manager.
- Links abertos em Espaço de correção de problemas de TI para os usuários com funções, sn_vul.app_security_chamion, ou sn_vul.app_developer.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Criar ou editar notificações de meta de correção no Resposta a vulnerabilidades de aplicações

Os administradores de vulnerabilidade podem editar a notificação de meta de correção ou adicionar novas, especificando quando enviar a notificação, quem a recebe e qual conteúdo está na notificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de meta de correção ou escolha **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultados
A partir da v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos em Vulnerability Manager Workspace para usuários com a função, sn_vul.app_sec_manager.
- Links abertos em Espaço de correção de problemas de TI para os usuários com funções, sn_vul.app_security_chamion, ou sn_vul.app_developer.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Gestão de exceções no Resposta a vulnerabilidades de aplicações

Quando sua organização não pode cumprir uma política de segurança ou gestão de vulnerabilidades, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável da aplicação (IVA) que não pode ser corrigido de acordo com a política.

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade.

Nota:

A partir da v21.0 de Resposta a vulnerabilidades de aplicações, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável da aplicação muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável da aplicação ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Ciclo de vida de uma exceção

Definição de uma exceção

Uma exceção é uma solicitação para adiar a correção de um AVI por um período especificado. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como solicitar uma exceção

Como desenvolvedor, você pode solicitar uma isenção para um AVI usando o processo de gestão de exceções. Depois que o analista de segurança de aplicações aprova essa solicitação, o IVA passa para o estado **Adiado**.

Regras de exceção

A partir da v20, você pode criar regras de exceção para adiar automaticamente os itens vulneráveis da aplicação (IVA) existentes e novos por um período específico se eles corresponderem às condições da regra. O uso de regras de exceção para adiar automaticamente AVIs minimiza o risco de acordos de nível de serviço ausentes. As regras podem ajudá-lo a gerenciar vários itens, pois você está eliminando a intervenção manual. Consulte Criar uma regra de exceção.

Como solicitar uma extensão para uma regra de exceção

A partir da v20, você pode enviar uma solicitação de extensão para a data **Adiado até** de uma regra de exceção. Você pode solicitar uma extensão para uma regra se descobrir que um grande número de registros criados pela regra não está sendo resolvido até a data **Adiado até**, a data em que a tarefa de correção para de aceitar novos AVIs. A extensão atualiza a regra de exceção para estender automaticamente a data de adiamento na regra existente. Você pode inserir datas de até um ano a partir da data atual e deve incluir um motivo para a extensão. Uma solicitação de extensão requer aprovação em dois níveis de grupos de aprovação separados.

Como aprovar uma solicitação de exceção

Os IVAs que não podem ser corrigidos imediatamente são revisados por analistas de segurança de aplicações, avaliados quanto ao risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de dois níveis. Se apenas o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção para Resposta a vulnerabilidades de aplicações.

Nota:

Depois que uma solicitação de exceção para um AVI for aprovada, você poderá executar as seguintes ações:

- Reabrir
- Obter mais detalhes

Acompanhamento de uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** do AVI.

Expiração de uma solicitação de exceção e solicitação de uma extensão para uma regra de exceção

Quando uma solicitação de exceção para um AVI específico expira, o AVI afetado é revertido para o estado **Aberto**.

No entanto, a partir da v20, você pode enviar uma solicitação para estender a data **Adiado até** na regra de exceção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar Gestão de exceções para Resposta a vulnerabilidades de aplicações

Limite a duração de uma exceção solicitada e adicione um questionário à solicitação de exceção ou falso-positivo usando o módulo. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Resposta a vulnerabilidades de aplicações. Você também pode solicitar uma exceção usando a integração GRC: Gestão de políticas e conformidade.

Antes de Iniciar

Função necessária: sn_vul.app_manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Resposta a vulnerabilidades estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Gestão de políticas e conformidade estiver instalado, você poderá selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica o objetivo de Política e Controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que está levantando a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista Gerenciar exceções usando.

   Nota: A partir da Resposta a vulnerabilidades versão 17.1, você pode selecionar Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade. Você deve ativar o plug-in GRC para usar GRC: Gestão de políticas e conformidade para solicitar uma exceção. Alterar a configuração não afeta os dados existentes.

3. Preencha os campos no formulário com base na opção selecionada.
   - Se você selecionou a opção Resposta a vulnerabilidades, preencha os campos do formulário.

Configurações do formulário Gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Opção para exibir o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso-positivo. O questionário para solicitação de falso-positivo é exibido por padrão.

- Se você selecionou a opção GRC: Gestão de políticas e conformidade, preencha os campos do formulário.

Configurações do formulário Gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso-positivo. O questionário para solicitação de falso-positivo é exibido por padrão.

4. Selecione **Salvar**.

Configurar regras de aprovação para Gestão de exceções

A partir da Resposta a vulnerabilidades de aplicações v15.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Resposta a vulnerabilidades de aplicações (AVR) pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Se você já for um usuário de VR, a opção padrão será fluxo de trabalho.
Se você implantou Resposta a vulnerabilidades de aplicações v15.0 ou posterior, o valor da propriedade do sistema *sn_vul.flow_designer_activation* será definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Resposta a vulnerabilidades de aplicações antes da v15.0, o valor desta propriedade do sistema será definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota: Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis da aplicação
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso-positivo para itens vulneráveis da aplicação

Nota: Você também pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Resposta a vulnerabilidades.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso-positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovaçãoy (dias) A partir da v21.0 de Resposta a vulnerabilidades de aplicações	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v21.0 de Resposta a vulnerabilidades de aplicações	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra.

Nota: Em cada página de configuração, você pode criar vários níveis de aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Adiamento de correção em Resposta a vulnerabilidades de aplicações

A partir da v20.0, você pode adiar a correção com o estado **Aguardando implementação** que está disponível para itens vulneráveis de aplicação (IVA) e tarefas de correção conforme eles passam por seus ciclos de vida. Você só pode fazer a transição de registros para este estado manualmente selecionando **Aguardando implementação** de AVI e registros de tarefa de correção no estado **Sob investigação**.

Caso de uso

Como especialista em correção, você pode mover um registro para **Aguardando implementação** para que sua equipe saiba que sua pesquisa e trabalho em uma tarefa foram concluídos. Você pode escolher esta atualização se descobrir que uma correção está pronta para implementação, mas não está disponível. Um exemplo de correção indisponível é um patch de software. Se a janela de manutenção de um patch não estiver disponível quando você terminar sua pesquisa, você poderá mover a tarefa para **Aguardando implementação** até que o patch possa ser implantado.

Campos necessários

Há dois campos editáveis obrigatórios nos registros do AVI e da tarefa de correção que estão no estado Aguardando implementação:

Data do compromisso de correção

A data de correção planejada.

Plano de correção

A descrição do plano de correção para correção. Este texto é exibido nas Anotações no registro.

Campos e propriedades do sistema

Há duas propriedades do sistema que são definidas como `verdadeiras` por padrão para o modal que aparece quando você faz a transição de um registro para **Aguardando implementação**. Se deixado em suas configurações padrão:

sn_vul.remediation_fields

Define a **data do compromisso** de **correção e o plano** de correção como campos obrigatórios. Se definido como `falso`, esses campos serão opcionais.

sn_vul.aguardando_implementação

Exibe o modal com os campos **Data do compromisso**de **correção e Plano** de correção depois que você seleciona **Aguardando implementação** em um registro. Se definido como `falso`, você pode alterar o estado de um AVI para Aguardando implementação sem um aviso para inserir uma data de compromisso ou um plano.

Módulo de data de compromisso de correção perdido

Exiba todos os IVAs que tenham perdido suas datas de compromisso de correção no módulo **Data** de compromisso de correção perdida. Navegar **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis** > **Data do compromisso de correção perdido** para exibir a lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rolldown de estado de tarefas de correção para AVIs

O botão de ação de IU para fazer a transição de um registro para **Aguardando implementação** só está visível em registros de tarefa de correção e item vulnerável da aplicação no estado **Sob investigação**. Para rolldown de estado, no modal que aparece quando você seleciona **Aguardando implementação** em uma tarefa de correção, há uma opção para **Substituir AVIs existentes**.

Opção	Descrição
Selecione **Substituir AVIs existentes**.	Selecione esta opção para substituir as datas do compromisso de correção e os planos de correção de todos os AVIs existentes na tarefa que já está no estado **Aguardando implementação**. Se selecionado, este recurso reverterá a data e os dados do plano na tarefa de correção para os AVIs.
Deixe **Substituir IVAs existentes** desativado.	Deixe a opção desativada para manter os valores de data e plano intactos para todos os AVIs existentes na tarefa que já está no estado **Aguardando implementação**. Se desativado, os AVIs já em **Aguardando Implementação** preservarão a data existente e os dados do plano e não serão afetados pela reversão do estado.

Exemplos de rolldown

Digamos que você queira fazer a transição de uma tarefa de correção de **Aberto** para **Aguardando Implementação** para que você possa atualizar a data de compromisso da tarefa e as informações do plano para uma janela de manutenção de patch de software. Suponha que haja um AVI nesta tarefa no estado **Aguardando implementação** e você deseja atualizar a data de compromisso e as informações do plano para corresponder à tarefa de correção.

Para substituir a data dos AVIs e os dados do plano para que correspondam à tarefa de correção, marque a caixa de seleção para **Substituir AVIs existentes** quando solicitado. Os valores de data e plano do AVI se tornam os valores de plano e data que você insere para a tarefa no prompt ao selecionar **Aguardando implementação**.

Se você não selecionar a opção de substituição neste caso e houver um AVI em **Aguardando implementação**, a data original e os dados do plano no AVI permanecerão intactos. Os valores de plano e data que você insere para a tarefa no prompt ao selecionar **Aguardando implementação** não são usados em nenhum AVIs que já esteja no estado **Aguardando implementação** na tarefa.

Se um AVI em uma tarefa estiver em **Resolvido** ou **Encerrado-fixo** e você fizer a transição da tarefa para **Aguardando Implementação**, selecionar **Substituir AVIs existentes** não mudará os AVIs de **Encerrado-fixo** e **Resolvido** para **Aguardando Implementação** devido a uma precedência de estado mais alta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a substituição não for selecionada ao mover a tarefa para **Aguardando implementação** e já houver um IVA em **Aguardando implementação** e você mover a tarefa de volta para **Aberto** ou **Sob investigação**, o AVI permanecerá em **Aguardando implementação**.

Adicionar um aprovador de exceção para Resposta a vulnerabilidades de aplicações

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção.

Antes de Iniciar

Função necessária: sn_vul.app_exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Uma solicitação de exceção para um item vulnerável da aplicação é aprovada usando o fluxo de aprovação padrão de dois níveis. A solicitação pode ser aprovada por dois níveis de aprovadores. A adição de usuários ao grupo de primeiro nível é obrigatória. Se não houver usuários no segundo nível, a solicitação será aprovada após a aprovação de primeiro nível.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na coluna Nome, pesquise por **Exceção**e clique em **Aprovador de exceção à aplicação - nível 1**.

   Nota: A partir de Resposta a vulnerabilidades de aplicações v12.8.1, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de falso-positivo ou exceção é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *sn_vul.app_exception_approver_L1*, *sn_vul.app_exception_approver_L2*ou *sn_vul.app_false_positive_approver_group* para alterar o valor da propriedade.

3. No formulário Aprovador de exceção da aplicação em grupo - Nível 1, clique na lista relacionada Membros do grupo.
4. Clique em **Novo** para criar uma lista.
5. No formulário, preencha os campos.

Formulário do usuário

Campo	Descrição
ID do Usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear o usuário fora da instância e encerrar todas as sessões ativas do usuário. O sistema evita que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ◦ Listas de usuários ◦ Lista de seleção em campos de referência (ícone de lupa) ◦ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço Web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário para o local deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...**.

Tradução automática

6. Clique em **Enviar**.
7. Opcional: Repita as etapas 1 a 5 para criar um Aprovador de exceção da aplicação - Nível 2.
   O aprovador deve navegar até **Resposta a vulnerabilidades da aplicação** > **Minhas aprovações** e aprovar as solicitações.

Como solicitar e aprovar uma exceção no Resposta a vulnerabilidades de aplicações

Você pode solicitar o adiamento da correção de um item vulnerável da aplicação e de uma tarefa de correção por um período especificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Você também pode criar regras de exceção e solicitar uma extensão de exceção para uma regra de exceção. Por padrão, são necessários dois níveis de aprovação para adiamentos, regras de exceção e solicitações de extensão de exceção.

Para solicitar ou aprovar uma exceção, consulte:

- Solicitar uma exceção para um item vulnerável da aplicação
- Solicitar uma exceção para vulnerabilidades da aplicação usando GRC: Gestão de políticas e conformidade
- Aprovar regras de exceção e solicitações de extensão de regra de exceção no Resposta a vulnerabilidades de aplicações
- Solicitar uma extensão para uma regra de exceção no Resposta a vulnerabilidades de aplicações

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v21.0 de Resposta a vulnerabilidades de aplicações, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável da aplicação muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável da aplicação ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Solicitar uma exceção para um item vulnerável da aplicação

Solicite uma exceção para um item vulnerável da aplicação que não pode ser corrigido imediatamente. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar

Função necessária: grupo de desenvolvedores

Procedimento

1. Navegar até **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis da aplicação** > **Todos** e selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto ou Sob investigação.

   Nota:

   A partir da v21.0 de Resposta a vulnerabilidades de aplicações, o estado anterior de um item vulnerável da aplicação é armazenado no campo **backup_state**.

2. No formulário Item vulnerável da aplicação, clique em **Solicitar exceção**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Dependendo se Resposta a vulnerabilidades está selecionado ou GRC: Gestão de políticas e conformidade no **Resposta a vulnerabilidades de aplicações** > **Gestão de exceção** Na tela, o formulário Solicitar exceção muda. Se GRC: Gestão de políticas e conformidade, consulte Solicitar uma exceção para vulnerabilidades da aplicação usando GRC: Gestão de políticas e conformidade

3. Se Resposta a vulnerabilidades for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado **Aberto**. **Nota:** A partir da versão 18.0 de Resposta a vulnerabilidades de aplicações (AVR), um item vulnerável da aplicação adiado pode ser fechado e reaberto por um scanner. Se o item for reaberto antes que a janela de exceção expire, o estado do AVIT será revertido para o estado adiado, respeitando a janela de exceção ativa. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema sn_vul.auto_defer_avit_in_active_exception_window como verdadeiro. Além disso, a data adiada Até persiste mesmo depois que o AVIT é fechado ou a exceção expira. A função necessária é sn_vul.app_manage_exception_configuration para leitura e gravação.
Motivo	Selecione o **Motivo**. As opções são: ◦ Risco aceito ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Redução do controle no local ◦ Outro Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	campo obrigatório deve ser atualizado pelo responsável pela correção.

4. Clique em **Solicitar aprovação** para enviar a solicitação de exceção.
   O estado do item de vulnerabilidade da aplicação muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma exceção para vulnerabilidades da aplicação usando GRC: Gestão de políticas e conformidade

Solicite exceções de política usando a capacidade de gestão de exceções de política GRCGestão de políticas e conformidade na aplicação [] de dentro de Resposta a vulnerabilidades de aplicações.

Antes de Iniciar

Antes de poder usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Gestão de políticas e conformidade do ServiceNow Store.

Função necessária: sn_vul.remediation_proprietário

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis da aplicação** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.
3. Se GRC: Gestão de políticas e conformidade for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

a. Clique em **Solicitar aprovação** para enviar a solicitação de exceção.
O estado dos itens vulneráveis muda para Em revisão e uma exceção à política é criada. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

b. Clique na lista relacionada Exceções às políticas para exibir a exceção à política.

c. Clique no número da exceção à política.

d. No campo **Aprovador**, selecione o nome do aprovador.

e. Clique na guia Origem e selecione um objetivo de **controle no campo Objetivo** de controle.

f. Clique na guia Avaliação de risco e selecione a classificação de **risco** no campo Classificação de risco.

g. Salve o formulário.

h. Clique na guia Controles afetados e clique em Adicionar para adicionar os controles.

i. Salve o formulário.

Nota: Você pode gerar uma revisão de conformidade clicando em **Solicitar revisão de conformidade**.

j. O formulário de aprovação é enviado ao aprovador.

k. Como aprovador, você pode aprovar a solicitação clicando em **Aprovar** ou solicitar aprovação adicional clicando em **Solicitar aprovação adicional**.
O estado do registro muda para Adiado. O motivo declarado é aquele que você selecionou ao gerar a solicitação de exceção. A guia Adiamento fornece anotações adicionais sobre o registro.

Nota: Se a solicitação for rejeitada, o registro será movido para o estado anterior.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.
   Para obter mais informações sobre a integração de exceção à política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Solicitar uma exceção para uma tarefa de correção da aplicação

Solicite uma exceção para adiar uma tarefa de correção de aplicação por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções nos espaços Resposta a vulnerabilidades. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Funções necessárias: sn_vul.remediation_owner, sn_vul.app_security_chamion ou sn_vul_container.remediation_owner.

Você também pode solicitar exceções para tarefas de correção de aplicação no ambiente clássico.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção** > **Todos**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No registro da tarefa de correção da aplicação, selecione **Solicitar exceção**.
4. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprovar regras de exceção e solicitações de extensão de regra de exceção no Resposta a vulnerabilidades de aplicações

Aprovar solicitações de exceção para itens vulneráveis da aplicação que não podem ser corrigidos imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar

Função necessária: sn_vul.app_exception_approver

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Definir mapeamento do motivo da política

Você pode definir as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar

Você deve ter a aplicação GRC: Policy and Compliance Management instalada. Esta aplicação está disponível no ServiceNow® Store com uma assinatura separada.

Para obter detalhes sobre os requisitos do sistema e a compatibilidade da família, consulte a lista de aplicativos no site ServiceNow Store .

Função necessária: sn_vul.compliance.manager e sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Políticas e conformidade** > **Exceções às políticas** > **Registro de Integração**.

   Nota: Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Escolhas de motivo ou adicionar um novo motivo.

2. Clique no registro de integração da sua aplicação, por exemplo, Resposta a **vulnerabilidades da aplicação, Resposta**a **vulnerabilidades**e assim por diante.
3. Para adicionar uma opção de motivo existente, execute as seguintes etapas:
   a. Na lista Escolhas de motivo, clique em **Novo**.
   b. Clique no ícone de lupa para selecionar um motivo.
4. Para adicionar novas opções de motivo à tabela Escolhas de motivo, execute as seguintes etapas:
   a. Na lista Escolhas de motivo, clique em **Novo**.
   b. Clique no ícone de lupa.
   c. Clique em **Nova**.
   d. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Lista de seleção de motivo

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamentos de motivo de exceção à política para as respectivas aplicações. Para navegar até esta tabela, insira sn_vul_policy_reason_mapping.LIST no navegador de filtros.
Ordem	Ordem para esta opção. Os motivos são ordenados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção à política sob demanda for solicitada. Se o registro de integração não contiver nenhuma opção específica da aplicação, todas as opções de motivo com o campo **Padrão** selecionado estarão disponíveis.
Ativo	Opção para exibir a opção na lista de opções de motivo.

5. Clique em **Enviar**.

Solicitar uma extensão para uma regra de exceção no Resposta a vulnerabilidades de aplicações

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Funções necessárias: Gerente de App-Sec sn_vul.app_sec_manager, Campeão de segurança sn_vul.app_security_chamion.

Por Que e Quando Desempenhar Esta Tarefa

Em um registro de regra de extensão, você pode solicitar uma extensão para a data **Adiado até** somente se a regra estiver no estado **Aprovado**. Você pode solicitar esta extensão para uma regra se descobrir que um grande número de registros criados pela regra não está sendo resolvido até a data **Adiado até**, a data em que a tarefa de correção para de aceitar novos AVIs. A extensão atualiza a regra de exceção para estender automaticamente a data de adiamento na regra existente.

Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ◦ Risco aceito ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção associadas e nos itens vulneráveis da aplicação. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para uma tarefa de correção adiada no Resposta a vulnerabilidades de aplicações

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento adiada. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Solicitar extensão**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
Com a aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis da aplicação, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis da aplicação devem estar no estado adiado e seus dados atuais até precedem a data atualizada até. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para um item vulnerável da aplicação adiada em Resposta a vulnerabilidades de aplicações

Solicite uma extensão para um item vulnerável da aplicação adiada antes que ele atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis**.
2. Abra um item vulnerável da aplicação adiada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Solicitar extensão**.

> **Nota:** O botão Solicitar extensão fica visível somente quando o estado do item vulnerável da aplicação é Adiado.

4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável da aplicação adiada deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

> **Nota:**
> ◦ A solicitação passa por dois níveis de aprovação.
> ◦ Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Criar, excluir e cancelar uma regra de exceção para Resposta a vulnerabilidades de aplicações

Crie uma regra para solicitar uma exceção automaticamente para itens vulneráveis da aplicação (IVA) que atendam a condições específicas.

Antes de Iniciar

Por exemplo, você pode criar uma regra com uma condição baseada em uma vulnerabilidade crítica ou conhecida específica que você sabe que não pode corrigir imediatamente. Com esta regra, você pode adiar AVIs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

- A regra de exceção é aplicada a partir da data **Válido de** até a data **Válido até** que você insere no registro da regra.
- A tarefa de correção (AVUL) é criada depois que a regra é aprovada para AVIs correspondentes no estado **Adiado**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O método de agrupamento para este AVUL é conhecido como Regras de exceção.
- Você não pode fechar, reabrir ou excluir este AVUL. AVIs novos e reabertos são adiados e adicionados a este AVUL a partir **da data Válido** até até que o grupo expire na data **Válido até**.

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Funções necessárias: App SEC Manager sn_vul.app_sec_manager e Campeão de segurança sn_vul.app_security_chamion.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de exceção**.
2. Na página de registro da nova regra de exceção, selecione **Novo**.
3. Preencha os campos.

Campo	Descrição
Nome	Nome da regra de exceção.
Estado	Somente leitura: rascunho
Válido de	Data a partir da qual esta regra está ativa para adiar IVAs.
Ordem de execução	Ordem exclusiva para cada regra de exceção. Um valor mais baixo precede um mais alto.
Válido até	Data em que a tarefa de correção para de aceitar novos IVAs.
Adiado até	Data até que as tarefas de correção e os AVIs sejam adiados. Nesta data, os AVULs são encerrados e todos os AVIs são movidos para fora das tarefas e reabertos. Regras de grupo são reaplicadas a esses AVIs.
Motivo	Motivo para criar esta regra de exceção.
Grupo de atribuição	Grupo ao qual a tarefa de correção está atribuída para rastrear os IVAs adiados.
Informação adicional	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	Condições de filtro para especificar quais AVIs correspondem a esta regra.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada. Se você deixar esta opção desativada, sua regra será executada diariamente pelo trabalho agendado *Associate existing AVIs with Auto Exception Rule*, começando com novos dados. Se você habilitar a opção Executar em dados existentes, um trabalho agendado será executado uma vez nos dados existentes na data **Válido de**.

4. Adicione o grupo de atribuição ao criar a regra.
5. Escolha um.

Opção	Descrição
Salvar a regra	Salve suas mudanças e a regra será exibida na lista Regra de exceção [sn_vul_auto_exception_rule]. Até que você envie a regra de exceção para aprovação, ela permanecerá no estado **Rascunho**.
Enviar a regra	Se você enviar a regra, o status da solicitação será alterado para **Em revisão**. Uma aprovação de regra de exceção requer dois níveis de aprovação, um do Aprovador de exceção da aplicação - Nível 1 e outro do Aprovador de exceção da aplicação Nível -2.

Depois que a regra é aprovada, ela passa para o estado **Aprovado**. Sua regra avalia AVIs com o trabalho *Associate existing AVIs with Auto Exception Rule scheduled*. Se você selecionou **Executar em dados existentes**, ele avaliará os AVIs existentes. Uma tarefa de correção é criada automaticamente para a regra e todos os AVIs correspondentes que atendam às condições são associados à tarefa.

O trabalho agendado executa a regra de exceção uma vez nos dados existentes. A regra não é executada novamente em dados existentes, mesmo se nenhum AVI for encontrado. Ele só avalia novos dados porque os AVIs existentes que corresponderam à regra já foram adiados.

6. Para excluir uma regra, selecione **Excluir** no registro da regra de exceção.
   A seguinte mensagem será exibida: `Se você excluir a regra, a tarefa de correção associada será excluída e os itens vulneráveis relacionados serão reabertos. As regras de tarefa de correção serão aplicadas aos AVIs individuais e a regra de exceção será excluída.`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione**Manter regra** para parar ou **Excluir regra** para continuar.
8. Para desativar uma regra, mas mantê-la na lista Regras de exceção, selecione **Cancelar**. A seguinte mensagem será exibida: `Se você cancelar esta regra, a tarefa de correção associada será excluída e os itens vulneráveis relacionados serão reabertos. As regras de tarefa de correção serão aplicadas aos itens vulneráveis individuais e a regra de exceção será movida para o estado de rascunho.`
9. Selecione**Manter regra** para interromper ou **Cancelar** para mover a regra para **Rascunho** e desativá-la.

Resposta a vulnerabilidades de aplicações visão geral de tarefas de correção e regras de tarefa

Configure tarefas de correção (AVULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis de aplicação (IVA) e analisá-los em massa. Os critérios pelos quais as tarefas de correção são formadas são configurados para que os AVIs sejam atribuídos automaticamente às tarefas de correção. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Acompanhar contagens de adiamento para itens vulneráveis da aplicação e tarefas de correção

Rastreie o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou tarefa de correção foi adiado. O trabalho agendado *`set deferral counts`* é executado diariamente para publicar contagens dos registros que foram adiados mais de uma vez na coluna Contagem de adiamento. Os registros são exibidos nos módulos de vários adiamentos para VR, AVR e CVR.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem que você defina como os itens vulneráveis da aplicação são agrupados e atribuídos automaticamente. Uma **vulnerabilidade** de regra padrão está incluída no sistema de base que reúne AVIs com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis pelo AVI. Esses valores podem incluir item de configuração (IC), entrada de vulnerabilidade e assim por diante.

Há regras de tarefa para a Resposta a vulnerabilidades de aplicações que estão incluídas com a aplicação Resposta a vulnerabilidades que está disponível quando você a ativa.

Você pode criar várias condições com o Construtor de condições. Na seção Agrupar por, depois de definir um par de campos, outra linha será exibida. Você pode ter até seis seleções **de Agrupar por**. Você também pode automatizar a atribuição de grupo. Para obter mais informações, consulte Atribuir itens vulneráveis de aplicação em Resposta a vulnerabilidades de aplicações automaticamente e Filtrando em Resposta a vulnerabilidades.

Por exemplo, você pode agrupar seus itens vulneráveis de aplicação pelo item de configuração ou pelo modelo de produto. Você pode ter uma regra de tarefa para vulnerabilidades de baixa gravidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades que expõem a empresa a mais riscos. Consulte Criar, editar e excluir Resposta a vulnerabilidades de aplicações regras de tarefa de correção para obter mais informações sobre as opções disponíveis.

Um conjunto diferente de regras pode ser usado para itens vulneráveis de aplicação que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado aos valores

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Agrupar por da regra da tarefa de correção para fazer a descrição resumida do novo registro.

Quando um novo item vulnerável de aplicação é criado, importado ou reaberto após ser fechado, as regras são avaliadas em relação a ele. Um AVI só é avaliado uma vez, automaticamente, a menos que seja reaberto após ser fechado ou as regras sejam reaplicadas manualmente.

O processo a seguir é usado para cada AVI novo ou reaberto:

- Para cada regra de tarefa de correção, o AVI é comparado ao filtro de regra de tarefa de correção.

- Para cada regra em que a condição da regra da tarefa de correção corresponde, a regra extrai os dados das seleções **Agrupar por** no AVI. Ele cria um nome de grupo e um campo. Neste caso, **Alto risco: QID-32342:** *resumo de QID-3242* (Nome: ID da vulnerabilidade: resumo da vulnerabilidade).

  Nota: O campo de descrição resumida está limitado a 160 caracteres. Resumos de vulnerabilidade mais longos são truncados.

  A regra verifica se há uma tarefa de correção **aberta** correspondente que esteja atribuída ao mesmo grupo de atribuição que o AVI.

  - Se a tarefa for encontrada, o AVI será adicionado à tarefa existente no estado **Aberto**.
  - Se nenhuma tarefa no estado **Aberto** for encontrada, a regra criará uma tarefa **de alto risco: QID-32342**, a atribuirá ao mesmo grupo de atribuição que o AVI e colocará o AVI na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições da regra da tarefa de correção antes de ser colocada em uma tarefa de correção, muitas regras podem afetar o desempenho. Configure suas regras de tarefa para que as condições ajudem a evitar a criação de tarefas de correção duplicadas.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelas **Regras de atribuição** no AVI ao agrupar os itens e atribui a tarefa de correção para corresponder aos AVIs.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras no módulo **Regras de atribuição**. Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Quando uma regra de tarefa é excluída do formulário ou da exibição de lista, você tem a opção de excluir todas as tarefas **Abertas** criadas por essa regra. As tarefas que não estão no estado **Aberto** são excluídas.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use o botão **Reaplicar** na página de regra de tarefa de correção para executar novamente a regra alterada em todas as tarefas de correção em **aberto** ativas criadas por essa regra. Ele exclui e recria automaticamente as tarefas de correção com base na regra alterada.

A reaplicação verifica somente as tarefas de correção existentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de selecionar **Reaplicar**, a seguinte mensagem será exibida: `A reaplicação desta regra de tarefa de correção excluirá e recriará as tarefas de correção para esta regra. As tarefas de correção que não estão no estado Aberto não são excluídas.`

Como criar tarefas de correção e adicionar AVIs manualmente

Você cria uma tarefa de correção de aplicação (AVUL) a partir de outro registro de tarefa de correção de aplicação e adiciona itens vulneráveis de aplicação (AVITs) manualmente. Para obter mais informações, consulte Criar uma tarefa de correção de aplicação manualmente no Resposta a vulnerabilidades de aplicações.

Regras de tarefa de correção e criação e atualização de AVI

Se um IC ou modelo de produto de uma verificação estiver associado a uma vulnerabilidade conhecida, um AVI será criado. Depois de criado, o AVI é avaliado em relação às condições das regras de tarefa de correção para uma correspondência. Se houver uma correspondência para uma tarefa de correção existente, o AVI será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o AVI.

Se qualquer propriedade capturada nas condições de filtragem da tarefa de correção for atualizada ou alterada em um AVI, o AVI atualizado também será avaliado em relação às regras de tarefa de correção para uma correspondência. Se houver uma correspondência com uma tarefa de correção existente, o AVI será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o AVI.

Rollup e rolldown de estado

Se você atualizar uma tarefa de correção para Aberto ou de Aberto para Sob investigação, o novo estado será revertido para todos os AVIs associados. A rolagem de estado ocorre imediatamente após a mudança de estado.

O acúmulo de estado de AVIs para a tarefa de correção ocorrerá somente se todos os AVIs na tarefa estiverem nos estados **Adiado** ou **Encerrado-fixo**. O acúmulo é feito com o trabalho agendado *`Rollup application vulnerable item values to vulnerability and group`*, que é executado a cada 15 minutos. O estado não é acumulado até que o trabalho seja executado. Para que um estado seja acumulado dos AVIs para a tarefa de correção, todos os AVIs devem estar no mesmo estado.

Criar, editar e excluir Resposta a vulnerabilidades de aplicações regras de tarefa de correção

Você pode criar regras para agrupar automaticamente itens vulneráveis de aplicação (IVA) em tarefas de correção (AVUL) com base nas condições do filtro. Essas regras agrupam automaticamente os AVIs conforme são importados ou criados manualmente.

Antes de Iniciar

Se você criar uma nova regra, ela não se aplicará aos dados existentes. Depois de enviá-lo, ele é executado em relação às novas importações.

Função necessária: gerente de App-Sec

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de tarefa de correção**.
2. Abra a regra ou selecione **Novo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

3. Preencha os campos no formulário ou edite-os.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra de tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condição	Condições de filtro opcionais para a regra. Por padrão, (caixa de seleção que**diferencia maiúsculas de minúsculas** não marcada), o texto de pesquisa que você insere no construtor de condições em registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefas. Um exemplo de condição é **Vulnerabilidade** > **é** > **VULNENT123451** (uma vulnerabilidade importada conhecida). Todos os AVIs que têm esta vulnerabilidade correspondem a esta condição.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis da aplicação de	A tabela que a regra usa para agrupar AVIs. Selecione os elementos da árvore: ◦ Item vulnerável da aplicação [sn_vuln_vulnerable_item] ◦ Item de configuração de item vulnerável da aplicação [cmdb_ci] ◦ Vulnerabilidade da aplicação de item vulnerável da aplicação [sn_vul_ third_party_entry] ◦ Modelo de produto de item vulnerável da aplicação **Nota:** Se você escolher uma tabela estendida, o **campo Usando** será aplicado somente para itens vulneráveis de aplicação que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar AVIs. Selecione as condições na árvore.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Você pode criar agrupar por condições para que nem todos os AVIs que compartilham dados sejam atribuídos à mesma tarefa de correção. Por exemplo, se você selecionar Grupo de atribuição e Endereço IP como os campos de uso e vários AVIs corresponderem à condição de filtragem inicial **Vulnerabilidade**, esses AVIs poderão ser atribuídos a grupos de atribuição distintos para correção usando as várias opções disponíveis na seção Agrupar por. As condições Agrupar por oferecem a flexibilidade de criar tarefas de correção distintas que podem ser atribuídas a grupos diferentes, mesmo que compartilhem alguns dados.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir automaticamente tarefas de correção, a opção Atribuição é usada além das opções **Agrupar por** para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para que cada AVI seja colocado em uma tarefa com um conjunto de grupo de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ◦ Agrupar por campo: se você selecionou qualquer campo de grupo de usuários nos valores de **campo Usando** na seção **Agrupar por**, eles serão exibidos no menu suspenso. ◦ Grupo de usuários: use a lista de pesquisa para selecionar um grupo de usuários estático.

Se você excluir uma regra do formulário ou da exibição de lista, terá a opção de excluir todas as tarefas de correção em **aberto** criadas por essa regra. Grupos que não estão no estado **Aberto** são excluídos.

4. Selecione **Enviar** para novas regras.
   Depois de selecionar **Enviar**, sua regra será exibida na lista Regras da tarefa de correção [sn_vul_grouping_rule]. As situações a seguir iniciam sua regra.
   - Quando novos IVAs são criados.
   - Quando você seleciona **Reaplicar**. Selecione **Reaplicar** para avaliar regras de tarefa somente em tarefas de correção existentes.
   - Quando os IVAs são atualizados, por você ou pelo sistema.

     Se um AVI for atualizado, as regras de tarefa serão avaliadas quanto a correspondências com as tarefas de correção existentes. Algumas atualizações comuns que iniciam uma verificação de regras são:
     - Quando o Estado muda de Encerrado para Aberto ou de Encerrado para Sob investigação.
     - O item de configuração (IC) foi alterado.
     - A vulnerabilidade foi alterada.

   O sistema verifica se todas as regras de tarefa correspondem ao AVI atualizado. Se as condições de uma regra corresponderem às condições de uma tarefa de correção, os AVIs correspondentes serão atribuídos a ela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se nenhuma correspondência for encontrada, uma nova tarefa de correção será criada.

Para obter mais informações sobre a distribuição de estado de AVIs para tarefas de correção e a distribuição de estado de tarefas de correção para AVIs, consulte Resposta a vulnerabilidades de aplicações visão geral de tarefas de correção e regras de tarefa.

Para obter um exemplo de uma regra de tarefa de correção, consulte Resposta a vulnerabilidades de aplicações exemplos de regra de tarefa de correção.

5. Para excluir uma regra de tarefa, selecione a regra na lista Regras da tarefa de correção e clique em **Excluir**.
   A seguinte mensagem é exibida: `A regra de tarefa de correção selecionada criou n tarefas de correção. Das tarefas de correção, n estão no estado Aberto.`.

Opção	Descrição
Caixa de seleção desativada (padrão).	Exclua somente a regra. As tarefas que não estão no estado **Aberto** são excluídas.
Caixa de seleção selecionada.	Inclua as tarefas de correção no estado **Aberto** ao excluir a regra da tarefa de correção. Exclua a regra e todas as tarefas de correção no estado **Aberto**.

6. Escolha uma opção e selecione **Excluir**.

Criar uma tarefa de correção de aplicação manualmente no Resposta a vulnerabilidades de aplicações

Crie uma tarefa de correção de aplicação (AVUL) a partir de outro registro de tarefa de correção de aplicação e adicione itens vulneráveis de aplicação (AVITs) manualmente.

Antes de Iniciar
Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Tarefas de correção** > **Todos**.
2. No canto superior direito da página, selecione **Novo**.
3. Na guia Configuração de grupo, para Método de agrupamento, selecione **Manual**.
4. Selecione **Enviar**.
5. Localize seu novo registro de tarefa (AVUL) na tabela Tarefas de correção de aplicações [sn_vul_app_vulnerability].
   O registro é criado no estado **Aberto**.
6. Abra o registro e adicione itens vulneráveis de aplicação novos ou existentes a este grupo usando a lista relacionada Itens vulneráveis da aplicação (**Editar** ou **Adicionar**).
7. Selecione **Atualizar** para salvar o registro ou outras ações de IU para fazer a transição do registro para outro estado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar regras de fechamento automático

Use regras de fechamento automático para fechar AVITs mais antigos automaticamente com base nas condições de filtro que você definir.

Antes de Iniciar

Função necessária: sn_vul.app_manage_auto_close_rules

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de fechamento automático**.
   O sistema de base fornece as seguintes regras de fechamento automático:

   Última verificação de vulnerabilidades da aplicação As vulnerabilidades não relatadas nos últimos 90 dias são transferidas para o estado **Obsoleto**.

2. Selecione **Novo** para criar uma nova regra de fechamento automático.
3. No formulário, preencha os campos.

Campo	Valor
Nome	Nome da regra de fechamento automático.
Ativo	Opção para ativar a regra. Se ativado, ele fechará automaticamente todas as detecções que correspondam aos critérios de filtro.
Ordem de execução	Valor exclusivo para a execução da regra de fechamento automático. Este valor determina a ordem de execução. O valor padrão é 100.
Tipo de integração	Integração de vulnerabilidade da aplicação
Descrição	Descrição da regra de fechamento automático.
Condição	Condições de filtro usadas para identificar detecções que devem ser encerradas.

4. Selecione **Enviar**.

   Os trabalhos agendados **de regras de fechamento automático são** executados todas as noites. Ele identifica AVITs com base nas condições especificadas e faz a transição das condições correspondentes para o estado **Obsoleto**. Nos casos em que há AVITs com status "Encerrado" e "Obsoleto", o AVIT é encerrado com o subestado definido como **Fixo**.

Configurar teste de invasão

Você pode configurar a duração do sprint e o esforço estimado para tipos de avaliação de teste de invasão. Isso fornece a funcionalidade de programação para proprietários de aplicações, ajudando-os a determinar um intervalo de tempo provisório para suas solicitações de avaliação de teste de invasão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: Ethical Hacker

Por Que e Quando Desempenhar Esta Tarefa
Definir as configurações de avaliação de teste de invasão para a equipe de invasão ética também ajuda a determinar o grupo e o ponto de contato que recebe a solicitação de avaliação de teste de invasão.

A partir da v19.0 de Resposta a vulnerabilidades, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais do Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão configurada em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte Veracode Vulnerability Integration.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão**.
2. Use a primeira seção para configurar o grupo de atribuição.
3. No formulário, preencha os campos.

Formulário de configuração do teste de invasão

Campo	Descrição
Grupo de usuários da equipe de testes de invasão	Grupo ao qual a solicitação de avaliação de teste de invasão está atribuída.
Atribuído padrão das solicitações de avaliação de testes de invasão	Ponto de contato para a solicitação de avaliação de teste de invasão.

4. Selecione **Atualizar**.
5. Use a segunda seção para configurar sprints.
   Para obter detalhes, consulte Configurar sprints para testes de invasão.
6. Use a terceira seção para configurar os tipos de avaliação.
   Para obter detalhes, consulte Configurar tipos de avaliação para testes de invasão.

Configurar sprints para testes de invasão

Configure a duração do sprint e a capacidade da equipe de invasão ética para que ela possa gerenciar a capacidade do sprint para avaliações de teste de invasão.

Antes de Iniciar
Função necessária: Ethical Hacking

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão**.
2. Selecione a opção **Configurar** para Configurar sprints.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de configuração de sprint

Campo	Descrição
Duração do sprint (dias)	Número de dias em um sprint.
Data de início	Data de início da duração do sprint.
Número de sprints	Número de sprints que podem ser gerados, com base nas datas de início e término do intervalo de sprint.
Data de término	Data de término da duração do sprint.
Capacidade de sprint	
Capacidade de sprint (h)	Capacidade de um sprint em horas.

4. Selecione **Gerar sprints**.
   Para exibir os sprints criados, selecione **Exibir sprints**.

   Nota: Depois que os sprints forem gerados e estiverem em andamento, se você selecionar **Gerar sprints** com a mesma duração, o sprint atual será concluído normalmente. Os sprints restantes são recalculados com base na configuração de sprint atualizada.

Configurar tipos de avaliação para testes de invasão

Configure o esforço estimado para cada tipo de avaliação de teste de invasão. Isso permite que você gerencie a capacidade de cada sprint, estimando o esforço necessário para cada tipo de avaliação.

Antes de Iniciar
Função necessária: Ethical Hacking

Por Que e Quando Desempenhar Esta Tarefa
Cada sprint é atribuído a uma solicitação de teste de invasão. Com base no esforço estimado para o tipo de avaliação, as horas são ajustadas para refletir o saldo de horas do sprint.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão**.
2. A partir da v19.0 de Resposta a vulnerabilidades, selecione **Configurar** para exibir Tipos de avaliação, Tamanho da aplicação e Esforço estimado.
3. Opcional: Selecione um registro de tipo de avaliação para atualizar os campos conforme necessário ou criar novos registros.

   (Optional) Os valores de tamanho da aplicação fornecem mais opções para ajudar a estimar o tempo e o esforço de teste com mais precisão. Você pode editar as horas desses registros ou selecionar **Novo** para criar suas próprias combinações.

   Você pode modificar o tipo de avaliação e o tamanho da aplicação em valores em registros de solicitação de teste de invasão existentes para que você possa programar testes para corresponder à capacidade de sprint. Por exemplo, se você preencher uma solicitação de teste, talvez não veja o número de sprints configurados, porque alguns sprints já foram usados para teste. Se as horas de esforço estimadas de um sprint

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

corresponderem à combinação necessária para o tipo e tamanho de um teste, elas não estarão disponíveis para novas solicitações.

Você pode ver os sprints atribuídos às solicitações de teste nos registros da lista de Sprints de teste de invasão em **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Configuração de testes de invasão** > **Configurar sprints**. Consulte Configurar sprints para testes de invasão para obter mais informações sobre como configurar sprints.

Os valores base para Tipo de avaliação, Tamanho da aplicação e Esforço estimado são:

Formulário de configuração do tipo de avaliação de teste de invasão

Tipo de avaliação	Tamanho da aplicação	Esforço estimado (h)
Teste focado	Pequeno	20
Teste focado	Médio	30
Teste focado	Grande	40
Teste focado	Padrão	40
Testar novamente	Pequeno	10
Testar novamente	Médio	15
Testar novamente	Grande	20
Testar novamente	Padrão	20
Teste de invasão completo	Pequeno	60
Teste de invasão completo	Médio	70
Teste de invasão completo	Grande	80
Teste de invasão completo	Padrão	80

4. Selecione Atualizar para salvar suas mudanças ou Enviar para um novo registro.
5. Antes da v19.0, selecione a opção **Configurar** para Configurar tipos de avaliação.
6. Atualize os valores dos tipos de avaliação conforme necessário.
   Os valores base são:

Formulário de configuração do tipo de avaliação de teste de invasão

Tipo de avaliação	Esforço estimado (h)
Teste focado	40
Testar novamente	20
Teste de invasão completo	80

7. Salve as mudanças.

Integração do Resposta a vulnerabilidades de aplicações a outras aplicações

Resposta a vulnerabilidades inclui suporte para integrações de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de terceiros

As integrações de vulnerabilidade da aplicação ajudam a aprimorar os dados de vulnerabilidade da aplicação em sua instância, recuperando dados de sistemas e fornecedores externos. Consulte os seguintes tópicos de visão geral para obter mais informações sobre integrações compatíveis:

- Integrações de vulnerabilidade do Fortify
- Integrações de vulnerabilidade de aplicação do GitHub
- Integração de vulnerabilidade do Invicti
- Veracode Vulnerability Integration
- Atlassian Jira Integration

Importante: No Espaço do gerenciador de vulnerabilidades, você pode criar um problema ágil manualmente usando a ação de lista e a ação de formulário para rastrear a correção de AVITs e RTs.

Nota:

Integrações de várias origens não são compatíveis com Resposta a vulnerabilidades de aplicações. As integrações de terceiros são tratadas separadamente. Se mais de uma aplicação de integração de terceiros estiver em uso em seu ambiente, não haverá desduplicação de item vulnerável da aplicação (IVA) entre as integrações.

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades de aplicações, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Integração de Resposta a vulnerabilidades com Black Duck

A integração [Resposta a vulnerabilidades com Integração de Resposta a vulnerabilidades com Black Duck usa os dados que são importados da ferramenta Análise de composição

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de software (SCA) do Black Duck para ajudá-lo a determinar o impacto e a prioridade das falhas em seu código.

Visão geral da integração

Com o Integração de Resposta a vulnerabilidades com Black Duck, você pode coletar SCA e disponibilizar esses dados para o Now Platform. A partir da v22.0.5 de Resposta a vulnerabilidades, você pode importar os dados de vulnerabilidades de SCA para sua instância para que possa identificar as vulnerabilidades em seus aplicativos de software. Para obter mais informações, consulte Exploração do Lista de materiais de software.

Uma API compartilhada ingere os dados de SCA.

Nota: Cada registro de integração tem um usuário executar como configurado. O valor padrão para este usuário é Sistema VR. Não altere este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente na ordem em que estão listadas. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versões disponíveis da Black Duck Integration

Versão de lançamento	Notas de versão
Integração de Resposta a vulnerabilidades com Black Duck 1.0.5	Notas de versão Resposta a vulnerabilidades de aplicações

Grupo de usuários e funções

O Integração de Resposta a vulnerabilidades com Black Duck é instalado por um usuário com a função de administrador e é configurado por um membro do grupo de gerentes de App-Sec. Para obter mais informações, consulte o Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

Para status de execução de integração, consulte Exibir o Integração de Resposta a vulnerabilidades com Black Duck status de execução de importação

Para exibir dados nas vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparar tarefas de pré-integração para Integração de Resposta a vulnerabilidades com Black Duck

Planeje e execute as tarefas de pré-integração para o Integração de Resposta a vulnerabilidades com Black Duck para que sua integração seja bem-sucedida. O Integração de Resposta a vulnerabilidades com Black Duck pressupõe que você esteja familiarizado com a aplicação Análise de composição de software (SCA) e as APIs do Black Duck.

Antes de Iniciar

Antes de instalar e configurar o Integração de Resposta a vulnerabilidades com Black Duck, você deve executar e instalar a integração de enumeração de pontos fracos comuns

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(CWE), que também é usada por Resposta a vulnerabilidades de aplicações. A integração do CWE é instalada com Resposta a vulnerabilidades por padrão.

Nota: Embora os dados do banco de dados de vulnerabilidades do NIST (NVD) não sejam necessários para instalar a integração de vulnerabilidade da aplicação Black Duck, seria útil ter. Para obter informações sobre o NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Cada registro de integração tem um usuário executar como configurado. O valor padrão para este usuário é VR.System. Não altere este valor.

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância pelo número de itens vulneráveis de aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

O Integração de Resposta a vulnerabilidades com Black Duck requer um URL de API e um token de API.

Procedimento

Crie o token de API e as credenciais de chave.

a. Faça login na plataforma Black Duck.

b. Acesse o menu da conta do usuário e selecione **Credenciais de API**.

c. Selecione **Gerar credenciais de API**.

d. Registre suas credenciais para uso posterior.

Instalar o ServiceNow Integração de Resposta a vulnerabilidades com Black Duck

Antes de executar a integração em sua instância, você deve concluir as etapas de instalação e configuração para que a ferramenta Análise de composição de software (SCA) do Black Duck se integre corretamente ao Resposta a vulnerabilidades de aplicações.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Você deve executar essas tarefas de configuração para que a ferramenta Análise de composição de software (SCA) do Black Duck se integre corretamente a Resposta a vulnerabilidades de aplicações.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração

Tarefas de configuração	Descrição
	> **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o usuário com a função de administrador instalará a aplicação e atribuirá usuários ao grupo de gerentes de App-Sec. Para obter informações sobre funções de grupo, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo de gerentes de App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Esta ferramenta SCA está disponível como uma assinatura separada.

Procedimento
1. Faça login na instância em que você deseja instalar o Integração de Resposta a vulnerabilidades com Black Duck.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise Integração de resposta a vulnerabilidades com a aplicação Black Duck.
4. Selecione o bloco da aplicação.
   Os detalhes sobre a aplicação que você está instalando são exibidos.

   Nota: Considere ler as seções Outros Requisitos e Dependências, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o nome da instância e o motivo da instância e selecione **Validar instância**.
8. Selecione **Solicitar**.
   Você receberá um e-mail com as instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Localize a aplicação, selecione-a e escolha **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Configure o Integração de Resposta a vulnerabilidades com Black Duck para o seu ambiente. Veja Configure o Integração de Resposta a vulnerabilidades com Black Duck

Configure o Integração de Resposta a vulnerabilidades com Black Duck

Antes de executar o Integração de Resposta a vulnerabilidades com Black Duck em sua instância, você deve concluir as etapas de instalação e configuração para que a ferramenta Análise de composição de software (SCA) do Black Duck se integre corretamente à aplicação Resposta a vulnerabilidades de aplicações.

Antes de Iniciar

Função necessária: grupo de usuários do App-Sec Manager

Por Que e Quando Desempenhar Esta Tarefa

O Integração de Resposta a vulnerabilidades com Black Duck está disponível como uma assinatura separada.

Procedimento

1. Navegar até **Todos** > **Integração da vulnerabilidade de Blackduck** > **Configuração**.
2. Selecione o tipo de Autenticação básica.
   A Autenticação básica requer um MID Server para instâncias que estão no local. Você pode gerar o token de API necessário para autenticação básica de sua conta do Black Duck.
3. No formulário, preencha os campos.
   Autenticação básica

Campo	Descrição
URL da API	URL da API Black Duck para instâncias empresariais ou no local. A instância no local é a URL do endpoint do Black Duck.
Token de API	Token que você gerou a partir do console do Black Duck.
MID Server	MID Server que é necessário para instâncias no local para autenticação básica.
Incluir SCA	Vulnerabilidades das verificações da Análise de composição de software (SCA) que são incluídas por padrão. As verificações de SCA identificam as vulnerabilidades em componentes de código aberto.
Selecione a opção para gerenciar falsos positivos na ServiceNow	ServiceNow Opção para gerenciar falsos positivos. Deixe esta opção ativada se quiser fazer a triagem dos itens vulneráveis da aplicação (IVAs) importados com os estados de **origem** marcados como **Falso-positivo** ou **Possível falso-positivo**. AVIs com esses estados de **origem** que normalmente são mapeados para um esta-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	do **Closed** em sua instância são mapeados para **Open**. Você pode solicitar um **falso-positivo** do registro AVI. ◦ Desative uma ou ambas as opções se quiser preservar os estados de **origem** que foram importados do scanner. ◦ Se desativado, as ações **Solicitar exceção** e **Falso-positivo** não ficarão visíveis nos AVIs.
Instância de Integração	Instância que você está usando para importar os dados.

4. Selecione **Salvar e testar credenciais**.
5. Execute a **integração da lista de projetos do Black Duck** antes de executar outras integrações.
   As outras integrações do Black Duck, como a integração da lista de aplicações do Black Duck e a integração do item vulnerável da aplicação do Black Duck, dependem do projeto atual e dos dados da aplicação que você importou da integração da lista de projetos.

Exibir o Integração de Resposta a vulnerabilidades com Black Duck status de execução de importação

Verifique o sucesso das execuções de integração, localize problemas e confirme suas decisões de correção exibindo a lista relacionada de execuções de integração de vulnerabilidade.

Antes de Iniciar
Função necessária: administrador

Procedimento
1. Navegar até **Todos** > **Integração da vulnerabilidade de Blackduck** > **Integrações**.
2. Selecione uma integração.
3. Selecione a lista relacionada Execuções de integração de vulnerabilidade.
4. Verifique se todas as importações foram bem-sucedidas.
   Solução de problemas:

   As causas mais comuns de falha na execução incluem:
   - Interrupção de rede.
   - Um problema na transferência de dados que resulta em dados corrompidos durante uma transformação.

   Se você encontrar alguma dessas condições, selecione **Executar agora**e execute novamente a integração.
5. Exiba os repositórios importados navegando até a lista de integrações e selecionando o registro Integração de Black Duck.
6. Selecione a lista relacionada Execuções de integração de vulnerabilidade e abra um registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transformação de dados para o Integração de Resposta a vulnerabilidades com Black Duck

Depois de identificar os dados que deseja importar, os dados são recuperados do Integração de Resposta a vulnerabilidades com Black Duck, processados por meio de um conjunto de fontes de dados e transformados em sua instância.

Integração de Resposta a vulnerabilidades com Black Duck

Os dados da API são carregados primeiro na tabela Importação de item AppVul de Black Duck [sn_vul_blackduck_appvul_item_import], e a transformação de item AppVul de Black Duck é usada para transformar as informações importadas.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação** e pesquise por **Black Duck AppVul Item Transform**. A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de item AppVul de Black Duck

Campo de origem	Campo de destino	Descrição
app_id	source_app_id	ID da aplicação.
ID do problema	source_avit_id	ID do AVIT.
app_name	app_name	Nome da aplicação.
versão	app_version	Versão da aplicação.
build_id	source_scan_id	ID de compilação da aplicação.
account_id	account_id	ID da conta.
sandbox_id	sandbox_id	ID da área restrita.
last_update_time	última_scan_data	Hora da última atualização.
app_name + last_scan_date	scan_summary_name	Resumo da verificação.
life_cycle_stage	status_sdlc_de_origem	Status do SDLC de origem.
nível	gravidade_origem	Gravidade de origem.
category_name	categoria	Categoria.
gravidade_origem	gravidade_origem	Gravidade de origem.
category_id + "CWE-" + cweId	source_entry_id	ID da entrada de origem.
source_vulnerability_summary	source_vulnerability_summary	Resumo da vulnerabilidade de origem.
recomendação_de_origem	recomendação_de_origem	Recomendação de origem.
descrição	descrição	Descrição da origem.
descrição	source_vulnerability_explanation	Explicação da vulnerabilidade de origem.
mitigação_status_desc	source_mitigação_status	Status de mitigação de origem.
status_remediação	source_remediation_status	Status de correção de origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de item AppVul de Black Duck

Campo de origem	Campo de destino	Descrição
linha	número_linha	Linha em que a falha foi encontrada.
módulo	application_module	Módulo da aplicação.
arquivo de origem	notas_de_origem	Anotações de origem.
afeta_conformidade_política	cumpre_com_política	Os valores podem ser Sim ou Não, com base nas informações de origem serem verdadeiras ou falsas.
Sourcefilepath + sourcefile	local	Mapeamento de local de uma falha estática.
URL	local	Mapeamento de local para uma falha dinâmica.
escopo, tipo, exploitLevel	source_additional_info	Campo de valor de nome preenchido com os valores da origem para falhas estáticas.

A tabela a seguir lista os scripts de transformação que são executados durante o processo de transformação.

Tempo e finalidade do script do mapa de transformação do Black Duck

Script do mapa de transformação do Black Duck

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação tiver criado uma transformação).	Script usado para processar o registro e atualizar o número de entidades criadas, atualizadas ou inalteradas e as que são importadas como parte desta integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto para importação concluir a transformação)	Script usado para definir o comportamento de registros inválidos e que devem ser ignorados. Além disso, usado para definir o objeto global para processamento de registros. Este script é para uso interno e não deve ser modificado ou excluído.

Mapeamento de estado de Integração com Black Duck

A tabela a seguir mostra os estados de origem da Integração de vulnerabilidade do Black Duck e os estados de destino em sua instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados de origem do Black Duck e seus estados Now Platform correspondentes

Estados de origem do Black Duck	Descrição dos estados de origem	Estado de destino na Now Platform
Novo	A vulnerabilidade afeta esta versão do componente.	Aberto
Precisa de revisão	Não pode ser determinado se uma vulnerabilidade afeta esta versão do componente.	Aberto
Correção necessária	A correção é necessária para esta versão.	Aberto
Correção concluída	A correção desta vulnerabilidade está concluída.	Encerrado
Mitigado	A vulnerabilidade foi atenuada.	Encerrado
Com patch	A vulnerabilidade foi corrigida.	Encerrado
Ignorado	A vulnerabilidade foi ignorada.	Encerrado

Importar as informações do projeto da instância de integração do Black Duck

Importe as informações do projeto da instância de integração do Black Duck para garantir que as integrações de vulnerabilidade sejam executadas sequencialmente. Uma integração bem-sucedida ajuda a identificar e ingerir os itens vulneráveis da aplicação (IVAs).

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Você pode importar todas as informações do projeto de Integração de Resposta a vulnerabilidades com Black Duck na tabela de projetos do [sn_vul_blackduck_project] Black Duck. Todos os atributos necessários, por exemplo, GUID do projeto, que são necessários para consultar diferentes versões do projeto, são capturados na tabela de projetos do Black Duck [sn_vul_blackduck_project].

Procedimento

1. Navegar até **Todos** > **Integração da vulnerabilidade de Blackduck** > **Integrações**.
2. Selecione uma integração.
   Por exemplo, você pode selecionar a **integração da lista de projetos do Black Duck.**
3. Selecione **Executar agora**.

> **Nota:** Cada Integração de Resposta a vulnerabilidades com Black Duck tem como objetivo fornecer a recuperação de dados mais completa. Executar essas integrações fora de ordem pode resultar em dados incompletos e requer ServiceNow e experiência em Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que a importação for concluída, você poderá ver os detalhes do projeto na tabela de projetos do [sn_vul_blackduck_project] Black Duck.

4. Para status de execução de integração, consulte Exibir o Integração de Resposta a vulnerabilidades com Black Duck status de execução de importação.
5. Opcional: Se você quiser modificar outros parâmetros de integração, deverá navegar até a instância de integração.

Importar Integração de Resposta a vulnerabilidades com Black Duck versões do projeto para a tabela Aplicações descobertas

Importe a integração da Resposta a vulnerabilidades com as versões do projeto Black Duck para a tabela Aplicações descobertas [sn_vul_release] para que as integrações de vulnerabilidade do Black Duck sejam executadas sequencialmente. Uma integração bem-sucedida ajuda a identificar e ingerir os itens vulneráveis da aplicação (IVAs).

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
Você pode adicionar e exibir todas as diferentes versões dos projetos (consulte os detalhes na tabela Projetos do Black Duck) que foram importados de Integração de Resposta a vulnerabilidades com Black Duck na tabela Aplicações descobertas [sn_vul_release].

Procedimento
1. Navegar até **Todos** > **Integração da vulnerabilidade de Blackduck** > **Integrações** .
2. Selecione uma integração.
   Por exemplo, você pode selecionar a **integração da lista de aplicações Black Duck**.
3. Selecione **Executar agora**.

   Nota: Cada versão de projeto das integrações tem como objetivo fornecer a recuperação de dados mais completa. Executar essas integrações fora de ordem pode resultar em dados incompletos e requer experiência da ServiceNow e da Resposta a vulnerabilidades de aplicações.

   Depois que a importação for concluída, você poderá ver as diferentes versões de um projeto na tabela Aplicações descobertas [sn_vul_release]. Se você estiver usando Regras de pesquisa de IC, essas aplicações descobertas serão vinculadas à tabela de item de configuração [cmdb_ci].

4. Veja o status das execuções de integração.
   Para obter mais informações, consulte Exibir o Integração de Resposta a vulnerabilidades com Black Duck status de execução de importação.

Importar os itens vulneráveis da aplicação do Integração de Resposta a vulnerabilidades com Black Duck

Importe os itens vulneráveis da aplicação (IVAs) da integração da Resposta a vulnerabilidades com Black Duck para que a integração seja executada sequencialmente. Uma integração bem-sucedida ajuda a identificar e ingerir os AVIs.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode exibir os resultados da verificação do Integração de Resposta a vulnerabilidades com Black Duck, inserir AVIs em sua instância e aprimorar seus dados de vulnerabilidade de terceiros. Por padrão, se o registro do scanner estiver no estado Fechado, os IVAs não serão criados. Você pode controlar AVIs existentes usando a propriedade sn_vul_create_closed.

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade do Black Duck** > **Integrações**.
2. Selecione uma integração.
   Por exemplo, você pode selecionar a **Integração de item vulnerável da aplicação Black Duck**.
3. Selecione **Executar agora**.

   Nota: O Integração de Resposta a vulnerabilidades com Black Duck tem como objetivo fornecer a recuperação de dados mais completa. Executar essas integrações fora de ordem pode resultar em dados incompletos e requer conhecimento de ServiceNow e Resposta a vulnerabilidades de aplicações.

   Depois de importar todas as vulnerabilidades de SCA do Integração de Resposta a vulnerabilidades com Black Duck, você pode exibir os AVIs e os dados de vulnerabilidade de terceiros.

Definir os tempos de importação para o Integração de Resposta a vulnerabilidades com Black Duck

Defina a hora de início das Integração de Resposta a vulnerabilidades com Black Duck importações. Você pode definir as integrações com antecedência para obter melhor desempenho e execuções de importação mais rápidas.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, as integrações de vulnerabilidade do Black Duck fazem uma importação completa sempre que são executadas.

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade do Black Duck** > **Integrações**.
2. Selecione uma integração.
3. Defina a nova **Hora**de início.
   O tempo é calculado em horas no horário local. O tempo padrão para as importações da Integração da lista de aplicações do Black Duck é 00:00:00. As outras integrações são **sob demanda** e encadeadas, o que significa que elas seguem uma sequência para serem executadas após a integração da lista de aplicações do Black Duck. Alterar a **hora de início** requer conhecimento avançado de ServiceNow e Gestão de vulnerabilidades de aplicações.
4. Selecione **Atualizar**.
   A nova hora será usada para a próxima importação agendada.

Incluir itens vulneráveis da aplicação Black Duck encerrada

Inclua itens vulneráveis de aplicação (IVAs) encerrados durante as importações de integração de itens vulneráveis do Black Duck porque, por padrão, eles não são criados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

durante as importações de integração. Se você quiser criá-los, deverá alterar a propriedade do sistema.

Antes de Iniciar
Verifique se o Integração de Resposta a vulnerabilidades com Black Duck está instalado e em execução.

Função necessária: administrador

Procedimento

1. No filtro de navegação, insira `sys_properties.list`.
2. No campo **Nome** da lista, insira `sn_vul.create_closed`.
3. Clique duas vezes no campo **Valor** e defina-o como **Verdadeiro**
4. Salve selecionando o ícone de marca de seleção .
   Os registros no estado Fechado na próxima importação do Black Duck são criados como AVIs em Resposta a vulnerabilidades de aplicações.

Integrações de vulnerabilidade do Fortify

O Integrações de vulnerabilidade do Fortify usa dados importados do produto Fortify para ajudar você a determinar o impacto e a prioridade das falhas no seu código.

Integrações de vulnerabilidade do Fortify

O produto Fortify coleta dados do scanner e os disponibiliza para o Now Platform®. Ele se integra facilmente ao recurso [ServiceNow® Resposta a vulnerabilidades de aplicações de Resposta a vulnerabilidades para mapear vulnerabilidades de terceiros que enriquecem os dados em sua instância.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente. Depois que todas as integrações são ativadas, elas são encadeadas para serem executadas em sequência. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas de versão
Integração da Resposta a vulnerabilidades com Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Notas de versão Resposta a vulnerabilidades de aplicações Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de vulnerabilidade do Fortify

Para exibir o Integrações de vulnerabilidade do Fortify, navegue até **Integrações de vulnerabilidade do Fortify** > **Integrações**.

As seguintes integrações estão incluídas no sistema de base. Essas integrações não estão ativas por padrão.

Após a execução inicial, todos os dias, os trabalhos agendados são encadeados para executar as integrações automaticamente na ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Fortify Integrações de vulnerabilidade

Integração	Descrição
Fortify integração da lista de aplicações sob demanda	Recupera Fortify dados do scanner de aplicações (vulnerabilidades, metadados) e aprimora os dados de aplicações de terceiros. Esta integração está definida para ser executada diariamente às 00:00:00. Está ativo por padrão.
Fortify Integração do resumo de verificação sob demanda	Recupera registros de verificação de Fortify. Esta integração é encadeada para ser executada após a Fortify integração da lista de aplicações sob demanda quando ativada. Está inativo, por padrão.
Fortify integração de item vulnerável da aplicação sob demanda	Recupera resultados de verificação de Fortify, insere AVITs e aprimora seus dados de vulnerabilidade de terceiros. Se o registro do scanner estiver no estado **Fechado**, os AVITs não serão criados. Os AVITs existentes ainda estão atualizados. A partir da v2.3, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para a integração de item vulnerável de aplicação. Esta integração está encadeada para ser executada após a Fortify Integração de resumo de verificação sob demanda quando ativada. Está inativo, por padrão.

Para status de execução de integração, consulte Exibir o Integrações de vulnerabilidade do Fortify status de execução de importação.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparando para o Integrações de vulnerabilidade do Fortify

Um Integrações de vulnerabilidade do Fortify bem-sucedido requer planejamento e a execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Integrações de vulnerabilidade do Fortify pressupõe que você esteja familiarizado com o produto Fortify e a API.

Antes de Iniciar

A integração de enumeração de pontos fracos comuns (CWE) também é usada por Resposta a vulnerabilidades de aplicações e deve estar em execução antes de instalar e configurar o Integrações de vulnerabilidade do Fortify.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar o Integrações de vulnerabilidade do Fortify, no entanto, eles fornecem enriquecimento e seria útil ter.

Para obter informações sobre o NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis de aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

O Integrações de vulnerabilidade do Fortify requer uma chave de API, segredo de API e URL raiz de API, disponíveis na sua conta Fortify on Demand.

Procedimento

Para criar uma chave secreta de API:

a. Faça login no portal Fortify on Demand.

b. Navegar até **Todos** > **Administração** > **Configuração** > **API**.

c. Adicione a ServiceNow como uma aplicação.

d. Clique em **Novo segredo** para gerar um segredo de API.

e. Registre seu segredo de API para uso posterior.

Instalar a ServiceNow® Integração de resposta a vulnerabilidades com Fortify

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Fortify se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao grupo de gerentes de App-Sec. Para obter informações sobre funções de grupo, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo de gerentes de App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: gerente de App-Sec

Procedimento

1. Faça login na instância em que você deseja instalar o Integrações de vulnerabilidade do Fortify.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a aplicação Integração de resposta a vulnerabilidades com Fortify.
4. Clique no bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira o **Nome** e **o motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Configure o Integrações de vulnerabilidade do Fortify para o seu ambiente. Consulte Configure o Integrações de vulnerabilidade do Fortify.

Configure o Integrações de vulnerabilidade do Fortify

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Fortify se integre corretamente ao recurso [

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações de Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar
Funções necessárias: gerente de App-Sec

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se a aplicação Resposta a vulnerabilidades Integration with Fortify está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar a ServiceNow Integração de resposta a vulnerabilidades com Fortify.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de gerentes de App-Sec. • O gerente do App-Sec supervisiona a configuração e verifica os resultados esperados.
Para Integrações de vulnerabilidade do Fortify, tenha o **ID** de **API e a chave** de API prontos.	Entre em contato com Fortify para obter o **ID** e **a chave de API**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login na instância em que você deseja instalar as integrações de vulnerabilidade da aplicação Fortify.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a integração [Resposta a vulnerabilidades com a aplicação Fortify.
4. Clique no bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira o **Nome** e **o motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.
11. Quando a instalação for concluída, navegue até **Integrações de vulnerabilidade do Fortify** > **Configuração do FoD**.
12. No formulário, preencha os campos.

Formulário de configuração do Fortify on Demand

Campo	Descrição
URL raiz da API	URL da instância do Fortify do usuário.
Chave de API	Identificador exclusivo enviado para a API Fortify.
Segredo da API	Segredo do cliente fornecido por Fortify.
Incluir DAST	Opção para incluir vulnerabilidades de verificações do DAST. As verificações DAST identificam vulnerabilidades no comportamento de sua aplicação geral.
Incluir SAST	Opção para incluir vulnerabilidades de verificações SAST. As verificações do SAST identificam vulnerabilidades no código.
Triagem de exceções e falso-positivos na ServiceNow (a partir da v20.0 da Resposta a vulnerabilidades)	Selecione opções para gerenciar fluxos de trabalho de gestão de exceções e falso-positivos para IVAs com ServiceNow automaticamente após a importação. Essas opções são ativadas por padrão. Para obter um exemplo de caso de uso, consulte Como gerenciar o mapeamento de estado para adiamentos e falso-positivos no Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Gerenciar exceções no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVIs importados marcados para o estado **Adiado**. AVIs com estados de **origem** que normalmente são mapeados para um estado **Adiado** em sua instância são mapeados para **Aberto**. Você **solicita uma exceção** do registro AVI. Gerenciar falsos positivos no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVIs importados com estados de **origem** marcados como **Falso-positivo** ou **Possível falso-positivo**. AVIs com esses estados de **origem** que normalmente são mapeados para um estado **Closed** em sua instância são mapeados para **Open**. Você solicita um **falso-positivo** do registro AVI. ◦ Desative uma ou ambas as caixas de seleção se quiser preservar os estados de **origem** importados do scanner. ◦ Esses AVIs são mapeados para os estados de destino e os estados de motivo do destino conforme são importados, mas não são triados pelos fluxos de trabalho de exceção e falso-positivo. As ações **Solicitar exceção** e **Falso-positivo** não estão visíveis nos AVIs.
Triagem na ServiceNow (anterior à v20.0 da Resposta a vulnerabilidades)	Gerencie a triagem de vulnerabilidade da aplicação na instância ServiceNow : ◦ Marque a caixa de seleção para fazer a triagem dos AVIs em ServiceNow. Se esta opção for selecionada, os AVIs serão importados no estado Aberto. Você pode solicitar uma exceção ou marcar o AVI como um falso-positivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Para manter o estado de origem, ou seja, o estado importado do scanner, certifique-se de que a caixa de seleção não esteja marcada. **Nota:** As opções **Marcar como falso-positivo** e **Solicitar exceção** estão disponíveis somente para IVAs sendo triados em ServiceNow.

13. Selecione **Salvar e testar credenciais**.

O que Fazer Depois

Se o seu ambiente exigir importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração.

Na instalação inicial, consulte Como configurar o Resposta a vulnerabilidades de aplicações para obter mais instruções.

Após a instalação inicial, para modificações, consulte Integrações de vulnerabilidade do Fortify modificação e atividades.

Exibir o Integrações de vulnerabilidade do Fortify status de execução de importação

Use a lista relacionada de **execuções de integração de vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o Fortify status de execução de importação:

- As aplicações Resposta a vulnerabilidades e Integrações de vulnerabilidade do Fortify devem ser instaladas e configuradas.
- As Integrações de vulnerabilidade do Fortify importações devem estar programadas e em execução.

Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades de aplicações, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Selecione uma integração.
3. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.
5. A partir da v2.3, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as integrações de item vulnerável da aplicação.

Integrações de vulnerabilidade do Fortify modificação e atividades

Configure modificações opcionais especificamente para Integrações de vulnerabilidade do Fortify.

Nota: Alterar outras configurações de Integrações de vulnerabilidade do Fortify, diferentes das listadas aqui, requer conhecimento avançado de ServiceNow e Resposta a vulnerabilidades de aplicações e está além do escopo da documentação do produto.

Executar uma importação manual de vulnerabilidade da aplicação Fortify

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independente do trabalho agendado diariamente.

Antes de Iniciar
Função necessária: gerente de App-Sec

Procedimento

1. Navegar até **Todos** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Escolha uma integração, por exemplo, Fortify Application List Integration.
3. Selecione **Executar agora**.

Nota: Para concluir a recuperação de dados, execute as integrações de vulnerabilidade da aplicação Fortify em sequência.

Importar dados usando o Integrações de vulnerabilidade do Fortify

Importe dados do scanner do Fortify para mapear itens vulneráveis de aplicação (IVAs), aprimorando assim os dados em sua instância.

Antes de Iniciar
Função necessária: gerente de App-Sec

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, Fortify integrações de vulnerabilidade fazem uma importação delta sempre que são executadas, recuperando os dados mais recentes. Consulte Executar uma importação manual de vulnerabilidade da aplicação Fortify para obter mais informações sobre importações completas.

Procedimento

1. Navegar até **Todos** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Escolha uma integração.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da execução de integração.
Ativo	Opção para ativar uma integração.
Executar	Frequência da execução da integração.
Hora	
Aplicação	Aplicação que contém este registro.
Integração de origem	Integração de origem para esta integração.
Instância de origem	Instância de origem para esta integração.
Próxima integração	Próxima integração em sequência, a ser executada após a execução da integração atual.
Hora de início	Data e hora de início da última execução de integração bem-sucedida. O tempo é calculado como Horas no horário local. A hora padrão para a execução inicial é 00:00:00.
Detalhes de Integração	
Script de integração	Inclusão de script que estende o *VulnerabilityIntegrationBase* a ser executado quando a integração é executada. Este script define como recuperar dados de um sistema de terceiros.
Script de fábrica de integração	Script que define como construir o script include selecionado para o script de integração.
Estratégia do processador de relatórios	Estratégia que você deseja usar para lidar com os dados retornados pelo script de integração quando a integração é executada.

4. Selecione **Executar agora** para executar a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incluir itens vulneráveis da aplicação Fortify on Demand encerrados

Por padrão, os Itens vulneráveis da aplicação **encerrados** (AVITs) não são criados durante Fortify importações de integração de item vulnerável. Se você quiser criá-los, deverá alterar uma propriedade do sistema.

Antes de Iniciar

O Integrações de vulnerabilidade do Fortify deve estar instalado e em execução.

Função necessária: gerente de App-Sec

Procedimento

1. Na caixa de texto **Navegador de filtros** à esquerda, digite `sys_properties.list`.
2. Na caixa de pesquisa **Nome** da lista, insira `sn_vul.create_closed`.
3. Clique duas vezes no campo **Valor** e defina como **Verdadeiro**
4. Clique no ícone de marca ícone de marca de seleção verde para salvar.
   Registros no estado **Encerrado** na próxima importação Fortify são criados como AVITs em Resposta a vulnerabilidades de aplicações.

Integrações de vulnerabilidade de aplicação do GitHub

O Integrações de vulnerabilidade de aplicação do GitHub importa dados de SAST (Static Application Security Testing, SAST) e Análise de composição de software (SCA) para ajudá-lo a exibir alertas de vulnerabilidade nos repositórios do seu ambiente GitHub.

Integrações de vulnerabilidade de aplicação do GitHub

O Integrações de vulnerabilidade de aplicação do GitHub coleta dados do scanner e os disponibiliza para o Now Platform®. Ele se integra facilmente ao recurso [ServiceNow® Resposta a vulnerabilidades de aplicações de Resposta a vulnerabilidades para mapear vulnerabilidades de terceiros e GitHub alertas em sua instância.

O ambiente GitHub oferece suporte a várias organizações. Essas organizações, tanto no local quanto no Enterprise, podem conter vários departamentos, como Engenharia, Qualidade, Documentação e assim por diante. Cada organização, por sua vez, pode oferecer suporte a vários repositórios. Depois de importar os dados da aplicação com a integração de repositórios GitHub, você pode importar dados de vulnerabilidade e alerta desses repositórios. Os dados importados são processados como uma aplicação na aplicação Resposta a vulnerabilidades de aplicações. Quando os verificadores detectam vulnerabilidades e geram alertas para os repositórios, as vulnerabilidades são criadas em Resposta a vulnerabilidades de aplicações.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Versão de lançamento	Notas de versão
Integrações de vulnerabilidade de aplicação do GitHub v1.2, v1.1, 1.0	Notas de versão Resposta a vulnerabilidades de aplicações Para obter informações de compatibilidade, consulte KB0856498 Matriz de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão de lançamento	Notas de versão
	compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações do GitHub

Integração	Descrição
GitHub Integração de repositórios	A partir da v1.1, importe todos os dados de aplicações para suas contas GitHub no local e na nuvem (Enterprise). A integração importa aplicações dos repositórios que você configurou para uma organização (no local) ou do seu ambiente empresarial (em nuvem). Execute esta integração antes de executar as outras GitHub integrações, pois elas dependem dos dados da aplicação atuais importados da integração de repositórios.
GitHub Integração do CodeScan	Recupera alertas de vulnerabilidade de verificação de código de GitHub repositórios para vulnerabilidades de segurança e erros de codificação. Os dados importados são mapeados para os resultados do SAST em sua instância.
GitHub Integração do Dependabot	Recupera alertas do Dependabot para dependências com vulnerabilidades conhecidas dos repositórios. Os dados importados são mapeados para os resultados de SCA em sua instância.
GitHub Varredura secreta	Recupera segredos do código de suas organizações junto com os resultados de testes de segurança da aplicação. Os dados são mapeados para os resultados de SCA em sua instância.
GitHub Local de verificação de segredo	Recupera o local e os números de linha dos segredos verificados no código da sua organização para ajudar os desenvolvedores a corrigir.

Carregando arquivos SBOM para Now Platform® de seus repositórios GitHub

Determine se SBOM arquivos gerados em seus pipelines de IC/CD (integração contínua e entrega/implantação contínuas) foram enfileirados com sucesso em sua instância Now Platform®.

- Proteja seus ambientes de componentes potencialmente prejudiciais durante os ciclos de desenvolvimento de software com GitHub Ações que você inicia em seu ambiente GitHub.
- Obtenha todas as GitHub Ações necessárias para SBOM upload no GitHub Marketplace.

As aplicações SBOM são necessárias para carregar arquivos SBOM. Para obter mais informações, consulte Exploração do Lista de materiais de software.

Exibição de dados importados

Os dados de aplicações importados da Integração de repositórios GitHub são exibidos na tabela Aplicações descobertas [sn_vul_app_release]. Execute esta integração primeiro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A integração de repositórios importa marcadores e tópicos que você configurou para um repositório em sua conta GitHub no menu Configurações. Todas as propriedades personalizadas estão localizadas no menu em seu Repositório. Os valores definidos para as propriedades são importados como pares de chave-valor. Para obter mais informações sobre onde exibir essas informações em sua instância, consulte Exibir o Integrações de vulnerabilidade de aplicação do GitHub status de execução de importação e os dados do repositório importados.

Os dados importados (descobertas) da integração GitHub do Dependabot são exibidos nas tabelas a seguir.

- Aplicações descobertas [sn_vul_app_release].
- Resumos de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary].
- Itens vulneráveis de aplicação [sn_vul_app_vulnerable_item].
- Pacotes [sn_vul_app_package].

Os dados importados da integração do GitHub CodeScan são exibidos nas tabelas a seguir.

- Aplicações descobertas [sn_vul_app_release].
- Resumos de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary].
- Entradas de vulnerabilidade da aplicação [sn_vul_app_vul_entry].
- Itens vulneráveis de aplicação [sn_vul_app_vulnerable_item].

Preparando para o Integrações de vulnerabilidade de aplicação do GitHub

Prepare-se para a integração executando estas tarefas. O Integrações de vulnerabilidade de aplicação do GitHub pressupõe que você esteja familiarizado com o produto GitHub e a API.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Funções necessárias:

- administrador para baixar, instalar e ativar aplicações e atribuir funções.
- Administrador do GitHub para obter credenciais e gerar tokens no console do GitHub.
- admin para configurar conexões e registros de alias em sua instância.

Tarefas de configuração

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração

Tarefas de configuração	Descrição
Verifique se o Integrações de vulnerabilidade de aplicação do GitHub está instalado e ativado.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar o ServiceNow Integrações de vulnerabilidade de aplicação do GitHub.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de usuários App-Sec Manager. • O gerente do App-Sec supervisiona a configuração e verifica os resultados esperados. • sn_vul_github_config_integration é herdado pelo grupo de usuários do App-Sec Manager. Esta função contém as funções connection_admin e oauth_admin.
Obtenha suas informações de credencial e conta do GitHub.	As informações da conta são necessárias nos registros que você cria para autenticação. Consulte Criação de credenciais OAuth 2.0 para aplicações GitHub - JWT para Integrações de vulnerabilidade de aplicação do GitHub para obter mais informações sobre os detalhes necessários e como configurar os registros necessários para a autenticação OAuth.
Verifique se você está importando dados de Enumeração de pontos fracos comuns (CWE).	A integração de enumeração de pontos fracos comuns (CWE) também é usada por Resposta a vulnerabilidades de aplicações e deve estar em execução antes de instalar e configurar a integração de vulnerabilidade do GitHub. Ele é instalado com Resposta a vulnerabilidades, por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração

Tarefas de configuração	Descrição
	Nota: Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar a integração de vulnerabilidade do GitHub. No entanto, eles fornecem enriquecimento e seria útil ter. Para obter informações sobre o NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Criação de credenciais OAuth 2.0 para aplicações GitHub - JWT para Integrações de vulnerabilidade de aplicação do GitHub

Execute as etapas a seguir para integrar seus aplicativos GitHub usando o token de portador JWT para o Integrações de vulnerabilidade de aplicação do GitHub.

Funções necessárias:

- sn_vul.app_sec_manager e admin para registros em seu Now Platform.
- Nenhuma função de instância necessária para tarefas na sua conta GitHub.

.

Criar e configurar o app GitHub para Integrações de vulnerabilidade de aplicação do GitHub

Crie um aplicativo GitHub personalizado de sua conta GitHub para ativar a autenticação OAuth 2.0 com seu Integrações de vulnerabilidade de aplicação do GitHub em sua instância.

Antes de Iniciar
Função necessária: nenhuma função de instância necessária

Por Que e Quando Desempenhar Esta Tarefa
Conclua essas etapas na sua conta GitHub. Confira Edifício GitHub Apps no site do desenvolvedor GitHub para obter instruções sobre como criar e configurar aplicações personalizadas.

Procedimento

1. Na sua conta GitHub, crie seu app GitHub navegando até **Configurações do desenvolvedor** > **Aplicações do GitHub**.
2. No campo **URL da página inicial**, insira `https://`<instance-name> .service-now.com .
3. No campo **URL de retorno de chamada de autorização do usuário**, insira `https://`<instance-name> .service-now.com/oauth_redirect.do .
4. Na seção **Identificação e autorização de usuários**, desmarque o campo **Tokens de autorização do usuário expirados**.
5. Na seção **Webhook**, selecione o campo **Ativo**.
6. No campo **URL do Webhook**, insira `https://instance-name>.service-now.com/`.
7. Deixe os campos restantes em branco (padrão).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Na seção **Permissões do repositório**, defina as seguintes configurações.

Verificação de código	Somente leitura
Conteúdos	Somente leitura
Propriedades personalizadas	Somente leitura
Alertas do Dependedabot	Somente leitura
Metadados	Somente leitura

Nota: Se você já estiver usando um app GitHub e atualizar qualquer uma das permissões, deverá revisar e aceitar essas permissões para seu app GitHub. Você pode navegar até seu app e selecionar **Configurar > Revisar solicitação > Aceitar novas permissões**.

9. Deixe as permissões restantes como `Sem acesso` (padrão).
10. Na seção **Assinar eventos**, selecione a opção **Regra de proteção de implantação**.
11. Clique com o botão direito do mouse no cabeçalho para salvar as mudanças.
12. Instale o aplicativo GitHub recém-criado nas contas de sua escolha.

    a. Na página de configurações de apps do GitHub, selecione seu app.

    b. Na barra lateral esquerda, selecione **Instalar app**.

    c. Selecione **Instalar** ao lado da organização ou da conta pessoal que contém o repositório correto.

    d. Instale o aplicativo em todos os repositórios ou selecione repositórios.
    Para obter mais informações, consulte Instalação de apps do GitHub .

13. Após a instalação, selecione as configurações (ícone de engrenagem) do seu aplicativo e anote ou anote as informações a seguir.

    Esses detalhes são necessários ao criar o registro da aplicação em sua instância Now Platform.

    - ID de aplicação
    - ID de cliente
    - Segredo do cliente.
    - Observe o token no URL. Este é o ID do token que você insere no URL do token em sua instância.

14. Role a página para baixo, gere uma nova chave privada e salve-a em sua máquina.

Gerar o certificado JKS para o Integrações de vulnerabilidade de aplicação do GitHub

Gere um certificado JKS para a autenticação JWT para o Integrações de vulnerabilidade de aplicação do GitHub.

Antes de Iniciar

Você precisa anotar a senha usada para gerar o arquivo .jks (senha do KeyStore).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Crie um certificado assinado por CA usando a chave privada do app GitHub :

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem
 -days 1095
```

2. Insira os detalhes necessários.
3. Crie o arquivo PKCS 12 usando a chave privada do app GitHub e o certificado assinado por CA:

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey
 <file-name>.pem -certfile <certificate-name>.pem -out
 <PKCS-12-file-name>.p12
```

4. Forneça a senha de exportação.
5. Crie o arquivo JKS:

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12
 -srcstoretype pkcs12 -destkeystore <JKS-certificate-filename>.jks
 -deststoretype JKS
```

6. Forneça as senhas do armazenamento de chaves de destino e de origem.

Anexe o certificado GitHub Java Key Store à sua instância para Integrações de vulnerabilidade de aplicação do GitHub

Ative a autenticação de token de Concessão de Portador JWT anexando o certificado GitHub Java KeyStore (JKS) válido à sua instância.

Antes de Iniciar

Um certificado Java KeyStore válido.

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Certificados**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Campos do formulário da certificação X.509

Campo	Descrição
Nome	Nome para identificar exclusivamente o registro. Por exemplo, `My GitHub App Certificate for AVR`.
Notificar no vencimento	Opção para especificar os usuários a serem notificados quando o certificado expirar.
Aviso emitido antes do vencimento (em dias)	Número de dias para enviar uma notificação antes que o certificado expire.
Ativo	Opção para habilitar o certificado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo	Opção para selecionar o tipo de certificado. Selecione **Armazenamento de chaves Java**.
Dias até o vencimento	Número de dias até o certificado expirar.
Senha do armazenamento de chaves	Senha associada ao certificado (dica: a senha do KeyStore de destino criada anteriormente).
Descrição resumida	Resumo sobre o certificado.

4. Selecione o ícone de anexos e anexe um certificado JKS.
5. Selecione **Validar armazenamentos/certificados**.
   Uma mensagem de key_store válido é exibida para arquivos de certificado válidos.

Crie uma chave de assinatura JWT para o GitHub certificado JKS para o Integrações de vulnerabilidade de aplicação do GitHub

Crie uma chave de assinatura JSON Web Token (JWT) para atribuir ao seu certificado GitHub Java KeyStore.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **OAuth de Sistema** > **Chaves de JWT**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Campos do formulário de chaves de JWT

Campo	Descrição
Nome	Nome para identificar exclusivamente a chave de assinatura JWT. Por exemplo, `My GitHub App JWT Key for AVR`.
Armazenamento de chaves de assinatura	Selecione o certificado JKS válido que você anexou na tarefa anterior.
ID de chave	Deixe esse campo em branco.
Algoritmo de assinatura	Deixe este valor como RSA 256.
Senha da chave de assinatura	Senha associada à chave de assinatura. Esta é a senha usada para gerar o arquivo JKS.
Ativo	Opção para habilitar a chave.

4. Clique com o botão direito do mouse em qualquer lugar no cabeçalho cinza da página e selecione **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um provedor JWT para sua chave de assinatura GitHub para Integrações de vulnerabilidade de aplicação do GitHub

Adicione um provedor JWT (JSON Web Token) à sua instância [ServiceNow para GitHub.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **OAuth de Sistema** > **Provedores JWT**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Campos de formulário do Provedor JWT

Campo	Descrição
Nome	Nome para identificar o provedor JWT de forma única. Por exemplo, `My GitHub App JWT Provider for AVR`.
Intervalo de Vencimento (s)	Número em segundos para definir a vida útil dos tokens do provedor JWT. Você pode deixar esta configuração no padrão.
Configuração de Assinatura.	Selecione a chave JWT que você criou nas etapas anteriores.

4. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.
5. Inserir seu GitHub App **ID** do app para o valor da declaração **iss**, na lista relacionada Declarações padrão.
   Este é o ID do app GitHubGitHub no console [] que você criou nas etapas anteriores.
6. Deixe os valores de **auditoria** e **sub** em branco (padrão).
7. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.

Registrar GitHub como um Provedor OAuth (JWT) para Integrações de vulnerabilidade de aplicação do GitHub

Use as informações geradas durante a configuração da conta do aplicativo GitHub para registrar GitHub como um provedor OAuth e permitir que a instância solicite tokens OAuth 2.0.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **OAuth de Sistema** > **Registro de aplicações**.
2. Selecione **Novo**.
   A **aplicação Que tipo de OAuth?** mensagem é exibida.
3. Selecione **Conectar-se a um provedor OAuth de terceiros**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

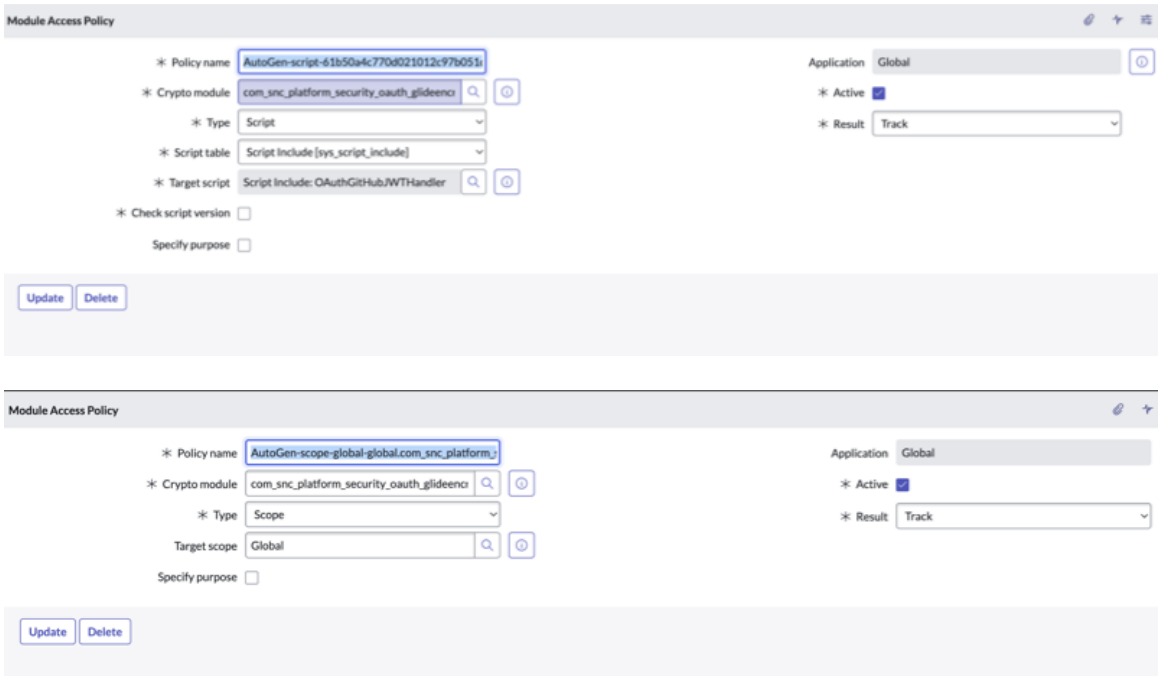
Campos de formulário de Registro de aplicações

Campo	Descrição
Nome	Nome para identificar exclusivamente o registro. Por exemplo, insira `Meu provedor de apps GitHub para AVR`.
ID de cliente	ID de cliente da sua aplicação GitHub. O ID de cliente é da aplicação GitHubGitHub no console [] que você criou nas etapas anteriores. Este ID está disponível na seção **Sobre** da configuração do aplicativo [GitHub em GitHub.
Acessível	Deixe esta configuração em seu valor atual.
Segredo do cliente	Segredo do cliente da sua aplicação GitHub. O segredo do cliente é da aplicação GitHubGitHub no console [] que você criou nas etapas anteriores. Este ID está disponível na seção **Sobre** da configuração do aplicativo [GitHub em GitHub.
Ativo	Opção para habilitar a chave. Deixe selecionado.
URL de Autorização	Este URL é gerado automaticamente.
URL de Token	O local do endpoint do token que a instância usa para recuperar e atualizar tokens. Insira o token do URL na sua aplicação GitHub. Este é o token exibido no URL depois que o app é instalado em GitHub. Na seção Instalar app na configuração do app GitHub em GitHub, selecione a engrenagem. O token é exibido no URL da página da web. ◦ Para nuvem: https://api.github.com/app/installations/49374672/access_tokens . ID de instalação: 9374672. ◦ Para no local: https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .
Script da API OAuth	Opção que permite fazer referência a uma inclusão de script OAuthUtil corrigida. Selecione **OAuthGitHubJWTHandler**.
Tipo de concessão padrão	Tipo de concessão associado ao registro de aplicações. Selecione **Portador JWT**.

5. Deixe o restante dos campos de formulário como padrão.
6. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.
7. Role até a lista relacionada **Perfis de entidade OAuth**, selecione-a e abra o perfil padrão que foi criado na lista.
8. Preencha o campo **Provedor JWT** com o provedor JWT criado anteriormente e salve o formulário.
9. Retorne ao arquivo de registro da aplicação e salve-o.
10. Navegar até **Gestão de chave** > **Políticas de Acesso ao Módulo** > **Todos**.
11. Selecione a política que tem `com_snc_platform_security_oauth_glideencrypter` como o valor do campo **Módulo de criptografia** e a Inclusão de script: `OAuthGitHubJWTHandler`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. Verifique se o campo **Resultado** está definido como `Rastrear` e salve suas mudanças.

Criar credenciais e conexões para o Integrações de vulnerabilidade de aplicação do GitHub

Crie um registro de credencial para o provedor de aplicações GitHub criado anteriormente para autorizar ações.

Antes de Iniciar

Funções necessárias:

- administrador
- sn_vul.app_sec_manager

Procedimento

1. Navegar até **Credenciais e conexões** > **Credenciais**.
2. Selecione **Novo**.
3. Selecione **Credenciais OAuth 2.0**.
4. Selecione **Novo** e preencha os campos.

Campo	Descrição
Nome	Nome exclusivo do registro.
Aplica-se a	Selecione as credenciais do OAuth 2.0 na lista.
Perfil de Entidade OAuth	Selecione o ícone de pesquisa e localize o perfil de entidade que você criou nas etapas anteriores.
Outros campos	Deixe esses campos em seus padrões.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique com o botão direito do mouse em qualquer lugar no cabeçalho da página e selecione **Salvar**.
   A lista Credenciais é exibida.
6. Abra o registro que você acabou de criar e selecione o link relacionado **Obter token OAuth**.
   É exibida uma mensagem informando que o token OAuth foi importado com sucesso.
7. Navegar até **Credenciais e conexões** > **Conexões**.
8. Selecione **Novo**.
9. Selecione **Conexão HTTP(s)**.
10. Selecione **Novo** e preencha os campos.

Campo	Descrição
Nome	Nome do registro.
Aplicação	Somente leitura.
Alias primário (opcional)	Selecione o ícone de pesquisa e escolha um na lista.
Tipo	Conexão e credencial.
Tipo de conexão	HTTP.
Suporte a várias conexões ativas (opcional)	Desativado.
Política de nova tentativa padrão	Política de Repetição de HTTP Padrão
Modelo de configuração	Deixe em branco.

11. Selecione **Enviar**.
    A lista Aliases de conexões e credenciais é exibida.
12. Abra seu registro e, na guia da lista relacionada a Conexões, selecione **Novo** e preencha os campos no registro de Conexão HTTP.

Campo	Descrição
Nome	Nome do registro.
Ativo	Ativado.
Credenciais	Selecione o registro de credencial que você criou nas etapas anteriores.
Alias de conexão	Seu registro é exibido.
Construtor de URL	Desativado.
URL de Conexão	Este é o URL base: https://api.github.com para Enterprise. O no local é o URL do endpoint do GitHub.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Usar MID Server (opcional)	O MID Server é necessário para o no local. É opcional para Enterprise.
Tempo limite de conexão	Insira um valor.

13. Selecione **Enviar**.
    A lista Aliases de conexões e credenciais é exibida. Agora você está pronto para concluir as etapas para Configure o Integrações de vulnerabilidade de aplicação do GitHub. No campo Conexão, insira as credenciais criadas nas etapas anteriores.

Instalar o ServiceNow® Integrações de vulnerabilidade de aplicação do GitHub

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que Integrações de vulnerabilidade de aplicação do GitHub se integre corretamente a Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar o Integrações de vulnerabilidade de aplicação do GitHub.
2. Navegue até o ServiceNow Store.
3. Na aplicação ServiceNow Store, pesquise a aplicação Integrações de vulnerabilidade de aplicação do GitHub.
4. Selecione o bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome** e **o motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e escolha **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

Configure o Integrações de vulnerabilidade de aplicação do GitHub

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto GitHub se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar
Funções necessárias:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Grupo de usuários do App-Sec Manager
- sn_vul.app_sec_manager necessário para a configuração do OAuth

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade do GitHub** > **Configuração**.
2. Escolha **Autenticação básica** ou **OAuth** para o tipo de autenticação.
   - A autenticação básica requer um MID Server para instâncias no local. Gere o token de API necessário para a autenticação básica da sua conta GitHub.
   - O OAuth requer o aplicativo OAuth, a credencial e a configuração de conexão descritas em Criação de credenciais OAuth 2.0 para aplicações GitHub - JWT para Integrações de vulnerabilidade de aplicação do GitHub.
3. Preencha os campos com base no tipo escolhido.
   Autenticação básica

Campo	Descrição
URL da API	A URL da API GitHub apropriada para Enterprise ou no local. O URL padrão é https://api.github.com . No local é o URL do endpoint GitHub.
Token de API	Token que você gerou a partir do console GitHub.
Tipo de API	Selecione um: Organização Escolha esta opção se quiser importar dados para uma organização específica por nome. O ambiente GitHub oferece suporte a várias organizações. Cada organização pode oferecer suporte a vários repositórios. Se você inserir uma organização, somente os dados dessa organização serão importados. Empresa O ambiente empresarial oferece suporte a várias organizações. Escolha esta opção se quiser importar dados de vulnerabilidade de todas as organizações em seu ambiente empresarial (nuvem).
Nome da organização	Nome do seu GitHub Repositório. Somente os dados da organização que você inserir são importados.
MID Server	Para instâncias no local para autenticação básica, um MID Server é necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecione opções para gerenciar a gestão de exceções e falso-positivos.	Selecione opções para gerenciar fluxos de trabalho de gestão de exceções e falso-positivos para itens vulneráveis (IVAs) de aplicações com ServiceNow automaticamente após a importação. Gerenciar exceções no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVIs importados marcados para o estado **Adiado**. AVIs com estados de **origem** que normalmente são mapeados para um estado **Adiado** em sua instância são mapeados para **Aberto**. Você **solicita uma exceção** do registro AVI. Gerenciar falsos positivos no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVIs importados com estados de **origem** marcados como **Falso-positivo** ou **Possível falso-positivo**. AVIs com esses estados de **origem** que normalmente são mapeados para um estado **Closed** em sua instância são mapeados para **Open**. Você solicita um **falso-positivo** do registro AVI. ◦ Desative uma ou ambas as caixas de seleção se quiser preservar os estados de **origem** importados do scanner. ◦ Se desativado, as ações **Solicitar exceção** e **Falso-positivo** não ficarão visíveis nos AVIs.
Instância de Integração	Instância para a qual você está importando dados.

OAuth

Campo	Descrição
URL da API	A URL da API GitHub apropriada para Enterprise ou no local. O URL padrão é

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	https://api.github.com . No local é o URL do endpoint GitHub.
Conexão	A conexão que você criou descrita em Criação de credenciais OAuth 2.0 para aplicações GitHub - JWT para Integrações de vulnerabilidade de aplicação do GitHub.
Tipo de API	Selecione um: Organização Escolha esta opção se quiser importar dados para uma organização específica por nome. O ambiente GitHub oferece suporte a várias organizações. Cada organização pode oferecer suporte a vários repositórios. Se você inserir uma organização, somente os dados dessa organização serão importados. Empresa O ambiente empresarial oferece suporte a várias organizações. Escolha esta opção se quiser importar dados de vulnerabilidade de todas as organizações em seu ambiente empresarial (nuvem). **Nota:** GitHub As aplicações não são compatíveis com APIs de nível empresarial.
Nome da organização	Nome da organização para seus repositórios GitHub. Somente os dados dos repositórios na organização que você inserir são importados.
Selecione opções para gerenciar a gestão de exceções e falso-positivos.	Selecione opções para gerenciar fluxos de trabalho de gestão de exceções e falso-positivos para itens vulneráveis (IVAs) de aplicações com ServiceNow automaticamente após a importação. Gerenciar exceções no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVIs importados marcados para o estado **Adiado**. AVIs com estados de **origem** que normalmente são mape-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	ados para um estado **Adiado** em sua instância são mapeados para **Aberto**. Você **solicita uma exceção** do registro AVI. Gerenciar falsos positivos no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVIs importados com estados de **origem** marcados como **Falso-positivo** ou **Possível falso-positivo**. AVIs com esses estados de **origem** que normalmente são mapeados para um estado **Closed** em sua instância são mapeados para **Open**. Você solicita um **falso-positivo** do registro AVI. ◦ Desative uma ou ambas as caixas de seleção se quiser preservar os estados de **origem** importados do scanner. ◦ Se desativado, as ações **Solicitar exceção** e **Falso-positivo** não ficarão visíveis nos AVIs.

4. Selecione **Salvar e testar credenciais**.
5. Execute a integração de repositórios GitHub antes de executar as outras integrações. As outras GitHub integrações dependem dos dados da aplicação atuais importados da integração de repositórios. Os dados da integração de repositórios são armazenados na tabela Aplicações descobertas [sn_vul_app_release]. Para obter mais informações, consulte Exibir o Integrações de vulnerabilidade de aplicação do GitHub status de execução de importação e os dados do repositório importados.

Exibir o Integrações de vulnerabilidade de aplicação do GitHub status de execução de importação e os dados do repositório importados

Use a lista relacionada de **execuções de integração de vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar
Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade do GitHub** > **Integrações**.
2. Selecione uma integração.
3. Selecione a lista relacionada **Execuções de integração de vulnerabilidade**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

4. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns de falha na execução incluem:

   - Interrupção de rede.
   - Um problema na transferência de dados que resultou em dados corrompidos durante a transformação.

   Se você encontrar alguma dessas condições, selecione **Executar agora**e execute novamente a integração.

5. Para exibir repositórios importados, navegue de volta para a lista de integrações e selecione o GitHub registro de integração de repositórios.
6. Selecione a lista relacionada **Execuções de integração de vulnerabilidade** e abra um registro.
   O número de repositórios importados com uma execução de integração é exibido na coluna Itens importados.

   Todos os marcadores e tópicos que você configurou para um repositório em sua conta GitHub do menu Configurações são importados. Todas as propriedades personalizadas importadas estão localizadas no menu em seu Repositório.

   Marcadores, tópicos e propriedades personalizadas serão importados para sua instância somente se estiverem configurados em sua conta GitHub.

   Se importadas, essas informações GitHub] serão exibidas em sua instância na coluna Informações adicionais de origem na tabela Aplicações descobertas [sn_vul_app_release] e nas informações adicionais de origem. seção em um registro de aplicação descoberto. As propriedades personalizadas são exibidas como pares de chave-valor e os marcadores e tópicos são exibidos em matrizes.

Exibir Integrações de vulnerabilidade de aplicação do GitHub conjuntos para importação

Exiba detalhes das informações de importação para Integrações de vulnerabilidade de aplicação do GitHub.

Antes de Iniciar

Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegue até o **Integração de vulnerabilidade do GitHub** > **Tabelas de conjunto para importação**.
2. Selecione um registro para uma integração.
3. Selecione um link relacionado para exibir as seguintes informações:
   - Conjuntos para importação
   - Mapas de transformação
   - Histórico de Transformações

Integração de vulnerabilidade do Invicti

O Integração de vulnerabilidade do Invicti usa dados de aplicações importados do produto Invincti para ajudá-lo a determinar o impacto e a prioridade das falhas em seu código.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de vulnerabilidade do Invicti

O Integração de vulnerabilidade do Invicti coleta dados do scanner e os disponibiliza para o Now Platform®. Ele se integra facilmente ao recurso [ServiceNow® Resposta a vulnerabilidades de aplicações de Resposta a vulnerabilidades para mapear informações de vulnerabilidade de aplicações de terceiros importadas para sua instância.

A integração importa os seguintes tipos de dados verificados.

- Testes dinâmicos de segurança da aplicação (DAST)
- Testes de segurança de aplicações interativos (IAST)

Para obter mais informações sobre DAST e IAST, consulte Explorando Resposta a vulnerabilidades de aplicações.

Versões disponíveis

Versão de lançamento	Notas de versão
Integração de vulnerabilidade do Invicti v1.1 Integração de vulnerabilidade do Invicti 1,0	Notas de versão Resposta a vulnerabilidades de aplicações Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações

As seguintes integrações estão incluídas no sistema de base. As integrações são encadeadas para que, após a conclusão bem-sucedida de uma integração, a próxima integração seja iniciada. As integrações são executadas na ordem listada na tabela a seguir.

Após a execução inicial, todos os dias, os trabalhos agendados são encadeados para executar essas integrações automaticamente em ordem. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Integrações de vulnerabilidade da aplicação Invincti

Integração	Descrição
Aplicação de lista de aplicações Invincti	Importa aplicações verificadas pelo Invincti para a tabela Aplicações descobertas [sn_vul_app_release] ou a tabela Aplicação verificada [sn_vul_app_scanned_application] com base em como a propriedade do sistema *sn_vul.use_product_model* está definida para os registros de regra de pesquisa de IC. • Se a propriedade do modelo de produto estiver definida como verdadeira, uma aplicação será inserida na tabela Versão da aplicação descoberta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de vulnerabilidade da aplicação Invincti

Integração	Descrição
	• Se a propriedade do modelo do produto estiver definida como falsa, uma aplicação será inserida na tabela Aplicação verificada. Você pode optar por ativar regras de pesquisa com itens de configuração (ICs) como os destinos de pesquisa, modificando a propriedade do sistema. Se você modificá-lo, também deverá ativar as regras de Pesquisa de IC para corresponder ao destino de pesquisa. Para obter mais informações, consulte: • Configure o Integração de vulnerabilidade do Invicti • Criar uma regra de pesquisa de IC • Como reaplicar regras de pesquisa de IC no Resposta a vulnerabilidades de aplicações
Integração da lista de verificação do Invincti	Esta integração é iniciada depois que a integração da lista de aplicações é concluída com sucesso. Esta integração importa dados sobre a data e a hora em que uma verificação foi executada.
Integração de item vulnerável da aplicação Invincti	Esta integração é iniciada depois que a integração da lista de verificação é concluída com sucesso. A partir da v1.1, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para a integração de item vulnerável de aplicação. Cada vulnerabilidade no Invincti tem um tipo, por exemplo,**DirectoryListing**. Este tipo é mapeado como um ID exclusivo em sua instância e exibido como parte do valor no campo Vulnerabilidade no registro de item vulnerável da aplicação (IVA): **Invincti-DirectoryListing**. Para obter mais informações sobre mapeamento, consulte Integração de vulnerabilidade do Invicti mapeamento de estado.

O limite superior de itens por página para todas as três integrações é 200.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparar para o Integração de vulnerabilidade do Invicti

Uma integração bem-sucedida requer planejamento e execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Integração de vulnerabilidade do Invicti pressupõe que você esteja familiarizado com o produto Invincti e a API.

A integração de enumeração de pontos fracos comuns (CWE) também é usada por Resposta a vulnerabilidades de aplicações e deve estar em execução antes de instalar e configurar a integração de vulnerabilidade do Invincti.

Nota: Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar a integração, no entanto, eles fornecem aprimoramento de vulnerabilidade e são úteis.

Para obter informações sobre o NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis de aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente. A função de administrador é necessária para instalar e configurar aplicações em sua instância da Now Platform.

Obtenha suas credenciais de API e token de API no console do Invincti. Revise as informações disponíveis no site do produto Invincti em Visão geral da API .

Instalar a ServiceNow® Integração de resposta a vulnerabilidades com Invincti

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que a aplicação Integração de vulnerabilidade do Invicti se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar o Integração de vulnerabilidade do Invicti.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a aplicação Integração de vulnerabilidade do Invicti.
4. Selecione o bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Insira o **Nome** e **o motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
10. Localize a aplicação, selecione-a e clique em **Instalar** para ativá-la.
    Sua aplicação é instalada automaticamente em sua instância.

Configure o Integração de vulnerabilidade do Invicti

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que Integração de vulnerabilidade do Invicti funcione corretamente com o recurso [Resposta a vulnerabilidades de aplicações de Resposta a vulnerabilidades.

Antes de Iniciar

Funções necessárias:

- administrador para instalar e ativar aplicações
- Grupo de usuários do App-Sec Manager para configurar a integração

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se o Integração de vulnerabilidade do Invicti está instalado e ativado.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar a ServiceNow Integração de resposta a vulnerabilidades com Invincti.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de gerentes de App-Sec. • O gerente do App-Sec supervisiona a configuração e verifica os resultados esperados.
Para a Integração de vulnerabilidade do Inviciti, tenha em mãos o **ID do usuário** e o **token de API**.	Entre em contato com o administrador do Invincti para obter o **ID do usuário** e o **token da API** se você não os souber. Para obter mais informações, consulte o site do produto Invincti em Visão geral da API .

Procedimento

1. Navegar até **Todos** > **Invicti** > **Configuração do Invicti**.
2. Preencha os campos.

Campo	Descrição
URL da API	URL da instância do Invincti do usuário. Estas são as informações que você obteve de Preparar para o Integração de vulnerabilidade do Invicti.
ID do Usuário	ID de usuário exclusivo.
Token de API	Token de API gerado a partir do console Invincti. Estas são as informações que você obteve de Preparar para o Integração de vulnerabilidade do Invicti.
Escolha o tipo de verificação. Você deve selecionar pelo menos um.	
Importar DAST	Opção para incluir vulnerabilidades de verificações do DAST. As verificações do DAST encontram vulnerabilidades para uma aplicação dinamicamente enquanto ela está em execução. Essa abordagem pode imitar um ataque externo.
Importar IAST	Opção para incluir vulnerabilidades de verificações IAST. As verificações IAST detectam vulnerabilidades de software interagindo com o programa enquanto ele está em execução. Observação humana, testes automatizados e sensores são usados em combinação para interagir com a aplicação para localizar vulnerabilidades.
Formato de data	Parâmetro que converte a hora de início para o formato compatível com a API Invincti usada pela Integração de item vulnerável da aplicação Invincti.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este parâmetro deve corresponder ao formato que você definiu ou selecionou na sua conta do Invincti, por exemplo, **dd/MM/yyyy**. Verifique se os formatos de data e hora no console Invincti correspondem aos que você insere para o formato de data em sua instância Now Platform. Para alterar este formato no console do Invincti: **a.** Faça login em Invicti Entrar . **b.** Selecione **Nome de usuário** no canto superior direito. **c.** Navegar até **Configurações do usuário** > **Formato de data e hora**. **Nota:** Falha nas importações pode ocorrer se você inserir um formato de data inválido na sua instância Now Platform. Se você inserir um formato válido em sua instância que seja diferente do formato de data no console do Invincti, o Invincti retornará uma carga vazia.
Gerenciar exceções no ServiceNow	Selecione um: Ativado (selecionado) Itens vulneráveis de aplicação (AVIT) do Invicti com estados como **Presente** e **AceitoRisco** que podem ser adiados em sua instância são mapeados para **Aberto** automaticamente. Desativado (não selecionado) Os estados de origem dos itens vulneráveis da aplicação (AVITs) importados do Invincti são preservados. Você deve gerenciar exceções para esses AVITs (adiá-las) dos registros de AVIT. Para obter mais informações sobre estados de origem e campos de destino do Invincti, consulte Integração de vulnerabilidade do Invicti mapeamento de estado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Gerenciar falsos positivos no ServiceNow	Selecione um: Ativado (selecionado) AVITs com estados do Invincti, como **Presente** e **Falso-positivo**, que podem fazer a transição para **Encerrado** em sua instância, são mapeados para **Aberto** automaticamente. Desativado (não selecionado) Os estados de AVIT importados do Invincti são preservados. Você deve gerenciar falsos positivos ou possíveis falsos positivos para esses AVITs de registros de AVIT.

3. Selecione **Salvar e testar credenciais**.
4. Opcional: Modifique suas regras de pesquisa para que sejam baseadas em itens de configuração.

   (Optional) Por padrão, a propriedade do sistema **sn_vul.use_product_model** é ativada (definida como `verdadeira`) para as regras de pesquisa listadas na tabela [sn_sec_cmn_ci_lookup_rule] com base no modelo do produto. Quando esta regra é ativada:

   - Esta regra identifica correspondências entre os dados importados e os dados em seu Configuration Management Database (CMDB) com base no modelo do produto.
   - Os registros são criados ou atualizados na tabela Aplicações descobertas [sn_vul_app_release].
   - Quando você cria ou edita suas regras de pesquisa para o Invincti, o **modelo do produto** é exibido no campo de **destino de pesquisa** no formulário de regra.

   Para modificar suas regras para que sejam baseadas em itens de configuração, você deve desativar manualmente (definir como `falso`) a propriedade do sistema **sn_vul.use_product_model**.

   a. Navegar até **Todos** > **Propriedades do sistema** e localize o registro **sn_vul.use_product_model** e defina o Valor como `falso`.

   b. Selecione **Atualizar**.

   c. Navegar até **Todos** > **Operações de segurança** > **CMDB** > **Regras de pesquisa**.

   d. Localize as regras Nome da aplicação e ID da aplicação de origem que têm o destino de pesquisa como **item de configuração**.

   e. Marque a caixa de seleção Ativo para essas regras.

   f. Selecione **Atualizar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao criar ou editar suas regras de pesquisa para o Invincti, observe que o **item de configuração** é exibido no campo **Pesquisar destino** no formulário de regra. Os registros são criados ou atualizados na tabela Aplicações verificadas [sn_vul_app_scanned_application].

Exibição do Integração de vulnerabilidade do Invicti status e registros de execução de importação

Use a lista relacionada de **execuções de integração de vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Exibição de status de importação, conjuntos para importação e registros

Para exibir o status de suas importações, como um usuário no grupo de usuários do App-Sec Manager, navegue até **Todos** > **Integração da vulnerabilidade do Invicti** > **Integrações** e selecione um registro de integração. Selecione a lista relacionada **Execuções de integração de vulnerabilidade**.

A partir da v1.1, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para a integração de item vulnerável de aplicação.

Para exibir os conjuntos para importação, navegue até **Todos** > **Integração da vulnerabilidade do Invicti** > **Integrações** > **Tabelas de conjunto para importação** e selecione uma integração.

A integração da lista de aplicações cria ou atualiza registros com base no destino da pesquisa:

- Modelo do produto: tabela Aplicações descobertas [sn_vul_app_release]
- Item de configuração: tabela Aplicações verificadas [sn_vul_app_scanned_application]

A integração da lista de verificação cria ou atualiza registros na tabela Aplicações verificadas [sn_vul_app_scan_summary].

A integração de item vulnerável de aplicação cria ou atualiza registros na tabela Itens vulneráveis de aplicação [sn_vul_app_vulnerable_item] e CWEs [sn_vul_cwe].

Nota: Cada vulnerabilidade no Invincti tem um "tipo", por exemplo, ProductDirectoryListing. Este tipo é importado mapeado como um ID exclusivo para sua instância e exibido como parte do valor no campo Vulnerabilidade no registro de item vulnerável da aplicação (AVIT). Neste exemplo, o valor é `Invincti-ProductDirectoryListing`e esse valor também é exibido como o ID exclusivo no registro de entrada de vulnerabilidade da aplicação. Os AVITs do Invincti são compatíveis com várias entradas de CWE (Common Weakness Enumeration), portanto, os CWEs não são usados como IDs exclusivos. Os CWEs também são exibidos no registro AVIT.

Para AVITs do Invincti, se houver tipos duplicados no Invincti para uma vulnerabilidade, a palavra "personalizado" será inserida no valor, por exemplo, `Invincti-custom-ProductDirectoryListing`. Se você criar um tipo personalizado para vulnerabilidades, o ID da vulnerabilidade poderá ser `Invincti-Custom-<title of vulnerability>`.

Novos campos: para o `tipo de verificação=Invincti`, os parâmetros afetados e os campos personalizados podem incluir dados que podem ajudar você a entender a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidade e a corrigi-la. Se não houver dados, esses campos não serão exibidos no AVIT.

Integração de vulnerabilidade do Invicti mapeamento de estado

Os seguintes estados de origem de Integração de vulnerabilidade do Invicti e seus estados de destino em sua instância são listados na tabela a seguir.

Estados de origem do Invincti e seus estados correspondentes da Now Platform

Estados de origem do Invincti	Descrição dos estados de origem	Estado de destino na Now Platform
Present	O problema foi identificado.	Aberto
Presente, Risco Aceito, Recuperado	O problema foi considerado e está marcado como uma vulnerabilidade de baixo risco.	Adiado
Presente, falso-positivo	O problema foi considerado e está marcado como uma vulnerabilidade não original.	Encerrado
FixoNão confirmado, Corrigido não confirmado	O problema foi corrigido, mas não confirmado pelo Invincti Enterprise.	Resolvido
Fixo (Confirmado), FixoConfirmado, FixoConfirmado, Risco Aceito, FixoConfirmado, Falso-positivo	O problema foi corrigido e confirmado pela Invincti Enterprise e nenhuma ação adicional é necessária.	Encerrado
Corrigido (não é possível testar novamente)	O problema foi identificado, mas o Invicti não pode testar novamente para confirmar se o problema foi corrigido ou não.	Resolvido
Revivido	O problema foi corrigido em verificações anteriores, mas foi encontrado novamente.	Aberto
Adiado, ignorado	O problema foi ignorado pelo usuário. No Invincti Enterprise, para ignorar um problema, um usuário atualiza seu status para "risco aceito".	Risco aceito

Mapeamento da versão da aplicação

Campo de origem	Campo de destino na Now Platform
ID	source_app_id
Criado em	app_creation_date
Atualizado em	app_updation_date

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	app_name
URL da raiz	Source_additional_info
Descrição	descrição
Marcadores	Marcadores

Mapeamento de vulnerabilidade

Campo de origem	Campo de destino na Now Platform
Tipo	Nome da categoria
Detalhe da vulnerabilidade	Resumo
Impacto	Ameaça
Referências de origem	Referências da web
Recomendação de origem	Solução
Tipo	source_entry_id/ID
Gravidade	gravidade_origem
Classificação[“Cwe”]	Lista do CWE
CvssVectorString	Campos do CVVS v3

Mapeamento de resumo de verificação

Campo de origem	Campo de destino
Origem	Origem
TotalVulnerabilityCount	Contagem_de_falha_detectada
Data de início	Data da verificação dinâmica
ID	source_scan_id

Mapeamento de item vulnerável da aplicação (AVIT)

Campo de origem	Campo de destino na Now Platform
Tipo	Tipo de verificação
ID do Site	ID de aplicação de origem
ID	ID de AVIT de origem
Data da última exibição	Último encontrado
Data da primeira visita	Primeiro encontrado
Data da última atualização	Data da última verificação
parâmetros	Parâmetro afetado
URL	URL afetado
Gravidade	Gravidade de origem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

URL	Link de origem
Detalhe da vulnerabilidade	Resumo da vulnerabilidade de origem
Referências externas	Referências de origem
Referências de correção + correção	Recomendação de origem
Estado	Status da correção da origem
Impacto	Explicação da vulnerabilidade de origem

Veracode Vulnerability Integration

A aplicação Resposta a vulnerabilidades Integration with Veracode usa dados importados do produto Veracode para ajudar você a determinar o impacto e a prioridade das falhas no seu código.

Veracode Vulnerability Integration

O produto Veracode coleta dados do teste de segurança da aplicação dinâmico (DAST), teste de segurança da aplicação estático (SAST) e dados do scanner manual e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente ao recurso [Resposta a vulnerabilidades de aplicações de Resposta a vulnerabilidades para mapear vulnerabilidades de terceiros que enriquecem os dados em sua instância.

A partir da v19.0 de Resposta a vulnerabilidades, você pode importar vulnerabilidades da Análise de composição de software (SCA) e dados de vulnerabilidade Lista de materiais de software (SBOM) para ajudá-lo a identificar pontos fracos em seus aplicativos de software. Para obter mais informações, consulte Exploração do Lista de materiais de software.

Uma API compartilhada ingere dados de DAST, SAST, SCA e resultados de testes de invasão manual.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Todos os dias, os trabalhos agendados invocam as integrações automaticamente na ordem em que são listadas. Você também pode executar trabalhos agendados individuais manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Obter mais detalhes de Veracode

A partir da v4.2, selecione **Obter mais detalhes** sobre itens vulneráveis de aplicação (AVITs) que têm Veracode como a origem na tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item] ou nas exibições de lista nos Espaços de resposta a vulnerabilidades para exibir os seguintes dados Veracode.

- Os detalhes da solicitação de origem HTTP e da resposta de origem para verificações do Teste de segurança da aplicação dinâmico (Dynamic Application Security Testing, DAST) são exibidos na lista relacionada Solicitação/resposta HTTP.
- As recomendações de solução de Veracode são exibidas na lista relacionada Descobertas.
- A solicitação de origem HTTP, a resposta de origem e as recomendações são exibidas na guia Detalhes nos espaços de resposta a vulnerabilidades Resposta a vulnerabilidades.
- A coluna Descrição é compatível com a tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis

Versão de lançamento	Notas de versão
Veracode v4.3 Veracode v4.2 Veracode v4.1	Notas de versão Resposta a vulnerabilidades de aplicações Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Grupo de usuários e funções

O Veracode Vulnerability Integration é instalado por um administrador do sistema [admin] e configurado por um membro do grupo de gerentes do App-Sec. Para obter mais informações, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

Veracode Vulnerability Integration

Para exibir as Veracode integrações de vulnerabilidade, navegue até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.

As seguintes integrações estão incluídas no sistema de base.

Veracode Vulnerability Integration

Integração	Descrição
A partir da versão 4.1: Veracode Vincular projetos de integração	Esta integração é ativada por padrão. Recupera todos os projetos associados a cada aplicação de Veracode. As aplicações podem ter vários projetos na aplicação Veracode. Os dados importados desta integração são exibidos nos seguintes registros: • A data da**última verificação de SCA, a data**de **criação da aplicação**e a **data de atualização** da aplicação são listadas nos registros em **Aplicações descobertas**. • Nos registros de resumo de verificação de vulnerabilidades da aplicação e nos itens vulneráveis da aplicação (AVITs), o **status do SDLC de origem** (ciclo de vida de desenvolvimento de software) é exibido. • **A exploração de origem** é exibida em registros de item vulnerável da aplicação (IVA).
Veracode Integração da lista de aplicações (JSON)	Esta integração está inativa por padrão. Recupera Veracode dados do scanner de aplicações (vulnerabilidades, metadados) e aprimora os dados da aplicação. Recupera registros de verificação de Veracode por meio de uma API baseada em JSON.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration

Integração	Descrição
Veracode Integração da lista de aplicações (XML)	Esta integração está inativa por padrão. A versão baseada em XML desta integração foi desativada (descontinuada). Recupera Veracode dados do scanner de aplicações (vulnerabilidades, metadados) e aprimora os dados da aplicação. Esta integração está definida para ser executada diariamente às 00:00:00. **Nota:** Uma API baseada em JSON de Veracode é usada para recuperar a lista de aplicações. Esta API importa a "data da última verificação de conformidade com a política" dessas aplicações, o que significa quando essas aplicações foram verificadas pela última vez por Veracode.
Veracode Lista de materiais de software (SBOM) Integração	A versão 4.3 do Veracode Vulnerability Integration inclui os seguintes aprimoramentos com arquivos Veracode SBOM : • Se você instalou o SBOM Response, terá a opção de incluir vulnerabilidades encontradas por Veracode nos arquivos SBOM carregados. • Veracode é mapeado para o campo **Origem** para registros na tabela Lista de materiais [sn_sbom_doc] para os arquivos Veracode SBOM. Esta integração é ativada por padrão. A partir da versão 4.2, o importa arquivos Lista de materiais de software nos formatos CycloneDX e SPDX gerados por Veracode e os enfileira para análise em sua instância. Você deve ter as aplicações Lista de materiais de software instaladas para importar esses dados e exibi-los.
Veracode Integração de resumo de verificação (JSON)	Esta integração está inativa por padrão. Recupera registros de verificação de Veracode por meio de uma API baseada em JSON. Esta integração substitui a integração de API baseada em XML. Ele é encadeado e segue a Veracode integração de lista de aplicações quando ativado.
Veracode Resumo da verificação (XML)	Esta integração está inativa por padrão. A versão baseada em XML desta integração foi desativada (descontinuada). Recupera registros de verificação de Veracode. Esta integração é encadeada e segue a Veracode integração de lista de aplicações quando ativada. **Nota:** Segue automaticamente a integração Veracode da lista de aplicações quando ela é ativada. Com a "Data da última verificação de conformidade com a política" das aplicações de Veracode, esta integração recupera dados somente das aplicações que foram verificadas após o "delta_start_time" desta integração.
Veracode Integração de JSON de item vulnerável da aplicação	A partir da v4.2, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as integrações de item vulnerável de aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration

Integração	Descrição
	Esta integração está inativa por padrão. Recupera resultados de verificação com mais dados de vulnerabilidade do que a integração baseada em XML de Veracode. Ele insere AVIs e aprimora seus dados de vulnerabilidade de terceiros.
Veracode Integração de item vulnerável da aplicação (XML)	A partir da v4.2, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as integrações de item vulnerável de aplicação. Esta integração está inativa por padrão. Recupera resultados de verificação de Veracode, insere Itens vulneráveis de aplicação (AVITs) e aprimora seus dados de vulnerabilidade de terceiros. Por padrão, se o registro do scanner estiver no estado **Fechado**, os AVITs não serão criados. Os AVITs existentes ainda estão atualizados. Esta integração é encadeada e segue a Veracode Integração de resumo de verificação quando ativada. A API baseada em XML está obsoleta para a Veracode integração JSON de resumo de verificação. **Nota:** Segue automaticamente a Veracode Integração de resumo de verificação. Com a "Data da última verificação de conformidade com a política" das aplicações de Veracode, esta integração recupera dados somente das aplicações que foram verificadas após o "delta_start_time" desta integração.
Veracode Integração de categorias	Esta integração está inativa por padrão. Recupera dados de Categorias aprimoradas de Veracode.
Veracode Integração do CWE	Esta integração é ativada por padrão. Recupera Veracode - dados específicos de Enumeração de pontos fracos comuns (CWE) para informações sobre ameaças e recomendações de correção. Esses dados são preenchidos e atualizados nos registros de entrada de vulnerabilidade da aplicação. Esta integração do CWE opera independentemente do trabalho agendado para a Integração do CWE Abrangente 2000 que você ativa para a aplicação Resposta a vulnerabilidades. Seus dados não serão duplicados se você tiver a integração Veracode do CWE e a integração do CWE Abrange 2000 ativadas.
Veracode Integração de DevOps	Esta integração está inativa por padrão. A integração pode ser visualizada na lista Integrações de vulnerabilidade da aplicação em Resposta a vulnerabilidades de aplicações. Se você tiver uma licença do DevOps Change Velocity, este recurso será estruturado para que os usuários do DevOps não precisem de uma licença do SecOps para exibir detalhes de resumo das verificações de vulnerabilidade de terceiros. Não há impacto ou mudança para Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para status de execução de integração, consulte Exibir o Veracode status de execução da importação da Integração de vulnerabilidade da aplicação.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparando para o Veracode Vulnerability Integration

Um Veracode Vulnerability Integration bem-sucedido requer planejamento e a execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Veracode Vulnerability Integration pressupõe que você esteja familiarizado com o produto Veracode e a API.

Antes de Iniciar

A integração de enumeração de pontos fracos comuns (CWE) também é usada por Resposta a vulnerabilidades de aplicações e deve estar em execução antes de instalar e configurar o Veracode Vulnerability Integration. Ele é instalado com Resposta a vulnerabilidades, por padrão.

Nota: Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar a integração de vulnerabilidade da aplicação Veracode, no entanto, eles fornecem enriquecimento e seria útil ter. Para obter informações sobre o NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Há um usuário executar como configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Nota: Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis de aplicação que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

O Veracode Vulnerability Integration requer um ID de API e uma chave de API.

Procedimento

Para criar o ID de API e as credenciais de chave:

a. Faça login na plataforma Veracode.

b. Acesse o menu da conta do usuário e selecione **Credenciais de API**.

c. Clique **em Gerar credenciais de API**.

d. Registre suas credenciais para uso posterior.

Instalar a ServiceNow® Integração de resposta a vulnerabilidades com Veracode

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Veracode se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao grupo de gerentes de App-Sec. Para obter informações sobre funções de grupo, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções. • O grupo de gerentes de App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar o Veracode Vulnerability Integration.
2. Navegue até o ServiceNow Store.
3. Em ServiceNow Store, pesquise a aplicação Integração de resposta a vulnerabilidades com Veracode.
4. Clique no bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Considere ler as seções **Outros Requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique em **Obter**.
7. Insira o **Nome** e **o motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você receberá um e-mail com instruções detalhadas de instalação.

9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente em sua instância.

O que Fazer Depois

Configure o Veracode Vulnerability Integration para o seu ambiente. Consulte Configure o Veracode Vulnerability Integration.

Configure o Veracode Vulnerability Integration

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Veracode se integre corretamente com Resposta a vulnerabilidades de aplicações. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se a aplicação Resposta a vulnerabilidades Integration with Veracode está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar a ServiceNow Integração de resposta a vulnerabilidades com Veracode.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	• Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de usuários App-Sec Manager. • O gerente do App-Sec supervisiona a configuração e verifica os resultados esperados.
Para a integração de vulnerabilidade da aplicação Veracode, tenha seu **ID** de **API e chave** de API prontos.	Entre em contato com Veracode para obter o**ID** e **a chave de API**. Consulte Preparando para o Veracode Vulnerability Integration. A partir da versão 4.0, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais do Veracode. Essas descobertas não estão vinculadas a nenhuma solicitação de avaliação de teste de invasão configurada em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre solicitações de teste de invasão em Resposta a vulnerabilidades de aplicações, consulte Configurar teste de invasão.

Função necessária: grupo de usuários do App-Sec Manager

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Configuração**.
2. Preencha os campos **ID** de **API e Chave** de API.
3. Escolha seus resultados de testes.

Opção	Descrição
Versão 4.0:	**a.** Selecione os tipos de dados **DAST** ou **SAST** a serem incluídos na importação. **Nota:** Você pode escolher um ou outro, ou ambos, mas deve selecionar pelo menos um. **b.** Selecione **SCA** para importar vulnerabilidades da Análise de composição de software (SCA). **c.** Selecione **Incluir manual** para importar os resultados do teste de invasão manual de Veracode. AVITs são criados para esses resultados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Versão 3.0	Selecione os tipos de dados **DAST** ou **SAST** a serem incluídos na importação. **Nota:** Você pode escolher um ou outro, ou ambos, mas deve selecionar pelo menos um.
Versão 1.0:	Os resultados de testes dinâmicos de segurança da aplicação são selecionados, por padrão.

4. Adicione o nível de Veracode **gravidade** para filtrar os dados importados.
   Este valor é importado de Veracode. Você pode adicionar vários valores ao campo. Se preenchida, a importação coletará somente dados que correspondam aos níveis de gravidade que você adicionou.
5. Salve e valide suas escolhas.

Opção	Descrição
Versão 3.0:	Clique **em Salvar e testar credenciais**. **Nota:** A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Se uma mensagem de erro for exibida durante a configuração, insira novamente os dados.
Versão 1.0:	Clique em **Salvar**. Verifique a configuração bem-sucedida clicando em **Testar credenciais**. **Nota:** A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Se uma mensagem de erro for exibida durante a configuração, insira novamente os dados.

6. Selecione como você deseja gerenciar exceções e falso-positivos para AVITs na importação.
   As opções para gerenciar AVITs na importação com ServiceNow Gestão de exceções e fluxos de trabalho falso-positivos são ativadas por padrão. Os fluxos de trabalho são acionados com base em como os estados de **origem** nos AVITs são mapeados em sua instância. Para obter um exemplo de caso de uso, consulte Como gerenciar o mapeamento de estado para adiamentos e falso-positivos no Resposta a vulnerabilidades de aplicações.

Ativado	Gerenciar exceções no ServiceNow

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Deixe esta opção ativada se quiser fazer a triagem de **AVITs** importados marcados para o estado Adiado. **AVITs** com estados de **origem** que normalmente são mapeados para um estado adiado em sua instância são mapeados para **aberto**. Você **solicita uma exceção** do registro AVI. Gerenciar falsos positivos no ServiceNow Deixe esta opção ativada se quiser fazer a triagem de AVITs importados com estados de **origem** marcados como **Falso-positivo** ou **Possível falso-positivo**. AVITs com esses estados de **origem** que normalmente são mapeados para um estado **Closed** em sua instância são mapeados para **Open**. Você solicita um **falso-positivo** do registro AVIT.
Desativado	Desative uma ou ambas as caixas de seleção se quiser preservar os estados de **origem** importados do scanner. Esses AVITs são mapeados para os estados **Meta** e **Motivo** da meta conforme são importados, mas não são triados pelos fluxos de trabalho de exceção e falso-positivo. As ações **Solicitar exceção** e **Falso-positivo** não estão visíveis nos AVITs.

7. A partir da versão 4.3, escolha ou verifique as configurações dos parâmetros a seguir.

Parâmetro	Descrição
Região da API	Selecione uma região na lista.
Tempo limite da API	O padrão é 30K. Você pode preferir deixar este campo em sua configuração padrão.
Incluir vulnerabilidades de SBOM	Selecione para incluir todas as vulnerabilidades ingeridas pelas integrações Veracode SBOMVeracode nos arquivos [] carregados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetro	Descrição
	Deixe o campo em branco para que Veracode vulnerabilidades não sejam analisadas em Veracode SBOM arquivos.

8. Selecione **Salvar e testar credenciais**.

O que Fazer Depois

Se o seu ambiente exigir importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração.

Na instalação inicial, consulte Como configurar o Resposta a vulnerabilidades de aplicações para obter mais instruções.

Após a instalação inicial, para modificações, consulte Veracode Vulnerability Integration modificações e atividades.

Exibir o Veracode status de execução da importação da Integração de vulnerabilidade da aplicação

Use a lista relacionada de **execuções de integração de vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o Veracode Vulnerability Integration status de execução de importação:

- Resposta a vulnerabilidades de aplicações e Veracode Vulnerability Integration devem ser instalados e configurados.
- As Veracode Vulnerability Integration importações devem estar programadas e em execução.

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades de aplicações, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Selecione uma integração.
3. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns de falha na execução incluem:

   - Interrupção de rede.
   - Um problema na transferência de dados que resultou em dados corrompidos durante a transformação.

   Se você encontrar alguma dessas condições, clique em **Executar agora**e execute novamente a integração.
5. A partir da versão 4.2, exiba detalhes como tempos totais de processamento, tempos médios para processos de execução de pré e pós-integração e relatórios sobre os registros de execução de integração para as integrações de item vulnerável da aplicação.
   Para obter mais informações sobre como exibir detalhes adicionais importados por Veracode, consulte Obter mais detalhes em Veracode Vulnerability Integration.

Exibir Veracode resumos de verificação

Exiba detalhes das informações de resumo da verificação da Integração de vulnerabilidade Veracode.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Procedimento

1. Navegue até a tabela Resumos de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary_list].
2. Selecione um registro para uma verificação de Veracode.
3. A partir da v19.0 de Resposta a vulnerabilidades e v4.0 do Veracode Vulnerability Integration, use o ícone de lista de personalização (ícone de engrenagem) para exibir as seguintes colunas.

   - Tamanho da verificação estática
   - Contagem de biblioteca de terceiros
   - Contagem de biblioteca de vulnerabilidades de terceiros
   - Contagem de falhas de terceiros por gravidade
   - Contagem do problema de biblioteca de terceiros

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Contagem do problema de licença de terceiros
- Contagem de falhas mistas
- Contagem de falhas mitigadas
- Contagem de falhas não mitigadas
- Contagem de falhas estáticas por gravidade
- Nova contagem de falhas por gravidade
- contagem de falhas não mitigadas por gravidade
- Total de contagem de falhas por gravidade
- Classificação da última verificação de SCA
- Data da última verificação de SCA
- Data publicada da verificação
- Marcadores

Transformação de dados para a integração de vulnerabilidade Veracode

Depois de identificar os dados que deseja importar, os dados são recuperados da aplicação Veracode, processados por meio de um conjunto de fontes de dados e transformados em sua instância.

Veracode Integração de item vulnerável da aplicação

Os dados da API são carregados primeiro na tabela Veracode AppVul Item Import [sn_vul_veracode_appvul_item_import], e a Veracode AppVul Item Transform é usada para transformar as informações importadas.

Para acessar este mapa de transformação, navegue até *System Import Sets > Transform Maps* e pesquise Veracode AppVul Item Transform. A tabela a seguir lista os campos do mapa de transformação por integração.

Veracode Campos do mapa de transformação de item AppVul

Campo de origem	Campo de destino	Descrição
app_id	source_app_id	ID da aplicação.
ID do problema	source_avit_id	ID do AVIT.
app_name	app_name	Nome da aplicação.
versão	app_version	Versão da aplicação.
build_id	source_scan_id	ID de compilação da aplicação.
account_id	account_id	ID da conta.
sandbox_id	sandbox_id	ID da área restrita.
last_update_time	última_scan_date	Hora da última atualização.
app_name + last_scan_date	scan_summary_name	Resumo da verificação.
life_cycle_stage	status_sdlc_de_origem	Status do SDLC de origem.
nível	gravidade_origem	Gravidade de origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Campos do mapa de transformação de item AppVul

Campo de origem	Campo de destino	Descrição
category_name	categoria	Categoria.
gravidade_origem	gravidade_origem	Gravidade de origem.
category_id + "CWE-" + cweId	source_entry_id	ID da entrada de origem.
source_vulnerability_summary	source_vulnerability_summary	Resumo da vulnerabilidade de origem.
recomendação_de_origem	recomendação_de_origem	Recomendação de origem.
descrição	descrição	Descrição da origem.
descrição	source_vulnerability_explanation	Explicação da vulnerabilidade de origem.
mitigação_status_desc	source_mitigação_status	Status de mitigação de origem.
status_remediação	source_remediation_status	Status de correção de origem.
linha	número_linha	Linha em que a falha foi encontrada.
módulo	application_module	Módulo da aplicação.
arquivo de origem	notas_de_origem	Anotações de origem.
afeta_conformidade_política	cumpre_com_política	Os valores podem ser Sim ou Não, com base nas informações de origem serem verdadeiras ou falsas.
Sourcefilepath + sourcefile	local	Mapeamento de local em caso de *static* falha.
URL	local	Mapeamento de local em caso de *dynamic* falha.
escopo, tipo, exploitLevel	source_additional_info	Campo de valor de nome preenchido com os valores da origem em caso de falhas estáticas.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Veracode tempo e finalidade do script do mapa de transformação

Quando o script é executado	Finalidade
onComplete (quando um conjunto de importação concluiu a transformação)	Script usado para processar a fonte de dados e atualizar a contagem de AVITs criados, atualizados ou inalterados e os importados como parte desta integração de Veracode. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration modificações e atividades

Configure modificações opcionais especificamente para Veracode Vulnerability Integration.

Exibição de dados adicionais importados pelo Veracode Vulnerability Integration

Nota: Alterar outras configurações de Veracode Vulnerability Integration, diferentes das listadas aqui, requer conhecimento avançado de ServiceNow e Resposta a vulnerabilidades de aplicações e está além do escopo da documentação do produto.

Obter mais detalhes de Veracode

A partir da v4.2, selecione **Obter mais detalhes** sobre itens vulneráveis de aplicação (AVITs) que têm Veracode como a origem na tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item] ou nas exibições de lista nos Espaços de resposta a vulnerabilidades para exibir os seguintes dados Veracode.

- Os detalhes da solicitação de origem HTTP e da resposta de origem para verificações do Teste de segurança da aplicação dinâmico (Dynamic Application Security Testing, DAST) são exibidos na lista relacionada Solicitação/resposta HTTP.
- As recomendações de solução de Veracode são exibidas na lista relacionada Descobertas.
- A solicitação de origem HTTP, a resposta de origem e as recomendações são exibidas na guia Detalhes nos espaços de resposta a vulnerabilidades Resposta a vulnerabilidades.
- A coluna Descrição é compatível com a tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item].

Modificar Veracode parâmetros de instância de integração

Após a instalação inicial, você pode modificar os parâmetros das integrações [Veracode na instância de integração Veracode.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Você pode modificar os parâmetros de uma integração de sua instância para determinar que tipo de dados você ingere. Para algumas dessas configurações, você também pode modificar esses parâmetros na página de configuração da integração.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Integrações**.
2. Selecione **Vulnerabilidade da aplicação Veracode** na coluna Instância de origem para a integração Veracode que você deseja modificar.
3. Selecione a guia **Parâmetros de instância de integração** e clique duas vezes em um campo na coluna Valor para modificar os valores.

   Começando com v19.0 de Resposta a vulnerabilidades e v4.0 de Veracode Vulnerability Integration, você pode configurar os seguintes parâmetros para as integrações de Veracode.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

importar manual

Insira `verdadeiro` para importar resultados de testes de invasão manuais de Veracode. Você também pode modificar este valor na página de configuração de integração.

Os testes de avaliação de invasão no Veracode Vulnerability Integration são descobertas manuais do Veracode. Essas descobertas não estão vinculadas a nenhuma solicitação de avaliação de teste de invasão configurada em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre solicitações de teste de invasão em Resposta a vulnerabilidades de aplicações, consulte Configurar teste de invasão.

import_sca

Insira `verdadeiro` para importar vulnerabilidades da Análise de composição de software (SCA). Você também pode modificar este valor na página de configuração de integração.

status

Insira `Aberto` ou `Fechado` para importar descobertas para os estados desejados. Se você deixar este campo em branco, a integração importará descobertas para os estados Aberto e Fechado.

policy_sandbox

Insira uma `política` ou `área restrita` para importar registros que correspondem a uma política ou a uma área restrita. Esses registros podem estar relacionados à forma como as aplicações são testadas em seu ambiente.

regra_de_política_aprovada

Insira `verdadeiro` ou `falso` para importar registros que foram aprovados em uma regra de política. Esses registros podem estar relacionados à forma como as aplicações são testadas em seu ambiente.

4. Selecione **Atualizar** para salvar suas mudanças.

Executar uma importação manual de vulnerabilidade da aplicação Veracode

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independente do trabalho agendado diariamente.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Escolha e integração, por exemplo, Veracode Application List Integration.
3. Clique em **Executar Agora**.

> **Nota:** Cada uma das Veracode integrações de vulnerabilidade da aplicação tem como objetivo fornecer a recuperação de dados mais completa. Executá-los fora de ordem requer a experiência de ServiceNow e Resposta a vulnerabilidades de aplicações e pode resultar em dados incompletos.

Quando a importação for concluída, as importações programadas serão retomadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para status de execução de integração, consulte Exibir o Veracode status de execução da importação da Integração de vulnerabilidade da aplicação.
5. Se você quiser modificar outros parâmetros de integração, deverá navegar até a instância de integração.

Definir Veracode Vulnerability Integration tempos de importação

Para sua conveniência, você pode redefinir a hora de início do Veracode Vulnerability Integration.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
Após a importação inicial, as Veracode integrações de vulnerabilidade fazem uma importação completa sempre que são executadas. Consulte Executar uma importação manual de vulnerabilidade da aplicação Veracode para obter mais informações sobre como realizar importações.

Procedimento
1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Escolha uma integração.
3. Defina a nova **Hora**de início.
   O tempo é calculado como Horas no horário local. O tempo padrão para as importações de Integração da lista de aplicações Veracode é 00:00:00. As outras integrações são **Sob demanda** e encadeadas para serem executadas após a Veracode Integração da lista de aplicações. Alterar a **hora de início** de qualquer um desses requer conhecimento avançado de ServiceNow e Gestão de vulnerabilidades de aplicações.
4. Clique em **Atualizar**.
   A nova hora será usada para a próxima importação agendada.

Incluir itens vulneráveis da aplicação Veracode encerrados

Por padrão, os itens vulneráveis da aplicação (IVAs) **encerrados** não são criados durante Veracode importações de integração de item vulnerável. Se você quiser criá-los, deverá alterar uma propriedade do sistema.

Antes de Iniciar
O Veracode Vulnerability Integration deve estar instalado e em execução.

Função necessária: administrador

Procedimento
1. Na caixa de texto **Navegador de filtros** à esquerda, digite `sys_properties.list`.
2. Na caixa de pesquisa **Nome** da lista, insira `sn_vul.create_closed`.
3. Clique duas vezes no campo **Valor** e defina como **Verdadeiro**
4. Clique no ícone de marca ícone de marca de seleção verde para salvar.
   Registros no estado **Encerrado** na próxima importação Veracode são criados como AVIs em Resposta a vulnerabilidades de aplicações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Corrigindo Resposta a vulnerabilidades de aplicações vulnerabilidades

O monitoramento da correção é um processo que começa com a revisão do status e termina com o fechamento dos itens vulneráveis da aplicação (AVITs). Resposta a vulnerabilidades de aplicações oferece ferramentas e procedimentos para tornar esse processo mais produtivo e eficiente.

Resposta a vulnerabilidades de aplicações processo de correção

A correção de item vulnerável da aplicação é feita manualmente.

Uma visão geral do processo:

- Faça login na sua instância Resposta a vulnerabilidades de aplicações.
- Valide se suas regras (Pesquisa de IC, Atribuição) para itens vulneráveis de aplicação estão funcionando conforme o esperado. Para obter informações sobre como revisar as Regras de pesquisa de IC, consulte Identificar aplicações em Resposta a vulnerabilidades de aplicações automaticamente. Para obter informações sobre regras de atribuição, consulte Atribuir itens vulneráveis de aplicação em Resposta a vulnerabilidades de aplicações automaticamente.
- Valide se suas metas de correção estão corretas. Consulte Automatizar o acompanhamento da meta de correção no Resposta a vulnerabilidades de aplicações para obter informações sobre como as regras de destino de correção funcionam e como revisá-las. Exibir o status da meta de correção de um item vulnerável da aplicação.

  Nota: As regras de destino de correção pertencem a AVITs. Essas regras são executadas quando o AVIT é importado.

- Revise os painéis ou relatórios. Por exemplo, exiba painéis que mostram o envelhecimento de AVITs por estados.

  Nota:

  Quando a aplicação Performance Analytics para Resposta a vulnerabilidades (com.snc.vulnerability.analytics) é ativada, os usuários com determinadas funções podem exibir dados de interesse para os membros dos grupos de gerentes de App-Sec e de defensores da segurança.

  Para gerentes de App-Sec, Performance Analytics para Resposta a vulnerabilidades contém a visão geral Resposta a vulnerabilidades de aplicações, que pode ajudá-lo a monitorar áreas de interesse. Consulte Soluções de análise e emissão de relatórios para opainel Application Vulnerability Response e Application Vulnerability Management [PA].

  A partir da versão 13.0 da aplicação Resposta a vulnerabilidades : para os Campeões de segurança, Performance Analytics para Resposta a vulnerabilidades contém o painel Minhas vulnerabilidades da aplicação, que pode ajudá-lo a monitorar suas áreas de interesse. Consulte Meu painel de vulnerabilidades da aplicação.

  A partir da versão 13.0 da aplicação Resposta a vulnerabilidades : para limitar a quantidade de dados coletados para relatórios ou listas relacionadas, consulte Definir classificações de serviço para Resposta a vulnerabilidades relatórios e listas relacionadas.

- Revise o estado dos AVITs, em ordem de prioridade, procurando o que mudou.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Revise o risco dos AVITs, conforme necessário. Para obter mais informações, consulte Criar uma calculadora de vulnerabilidade da aplicação.
- Reatribua o AVIT a um grupo de atribuição para correção, se necessário.
- Novas verificações são acionadas automaticamente pela programação de importação de terceiros.
- Após a nova verificação, se o estado for **Fixo**, os AVITs serão fechados automaticamente durante a importação.
- Após a verificação, se o estado não for **Fixo**, o AVIT será reaberto.

Obter mais detalhes de Veracode

Selecione **Obter mais detalhes** sobre itens vulneráveis da aplicação (AVITs) que têm Veracode como a origem na tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item] ou nas exibições de lista nos Espaços de resposta a vulnerabilidades para exibir os seguintes dados Veracode.

- Os detalhes da solicitação de origem HTTP e da resposta de origem para verificações do Teste de segurança da aplicação dinâmico (Dynamic Application Security Testing, DAST) são exibidos na lista relacionada Solicitação/resposta HTTP.
- As recomendações de solução de Veracode são exibidas na lista relacionada Descobertas.
- A solicitação de origem HTTP, a resposta de origem e as recomendações são exibidas na guia Detalhes nos espaços de resposta a vulnerabilidades Resposta a vulnerabilidades.
- A coluna Descrição é compatível com a tabela Item vulnerável da aplicação [sn_vul_app_vulnerable_item].

Exibir bibliotecas de vulnerabilidades

Você pode exibir dados de vulnerabilidade importados do Banco de dados nacional de vulnerabilidades (NVD), Enumeração de pontos fracos comuns (CWE) ou de terceiros para decidir se deve escalar um grupo de vulnerabilidades.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > para **bibliotecas**.

   As seguintes bibliotecas estão disponíveis:

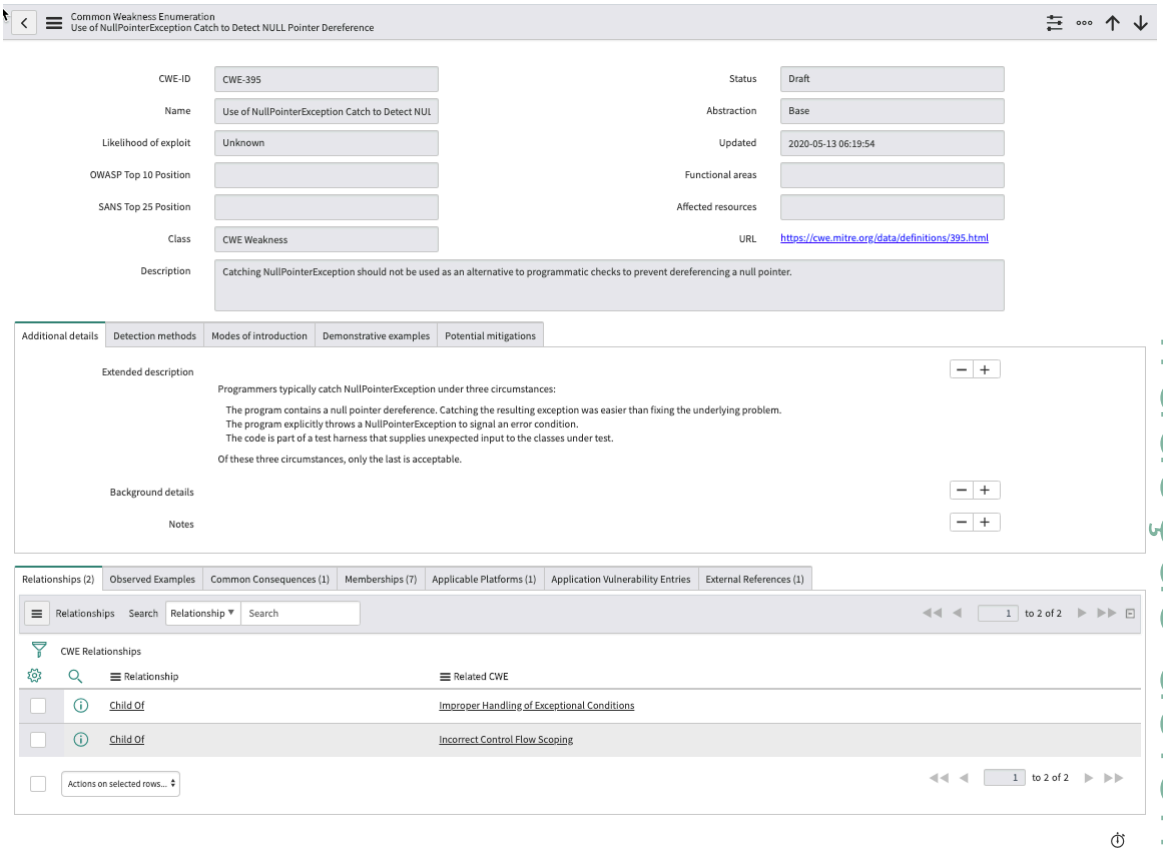
Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, erros de configuração, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de pontos fracos comuns, é apenas para referência.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
Terceiro	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações, CWEs e CVEs.

2. Escolha uma biblioteca para exibir vulnerabilidades.



Para obter informações sobre campos específicos, consulte Campos de vulnerabilidade da aplicação.

Campos de vulnerabilidade da aplicação

As vulnerabilidades são criadas automaticamente quando os registros são baixados do Banco de dados nacional de vulnerabilidades (NVD), Enumeração de pontos fracos comuns (CWE) ou integrações de terceiros. O NVD e o CWE são armazenados em **Bibliotecas** em Resposta a vulnerabilidades ou em **Vulnerabilidades** em Resposta a vulnerabilidades de aplicações.

Campos de entrada de vulnerabilidade do CWE

Os campos nesta tabela são somente leitura.

Campo	Descrição
CWE-Identificador	Identificador desta entrada de vulnerabilidade. Este identificador é usado para Categorias e Pontos Fracos e é exclusivo entre os dois conjuntos de dados.
Nome	Nome descritivo atribuído a este CWE-ID.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Probabilidade de exploração	A probabilidade de o ponto fraco ser explorado, em uma escala qualitativa. Um dos seguintes: • Baixo • Médio • Alto(a)
10 principais posições da OWASP	A posição numérica desta vulnerabilidade na lista das 10 principais da OWASP.
SANS para 25 posições	A posição numérica desta vulnerabilidade na lista das 25 principais da SAN.
Classe	Tipo de fraqueza
Status	Um dos seguintes: • Incompleto • Rascunho • Estável • Preterido • Obsoleto • Instável
Subtração	Um dos seguintes: • Variante • Classe • Base • Composto
Atualizado em	Última vez em que o registro foi atualizado na instância.
Áreas funcionais	Lista de áreas funcionais afetadas. Por exemplo, **Processamento de arquivo**. Preenchido somente para pontos fracos do 24/862.
Recursos afetados	Lista de recursos afetados. Por exemplo, **Arquivo** ou **Diretório**. Preenchido somente para pontos fracos 51/863.
URL	Artigo da base de conhecimento associado a esta vulnerabilidade.
Descrição	Descrição da vulnerabilidade.
Execução de integração	A execução de integração em que este CWE foi importado.
Seções	
Detalhes adicionais	Descrições do conceito de software que explicam melhor o ponto fraco. Inclui:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• Descrição estendida • Detalhes do plano de fundo • Anotações
Métodos de detecção	Detalhes sobre como você pode detectar esse ponto fraco em uma aplicação.
Modos de introdução	As fases em que o ponto fraco é introduzido, por exemplo, **Implementação**, **Arquitetura e design**e assim por diante.
Exemplos demonstrativos	Exemplos de código da fraqueza com as descrições que os acompanham.
Mitigações potenciais	Detalhes sobre como evitar o ponto fraco, incluindo em qual fase do ciclo de vida da aplicação ele ocorre e a eficácia da mitigação.
Listas relacionadas	
Relacionamentos	CWEs associados a esta vulnerabilidade. Lista os relacionamentos entre este CWE e outros. Pode incluir primário/secundário, segue/ precede, exigidopor/requer (para fraquezas compostas), CanAlsoBe, PeerOf, MemberOf .
Exemplos observados	Alguns CVEs que são representativos desta fraqueza.
Consequências Comuns	Consequências de uma exploração bem-sucedida, em termos de escopo e impacto. Por exemplo: Escopo: confidencialidade Impacto: ler dados da aplicação
Associações	Associações do CWE com esta vulnerabilidade.
Plataformas aplicáveis	Plataformas associadas a esta vulnerabilidade.
Entradas de vulnerabilidade da aplicação	Outras entradas de vulnerabilidade da aplicação associadas a uma.
Referências externas	Informações sobre a vulnerabilidade de fontes externas.

Tradução automática

Campos de entrada de vulnerabilidade da aplicação

Os campos nesta tabela são somente leitura.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Origem	Origem da vulnerabilidade - seja um scanner ou teste físico.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de gravidade são fornecidos para NVD e com ServiceNow integrações

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Mapear a gravidade de um item vulnerável de aplicação automaticamente.
Versão 13.0: CWE primário Versão 12.1: entrada do CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns em que esta vulnerabilidade se encaixa melhor. Se houver mais de um CWE associado à vulnerabilidade, o CWE primário será determinado da seguinte forma: • O CWE está mapeado para os 10 principais OWASP. Em caso afirmativo, use este CWE. Caso contrário, continue. • O CWE está mapeado para as 25 principais SANs? Em caso afirmativo, use este CWE. Caso contrário, continue. • O CWE tem a severidade mais alta? Em caso afirmativo, use este CWE. Caso contrário, continue. • Selecione o mais recente de todos os CWEs. O CWE mais recente é aquele com o valor do campo **atualizado** mais recente no registro do CWE.
Nome da categoria	Classificação fornecida pela integração de terceiros. Ajuda na atribuição.
Detalhes da Vulnerabilidade	
Ameaça	Descrição da ameaça desta vulnerabilidade.
Descrição da mitigação	Descrição das etapas que podem ser realizadas para atenuar a vulnerabilidade.
Lista relacionada	
Versão 13.0: CWEs	Lista dos CWEs associados a esta vulnerabilidade. Não aplicável para Veracode Vulnerability Integration.

Campos de entrada do NVD

Os campos importados nesta tabela são somente leitura.

Nota:

Os dados do NVD não são usados em Resposta a vulnerabilidades de aplicações e as entradas representam somente os dados Resposta a vulnerabilidades.

Os CWEs, que são usados em Resposta a vulnerabilidades de aplicações, podem apontar para entradas do NVD, como exemplos de um ponto fraco, e são fornecidos aqui apenas para fins informativos.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Pontuação de risco	(Oculto quando não há Resposta a vulnerabilidades itens vulneráveis (VIs) associados à vulnerabilidade)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Pontuação de risco quantificado que separa os IVs em Crítico, Alto, Médio, Baixo e Nenhum.
Pontuação de risco	(Oculto quando não há IVs associados à vulnerabilidade) Valor calculado de risco que o item vulnerável representa para o seu ambiente.
Gravidade	Grau normalizado de severidade desta vulnerabilidade em Resposta a vulnerabilidades. Mapas de gravidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Resposta a vulnerabilidades de aplicações **A gravidade** é derivada da **gravidade de origem** importada e não do NVD. Para obter informações sobre Resposta a vulnerabilidades de aplicações mapeamento de gravidade, consulte Mapear a gravidade de um item vulnerável de aplicação automaticamente.
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Explorar nível de habilidade	Nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Explorar vetor de ataque	Vetor de ataque mais vulnerável das explorações para esta vulnerabilidade.
IVs ativos	(Oculto quando não há IVs associados à vulnerabilidade) Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Fechado. Se não houver AVIs ativos para esta vulnerabilidade, a **Classificação** de **risco e a Pontuação** de risco não serão exibidas.
Entrada de CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns em que esta vulnerabilidade se encaixa melhor de acordo com o NVD.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados do CVSS v3 importados, não disponíveis antes de 2015.
Solução preferencial	(Oculto quando não há IVs associados à vulnerabilidade) Solução de substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais elevada na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído em importações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	subsequentes. A definição deste valor manualmente deve ser feita no item vulnerável.
Status da Correção (Oculto quando não há IVs associados à vulnerabilidade)	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis de aplicação ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Percentual de VIs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
Percentual de VIs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Antes da v13.0: forçar importação de vulnerabilidade de software **Nota:** Removido em v13.0	(Obsoleto) Recalcula o mapeamento do produto com Gestão de ativos de software do ITSM com base nas informações do NVD. Atualiza a biblioteca de software vulnerável.
Atualizar status	Exibe a data e a hora da última atualização. Atualiza o seguinte: • Estado do grupo de vulnerabilidade • Pontuação e classificação de risco • Métricas como VIs ativos, VIs totais da seção Status de correção
Listas relacionadas	
Itens vulneráveis	(Oculto quando não há IVs associados à vulnerabilidade) Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
Explorações	Explorações associadas a esta vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Soluções	(Oculto quando não há IVs associados à vulnerabilidade) Todas as Solução de gestão de vulnerabilidade soluções de integração associadas a esta vulnerabilidade.
Versão 13.0: Pontos fracos	Dados importados de vulnerabilidade do CWE associados a vulnerabilidades e exposições comuns (CVE).
Versão 13.0: Software Vulnerável	(Oculto quando não há IVs associados à vulnerabilidade) Dados importados de Enumeração de plataforma comum (CPE) associados à vulnerabilidade.

Identificar aplicações em Resposta a vulnerabilidades de aplicações automaticamente

Quando os dados são importados de uma integração de terceiros, Resposta a vulnerabilidades de aplicações usa automaticamente os dados da aplicação para pesquisar correspondências no Configuration Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras identificam aplicações para o registro de item vulnerável da aplicação (IVA) para ajudar na correção.

Conforme as aplicações são importadas, uma pesquisa é realizada na aplicação verificada [sn_vul_app_scanned _application] tcapaz de usar source_app_id e app_name para encontrar correspondências com aplicações de importações anteriores. Quando uma correspondência de ID de aplicação é encontrada, seus valores são usados nos campos **Aplicação** e **Versão** da aplicação no registro de item vulnerável da aplicação.

Se uma correspondência não for encontrada ou o campo ID da aplicação estiver vazio, as regras usarão as outras informações da aplicação para tentar identificar corretamente a aplicação. Se uma correspondência ainda não for encontrada, um registro de aplicação verificado com espaço reservado será criado somente com os campos **Nome** da **aplicação e ID** da aplicação.

As regras de pesquisa **de Id da aplicação de origem** e **Nome** da aplicação são enviadas com o Veracode Vulnerability Integration, por padrão.

Nota: As regras de pesquisa de IC padrão para Resposta a vulnerabilidades de aplicações estão disponíveis somente para a Integração de vulnerabilidade Veracode.

Ao tentar uma correspondência, as regras de pesquisa são avaliadas pelo valor de **Ordem** mais baixo primeiro. Eles param quando uma regra retorna um único IC como uma correspondência.

Nota: Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Para facilitar a localização de problemas de correspondência, quando uma correspondência é encontrada, a regra de pesquisa de IC usada para encontrá-la é adicionada ao campo de **regra de correspondência de IC** para aplicações verificadas.

Clique no Atualizar lista personalizada na parte superior da exibição de lista de aplicações verificadas para adicioná-la à exibição.

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Se compatível, cada origem pode ter várias implantações. Por exemplo, a Veracode Integração de vulnerabilidade pode ter várias implantações da Veracode Integração de vulnerabilidade. Cada implantação tem seu próprio conjunto de regras de pesquisa de IC.

Nota: As regras de pesquisa de IC são compartilhadas por todas as implantações da integração de vulnerabilidade. Se uma regra for excluída ou modificada, a exclusão ou as mudanças afetarão todas as implantações da integração de vulnerabilidade.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência dentro do CMDB pode resultar em longos tempos de processamento. Para evitar qualquer degradação potencial de recursos ou complicações de desempenho, teste todas as regras de pesquisa de IC personalizadas ou modificações nas **regras de pesquisa de IC** predefinidas. Consulte Impedir registros duplicados ou órfãos após executar regras de pesquisa de IC da Resposta a vulnerabilidades da aplicação para obter mais informações sobre como evitar registros órfãos duplicados, excluir dados e limpar dados.

Informações relacionadas

Gestão de configuração e o CMDB

Criar uma regra de pesquisa de IC

O módulo **Regras de pesquisa de IC** contém regras que definem quais campos têm dados correspondentes no Configuration Management Database (CMDB). Essas regras são usadas para identificar aplicações e versões de aplicações e adicioná-las ao registro de item vulnerável da aplicação (IVA) para ajudar na correção.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

A criação de regras de pesquisa de IC requer conhecimento avançado de ServiceNow e Gestão de vulnerabilidades de aplicações. Em vez de modificar uma das regras de pesquisa existentes, considere copiá-la e modificar a cópia. Quando você estiver satisfeito com a nova regra fazendo o que você deseja, desative a original.

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **CMDB** > **Regras de Pesquisa de IC**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regra de pesquisa de IC

Campo	Descrição
Nome	Nome da regra.
Método de pesquisa	Método usado para correspondência. As opções são: ◦ **Script**: script pré-criado ou personalizado. ◦ **Correspondência de campo**: pesquise na tabela ou no campo no CMDB.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

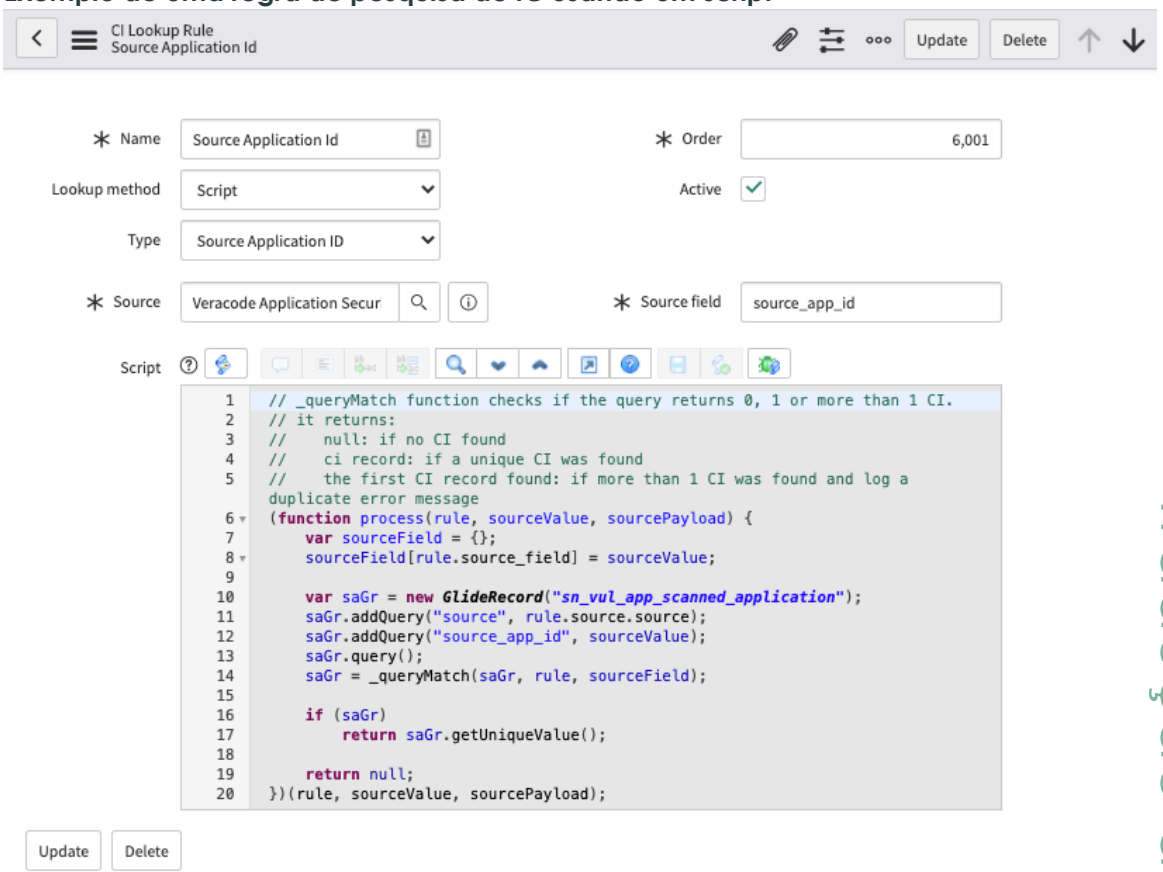
Campo	Descrição
Tipo	Tipo usado com o **método Pesquisa**de script.
Ordem	Ordem de precedência da regra. As correspondências com a ordem mais baixa são avaliadas primeiro.
Ativo	Caixa de seleção para saber se a regra está ativa ou desabilitada.
Origem	Origem usada como entrada para esta regra. Depois de escolhido, os filtros de condição serão exibidos.
Campo de origem	Campo de origem usado como entrada para esta regra. Os campos devem ser uma cadeia de caracteres ou um número.
Descrição	Texto que descreve a regra.
V19.0: destino da pesquisa	Abordagem de pesquisa que você deseja seguir. Selecione entre: ◦ Item de configuração ◦ Modelo de produto
Script	O script de amostra editável, com base no **Tipo**, é mostrado. Implemente o script personalizado seguindo os comentários incluídos no modelo da função padrão. **Nota:** A função de processo tem três parâmetros: *`rule`*, *`sourceValue`*e *`sourcePayload`*
Pesquisar na tabela IC	Tabela a ser pesquisada no CMDB. Usado com campo correspondente ao **Método de pesquisa**.
V19.0: pesquisar na tabela de produtos	Se você escolher o **destino Pesquisa**do modelo de produto , o valor padrão será Modelo da aplicação.
Pesquisar no campo IC	Campo que contém informações que podem ser usadas para localizar um IC. Usado com o campo correspondente ao **Método de pesquisa**. Este campo pode estar no registro de IC ou em um registro relacionado, como um adaptador de rede.
V19.0: pesquisa no campo do modelo do produto	Se você escolher o **destino de pesquisa**do modelo de produto , o valor padrão será Nome.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.

Exemplo de uma regra de pesquisa de IC usando um script



Informações relacionadas

Campos de item vulnerável da aplicação

Como reaplicar regras de pesquisa de IC no Resposta a vulnerabilidades de aplicações

Você pode reaplicar suas regras de pesquisa de item de configuração (IC) para atualizar ICs existentes (aplicações verificadas e modelos de produto) em registros de aplicações descobertos.

Reaplicar uma regra de pesquisa

A reaplicação das regras de pesquisa de IC aplicará todas as regras ativadas às aplicações descobertas existentes. A atualização dos registros de aplicações descobertas pode levar algum tempo.

Para reaplicar as regras a aplicações descobertas existentes, navegue até **Todos** > **Operações de segurança** > **CMDB** > **Regras de pesquisa** e selecione **Aplicar mudanças**.

Como definir o destino da pesquisa

Por padrão, a propriedade do sistema *sn_vul.use_product_model* está ativada (definida como **verdadeira**). Dependendo de como a propriedade do sistema está definida nos registros da regra de pesquisa de IC, os registros da aplicação descoberta são atualizados da seguinte maneira:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o campo Valor estiver definido como **verdadeiro**, o modelo de produto será o destino de pesquisa das regras de pesquisa de IC e as aplicações descobertas serão atualizadas com os modelos de produto.
- Se o campo Valor estiver definido como **falso**, o item de configuração (apps verificados) será o destino da pesquisa e as aplicações descobertas serão atualizadas com os itens de configuração (aplicativos verificados).

Para modificar a propriedade do sistema *sn_vul.use_product_model* para que os itens de configuração sejam usados como destino:

1. Como um usuário com a função sn_vul.app_sec_manager, navegue até **Todos** > **Propriedades do sistema** > **Todos**
2. Localize *sn_vul.use_product_model*.
3. Abra o registro.
4. Defina o campo Tipo como **falso**.
5. Selecione **Atualizar**.

Se você redefinir esta propriedade do sistema, deverá modificar suas regras para que os destinos de pesquisa correspondam à configuração da propriedade do sistema. Por exemplo, se você redefinir a propriedade do sistema para usar o item de configuração como destino, localize as regras que têm o destino de pesquisa como item de configuração.

1. Marque a caixa de seleção Ativo para essas regras e selecione **Atualizar**.
2. Localize as regras que usam o modelo de produto como destino e desative-as desmarcando a caixa de seleção Ativo e selecionando **Atualizar**.

Se você estiver criando uma nova regra de pesquisa, defina o destino de pesquisa para a regra no formulário de regra. Para obter mais informações, consulte Criar uma regra de pesquisa de IC.

Impedir registros duplicados ou órfãos após executar regras de pesquisa de IC da Resposta a vulnerabilidades da aplicação

Tome medidas para evitar registros duplicados ou órfãos resultantes da correspondência (itens de configuração (ICs) no CMDB.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência no CMDB pode resultar em tempos de processamento demorados. O teste completo e a depuração de scripts de processamento nas regras ajudam a aliviar o potencial de problemas posteriores no processo.

Como evitar registros duplicados ou órfãos

- Use pequenos subconjuntos de dados que são específicos para a regra de pesquisa de IC que está sendo testada.
  - Defina todas as **Regras de pesquisa de IC**, exceto a que está sendo testada, como **Inativas**.
  - Analise as aplicações importadas e os itens de configuração (ICs) para garantir que você esteja observando o comportamento esperado e que a correspondência esteja ocorrendo corretamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Revise os estados do IC, como **Descontinuado**.
- Remover dados de teste. Depois de começar a observar o comportamento correto ou esperado na correspondência de IC, reinicie. Isso pode ser feito por:
  - Excluindo os dados usados para testes: (consulte a seção **Excluindo dados de tabelas**)
    - Aplicações verificadas
    - Itens vulneráveis de aplicação (IVAs)
  - Execute novamente as integrações manualmente.

.

Excluindo dados de tabelas

Às vezes, você importou dados e percebeu que algo está errado. Se isso acontecer em um ambiente de desenvolvimento ou desempenho, você poderá recriar a partir de um ambiente melhor, mas isso nem sempre é uma opção.

Nota: A execução dessas ações requer conhecimento avançado ServiceNow.

Existem quatro opções para excluir dados de tabelas:

- Usando **Excluir todos os registros** na **configuração da tabela**.
- Configure o **limpador de tabela** navegando até **Limpezas automáticas** (sys_auto_flush.list) e criando um novo registro **de limpeza automática**.
- Truncar gs.truncateTable usando um script em segundo plano.

  Nota: Nunca use *truncateTable* em um ambiente de produção. Consulte o representante de suporte antes de executar grandes exclusões em ambientes compartilhados ou de produção.

- Crie uma solicitação no HI para que os dados sejam excluídos.

Atribuir itens vulneráveis de aplicação em Resposta a vulnerabilidades de aplicações automaticamente

Atribua automaticamente vulnerabilidades de aplicação com base em marcadores de aplicação ou em qualquer um dos grupos de atribuição no item de configuração [cmdb_ci] ou grupos de atribuição de plataforma, para reduzir o tempo médio de atribuição.

Atribuição automática de itens vulneráveis da aplicação

Existem três maneiras diferentes de atribuir AVIs usando **Atribuir usando**:

Nota: O recurso de recomendação de atribuição em Resposta a vulnerabilidades não está disponível para Resposta a vulnerabilidades de aplicações.

- Grupo de usuários: esta opção permite selecionar qualquer um dos Now Platform® grupos de usuários existentes.
- Campo de grupo de usuários: esta opção permite que você escolha qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir no menu de lista em **Campo de grupo de usuários**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Nenhum: indica que não há valor padrão para este campo obrigatório
- Item de configuração: grupo de aprovação
- Item de configuração: grupo de atribuição
- Item de configuração: grupo de suporte

- Script: esta opção permite definir as condições usando um script. Esta opção requer codificação ou conhecimento avançado ServiceNow.

Execute regras de alta prioridade (itens que precisam de tratamento especial, onde o risco é crítico ou um AVI deve ser tratado pela conformidade regulatória) primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir AVIs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.

Processo de avaliação da regra de atribuição

Quando um novo AVI é criado, importado ou reaberto após ser fechado, as regras de atribuição são avaliadas em relação a ele. Um AVI só é avaliado uma vez, a menos que seja reaberto após ser fechado. Você pode reaplicar as regras manualmente após as mudanças.

O processo a seguir é usado para cada AVI novo, atualizado ou reaberto:

- Para cada regra de atribuição de vulnerabilidade, o AVI é comparado ao filtro de atribuição, com a regra de ordem mais baixa primeiro.
- Onde a condição corresponder, o AVI será atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Onde as condições não encontrarem uma correspondência entre todas as outras regras, o AVI será atribuído ao grupo de atribuição padrão, se houver uma regra padrão.

Nota: Se não houver regra padrão, o AVI permanecerá não atribuído.

O**tipo de atribuição**, seja **Manual** ou **Regra** e **regra de atribuição,** está disponível no slushbucket de Layout de formulário no formulário de item vulnerável da aplicação (IVA). Qualquer AVI que foi atribuído originalmente por uma regra, mas posteriormente reatribuído manualmente, contém uma referência à regra original. Use as informações de **Regra** de **atribuição e Tipo** de atribuição para identificar casos em que as regras de atribuição não encontraram uma correspondência correta para o destinatário pretendido. Ou quais regras tiveram mais reatribuições.

Nota: As regras de atribuição não reavaliam atribuições criadas manualmente.

Reaplicando regras de atribuição

Ao alterar uma regra de atribuição, use o botão **Aplicar mudanças** na exibição de lista Regras de atribuição para executar novamente todas as regras alteradas em todos os AVIs abertos ativos (exceto aqueles que foram atribuídos manualmente).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se o *Reapply all vulnerability assignment rules* trabalho agendado não tiver sido executado antes da primeira vez em que você usar **Aplicar mudanças**, ele executará todas as regras de atribuição em todos os AVIs abertos, exceto os AVIs que foram atribuídos manualmente. Depois disso, todos os usos subsequentes de **Aplicar mudanças** executam novamente somente as regras alteradas e quaisquer regras dependentes. Mudanças em uma regra podem resultar em um AVI correspondendo a uma regra não modificada diferente.

O trabalho agendado [*Reapply all assignment rules*] está inativo, por padrão. Quando ativado, ele aplica todas as regras a todos os IVAs abertos, exceto aqueles atribuídos manualmente. Ele pode ser executado **Diariamente**, **Semanalmente**, **Mensalmente**, **Periodicamente**, **Uma vez**ou **Sob demanda**. Dependendo de quantos AVIs ativos você tiver em seu ambiente, lembre-se de definir o campo **Executar** corretamente após a execução inicial para evitar impactos no desempenho.

Criar ou editar Resposta a vulnerabilidades de aplicações regras de atribuição

Você pode criar regras para atribuir automaticamente itens vulneráveis de aplicação (IVAs) com base nas condições do filtro. Essas regras atribuem AVIs conforme eles são importados ou criados manualmente.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
Com regras de atribuição, você define a condição de atribuição e a ordem de execução. Quando um AVI corresponde a uma condição de regra, a pesquisa de atribuição é interrompida. Para obter mais informações, consulte Filtrando em Gestão de vulnerabilidades de aplicações.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de atribuição**.
2. Clique em **Nova**.
3. Se for **Novo**, preencha os campos no formulário, conforme apropriado.

Regra de atribuição de vulnerabilidade da aplicação

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se a regra de atribuição está ativa.
Ordem de execução	Ordem na qual as regras são avaliadas. Regras de alta prioridade, itens que precisam de tratamento especial, onde o risco é crítico ou um AVI deve ser tratado pela conformidade regulatória, para ser executado primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é rnecessário, e você sabe quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir AVIs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição da regra de atribuição.
Condição	
Campos de condição	Condições que devem ser atendidas.
Novos critérios	Adiciona mais campos de filtro de condição para escolher.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ◦ Grupo de usuários: selecione um grupo de usuários na tabela de pesquisa. ◦ Campo de grupo de usuários: selecione um campo de grupo de usuários no menu de lista. ◦ Script: crie ou edite um script. **Nota:** Criar ou editar um script requer ServiceNow conhecimento.

4. Clique em **Enviar**.
   Regras novas ou atualizadas são avaliadas na próxima importação.

Calcular risco em Resposta a vulnerabilidades de aplicações automaticamente

As calculadoras de vulnerabilidade da aplicação automatizam o cálculo dos valores de risco inicial dos campos nos itens vulneráveis da aplicação (IVAs). Os cálculos de risco oferecem informações sobre como priorizar a correção. A condição de cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

Calculadoras de vulnerabilidade da aplicação

O sistema de base Resposta a vulnerabilidades de aplicações inclui duas calculadoras de vulnerabilidade que definem a **pontuação de risco** básica no item vulnerável da aplicação.

- **Calculadora de risco básico**
- **Calculadora do Risco avançado**

As calculadoras de vulnerabilidade da aplicação podem ser criadas para priorizar e classificar o impacto dos IVAs com base em qualquer critério usando filtros de condição. Seja o impacto da vulnerabilidade nos negócios, a classe do item de configuração (IC) ou a idade do IVA, você pode criar calculadoras de vulnerabilidade adicionais para definir outros campos nos AVIs. Ou você pode personalizar as calculadoras de vulnerabilidade existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades. Para obter mais informações, consulte Filtrando em Gestão de vulnerabilidades de aplicações.

Os IVAs contêm o valor de **pontuação de risco** derivado das calculadoras de risco.

Nota: Um AVI exibe a **gravidade de origem**, mas não a gravidade normalizada. A severidade normalizada é usada pelas calculadoras para obter o valor de **pontuação de risco**, mas não é mostrada em AVIs.

Cada calculadora contém uma lista de regras de calculadora, com uma condição que determina quando aplicá-la. Quando a calculadora é executada, a condição de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

cada regra de calculadora é avaliada na ordem e a primeira regra de calculadora correspondente é usada.

Todas as calculadoras de vulnerabilidade habilitadas definem os campos selecionados sempre que um AVI é criado, quando um IC associado ou uma vulnerabilidade muda.

A calculadora de **risco básico** calcula a **pontuação** de risco para IVAs usando a severidade da vulnerabilidade normalizada.

Nota: Somente uma calculadora por campo de destino (**Pontuação de risco**) pode estar ativa por vez.

O **risco básico** está habilitado por padrão. A **Calculadora de risco avançada** está inativa por padrão.

Regras da calculadora de vulnerabilidade da aplicação

A calculadora **da Calculadora de risco básica do** sistema base contém regras de calculadora que atribuem a cada nível de gravidade (Nenhum a Crítico) um valor (0-100) para **Pontuação de risco** com base na gravidade. A**Severidade Desconhecida** é atribuída automaticamente a uma pontuação de risco de 100. Esses valores podem ser ajustados e, como a **Calculadora de risco avançado**, novas regras de calculadora ou novas regras de risco podem ser criadas.

Nota: A partir da v23.0 de Resposta a vulnerabilidades de aplicações, sempre que a pontuação de risco é atualizada em um AVIT, a seção **Anotações** é atualizada com os seguintes detalhes:

- Nome do grupo de calculadoras
- Nome da calculadora: dependendo se a regra da calculadora é baseada em um modelo ou em um script, o nome é acrescentado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e marque a caixa de seleção **Exibição avançada**. Na caixa suspensa **Tipo de valor**, selecione a opção necessária. Se o **modelo** for selecionado, a pontuação de risco será atualizada de acordo com a condição especificada na regra. Se **Script** estiver selecionado, você poderá adicionar ou atualizar o script existente.

A calculadora da **Calculadora de risco avançada** do sistema base contém uma regra de calculadora de vulnerabilidade especializada chamada **Regra de risco padrão**. Ele calcula a **pontuação de risco** com base em vários valores:

- Gravidade da vulnerabilidade
- 10 principais da OWASP
- 25 principais da SANS

Você pode personalizar os critérios para a regra de risco padrão. Para obter mais informações, consulte Definir campos e pesos para a regra de risco.

Você pode ajustar os valores a serem usados na **Regra de risco padrão** e quanto peso atribuir a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a **Pontuação de risco**.

Cada regra tem uma configuração de **Ordem**, no entanto, a primeira a corresponder às condições atualiza o campo **Pontuação de risco** no AVI. Regras de calculadora sem script normalmente criam menos impacto no desempenho do que as regras de calculadora com script.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ponderações de pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação e classificação de risco com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio *Update Risk Rating from Risk Score* na tabela de itens vulneráveis é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Antes da versão 17.1 da aplicação Resposta a vulnerabilidades (VR), as seguintes classificações de risco eram fornecidas como parte da inclusão de script `VulnerabilityUtils`, que era codificada.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

A partir da versão 18.0 de Resposta a vulnerabilidades,

- Os tipos de classificação de risco são enviados na tabela base como avr_risk_rating. Esses tipos são passados como parte da regra de negócio em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e regras de negócio relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as vulnerabilidades e exposições comuns associadas (CVEs) ou entradas de terceiros (TPEs) nos itens de vulnerabilidade (VIs) estão vinculadas a uma vulnerabilidade de exploração conhecida (KEV) de CVE.

Definir campos e pesos para a regra de risco

Personalize os parâmetros e pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de vulnerabilidade e ativo exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Função necessária: sn_vul.app_manage_risk_score_configuration

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Na página Calculadoras de vulnerabilidade, clique **em Calculadora de risco avançado**.
3. Navegar até **Página da Calculadora de vulnerabilidade** > **Guia Regras da calculadora de vulnerabilidade** > **Regra de Risco Padrão**.
4. Opcional: Na seção Critérios da calculadora de risco da página Regra de risco de vulnerabilidade, defina o peso de cada critério de acordo com sua importância no cálculo de pontuação de risco geral.
5. Para desativar a regra, você deve desmarcar a caixa de seleção **Ativo**.
6. Para adicionar campos de regra de risco aos critérios da calculadora de risco, clique em **Adicionar critérios**.
7. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	Tabela que você usa para definir o peso da pontuação de risco. Você pode selecionar uma destas opções: ◦ **Item vulnerável da aplicação**: adicione campos que são diretamente percorridos por pontos a partir do item vulnerável (VI). ◦ **Item vulnerável da aplicação - Item de configuração**: adicione campos de referência com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela base (cmdb_ci). ◦ **Item vulnerável da aplicação - Vulnerabilidade**: adicione campos de referência com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, Entrada de terceiro. Esses campos não fazem parte da tabela base de entrada de vulnerabilidade. ◦ **Tabela de referência de item vulnerável da aplicação**: adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao item vulnerável. Esses campos não são passíveis de referência com pontos diretamente do VI. ◦ **Tabela de referência de item de configuração**: adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	não são passíveis de referência com pontos diretamente do VI. ◦ **Tabela de referência de vulnerabilidade**: adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vul_entry ou tabelas que têm uma referência a sn_vul_entry. Esses campos não são passíveis de referência com pontos diretamente do VI. ◦ **Condições personalizadas**: use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Tabela	Campo que aparece somente quando uma das seguintes opções é selecionada na tabela Escolher referência: ◦ **Item vulnerável da aplicação -> Item de configuração** ◦ **Item vulnerável da aplicação -> Vulnerabilidade** ◦ **Tabela de referência do item vulnerável da aplicação** ◦ **Tabela de referência do item de configuração** ◦ **Tabela de referência de vulnerabilidade**
Campo	Campo a ser usado para cálculo de pontuação de risco para esta regra.
Agregação	Campo que aparece somente quando uma tabela de referência é selecionada em Escolher tabela de referência. Selecione o valor mínimo ou máximo a ser considerado para cálculos quando Campo for selecionado nas Tabelas relacionadas (m2m).
Ponderação	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Definir ponderação de valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, os valores de campo podem ser definidos como um intervalo (por exemplo, 1–5). Os pesos devem ser um número inteiro entre 0 e 100.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo não aparecerá se a opção Condições personalizadas for selecionada na tabela Escolher referência.
Tabela de condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Selecione uma condição na lista.
Nome do campo	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Insira um nome para os critérios de risco.
Condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Visualize os itens nesta tabela que correspondem às condições definidas.

8. Clique em **Enviar**.
9. Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco nos itens vulneráveis ativos.

Example:
Adicione a gravidade de origem como um critério para uma regra de risco.

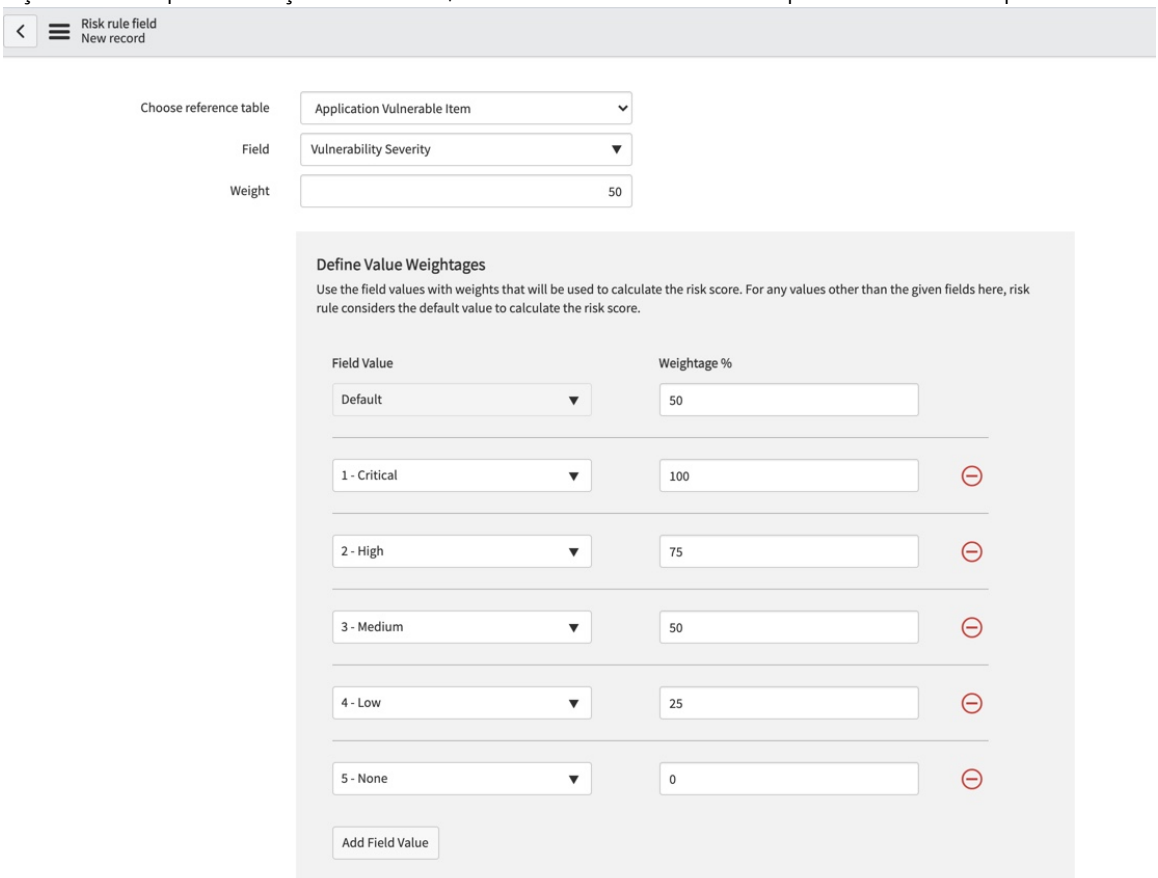
Caso de uso: fornecedores de terceiros, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo **Gravidade de origem** na tabela sn_vul_entry. Use este campo para cálculos de pontuação de risco. Para usar esta pontuação para calcular a pontuação de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos critérios da calculadora de risco, clique em **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione o **item Vulnerável da aplicação**.
5. Na lista Campo, selecione **Vulnerability.Severity**.
6. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Na seção Definir ponderação de valor, adicione valores de campo e atribua um peso a eles.



8. Clique em **Enviar**.

Informações relacionadas

Calculadoras da Resposta a vulnerabilidades e regras da calculadora de vulnerabilidade

Criar uma calculadora de vulnerabilidade da aplicação

Uma calculadora de vulnerabilidade da aplicação é uma fórmula predefinida para calcular um campo de destino quando determinados critérios são atendidos. As calculadoras, que calculam a **pontuação de risco**do item vulnerável da aplicação (IVA), podem conter **regras de risco**. Os cálculos de risco oferecem informações sobre como priorizar a correção.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Nota: Você pode notar uma degradação no desempenho ao executar calculadoras de vulnerabilidade de aplicações que contêm scripts.

Ordene suas regras para executar as regras mais simples primeiro. Execute scripts somente nos itens que não podem ser tratados com uma condição e valor de modelo ou uma regra de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Formulário de calculadora de vulnerabilidade

Campo	Descrição
Nome	O nome da calculadora de vulnerabilidade da aplicação.
Tabela	Preenchido automaticamente com o nome da tabela AVI.
Aplicação	Preenchido automaticamente com Resposta a vulnerabilidades.
Campo de destino	Campo a ser calculado.
Descrição	Descrição de texto da calculadora.
Ativo	Ligue ou desligue a calculadora.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar**.
   A seção **Regras da calculadora de vulnerabilidade** é exibida.
5. Crie uma regra para a calculadora clicando em **Novo**.

> **Nota:** Para o formulário **Novas regras de risco** (disponível somente quando o **campo Destino** é **Pontuação de risco**), consulte a etapa 10.

6. Preencha os campos, se for o caso.

Formulário Regra da calculadora de vulnerabilidade

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionadas, as condições com script e os valores com script podem ser selecionados em Tipo de **condição** e **Tipo de valor**.

7. Preencha os campos na guia **Quando esta condição for atendida**, conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Quando esta condição for atendida

Campo	Descrição
Tipo de condição	Disponível quando você seleciona a **exibição Avançada**. As opções incluem: ◦ Filtro: usa condições de filtro. ◦ Grupo de filtros: consulte criar e definir grupos de filtros para definir os critérios da calculadora. ◦ Script: condição de script usada para determinar quando aplicar esta calculadora. **Nota:** Antes de escrever scripts para determinar quando aplicar as calculadoras, retorne à lista **Calculadoras de vulnerabilidade da aplicação**. Explore os registros da calculadora de vulnerabilidade enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada ou não. A seleção dos tipos **Grupo de filtros** ou Condição de **script** oculta este campo.

8. Clique na guia **Definir estes valores** e preencha os campos no formulário, conforme apropriado.

Guia Definir estes campos

Campo	Descrição
Tipo de valor	Disponível quando você seleciona a **exibição Avançada**. As opções incluem: ◦ Modelo: defina os valores a serem definidos em cada campo. ◦ Script: usado para definir os valores em cada campo.
Valores de Script	Disponível se você selecionou o tipo de valor **Script**. Define a quais valores os cálculos serão aplicados.
Modelo	Selecione os campos e valores que você deseja usar para a calculadora. A seleção do tipo de valor **Script** oculta este campo.

9. Quando tiver concluído todas as entradas, clique em **Enviar**.

Nota: Ao editar uma calculadora existente e quiser atualizar todas as pontuações existentes, você pode usar o botão **Reaplicar calculadora**. Ele é executado em todos os AVIs ativos e, se essa calculadora for usada para definir seu valor, recalculará o valor desses AVIs. Como a reaplicação de uma calculadora pode levar muito tempo, um trabalho agendado lida com isso.

10. Para o formulário **Novas regras de risco**, preencha os campos conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

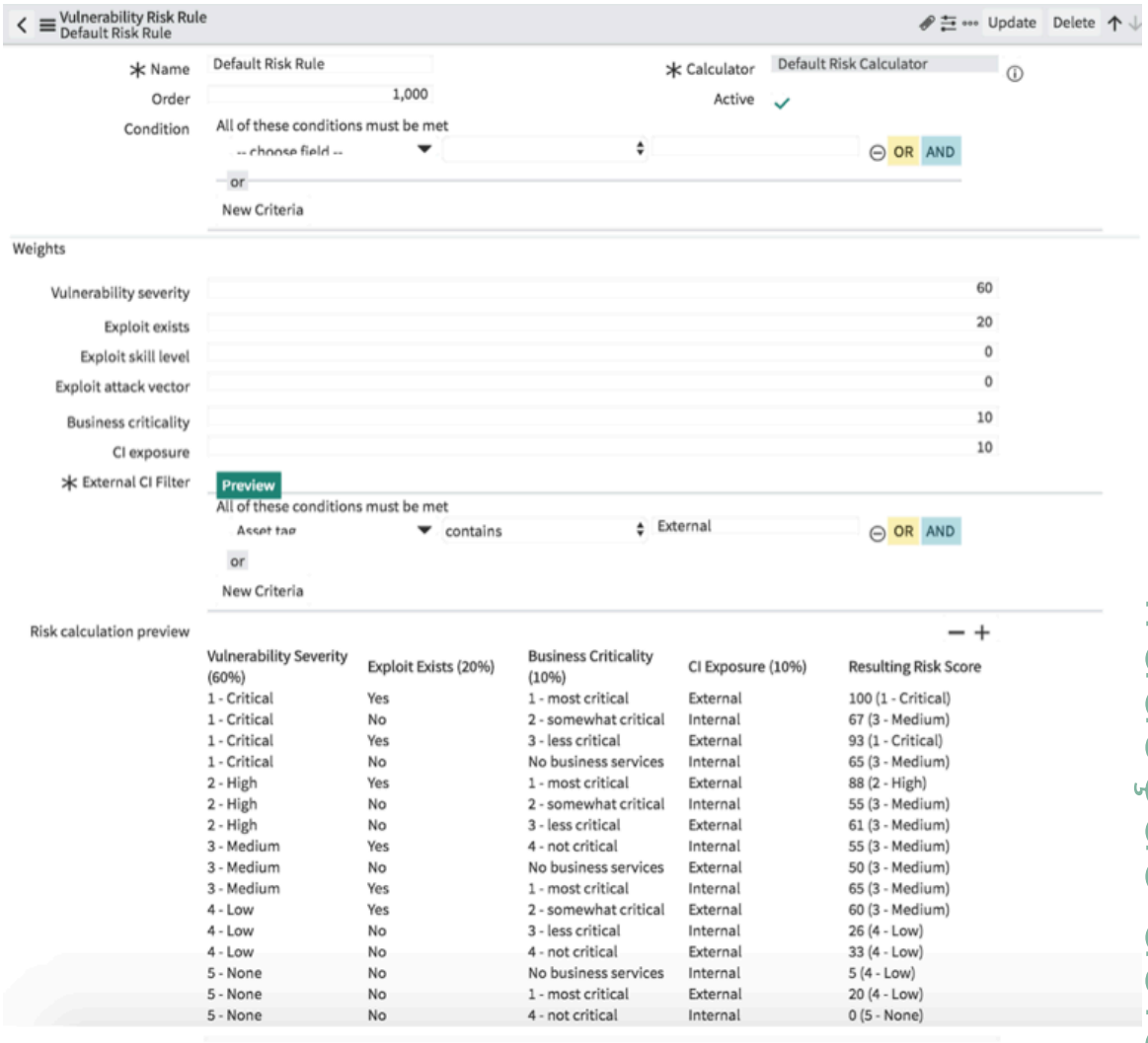
Defina cada peso de acordo com a porcentagem do resultado que deve vir desse valor. Para todos os dados que o scanner não fornecer ou para dados que não devam fazer parte da pontuação de risco, defina o peso como zero.

Conforme você atualiza os pesos, os cenários exibem os pesos restantes, bem como os resultados de **pontuação de risco** antecipados.

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora será executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada. A seleção dos tipos **Grupo de filtros** ou Condição de **script** oculta este campo.
Pesos	
Severidade da Vulnerabilidade	Percentual do resultado proveniente da gravidade.
10 principais da OWASP	Percentual do resultado proveniente da presença da vulnerabilidade na lista das 10 principais da OWASP. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
25 principais da SANS	Porcentagem do resultado que vem da presença da vulnerabilidade na lista das 25 principais da SANS. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Total da execução	Percentuais totais calculados automaticamente. Quando esse valor atinge 100, a visualização do cenário mostra amostras de pontuações de risco em diferentes cenários.
Cenários de exemplo	Quando todos os pesos totalizam 100%, os cenários de pontuação de risco são exibidos, fornecendo uma visualização da pontuação de risco em alguns dos cenários possíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Clique em **Enviar**.

Mapear a gravidade de um item vulnerável de aplicação automaticamente

Resposta a vulnerabilidades de aplicações mapeamento de severidade transforma campos de severidade de origem de terceiros em campos reconhecíveis em Resposta a vulnerabilidades.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Resposta a vulnerabilidades de aplicações integrações de terceiros, como Veracode Vulnerability Integration, fornecem mapeamentos de gravidade na instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

A criação ou a edição de um mapa de severidade se destina somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente e requer a experiência de Resposta a vulnerabilidades de aplicações e ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Mapeamento de gravidade normalizada**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Mapeamento de campo

Campo	Descrição
Origem	O nome da origem do mapeamento de gravidade.
Valor de origem	O valor da severidade de origem.
Valor de meta	O valor da severidade desejada. As opções são: ◦ 1- Crítica ◦ 2 - Alto ◦ 3 – Médio ◦ 4 - Baixo(a) ◦ 5 - Nenhum

4. Repita a Etapa 3 para cada nível de severidade de origem.
5. Clique em **Enviar**.

Filtrando em Gestão de vulnerabilidades de aplicações

Calculadoras e Regras de atribuição usam condições durante a importação, criadas usando o **Construtor de condições**. As mudanças nos critérios podem afetar o desempenho, já que cada registro é avaliado usando esses filtros.

As regras e calculadoras enviadas com o sistema base são otimizadas para desempenho. A edição ou criação de regras ou calculadoras é cuidadosa e pode exigir a experiência de ServiceNow e Resposta a vulnerabilidades de aplicações. Dito isso, algumas orientações estão disponíveis.

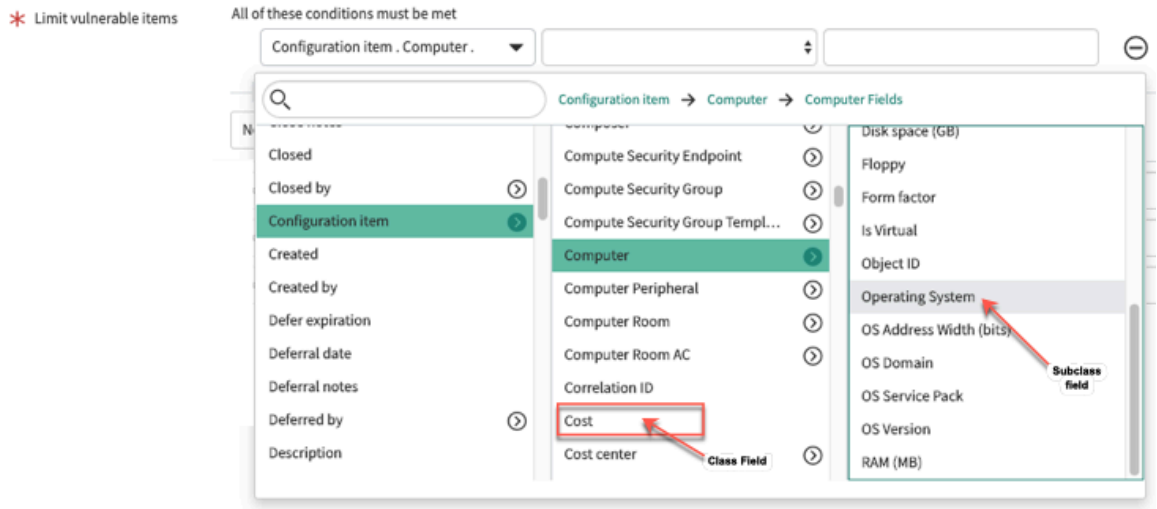
Evite filtrar com base em campos de subclasse

Algumas tabelas oferecem suporte à extensão. Um exemplo disso é a tabela IC do CMDB [cmdb_ci]. Tabelas como cmdb_ci_hardware e cmdb_ci_computer estendem esta tabela. Se você filtrar com base em um campo que não está na tabela primária, esse filtro pode ser caro para construir e avaliar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Menu suspenso de filtro de condição



Por exemplo, filtrar em **Item de Configuração** > **Custo** não afetaria negativamente o desempenho porque **Custo** é um campo de classe, e não um campo de subclasse, do **Item de configuração**.

Item de Configuração > **Computador**, no entanto, é uma subclasse que requer uma referência com pontos para outro campo, neste caso, **Sistema operacional**. Esse processo pode levar muitos milissegundos, que se somam rapidamente, quando milhões de itens vulneráveis estão sendo importados e afetam o desempenho.

Nota: O uso da condição [contém] é como uma pesquisa curinga e pode causar impacto no desempenho. Usar [is], sempre que possível, é mais eficiente.

Automatizar o acompanhamento da meta de correção no Resposta a vulnerabilidades de aplicações

As Regras de destino de correção da aplicação definem o intervalo de tempo esperado para corrigir itens vulneráveis de aplicação (IVAs), fornecendo um intervalo de tempo para corrigir a própria vulnerabilidade. Por exemplo, se um item vulnerável de aplicação contiver uma classificação de risco crítica, a vulnerabilidade nesse item precisará ser corrigida em 15 dias.

Os gerentes de App-Sec podem criar regras de destino de correção de aplicação definindo:

- A meta de correção.
- O destino do lembrete.

Os gerentes de App-Sec podem ver a data da meta de correção no formulário AVI e nas exibições de lista. No entanto, as datas não são atualizadas para AVIs no estado **Adiado**, **Resolvido**ou **Encerrado**.

A **data da meta** de correção é codificada por cores na exibição de lista do AVI como pontos, da seguinte forma:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- IVAs que não atingiram a data de notificação são mostrados em verde.
- Os IVAs que se aproximam da data da meta de correção são mostrados em laranja.
- IVAs após a data de meta de correção são mostrados em vermelho.

Regras padrão

Resposta a vulnerabilidades de aplicações vem com três regras padrão que estão inativas por padrão:

- Regra de classificação de risco crítico: uma meta de correção com uma classificação de risco **1-Crítico**, uma meta de correção de 15 dias e um lembrete de **7** dias antes da data prevista.
- Regra de classificação de risco médio-alto: uma meta de correção com uma classificação de risco **2-Alto** ou **3-Médio**, uma meta de correção de 30 dias e um lembrete de **7** dias antes da data de destino.
- Regra de classificação de risco menos crítico: uma meta de correção com uma classificação de risco **4-baixo**, uma meta de correção de 45 dias e um lembrete de **7** dias antes da data de destino.

As regras de destino de correção podem ser desativadas ou excluídas

Quando uma regra é desativada, as datas de meta de correção atuais dos IVAs aos quais ela foi aplicada são apagadas. Se um AVI atender a qualquer regra ativa, essa regra será aplicada, caso contrário, o AVI não terá regra ou data de destino e seu status será **Sem destino**.

Quando as regras são excluídas, a data de **meta** de correção e os campos relacionados nos AVIs encerrados são preservados. A data de **meta** de correção e os campos relacionados em AVIs não encerrados são limpos e todas as regras dependentes são reaplicadas.

Cenário da regra de correção

Quando várias regras de destino de correção são aplicadas ao mesmo AVI, a regra mais restritiva é aplicada.

Por exemplo, se um AVI atender à condição para duas regras de destino de correção de aplicação:

Cenário: AVI aberto pela última vez em 01/03/2018 às 10:00:00.

- Regra de meta de correção da aplicação 1: Aberto pela última vez em 03/07/2018; a meta de correção é de 15 dias desde que foi aberta pela última vez; A data da meta de correção calculada é 16/03/2018 10:00:00.
- Regra de meta de correção da aplicação 2: Aberto pela última vez em 10/03/2018; a meta de correção é de 10 dias desde que foi aberta pela última vez; A data da meta de correção calculada é 11/03/2018 10:00:00.

Neste cenário, a regra 2 de meta de correção da aplicação se aplica ao AVI, já que ele tem a data mais restritiva. 10 dias desde que o IVA foi identificado pela primeira vez versus 15 dias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As metas de correção da aplicação são calculadas a partir da data da **última abertura** mais o número de dias (medidos como incrementos de 24 horas). Você pode adicionar este campo ao formulário AVI a partir do slushbucket de Layout de formulário. É a data em que o AVI foi aberto mais recentemente em sua instância.

A partir da V17.1, as metas de correção são calculadas a partir da **meta de (data)**. O valor padrão permanece **Data da última abertura**.

Nota: Depois que a regra de meta de correção da aplicação é definida, as datas de meta de correção são calculadas pelo trabalho agendado *Evaluate remediation targets* ou pelo botão **Aplicar mudanças** na exibição de lista Regras de meta de correção.

Sobre o trabalho agendado Avaliar metas de correção

Evaluate remediation targets é executado uma vez às 4:00:00 diariamente.

Evaluate remediation targets itera por meio de todas as regras de vulnerabilidade ativas, começando com as regras com a data de meta de correção mais antiga. Ele verifica todos os AVIs que:

- Não estão em um estado **Encerrado**, **Adiado**ou **Resolvido**.
- Não têm data de meta de correção.
- Ter uma data de meta de correção posterior à data na regra de meta de correção da aplicação.

Evaluate remediation targets adiciona uma data de meta de correção, se não existir uma, ou se esta regra contiver uma data anterior à do registro, ela atualizará a data de meta existente. Por fim, ele atualiza os campos **Data de meta** de **correção e Status** da correção no formulário AVI. Para regras inativas, **Avaliar metas de correção** limpa os campos de correção no AVI.

Reaplicar regras de destino de correção

Ao alterar uma regra de destino de correção, use o botão **Aplicar mudanças** na página da lista Regras de destino de correção para executar novamente todas as regras alteradas em todos os AVIs abertos ativos, exceto aqueles no estado **Encerrado**, **Adiado** ou **Resolvido**.

Nota:

Se o trabalho agendado, *Evaluate remediation targets* estiver em execução, você não poderá iniciar um processo de reaplicação. No entanto, se um processo de reaplicação já estiver em execução e o trabalho agendado for acionado, eles serão executados em paralelo.

Os processos de reaplicação em Resposta a vulnerabilidades e Resposta a vulnerabilidades de aplicações são independentes e podem ser executados em paralelo.

Criar ou editar regras de destino de correção da aplicação

Conduza a correção de vulnerabilidades de alto risco em tempo hábil configurando uma regra de meta de correção no nível do item vulnerável da aplicação (IVA).

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O sistema base é fornecido com três regras de destino de correção.

- Regra de classificação de risco crítico
- Regra de classificação de risco menos crítico
- Regra de classificação de risco médio-alto

Essas regras estão inativas por padrão. Se você optar por editar um, em vez de criar um novo, lembre-se de marcar a caixa**Ativo** antes de salvar.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Administração** > **Regras de destino de correção**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	Nome da regra.
Meta (dias)	Especifique o número de dias em que os AVIs devem ser corrigidos, desde a última abertura.
V17.1: destino de (data)	Data a partir do momento em que os SLAs de destino são calculados. Você pode especificar somente a data ou os campos de tipo de data e hora. O valor padrão é Data da última abertura. Para personalizar os valores deste campo, consulte KB1642413 .
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra de meta de correção está ativa. Se esta caixa de seleção estiver desmarcada, esta regra não se aplicará aos novos IVAs criados no sistema.
Notificar (dias antes do vencimento)	Número de dias antes do tempo de correção de destino para um lembrete a ser definido. A data de notificação calculada usando este valor é usada para mostrar o status de correção e a codificação de cores. Se a data for anterior à data de notificação, o status da correção será "Em andamento". Se já tiver passado da data de notificação e for anterior à data da meta de correção, o status será mostrado como se aproximando da meta. **Nota:** Se este campo estiver definido como 0, somente uma notificação de **destino não atingido** será definida.
A regra se aplica a	Usando o filtro de condição, selecione os critérios para aplicar a regra aos AVIs. Para evitar impacto no desempenho, teste suas condições em toda a escala de produção. Os testes permitem que você determine quanto tempo o trabalho **Avaliar metas de correção** leva para ser executado, de acordo com as condições e o tamanho do seu Configuration Management Database (CMDB).
Atualizar histórico	
Atividades	Não usado para a criação inicial de uma regra. Posteriormente, as anotações de trabalho do sistema são registradas aqui.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta regra entra em vigor durante a próxima execução do trabalho agendado, *Evaluate remediation targets*. O mesmo se aplica quando uma regra existente é atualizada ou ao usar o botão **Aplicar mudanças** na exibição de lista Regras de destino de correção. O mesmo acontece quando uma regra existente é atualizada. Para obter mais informações sobre o trabalho agendado e **Aplicar mudanças**, consulte Automatizar o acompanhamento da meta de correção no Resposta a vulnerabilidades de aplicações.

Exibir o status da meta de correção de um item vulnerável da aplicação

Quando um item vulnerável de aplicação (IVA) quase atingiu (ou passou) sua data de meta de correção, conforme definido por uma regra de meta de correção, o registro AVI é atualizado com um status. Essas informações podem ajudá-lo a monitorar proativamente as próximas atividades de correção.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
O trabalho agendado **Avaliar metas de correção** é executado uma vez por dia para comparar a data atual com a data de correção do item vulnerável especificada na regra de meta de correção associada. Quando a data atual estiver dentro do número de dias anteriores ao vencimento da correção, um status de correção será adicionado ao registro do item vulnerável.

Procedimento

Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis**.
Se a data de correção do AVI estiver dentro do intervalo das condições definidas na regra de meta de correção, verifique as colunas Status da meta de correção, visíveis na exibição de lista de itens vulneráveis. Se a data da meta de correção tiver passado para um AVI, uma anotação será exibida no formulário AVI.

Nota: Para exibir o número de AVIs que estão **Aproximando**-se da meta , **Em curso**e**Meta passada**, consulte Painel Gestão de vulnerabilidades de aplicações [PA].

Informações relacionadas

Criar ou editar regras de destino de correção da aplicação

Fechar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção de aplicação pode ser encerrado imediatamente sem análise adicional, poderá usar o recurso **Fechar**. A partir da v23.0 de Resposta a vulnerabilidades, o botão **Fechar** foi removido para uma tarefa de correção de aplicação.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Nos espaços Resposta a vulnerabilidades, uma tarefa de correção passa pelos mesmos estados que uma tarefa de correção anterior tinha nas versões anteriores do Resposta a vulnerabilidades. Quando todos os itens vulneráveis (VITs) em uma tarefa de correção são encerrados, a tarefa de correção faz a transição para o estado Inativo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção , a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados `Encerrado` ou `Adiado`.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Selecione o botão **Fechar**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Estado	Selecione o estado como Encerrado.
Motivo	Insira o motivo para fechar o problema.
Informação adicional	Insira outras informações relevantes.

4. Selecione **Enviar**.
   A tarefa de correção é marcada como **Encerrada**.

Teste de invasão

O teste de invasão em Resposta a vulnerabilidades de aplicações permite que os responsáveis pela aplicação avaliem a postura de segurança de sua aplicação. É o teste manual de uma aplicação pela equipe de hacking ético.

Funções necessárias

O teste de invasão requer as seguintes funções:

Gerente App-Sec: contém gerentes de segurança e responsáveis pela aplicação que gerenciam as solicitações de avaliação de teste de invasão. Ele contém as seguintes funções granulares:

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

Ethical Hacker: contém membros da equipe de hacking ético que realizam testes de invasão de aplicações. Inclui as seguintes funções granulares:

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_read_all

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Para obter mais informações sobre essas funções, consulte Resposta a vulnerabilidades de aplicações grupos de usuários e funções.

A partir da v19.0 de Resposta a vulnerabilidades, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais do Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão configurada em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte Veracode Vulnerability Integration.

Ciclo de vida do teste de invasão

Como proprietário da aplicação, você pode solicitar à equipe de invasão ética uma avaliação de teste de invasão da sua aplicação. A equipe de invasão ética atua nesta solicitação e cria descobertas de testes de invasão. Essas descobertas são Itens vulneráveis de aplicação (IVAs) criados manualmente.

O fluxo de trabalho de teste de invasão cobre o ciclo de vida do teste de invasão, desde a solicitação de teste até a resolução das descobertas da equipe de invasão ética.

Como solicitar uma avaliação de teste de invasão

A partir da v19.0, você pode criar novas solicitações ou copiar solicitações existentes em **Todos** > **Solicitações de avaliação de teste de invasão** > **Todos**.

Antes da v19.0, como proprietário da aplicação, você pode solicitar uma avaliação de teste de invasão para sua aplicação usando o Catálogo de serviços do ITSM.

Como revisar a solicitação de avaliação de teste de invasão

A equipe de invasão ética revisa e avalia a aplicação e o escopo da solicitação de avaliação de teste de invasão e os adiciona ao backlog existente.

Preparando um ambiente

A equipe de invasão ética envia uma solicitação ao proprietário da aplicação para fornecer um ambiente para que ele comece a testar. Quando o ambiente estiver pronto, o responsável pela aplicação informará a equipe de invasão ética.

Para obter mais informações sobre como configurar solicitações de teste, consulte Configurar teste de invasão.

Como testar e relatar as descobertas do teste de invasão

A equipe de invasão ética testa a aplicação e relata as descobertas ao proprietário da aplicação. A equipe de invasão ética também define os Acordos de nível de serviço (ANSs) para as descobertas do teste de invasão usando a data de meta de correção. Essas descobertas são os AVIs criados manualmente. O proprietário da aplicação, por sua vez, revisa os AVIs criados pela equipe de invasão ética. Eles planejam as correções e as atribuem à equipe de aplicações.

Nota: As regras de destino de correção não se aplicam às descobertas do teste de invasão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A equipe de invasão ética pode criar uma biblioteca de entradas de vulnerabilidade da aplicação (AVEs) e reutilizá-las ao relatar os AVIs. Eles também podem rastrear o status das descobertas do teste de invasão.

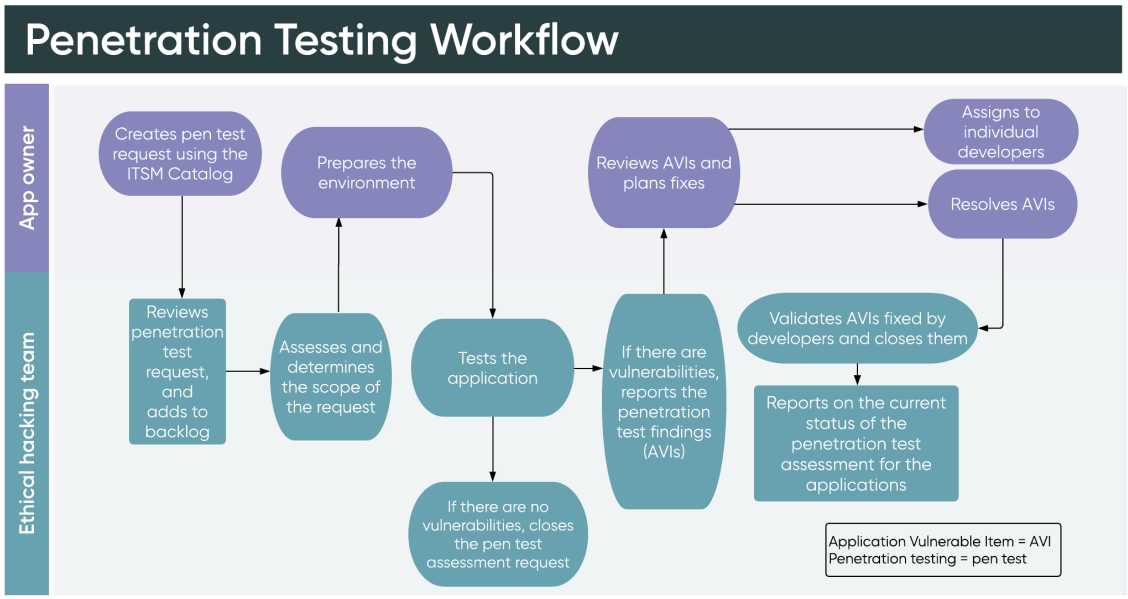
Corrigindo e validando as descobertas do teste de invasão

Depois que as descobertas do teste de invasão são corrigidas e resolvidas pela equipe de aplicações, as correções são validadas manualmente e encerradas pela equipe de invasão ética.

Gestão de vulnerabilidades de aplicações relatórios

Use os relatórios disponíveis no Gestão de vulnerabilidades de aplicações painel do PA para rastrear as descobertas do teste de invasão.

Ciclo de vida do teste de invasão



Criar uma solicitação de avaliação de teste de invasão a partir de solicitações existentes (v19.0)

A partir da v19.0, você cria solicitações de avaliação de teste de invasão diretamente da lista de solicitações existentes. Você também pode copiar solicitações existentes no estado Fechado nesta lista para criar solicitações.

Antes de Iniciar
Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
A partir da v19.0 de Resposta a vulnerabilidades, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais do Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão configurada em Resposta a vulnerabilidades de aplicações. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte Veracode Vulnerability Integration.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Solicitações de avaliação de teste de invasão** > **Todos**.
2. Opcional: Como alternativa, você pode criar uma solicitação replicando solicitações encerradas.
   Todos os valores da solicitação original são preservados no novo formulário. Os itens vulneráveis da aplicação (IVAs) ativos são copiados automaticamente para a nova solicitação. Selecione **Copiar e criar solicitação** nos registros no estado Fechado.
3. Selecione Novo e preencha os campos.

Formulário de solicitação de avaliação de teste de invasão

Campo	Descrição
Número	Identificador exclusivo gerado para a solicitação de avaliação de teste de invasão.
Estado	Selecione um valor com base no status da solicitação.
Solicitados por	Pessoa que está solicitando a avaliação da aplicação.
Grupo de atribuição	Grupo selecionado para trabalhar nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente do App-Sec. Para configurar grupos, consulte Configurar teste de invasão.
Aplicação	Selecione uma aplicação usando a opção de pesquisa.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente do App-Sec.
Tipo de aplicação	Selecione uma opção de: ◦ Serviço web (conhecido como API antes da v16.1) ◦ Aplicação Web ◦ Cliente espesso ◦ Móvel (se você selecionar **Móvel**, a guia Móvel será exibida na parte inferior do formulário com campos adicionais)
Sprint	Exibe os sprints com largura de banda disponível para acomodar a solicitação de avaliação com base no campo Tipo de avaliação selecionado. Consulte Configurar sprints para testes de invasão e Configurar tipos de avaliação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	para testes de invasão para obter mais informações sobre como modificar a capacidade de sprint e testar o escopo.
v19.0: tamanho da aplicação	Selecione o tamanho da aplicação que você deseja testar. ◦ Pequeno ◦ Médio(a) ◦ Grande ◦ Padrão (selecione esta opção se você não tiver certeza do tamanho) Consulte mais Configurar teste de invasão mais informações sobre como modificar a capacidade de sprint e testar o escopo com o tamanho da aplicação e a capacidade de sprint.
Criação	Data e hora em que a solicitação foi criada.
Tipo de avaliação	Selecione o tipo de avaliação em: ◦ Teste de invasão completo ◦ Teste focado ◦ Testar novamente Para obter mais detalhes sobre como testar combinações e testar escopo, consulte Configurar tipos de avaliação para testes de invasão.
Atualizado em	Data e hora em que a solicitação foi atualizada pela última vez.
Data da demonstração	Data em que esta aplicação pode ser demonstrada.
Implantação de produto planejada em	Data planejada para implantar esta aplicação na produção.
Versão/liberação da aplicação planejada para implantação	Versão da aplicação planejada para implantação de produção.
v19.0: aplicação de propriedade de fornecedor terceirizado ou de uma guia de empreendimento conjunto Se você selecionar Sim para este campo, a guia Informações do fornecedor/ empreendimento conjunto será exibida. Preencha os campos adicionais.	
Existe uma cláusula que nos permite realizar o teste de invasão?	O termo "Cláusula" pode se referir a padrões de teste que incluem quaisquer acordos existentes entre duas ou mais partes que você deseja adicionar. Se você selecionar **Sim**, adicione a cláusula.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
A cláusula que cita a permissão para executar o teste de invasão	
Nome jurídico completo e endereço do fornecedor	
Sistema de detecção de intrusão	
Contato técnico do fornecedor	
As informações registradas em log foram revisadas de atividades mal-intencionadas?	
A aplicação é hospedada por outro fornecedor terceirizado?	
Contato do fornecedor que encerrará o teste de invasão	
Guia Detalhes da aplicação	
Finalidade da aplicação	Descrição da funcionalidade da aplicação.
Detalhes das stacks de tecnologia	Pilha de tecnologia completa do front-end ao back-end, bancos de dados e outras tecnologias importantes.
É uma aplicação de terceiros?	Confirma se esta aplicação pertence a um fornecedor terceirizado.
Tipos de lista de dados confidenciais acessíveis pela aplicação	Tipos de dados confidenciais acessíveis pela aplicação. Por exemplo, dados PII, dados PHI e dados financeiros, como números de cartão de crédito.
Tipo de autenticação	Especifica se esta aplicação usa autenticação LDAP, sua própria autenticação nativa ou outras formas de autenticação.
A aplicação está no escopo de algum programa de conformidade?	Especifica se esta aplicação afeta quaisquer programas de conformidade, como PCI.
Contatos da equipe de aplicações	Membros da equipe de aplicações a serem contatados pela equipe de invasão ética em caso de dúvidas.
Lista de programas de conformidade	
Interfaces ou aplicações de terceiros relacionados	
Endereço IP	
Número aproximado de usuários na produção?	
Existe um script automatizado?	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
A versão de produção deste app é externa?	
v 19.0: Impacto nos negócios	
Dano financeiro	Selecione uma opção da lista.
Não conformidade	Selecione uma opção da lista.
Dano à reputação	Selecione uma opção da lista.
Violação de privacidade	Selecione uma opção da lista.
Guia Detalhes de teste	
URLs para teste	URLs que devem ser incluídos no teste de invasão.
URLs a serem excluídos	URLs que devem ser excluídos do teste de invasão.
Essa aplicação já foi testada?	Especifica se esta aplicação já foi testada contra invasão.
Motivo para testar novamente	Motivo para solicitar uma reavaliação do teste de invasão se a aplicação tiver sido testada anteriormente.
Quando a aplicação foi testada?	Intervalo de tempo em que a aplicação foi testada quanto à invasão.
Detalhes da conta de teste	Detalhes da conta de teste que pode ser usada pela equipe de invasão ética para testes de invasão.
Funções da aplicação	Funções compatíveis com a aplicação para seus usuários.
Funções mais usadas	Funções mais usadas na aplicação.
Guia Comentários adicionais	
Anotações de trabalho	

Tradução automática

4. Selecione **Salvar** para salvar suas edições ou **Enviar** para iniciar a solicitação.

Criar uma solicitação de avaliação de teste de invasão (anterior à v19.0)

Inicie uma solicitação de avaliação de teste de invasão para suas aplicações web ou APIs. Essas solicitações são enviadas para a equipe de hackers éticos, que prossegue para testar essas aplicações e relatar manualmente as descobertas do teste de invasão.

Antes de Iniciar

Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

O proprietário da aplicação gera uma solicitação de avaliação de teste de invasão para verificar manualmente sua aplicação ou APIs. A equipe de invasão ética testa a aplicação e cria manualmente as descobertas do teste de invasão. Essas descobertas são itens vulneráveis da aplicação (IVAs) criados manualmente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O grupo de atribuição padrão para a descoberta do teste de invasão é o grupo configurado no campo "Equipe da aplicação" da solicitação de avaliação do teste de invasão associada. O tipo de atribuição da descoberta do teste de invasão é Manual. As regras de atribuição não podem substituir a atribuição dessas descobertas de teste de invasão.

A partir da v19.0, você pode criar solicitações de avaliação de teste de invasão diretamente da tabela Solicitações de avaliação de teste de invasão [sn_vul_pen_test_assessment_request_list]. Para obter mais informações, consulte Criar uma solicitação de avaliação de teste de invasão a partir de solicitações existentes (v19.0).

Procedimento

1. Antes da v19.0, navegar para **Todos** > **Autoatendimento** > **Catálogo de serviços** > **Serviços** > **Solicitação de avaliação de teste de invasão**.
2. Opcional: Como alternativa, você pode criar uma solicitação replicando solicitações encerradas.
   Todos os valores da solicitação original são preservados. Os itens vulneráveis da aplicação (IVAs) ativos são copiados automaticamente para a nova solicitação.
3. No formulário, preencha os campos.

Formulário de solicitação de avaliação de teste de invasão

Campo	Descrição
Número	Identificador exclusivo gerado para a solicitação de avaliação de teste de invasão.
Solicitados por	Pessoa que está solicitando a avaliação da aplicação.
Solicitação de avaliação primária	Solicitação de avaliação de teste de invasão original usada para criar a solicitação secundária. Ele é criado usando uma solicitação de avaliação encerrada. Visível somente no formulário de solicitação de avaliação secundária.
Aplicação	Selecione uma aplicação usando a opção de pesquisa.
Tipo de aplicação	Selecione uma opção de: ◦ Serviço Web (conhecido como API antes da v16.1) ◦ Aplicação Web ◦ Cliente espesso ◦ Móvel (se você selecionar Móvel, a guia Móvel será exibida na parte inferior do formulário com campos adicionais)
v19.0: tamanho da aplicação	Selecione o tamanho da aplicação que você deseja testar. ◦ Pequeno ◦ Médio(a)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Grande ◦ Padrão (selecione esta opção se você não tiver certeza do tamanho)
Tipo de avaliação	Selecione o tipo de avaliação em: ◦ Teste de invasão completo ◦ Teste focado ◦ Testar novamente Para obter detalhes, consulte Configurar tipos de avaliação para testes de invasão.
Finalidade da aplicação	Descrição da funcionalidade da aplicação.
Detalhes das stacks de tecnologia	Pilha de tecnologia completa de front-end a back-end, bancos de dados e outras tecnologias importantes.
É uma aplicação de terceiros?	Confirma se esta aplicação pertence a um fornecedor terceirizado.
Tipos de lista de dados confidenciais acessíveis pela aplicação	Tipos de dados confidenciais acessíveis pela aplicação. Por exemplo, dados PII, dados PHI e dados financeiros, como números de cartão de crédito.
Tipo de autenticação	Especifica se esta aplicação usa autenticação LDAP, sua própria autenticação nativa ou outras formas de autenticação.
A aplicação está no escopo de algum programa de conformidade?	Especifica se esta aplicação afeta quaisquer programas de conformidade, como PCI.
Contatos da equipe de aplicações	Membros da equipe de aplicações a serem contatados pela equipe de invasão ética em caso de dúvidas.
Data da demonstração	Data em que esta aplicação pode ser demonstrada.
Implantação de produto planejada em	Data planejada para implantar esta aplicação na produção.
Versão/liberação da aplicação planejada para implantação	Versão da aplicação planejada para implantação de produção.
v19.0: aplicação de propriedade de fornecedor terceirizado ou empreendimento conjunto	Se você selecionar Sim para este campo, a guia Informações do fornecedor/ empreendimento conjunto será exibida com campos adicionais. O termo "Cláusula" pode se referir a padrões de teste que incluem quaisquer acordos existentes entre duas ou mais partes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	Selecione um valor com base no status da solicitação.
Grupo de atribuição	Grupo selecionado para trabalhar nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente do App-Sec.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente do App-Sec.
Sprint	Exibe os sprints com largura de banda disponível para acomodar a solicitação de avaliação com base no campo Tipo de avaliação selecionado.
Criação	Data e hora em que a solicitação foi criada.
Data de início dos testes	Data e hora em que o teste começa.
Atualizado em	Data e hora em que a solicitação foi atualizada pela última vez.
Detalhes do teste	
URLs para teste	URLs que devem ser incluídos no teste de invasão.
URLs a serem excluídos	URLs que devem ser excluídos do teste de invasão.
Essa aplicação já foi testada?	Especifica se esta aplicação já foi testada contra invasão.
Motivo para testar novamente	Motivo para solicitar uma reavaliação do teste de invasão se a aplicação tiver sido testada anteriormente.
Quando a aplicação foi testada?	Intervalo de tempo em que a aplicação foi testada quanto à invasão.
Detalhes da conta de teste	Detalhes da conta de teste que pode ser usada pela equipe de invasão ética para testes de invasão.
Funções da aplicação	Funções compatíveis com a aplicação para seus usuários.
Funções mais usadas	Funções mais usadas na aplicação.

4. Selecione **Enviar**.
   Uma notificação por e-mail é enviada à equipe de invasão ética de que a solicitação foi criada para a aplicação relevante.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Replicar uma solicitação de teste de invasão no estado fechado

Crie uma solicitação de avaliação de teste de invasão replicando uma solicitação no estado Encerrado. Os itens vulneráveis da aplicação (IVAs) ativos são copiados para a nova solicitação.

Antes de Iniciar
Função necessária: equipe de aplicações

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Solicitações de avaliação de teste de invasão** > **Todos**.
2. Selecione uma solicitação no estado Encerrado.
3. Selecione **Copiar e criar solicitação**.
   Uma nova solicitação é criada e os AVIs ativos são copiados para esta solicitação com dados atualizados. Para exibir o estado original dos AVIs da solicitação primária, navegue até a guia **Snapshot de descobertas do teste de invasão**.

Criar descobertas de testes de invasão com base em solicitações de avaliação (anteriores à v19.0)

Crie descobertas de teste de invasão com base na solicitação de avaliação de teste de invasão. Essas descobertas são itens de vulnerabilidade da aplicação (IVAs) criados manualmente.

Antes de Iniciar
Função necessária: Ethical Hacker

Procedimento

1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de serviços** > **Serviços** > **Solicitações de avaliação de teste de invasão**.
2. Para criar um AVI para uma solicitação de avaliação de teste de invasão, selecione a solicitação relevante.
3. Na seção Itens vulneráveis da aplicação, selecione **Novo**.
4. No formulário, preencha os campos.

Formulário de item vulnerável da aplicação (exibição do teste de invasão)

Campo	Descrição
Número	Identificador AVI gerado automaticamente para este registro.
Solicitação de avaliação	Solicitação de avaliação de teste de invasão à qual este AVI está associado.
Vulnerabilidade	Vulnerabilidade selecionada na tabela Entradas de vulnerabilidade usando a opção de pesquisa.
Pontuação de risco	**Pontuação de risco** quantificado que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Calcular risco em

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Resposta a vulnerabilidades de aplicações automaticamente. A partir da V16.1, por padrão, o valor é o mesmo que a gravidade da vulnerabilidade.
Impacta algum programa de conformidade?	Confirma se há um impacto em algum programa de conformidade. As opções são Sim e Não.
Lista de programas de conformidade afetados	Este campo é exibido quando o valor do campo "Afeta qualquer programa de conformidade" está definido como *Yes*. Lista os programas de conformidade afetados.
Versão planejada de liberação/correção	Libere até quando as descobertas do teste de invasão devem ser resolvidas.
Estado	O valor padrão é **Aberto** quando o AVI é criado. Consulte Estados de item vulnerável de aplicação (IVA) para obter mais informações sobre como os estados são mapeados.
Grupo de atribuição	Grupo selecionado para trabalhar neste AVI. Pode ser adicionado ou editado manualmente por um gerente do App-Sec.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha neste AVI. Pode ser adicionado ou editado manualmente por um gerente do App-Sec.
Meta de correção	Data em que os AVIs devem ser corrigidos, desde a primeira identificação. Este campo aparece somente quando aplicável. Para obter mais informações sobre metas de correção, consulte Automatizar o acompanhamento da meta de correção no Resposta a vulnerabilidades de aplicações.
Criação	Carimbo de data/hora da criação do item vulnerável da aplicação (IVA).
Atualizado em	Carimbo de data/hora de quando o item vulnerável da aplicação (IVA) foi atualizado.
Aberto por	Usuário que criou esta descoberta de teste de invasão.
Contato da equipe de segurança	Ponto de contato na equipe de invasão ética.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Breve explicação da descoberta do teste de invasão.
Detalhes	
Detalhes técnicos	Detalhes técnicos da descoberta do teste de invasão.
Impacto	Avaliação do impacto da descoberta do teste de invasão.
Etapas para reproduzir	Documente as etapas para reproduzir e revisar a descoberta do teste de invasão.
Recomendação	Registre as ações recomendadas neste campo.
Anotações	
Anotações de trabalho	Adicione anotações para comunicar informações sobre transições de estado e outras atualizações de campo.
V16.1: URLs afetados	Mais informações relacionadas aos URLs afetados.
V16.1: parâmetros afetados	Mais informações relacionadas aos parâmetros afetados.
V16.1: funcionalidades afetadas	Mais informações relacionadas às funcionalidades afetadas.

5. Para salvar o formulário, selecione **Enviar**.

Criar uma entrada de vulnerabilidade da aplicação

Crie uma entrada de vulnerabilidade da aplicação para a vulnerabilidade especificada para a descoberta do teste de invasão. As vulnerabilidades da aplicação são vulnerabilidades nas aplicações de software personalizadas.

Antes de Iniciar
Função necessária: Ethical Hacker

Por Que e Quando Desempenhar Esta Tarefa
Resposta a vulnerabilidades de aplicações relaciona uma vulnerabilidade a uma aplicação para criar a descoberta do teste de invasão. Essas descobertas são itens vulneráveis da aplicação (IVAs) criados manualmente. Você pode reutilizar uma entrada existente ou criar uma manualmente para cada vulnerabilidade durante o teste de invasão.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Bibliotecas** > **Terceiros**.

2. Na página Entradas de vulnerabilidade da aplicação, selecione **Novo**.

3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Entrada de vulnerabilidade da aplicação (exibição do teste de invasão)

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de gravidade são fornecidos para o NVD e com integrações de terceiros da ServiceNow. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Mapear a gravidade de um item vulnerável de aplicação automaticamente.
CVE primário	Referência ao elemento de Enumeração de Pontos Fracos Comuns em que esta vulnerabilidade se encaixa melhor.
Nome da categoria	Classificação fornecida pela integração de terceiros. Ajuda na atribuição.
Detalhes da Vulnerabilidade	
Vetor de ataque	Vetor de ataque mais vulnerável para esta vulnerabilidade.
Complexidade de ataque	Métrica que descreve as condições além do controle do invasor que devem existir para explorar a vulnerabilidade.
Escopo	Métrica para medir a capacidade de uma vulnerabilidade de software de afetar os recursos além de seus meios.
Integridade	Métrica para medir o impacto na integridade de uma vulnerabilidade explorada com sucesso.
Vetor CVSS	Estrutura aberta para capturar as características e a gravidade das vulnerabilidades do software.
Privilégios necessários (PN):	Nível de privilégios que um invasor deve possuir antes de explorar a vulnerabilidade com sucesso.
Interação do usuário	Requisito de interação humana para explorar com sucesso uma vulnerabilidade.
Confidencialidade	Impacto na confidencialidade dos recursos de informações devido a uma vulnerabilidade explorada com sucesso. Esses recursos são gerenciados por um componente de software.
Disponibilidade	Impacto na disponibilidade do componente afetado resultante de uma vulnerabilidade explorada com sucesso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pontuação base de CVSS	Representação numérica (0-10) da gravidade de uma entrada de vulnerabilidade da aplicação.
Ameaça	Descrição da ameaça desta vulnerabilidade.
Descrição da mitigação	Descrição das etapas para atenuar a vulnerabilidade.

4. Para salvar o formulário, selecione **Enviar**.

Nota: Os AVEs são criados na tabela Entrada de vulnerabilidade da aplicação (sn_vul_app_vul_entry). A tabela Entrada de vulnerabilidade da aplicação é secundária da tabela Entrada de vulnerabilidade (*sn_vul_entry*). Portanto, os AVEs criados também são adicionados à tabela de entrada de vulnerabilidade.

Soluções Análise da plataforma e relatórios para Resposta a vulnerabilidades de aplicações

Soluções Análise da plataforma e relatórios contêm conteúdo Análise da plataforma] pré-empacotado para uso com outros produtos Now Platform. Este Solução Performance Analytics e relatórios apresenta métricas importantes para analisar o processo de Gestão de vulnerabilidades de aplicações.

Visão geral

O pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades está disponível em ServiceNow® Store como uma assinatura separada. A aplicação não é instalada automaticamente com a aplicação Resposta a vulnerabilidades. O pacote de conteúdo da Resposta a vulnerabilidades de aplicações faz parte do pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades.

Para obter mais informações sobre como definir, instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades, consulte Instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades [PA].

Termos principais

Análise de desempenho (PA)

Solução que cria painéis de gestão, relatórios sobre KPIs e métricas e responde a perguntas de negócios importantes para ajudar a aumentar a qualidade e reduzir custos.

Item vulnerável da aplicação (IVA)

Uma vulnerabilidade da aplicação relatada por um scanner de vulnerabilidade de terceiros que está presente em um item de configuração (IC).

Indicador de PA

Define uma medida de desempenho feita em intervalos regulares de uma atividade ou comportamento organizacional, por exemplo, 10 principais aplicações com os itens vulneráveis de aplicação mais críticos.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, AVI ativo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O painel Minhas vulnerabilidades da aplicação rastreia o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise/detecção inicial até a contenção ou correção.
- Exiba as taxas de cumprimento da meta de correção e determine com eficiência quais itens vulneráveis da aplicação (IVAs) apresentam mais riscos para sua organização.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta Solução:

- Now Platform administrador (admin): instale e ative esta solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Os painéis a seguir fornecem uma exibição gráfica da atividade AVI para ajudar a determinar os planos de correção e o andamento do status. Você pode se concentrar nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade.

- O painel da Gestão de vulnerabilidades de aplicações (PA) comunica os KPIs de risco e predominância de vulnerabilidade, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dias, um mês, 3 meses, 6 meses, acumulado no ano, 1 ano ou todos.
- O painel Minhas vulnerabilidades da aplicação rastreia o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise/detecção inicial até a contenção ou correção.

> **Nota:** O painel Minhas vulnerabilidades da aplicação é um subconjunto do painel Visão geral e só está disponível quando um membro do grupo de usuários do Campeão de segurança faz login em uma instância. Para obter mais informações sobre o painel Minhas vulnerabilidades de aplicações, consulte Painel Minhas vulnerabilidades de aplicações.

Gestão de vulnerabilidades de aplicações Painel do (PA)

Rastreie o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise e detecção iniciais até a contenção ou correção.

Casos de uso

Usuário	Uso do painel
Gerentes de vulnerabilidade	Com o painel Gestão de vulnerabilidades de aplicações, a gestão de vulnerabilidades pode determinar quais itens vulneráveis de aplicação (IVAs) apresentam mais riscos para suas organizações. Esses painéis fornecem uma exibição gráfica da atividade do AVI para ajudá-los a determinar os planos de correção e o andamento do status. Concentre-se nos KPIs

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
	associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade.

Funções Now Platform, configuração e guias do painel necessárias

O painel da Gestão de vulnerabilidades de aplicações (PA) está incluído como parte do pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades. O pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com a aplicação Resposta a vulnerabilidades. Ele está disponível no ServiceNow® Store como uma assinatura separada.

Para obter mais informações sobre como definir, instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades, consulte Instalar e configurar a aplicação Performance Analytics para Resposta a vulnerabilidades [PA].

Para exibir o painel, como um usuário atribuído aos grupos de usuários Campeão de segurança, Gerente de App-Sec ou Desenvolvedor, navegue até **Resposta a vulnerabilidades de aplicações** > **Visão geral**.

Nota: O painel Minhas vulnerabilidades da aplicação é um subconjunto do painel Visão geral e só está disponível quando um membro do grupo de usuários do Campeão de segurança faz login em uma instância. Para obter informações sobre o painel Minhas vulnerabilidades da aplicação, consulte Meu painel de vulnerabilidades da aplicação.

A partir da versão 19.0 do Resposta a vulnerabilidades de aplicações, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace e Visão geral dos painéis.

O painel Visão geral comunica KPIs de risco e predominância de vulnerabilidade, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dias, um mês, 3 meses, 6 meses, acumulado no ano, 1 ano ou todos.

Detalha os dados no painel Gestão de vulnerabilidades de aplicações por **tipo de verificação**, **aplicação** ou **unidade de negócios**. Cada uma dessas opções tem um filtro adicional, **Selecionar elementos**, para refinar suas seleções. A partir da Resposta a vulnerabilidades de aplicações v15.0, as aplicações de negócios e de IC foram adicionadas às opções do filtro **Aplicação**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

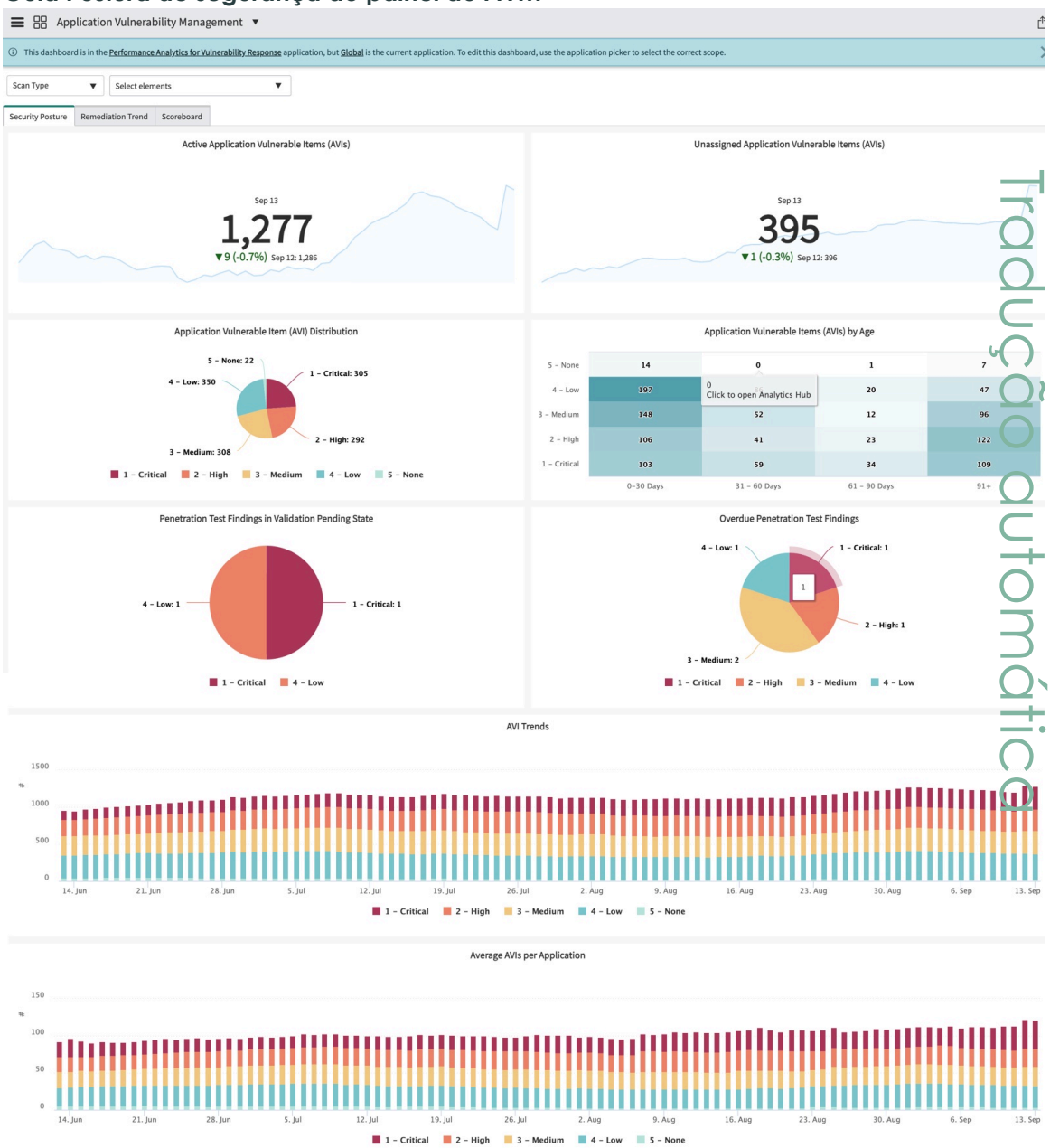
Guia Postura de segurança

A guia Postura de segurança ajuda a entender sua postura de segurança e o andamento das ações de correção.

A partir da Resposta a vulnerabilidades de aplicações v15.0, você pode exibir os relatórios de descobertas de testes de invasão. As descobertas do teste de invasão são Itens vulneráveis de aplicação (IVAs) criados manualmente com base nas solicitações de avaliação do teste de invasão.

Nota: O Tipo de verificação desses widgets é Manual.

Guia Postura de segurança do painel do AVM

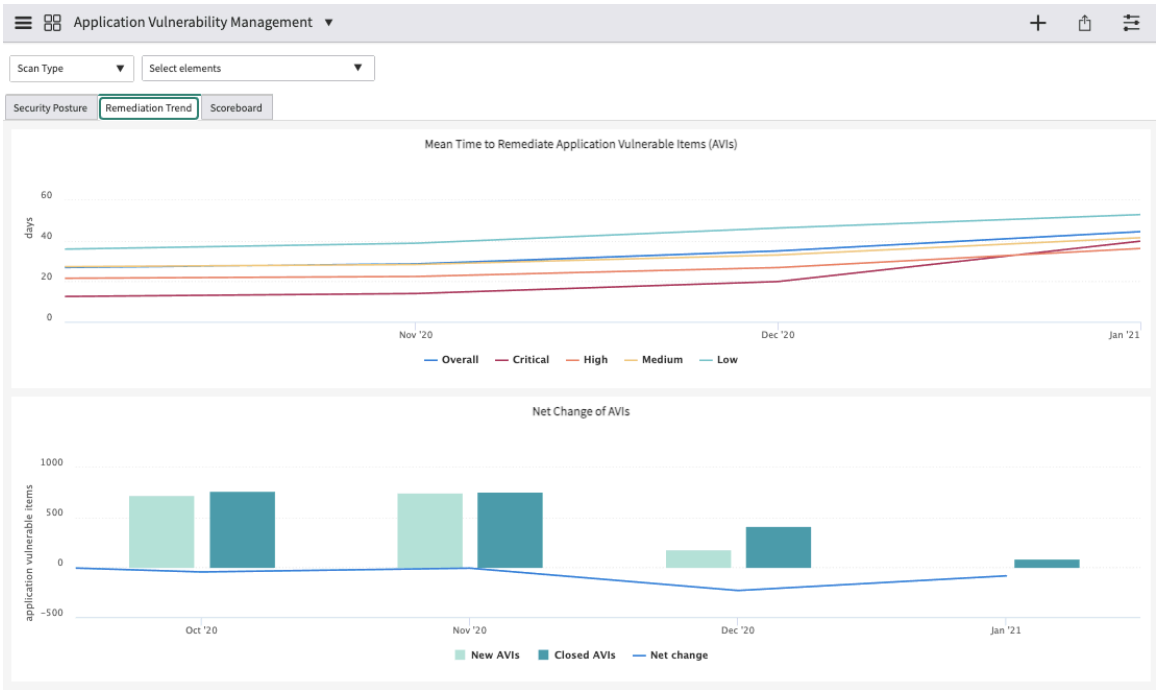


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Tendência de correção

A guia Tendência de correção ajuda a entender o andamento das ações de correção.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

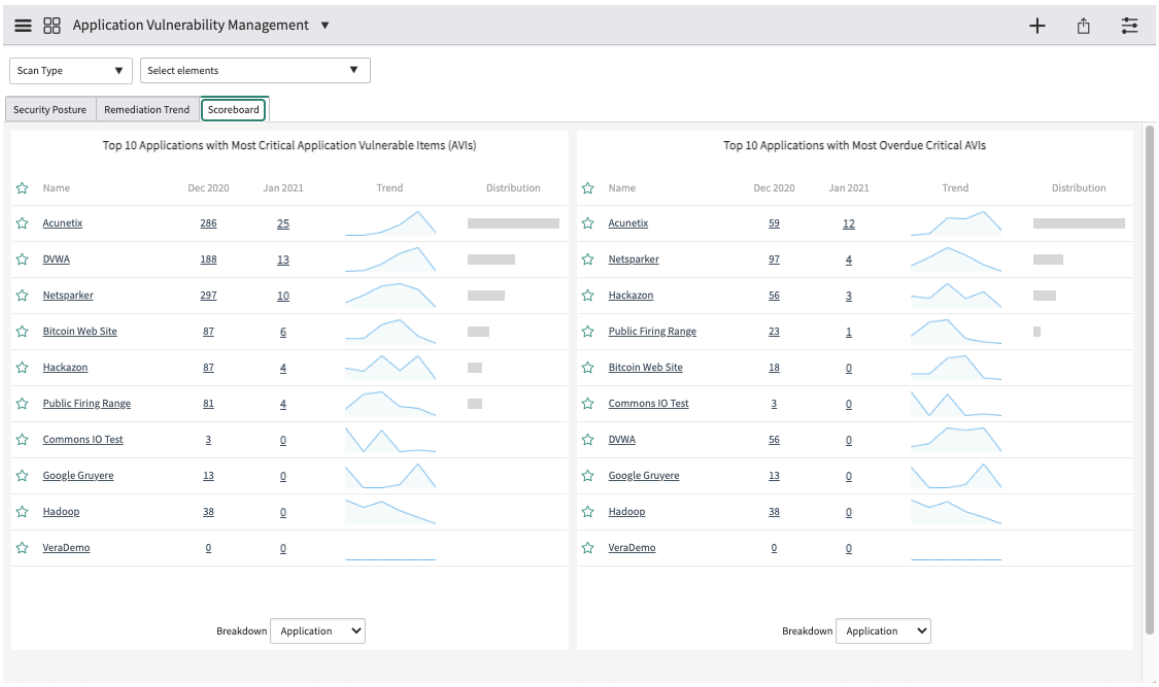
Guia Placar

A guia Placar ajuda a entender o andamento das ações de correção e quais IVAs precisam de mais assistência para concluí-las.

Elementos de tipo de verificação:

- Dinâmico: use somente métricas de importação de dados dinâmicos
- Estático: use somente métricas de importação de dados estáticos

Você pode escolher um ou ambos.



Indicadores

Tempo médio para corrigir IVAs baixos

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]]`. O objetivo é minimizar.

Versões da aplicação

É a contagem distinta em aplicações de AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação

É a contagem de itens de vulnerabilidade da aplicação AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

IVAs médios por aplicação

`[Itens vulneráveis da aplicação ativos]] / [[Versões da aplicação]]`. O objetivo é minimizar.

IVs não atribuídos

É a contagem na origem do indicador AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

`[[Soma da duração de itens vulneráveis de aplicação encerrados]] / [[Itens vulneráveis de aplicação encerrados]]`. O objetivo é minimizar.

Tempo médio para corrigir IVAs altos

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 2 - Alto]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 2 - Alto]]`. O objetivo é minimizar.

Itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é maximizar.

Tempo médio para corrigir IVAs críticos

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]]`. O objetivo é minimizar.

Novos itens vulneráveis da aplicação

É a contagem na origem do indicador AVI.New, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs médios

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 3 - Médio]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 3 - Médio]]`. O objetivo é minimizar.

Mudança líquida em IVs

`[[Novos itens vulneráveis de aplicação]] - [[Itens vulneráveis de aplicação encerrados]]`. O objetivo é minimizar.

Soma da duração de itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação atrasados críticos

É a contagem na fonte de dados AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação críticos

É a contagem nas aplicações de origem do indicador com IVAs ativos, que está usando a tabela: sn_vul_analytics_app_ci_dept_bu. O objetivo é minimizar.

Detalhamentos

- Idade
- Momento do fechamento
- Aplicação
- Unidade de negócios
- Pontuação de risco
- Tipo de Verificação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Postura de segurança

Nome	Tipo	Descrição
V15.0: descobertas do teste de invasão no estado pendente de validação	Gráfico	Descobertas do teste de invasão no estado Resolvido, mas com validação pendente, agrupadas por classificação de risco.
V15.0: descobertas de testes de invasão atrasados	Gráfico	Descobertas críticas do teste de invasão que não atingiram a data da meta de correção, agrupadas por classificação de risco.
Itens vulneráveis de aplicação (IVAs) ativos	Pontuação	Número de itens vulneráveis da aplicação ativos (não encerrados).
Itens vulneráveis de aplicação (IVAs) não atribuídos	Pontuação	Número de itens vulneráveis de aplicação (IVAs) sem um atribuído ou grupo de atribuição.
Distribuição de item vulnerável da aplicação (IVA)	Gráfico	Distribuição de todos os itens vulneráveis de aplicação (IVAs) agrupados por avaliação de risco.
Itens vulneráveis de aplicação (IVAs) por idade	Mapa térmico	Número de itens vulneráveis de aplicação (IVAs) agrupados por classificação de risco e idade (em dias).
Tendências de IVA	de tendências	Tendência de todos os itens vulneráveis da aplicação (IVAs) ativos agrupados por avaliação de risco.
IVAs médios por aplicação	de tendências	Tendência dos itens vulneráveis de aplicação (IVAs) por aplicação, agrupado pela avaliação de risco.

Tendência de correção

Nome	Tipo	Descrição
Tempo médio para corrigir itens vulneráveis da aplicação (IVAs)	Linha de linha	Tendência do tempo médio de correção dos itens vulneráveis da aplicação (IVAs) por classificação de risco.
Mudança líquida de IVAs	Ícone de	Tendência de novos itens vulneráveis da aplicação (AVIs) detectados versus encerrados por mês.

Placar

Nome	Tipo	Descrição
10 principais aplicações com itens vulneráveis da aplicação (IVAs) mais críticos	Cartão de pontuação e barra de distribuição do cartão de pontuação Ícone de distribuição	Aplicações com o número maior de itens vulneráveis da aplicação (IVAs).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Placar

Nome	Tipo	Descrição
10 principais aplicações com itens vulneráveis de aplicação críticos (IVAs) mais atrasados	Cartão de pontuação e barra de distribuição do cartão de pontuação Ícone de distribuição	Aplicações com o maior número de itens vulneráveis de aplicação (IVAs) ativos que já passaram das datas de meta de correção.

Meu painel de vulnerabilidades da aplicação

Este painel apresenta métricas importantes para analisar o processo de Gestão de vulnerabilidades de aplicações, como a exibição das taxas de cumprimento da meta de correção.

Funções Now Platform necessárias e exibição do painel

Nota:

- Este painel faz parte do pacote de conteúdo da Resposta a vulnerabilidades da aplicação. O pacote de conteúdo da Resposta a vulnerabilidades de aplicações faz parte do pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades.
- O pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades está disponível em ServiceNow® Store como uma assinatura separada.
- O pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com a aplicação Resposta a vulnerabilidades.

O painel Minhas vulnerabilidades da aplicação está disponível somente quando um membro do grupo de usuários do Campeão de segurança faz login em uma instância. Para obter informações sobre o painel Visão geral, consulte Painel Gestão de vulnerabilidades de aplicações [PA].

Para exibir o painel, navegue até **Resposta a vulnerabilidades de aplicações** > **Minhas vulnerabilidades de aplicações**.

A partir da versão 19.0 do Resposta a vulnerabilidades de aplicações, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace e Visão geral dos painéis.

Exibir relatórios que mostram dados de tendências ao longo do tempo. Visualize tendências de métricas importantes em uma programação regular para analisar seus processos de negócios gerais e identificar áreas de melhoria.

O painel Minhas vulnerabilidades de aplicações está incluído no pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades. O pacote de conteúdo do Performance Analytics para Resposta a vulnerabilidades não é instalado automaticamente com a aplicação Resposta a vulnerabilidades. Ele está disponível no ServiceNow® Store como uma assinatura separada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos de uso

Usuário	Uso do painel
Especialistas em TI, proprietários de correção ou analistas que corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem.	Um Campeão de segurança usa o painel Minhas vulnerabilidades da aplicação para rastrear o volume, o desempenho e o andamento da correção das vulnerabilidades da aplicação. Determine com eficiência quais itens vulneráveis de aplicação (IVAs) apresentam mais riscos para sua organização. Esses painéis fornecem uma exibição gráfica da atividade do AVI para ajudar a determinar os planos de correção e o andamento do status. Você pode se concentrar nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade. Obtenha informações rapidamente sobre sua exposição a vulnerabilidades e postura de segurança. Rastreie desde a análise e detecção iniciais até a contenção ou correção.

Guias do painel Minhas vulnerabilidades da aplicação [PA]

O painel Minhas vulnerabilidades da aplicação comunica KPIs de risco e predominância de vulnerabilidade, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dias, um mês, 3 meses, 6 meses, acumulado no ano, 1 ano ou todos.

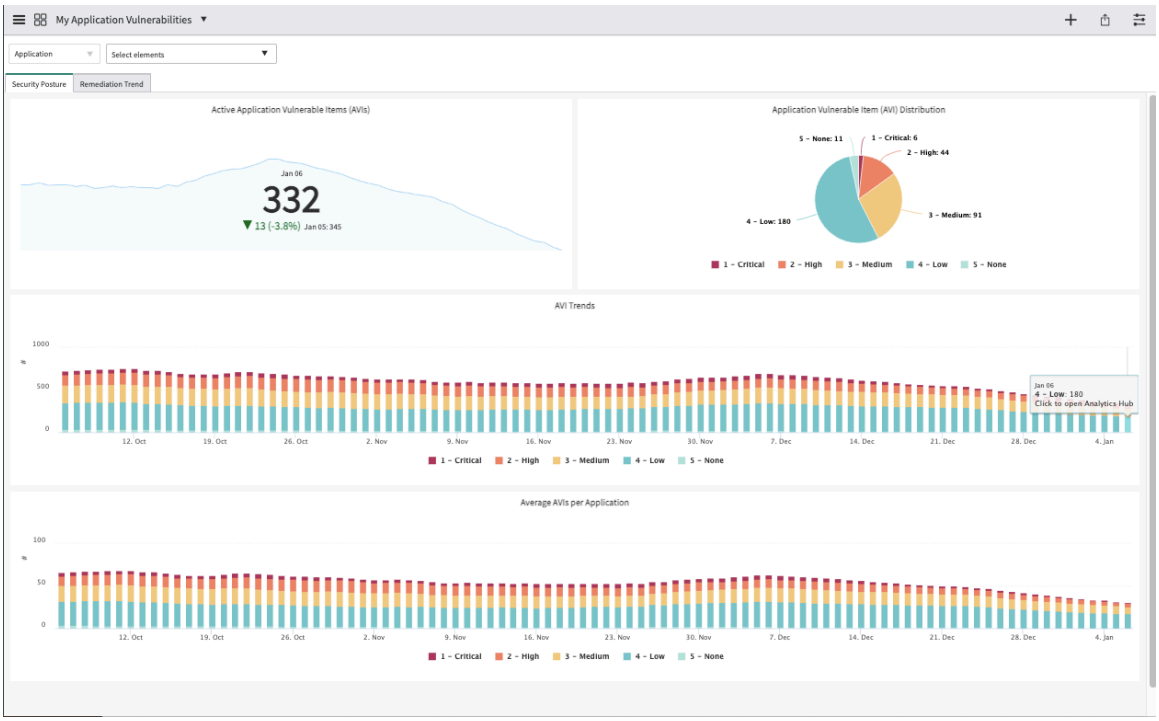
Os dados são divididos no painel por **aplicação**. Use a lista **Selecionar elementos** para refinar suas seleções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

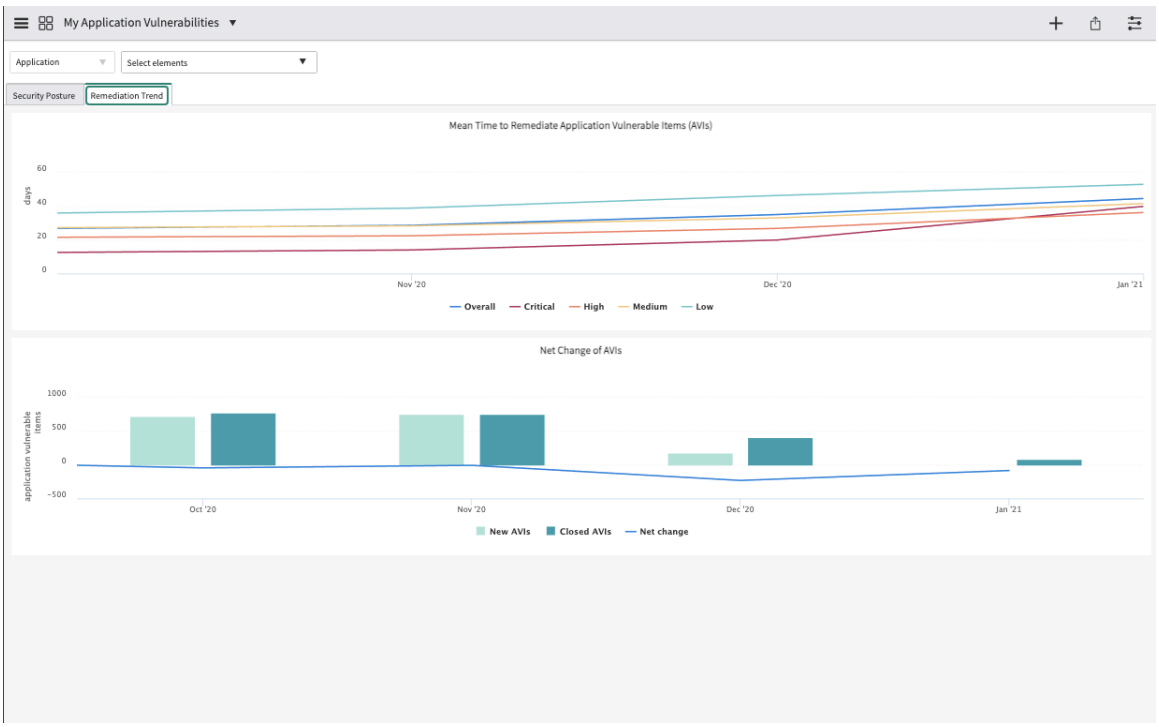
Guia Postura de segurança

A guia Postura de segurança ajuda a entender sua postura de segurança e o andamento das ações de correção. Detalha os dados no painel da Gestão de vulnerabilidades de aplicações por **tipo de verificação**, **aplicação** ou **unidade de negócios**. Cada uma dessas opções tem um filtro adicional, **Selecionar elementos**, para refinar suas seleções.



Guia Tendência de correção

A guia Tendência de correção ajuda a entender o andamento das ações de correção.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Tempo médio para corrigir IVAs baixos

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]]`. O objetivo é minimizar.

Versões da aplicação

É a contagem distinta em aplicações de AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação

É a contagem de itens de vulnerabilidade da aplicação AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

IVAs médios por aplicação

`[Itens vulneráveis da aplicação ativos]] / [[Versões da aplicação]]`. O objetivo é minimizar.

IVs não atribuídos

É a contagem na origem do indicador AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs

`[[Soma da duração de itens vulneráveis de aplicação encerrados]] / [[Itens vulneráveis de aplicação encerrados]]`. O objetivo é minimizar.

Tempo médio para corrigir IVAs altos

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 2 - Alto]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 2 - Alto]]`. O objetivo é minimizar.

Itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é maximizar.

Tempo médio para corrigir IVAs críticos

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]]`. O objetivo é minimizar.

Novos itens vulneráveis da aplicação

É a contagem na origem do indicador AVI.New, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs médios

`[[Soma da duração de itens vulneráveis da aplicação encerrados > Classificação de risco = 3 - Médio]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 3 - Médio]]`. O objetivo é minimizar.

Mudança líquida em IVs

`[[Novos itens vulneráveis de aplicação]] - [[Itens vulneráveis de aplicação encerrados]]`. O objetivo é minimizar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Soma da duração de itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação atrasados críticos

É a contagem na fonte de dados AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação críticos

É a contagem nas aplicações de origem do indicador com IVAs ativos, que está usando a tabela: sn_vul_analytics_app_ci_dept_bu. O objetivo é minimizar.

Detalhamentos

- Idade
- Momento do fechamento
- Aplicação
- Unidade de negócios
- Pontuação de risco
- Tipo de Verificação

Visualizações de dados

Postura de segurança

Nome	Tipo	Descrição
Itens vulneráveis de aplicação (IVAs) ativos	Pontuação	Número de itens vulneráveis da aplicação ativos (não encerrados).
Distribuição de item vulnerável da aplicação (IVA)	Gráfico	Distribuição de todos os itens vulneráveis de aplicação (IVAs) agrupados por avaliação de risco.
Tendências de IVA	de tendências	Tendência de todos os itens vulneráveis da aplicação (IVAs) ativos agrupados por avaliação de risco.
IVAs médios por aplicação	de tendências	Tendência dos itens vulneráveis de aplicação (IVAs) por aplicação, agrupado pela avaliação de risco.

Tendência de correção

Nome	Tipo	Descrição
Tempo médio para corrigir itens vulneráveis da aplicação (IVAs)	Linha de linha	Tendência do tempo médio de correção dos itens vulneráveis da aplicação (IVAs) por classificação de risco.
Mudança líquida de IVAs	Ícone de	Tendência de novos itens vulneráveis da aplicação (AVIs) detectados versus encerrados por mês.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estrutura de relatórios agregados

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas em tempo real complexas e de longa execução para melhor desempenho.

A estrutura de relatórios agregados melhora o desempenho:

- usando menos recursos e renderizando relatórios com mais rapidez,
- agregar os dados e reutilizar agregações e detalhamentos (Agrupar por) e
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de itens vulneráveis, use a estrutura fornecida em Vulnerability Response Common ao lado dos relatórios padrão.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- Now Platform administrador (admin): instale e ative este Solução Performance Analytics e relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics administrador (pa_admin): revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Administrador (sn_vul_cmn.admin): criar agregações.
- Gravação de VR (sn_vul_cmn.write): edite os dados em Agregações e Resultados agregados.
- Leitura de VR (sn_vul_cmn.read): revise os dados em Agregações e Resultados agregados.
- Analista de vulnerabilidade (sn_vul.vulnerability_analyst): revisa os resultados agregados.

Informações relacionadas

Configurar uma agregação para dados de origem

Executar várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Criar um relatório usando uma agregação

Configurar uma agregação para dados de origem

Para analisar o desempenho de um aspecto específico em um processo de negócios registrado em uma tabela ServiceNow, crie uma agregação específica para o aspecto e crie um relatório para essa agregação.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Procedimento

1. Navegar até **Todos** > **Relatórios de agregados** > **Definições de agregação** > **Todos** e clique em **Novo**.
2. No campo **Nome**, dê à agregação um nome descritivo.
3. No campo **Descrição**, forneça uma breve descrição sobre a agregação.
4. Na guia **Origem**, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos da guia Origem

Campo	Descrição
Tabela	Tabela da qual você deseja buscar os dados do relatório. Esta lista suspensa contém somente as tabelas app-sec common, app-vul, app-vulc, app-vul-container e de vulnerabilidade da aplicação.
Agregar função	Função a ser aplicada à coluna selecionada em **Campo**. ◦ **Contagem**: número de registros. ◦ **Soma**: soma total dos valores na coluna selecionada em **Campo**. ◦ **Média**: média de todos os valores em uma coluna selecionada em **Campo**. ◦ **Máximo**: valor máximo na coluna selecionada em **Campo**. ◦ **Mínimo**: valor mínimo da coluna selecionada em **Campo**. ◦ **Contagem separada**: valores exclusivos na coluna selecionada em **Campo**.
Campo	Coluna na qual você deseja aplicar a função. **Nota:** Este campo não aparece quando você seleciona **Contagem** no campo **Função agregada**.

5. Na guia **Condições adicionais**, forneça a condição no campo **Condições** para selecionar um conjunto específico de registros para o qual você deseja obter os resultados agregados.
6. Na guia **Agrupar por**, selecione as colunas da tabela pelas quais você deseja agrupar ou empilhar os dados.
   Você pode selecionar até dois detalhamentos.

   Se você selecionar a coluna de **data** em qualquer campo agrupar por, o campo **Tendência por** será exibido. Você pode obter os resultados de agregação categorizados por semana, dia, minutos etc. selecionando as opções no campo **Tendência por**.
7. Na guia **Programação**, selecione ou crie uma programação de agregação, que define a frequência na qual você pode executar a agregação para buscar os dados.
   Para criar uma programação de agregação, consulte Executar várias agregações simultaneamente.

   Nota: Você não pode programar a execução de agregação para uma definição de agregação inativa.
8. Clique em **Enviar** para criar a agregação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A agregação aparece na lista Agregação. Na frequência predefinida, a agregação é executada e um registro é criado junto com uma data e hora de execução na lista relacionada Execuções programadas para cada execução.

9. Navegar até **Todos** > **Resultados agregados** e abra sua agregação para ver os resultados agregados e as execuções programadas.
   Os resultados agregados são listados na lista relacionada **Resultados agregados**. Se a execução de agregação falhar, consulte a coluna **Anotações** na lista relacionada **Execuções programadas** para obter mais informações.
10. Opcional: Selecione **Executar agora** para coletar os resultados da agregação, independentemente da programação de agregação.
    Se você encerrar a execução programada quando ela estiver em andamento, nenhuma mudança será feita nos resultados agregados. Você também pode excluir ou desativar uma agregação.

O que Fazer Depois

Crie um relatório usando sua agregação. Para obter mais informações sobre como criar um relatório usando uma agregação, consulte Criar um relatório usando uma agregação.

Informações relacionadas

- Estrutura de relatórios agregados
- Executar várias agregações simultaneamente
- Configure o número de agregações que podem ser executadas simultaneamente
- Criar um relatório usando uma agregação

Executar várias agregações simultaneamente

Você pode programar a execução de várias agregações usando uma única programação de agregação.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa

Suponha que você queira executar seis agregações ao mesmo tempo. Crie uma programação de agregação e adicione todas as agregações a ela. Essas agregações são executadas na frequência e no tempo definidos.

Procedimento

1. Navegar até **Todos** > **Relatórios de agregados** > **Programação**.
2. Selecione **Novo**.
3. No formulário Programação de agregação, preencha os campos.

Campo	Descrição
Nome da programação	Nome da programação de agregação.
Programar trabalho	Execução de script agendada que define a frequência na qual as agregações devem ser executadas. Você pode criar um trabalho agendado selecionando o botão **Novo**.

4. Selecione **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A programação de agregação aparece na lista Programação de agregações.

5. Abra sua programação de agregação.
6. Selecione **Editar**, adicione as agregações à **Lista**de agregação e selecione **Salvar**.
   As agregações selecionadas aparecem na lista relacionada Agregações.

   Nota: Se você adicionar uma agregação inativa a uma programação, a execução programada não será iniciada.

7. Selecione **Atualizar**.
   Essas agregações são executadas na frequência definida na programação de agregação.

Informações relacionadas

Estrutura de relatórios agregados

Configurar uma agregação para dados de origem

Configure o número de agregações que podem ser executadas simultaneamente

Criar um relatório usando uma agregação

Configure o número de agregações que podem ser executadas simultaneamente

Um novo processador ou um trabalho em segundo plano, o Processador do Aggregated Reporting Framework, é enviado com o sistema base, que executa os trabalhos agendados relacionados à tabela do Aggregated Reports Framework. Isso permite que o subsistema inteiro seja executado em segundo plano e permite uma melhor utilização dos recursos do sistema quando eles estão disponíveis.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Configuração de trabalho em segundo plano – Calculadora de resultado de agregação comum da Resposta a vulnerabilidades**.
2. Defina o número de agregações que você deseja executar simultaneamente no campo **Máximo de threads simultâneos** e selecione **Salvar**.
   Por padrão, quatro agregações são executadas simultaneamente.
3. Navegue até a lista Pools de processadores de trabalho em segundo plano, **sn_sec_cmn_background_job_processor_pool.list**e selecione **Novo** para criar um processador de trabalho em segundo plano para a Estrutura de relatórios agregados. Para obter mais informações sobre como criar um pool de processadores de trabalho em segundo plano, consulte Processamento paralelo avançado para trabalhos em segundo plano na Resposta a vulnerabilidades .

   Nota: O número de processadores de trabalho em segundo plano deve ser igual ao número máximo de threads simultâneos fornecido no formulário **Configuração de trabalho em segundo plano – Calculadora de resultado de agregação comum de Resposta a vulnerabilidades**. Consulte a Etapa 2.

Informações relacionadas

Estrutura de relatórios agregados

Configurar uma agregação para dados de origem

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar várias agregações simultaneamente

Criar um relatório usando uma agregação

Criar um relatório usando uma agregação

Para visualizar e analisar os dados específicos de uma agregação que você criou, gere um relatório fornecendo uma condição para a agregação no Construtor de condições.

Antes de Iniciar

Função necessária: pa_admin

Procedimento

1. Navegar até **Todos** > **Relatórios** > **Criar novo(a)**.
2. Na guia **Dados**, preencha os campos.

Campos da guia Dados

Campo	Descrição
Nome do relatório	Nome do relatório.
Tipo de origem	Tipo de origem da qual os dados são obtidos. Selecione **Tabela**.
Tabela	Nome da tabela para a qual a agregação é criada. Selecione a tabela de resultados **agregados, Resultado agregado [sn_vul_cmn_aggregate_result]**.

3. No Construtor de condições, defina a condição para a agregação para a qual você deseja gerar um relatório.

Condição no Construtor de condições

Parte	Descrição
Campo	Selecione **Agregação**.
Operador	Selecione **é**.
Valor	Nome da agregação.

4. Na guia **Dados**, clique em **Avançar**.
5. Na guia **Tipos**, selecione como você deseja visualizar os dados e clique em **Avançar**. Para saber mais sobre os tipos de relatório, consulte Criação de relatórios .

   As visualizações compatíveis são gráfico de barras, gráfico de pizza e mapa térmico. Você pode modificar os gráficos de linhas e outras visualizações de tendências para usar as visualizações compatíveis com o resultado agregado para representar os mesmos dados. A exibição de lista não é compatível.

6. Na guia **Configurar**, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Agrupar por	Selecione **Agrupado por 1** que você selecionou na guia **Agrupar por** da agregação.
Empilhar por	Selecione **Agrupado por 2** que você selecionou na guia **Agrupar por** da agregação.
Agregação	Aplique a função **Mínimo** ou **Máximo** em **Valor**.

7. Na guia **Estilo**, preencha os campos conforme apropriado e clique em **Executar**.
   Para obter mais informações sobre os campos nas guias **Configurar** e **Estilo**, consulte o vídeo Criação de um relatório .
8. No Construtor de condições, defina a condição da agregação para a qual você deseja gerar um relatório e clique em **Executar**.

   O relatório é exibido.
9. Para classificar os valores no eixo x, selecione **Adicionar classificação**.

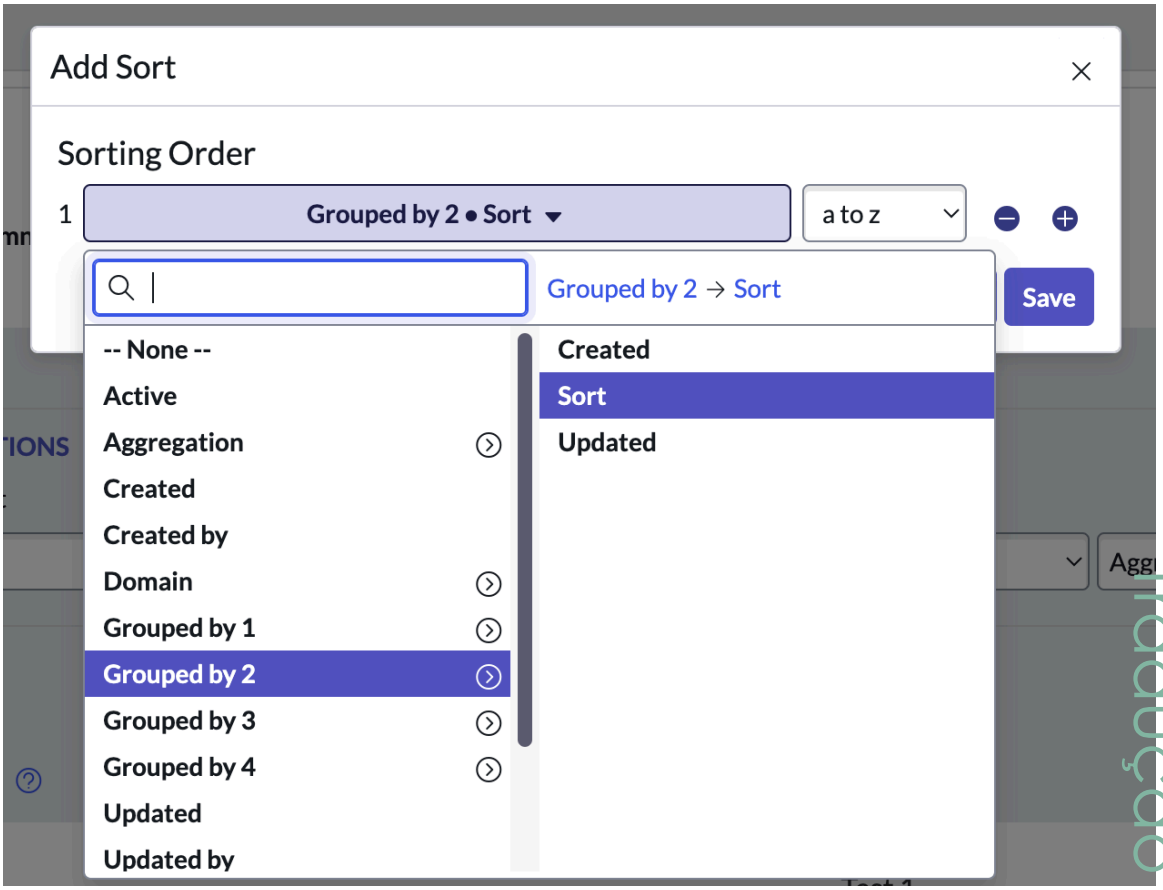
   a. Para cadeias de caracteres, forneça a condição como **Agrupado por > az ou za** para classificar as cadeias de caracteres em ordem alfabética.

   b. Para valores de tipo de dados inteiros e de data, forneça a condição como **Agrupado por.classificar > az ou za** para classificar os valores em ordem crescente e decrescente, respectivamente.

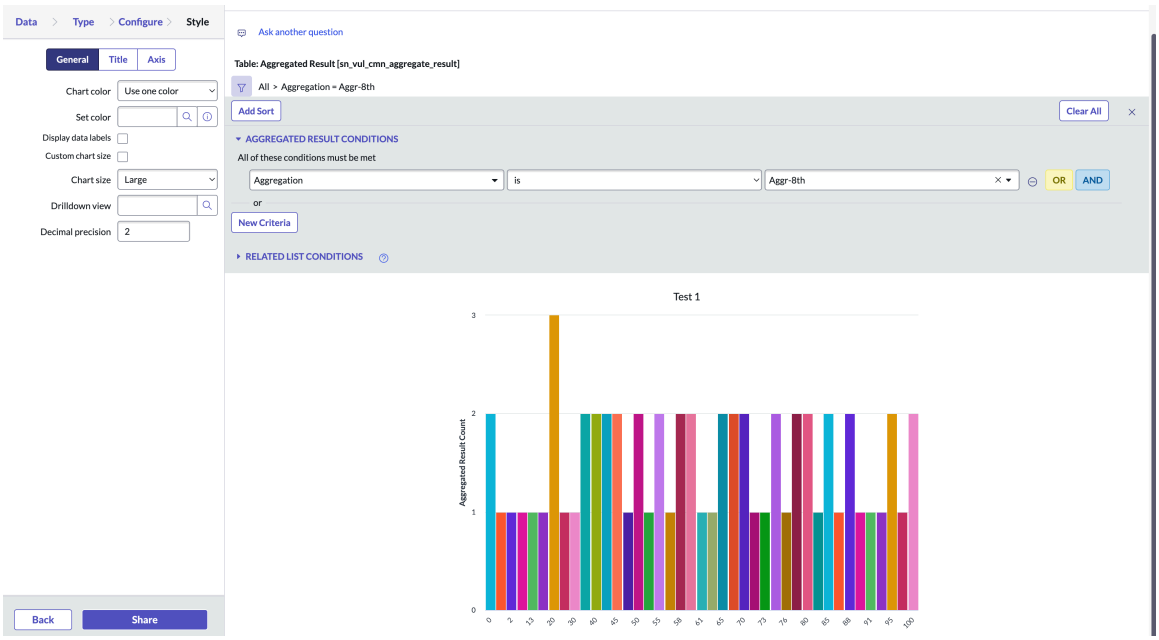
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Classificando números inteiros no eixo X



c. Selecione **Executar**.
Os valores inteiros e de data são classificados no eixo X.



10. Clique em **Salvar** para salvar seu relatório.
O relatório gerado para uma agregação é exibido na guia **Resultados** do respectivo formulário de **Agregação**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Opcional: Adicione seu relatório a um painel.
    Para obter mais informações sobre como adicionar um relatório a um painel, consulte Como adicionar um relatório a um painel dinâmico .

    O painel **Gestão de vulnerabilidades [Agregado]** que consiste em relatórios criados usando a estrutura de relatórios em cache é enviado com o sistema de base. Para exibir este painel, navegue até **Todos** > **Análise de desempenho** > **Painéis** > **Todos** > **Gestão de vulnerabilidades [Agregado]**. As agregações ativas correspondentes aos relatórios neste painel são enviadas com o sistema de base.

12. Compartilhe seu relatório com outros usuários.
    Para obter mais informações sobre como compartilhar relatórios, consulte Distribuir relatórios .

Informações relacionadas

Configurar uma agregação para dados de origem

Estrutura de relatórios agregados

Executar várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

referências de Resposta a vulnerabilidades de aplicações

Tópicos de referência que contêm informações sobre tabelas, funções e propriedades instaladas com a aplicação Resposta a vulnerabilidades de aplicações.

Para obter detalhes, consulte:

- Resposta a vulnerabilidades de aplicações grupos de usuários e funções
- Componentes instalados com Resposta a vulnerabilidades de aplicações
- Estados de item vulnerável de aplicação (IVA)
- Campos da aplicação verificados
- Campos de item vulnerável da aplicação
- Campos de vulnerabilidade da aplicação
- Estados dos testes de invasão

Resposta a vulnerabilidades de aplicações grupos de usuários e funções

Antes de corrigir vulnerabilidades com sucesso com Resposta a vulnerabilidades de aplicações (AVR), você deve atribuir usuários a grupos de usuários.

As funções definem o que você e seus grupos podem ver e fazer em Resposta a vulnerabilidades de aplicações, Performance Analytics para Resposta a vulnerabilidadese integrações de terceiros com Resposta a vulnerabilidades de aplicações.

Grupos de usuários

A seguir estão os grupos de usuários padrão que oferecem suporte a Resposta a vulnerabilidades de aplicações:

- Gerente App-Sec: contém gerentes de segurança. A partir da Resposta a vulnerabilidades de aplicações v15.0, ele também conterá responsáveis pela aplicação que gerenciam as solicitações de avaliação de teste de invasão.
- Campeão de segurança: contém contatos entre o grupo de desenvolvimento e os gerentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desenvolvedor: contém colaboradores individuais.
- V15.0: Ethical Hacker: contém membros da equipe de hacking ético que realizam testes de invasão de aplicações.

A função de administrador do sistema [admin] é necessária para atribuir usuários aos grupos de usuários padrão Resposta a vulnerabilidades de aplicações, usando o módulo Administração de usuários,

Nota:

A atribuição de usuários AVR aos grupos de usuários Resposta a vulnerabilidades de aplicações para Resposta a vulnerabilidades de aplicações não está disponível no recurso Resposta a vulnerabilidades do Assistente de configuração. Somente funções Resposta a vulnerabilidades são atribuídas lá.

A tabela a seguir lista os grupos de usuários Resposta a vulnerabilidades de aplicações disponíveis e as funções associadas a eles. Use esta tabela para determinar quais usuários devem ser atribuídos a quais grupos.

Grupo de Usuários	Funções neste grupo
Campeão de segurança Os membros deste grupo podem: • Ler e gravar itens vulneráveis da aplicação (IVAs) atribuídos a você. • Atribua um AVI atribuído a você a outro indivíduo ou grupo. • V20.0: criar, atualizar, excluir e cancelar (desativar) regras de exceção.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
Gerente App-Sec Os membros deste grupo podem: • V20.0: criar, atualizar, excluir e cancelar (desativar) regras de exceção. • Ler, gravar, excluir e todas as operações nas regras de tarefa de correção da aplicação. • Leia e grave todos os AVIs. • Configure o AVR criando e gerenciando regras, calculadoras e mapas de severidade. • Configurar integrações. • Excluir IVAs. • Atribua IVA a indivíduos ou grupos. • Gerenciar aplicações. • Permite acesso ao módulo Aplicação.	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_read_all • sn_vul.app_write_all • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations **Nota:** Por padrão, esta função contém funções granulares para configuração de integração de terceiros. Para definir ou editar um grupo de usuários do App-Sec Manager por integrações únicas ou específicas, consulte Resposta a vulnerabilidades personas e funções granulares. • sn_vul.app_manage_assignment_rules

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupo de Usuários	Funções neste grupo
• Programe, configure e execute a integração. • Leia e execute integrações. • Exiba painéis e relatórios de AVR Performance Analytics. • V15.0: gerenciar solicitações de avaliação de teste de invasão.	• sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Versão 13.0: sn_vul.app_manage_app_sc • Somente versão 12.0: sn_vul.app_read_application_release [Removido na v12.1. Não use] • sn_sec_int.admin • Versão 13.0: pa_power_user • pa_viewer **Nota:** A partir da Resposta a vulnerabilidades v13.0, o pa_viewer está incluído no pa_power_user e não é mais necessário por si só. • V15.0: sn_vul.app_manage_pen_test_request • V15.0: sn_vul.app_update_state • V15.0: cmdb_read
Desenvolvedor Os membros deste grupo podem: • Ler e gravar registros AVR atribuídos a você. • Atribua um AVI atribuído a você a outro indivíduo ou grupo.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view
V15.0: Ethical Hacker Os membros deste grupo podem: • Configure o grupo de atribuição padrão e o designado para solicitações de avaliação de teste de invasão. • Gerenciar descobertas de testes de invasão. • Gerenciar solicitações de avaliação de teste de invasão.	• V15.0: sn_vul.app_update_state • V15.0: sn_vul.app_manage_pen_test_request • V15.0: itil • V15.0: sn_vul.app_read_all • V15.0: sn_vul.app_manage_pen_test_request_config • V15.0: sn_vul.app_manage_manual_avits

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupo de Usuários	Funções neste grupo
• Exibir itens vulneráveis da aplicação. • Atualize a atribuição de itens vulneráveis da aplicação.	• V15.0: sn_vul.app_update_assigned_to • V15.0: sn_vul.app_update_assignment_group

Atribuir usuários a grupos de usuários no Resposta a vulnerabilidades de aplicações

Atribua usuários a grupos usando o módulo Administração de usuários em sua instância.

Antes de Iniciar
Função necessária: administrador

Procedimento

Para atribuir ou remover um usuário de um grupo:

a. Navegar até **Administração** > **Grupos**.

b. Localize e abra o grupo apropriado, por exemplo, **App-Sec Manager**.
O registro do grupo é exibido.

c. Selecione a guia **Membros do grupo**.
Os membros atuais do grupo são exibidos.

d. Clique em **Editar**.
O formulário Editar membros é exibido.

e. Na lista **Coleção**, selecione usuários para adicionar ou remover do grupo.

f. Depois que todos os usuários tiverem sido adicionados à **Lista de membros do grupo** ou removidos, clique em **Salvar**.
Você retornará à guia **Membros do grupo**.

g. Clique em **Atualizar** para salvar suas mudanças e retornar à lista Grupos.

Informações relacionadas

Componentes instalados com Resposta a vulnerabilidades de aplicações

Componentes instalados com Resposta a vulnerabilidades de aplicações

Vários tipos de componentes são instalados com a ativação do recurso Resposta a vulnerabilidades de aplicações, incluindo tabelas, funções de usuário e trabalhos agendados.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas

Funções granulares em Resposta a vulnerabilidades de aplicações são atribuídas a grupos de usuários específicos, por padrão.

Nota: O uso de funções granulares fora desses grupos de usuários requer codificação e conhecimento avançado Resposta a vulnerabilidades de aplicações ou ServiceNow.

Título da função [name]	Descrição	Contém as funções
V20.0: sn_vul.app_manage_auto_exception_rule	Criar, atualizar, excluir e cancelar (desativar) regras de exceção.	sn_vul.app_read_auto_
sn_vul.app_manage_group_rules	Ler, gravar, excluir e todas as operações nas regras de tarefa de correção da aplicação.	• sn_vul.app_read_all • sn_vul.app_read_grou
V20.0: sn_vul.app_exception_approver	Aprova regras de exceção e solicitações de extensão de regra de exceção. A partir da v20.0, a função granular, sn_vul.app_read_all, foi removida para que você possa acessar os itens vulneráveis de aplicação e tarefas de correção atribuídos a você e seu grupo em vez de todos os itens vulneráveis de aplicação e tarefas de correção.	sn_vul.app_read_auto_
sn_vul.app_read_assigned	Exiba os itens vulneráveis da aplicação (IVAs) atribuídos a você.	
sn_vul.app_read_all	Exibir todos os IVAs e informações relacionadas.	
sn_vul.app_write_assigned	Atualize os IVAs atribuídos a você.	
sn_vul.app_write_all	Atualize todos os IVAs e informações relacionadas.	
sn_vul.app_update_assignment_group	Atualize o grupo de atribuição de IVA.	**Nota:** Quando us do grupo de usuári requer sn_vul.app_ sn_vul.app_write_as
sn_vul.app_update_assigned_to	Atualizar atribuído de AVI.	**Nota:** Quando us do grupo de usuári requer sn_vul.app_ sn_vul.app_write_as
sn_vul.app_configure_integrations	Configure integrações de terceiros.	sn_vul.app_read_all

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
		sn_vul.app_read_integra sn_sec_int.admin sn_vul_veracode.config sn_vul.configure_nvd_a **Nota:** Para definir grupo de usuários c Manager por integr ou específicas, con vulnerabilidades pe granulares.
sn_vul.app_read_integrations	Exibir todas as integrações de terceiros.	
sn_vul_veracode.configure_integration	Defina, atualize e exclua integrações do Veracode.	
sn_vul.app_manage_assignment_rules	Defina, atualize e exclua regras de atribuição de AVI.	sn_vul.app_read_all sn_vul.app_read_assign
sn_vul.app_read_assignment_rules	Exibir regras de atribuição.	
sn_vul.app_manage_remediation_target_rules	Defina, atualize e exclua regras de destino de correção AVI.	sn_vul.app_read_all sn_vul.app_read_remed
sn_vul.app_manage_risk_score_configurations	Defina, atualize e exclua calculadoras AVR e regras de risco.	sn_vul.app_read_all sn_vul.app_read_risk_sc sn_sec_cmn.calcul.write
sn_vul.app_read_risk_score_configuration	Veja as calculadoras AVR e as regras de risco.	
sn_vul.app_manage_applications	Exibir, atualizar e excluir registros de aplicações.	
sn_vul.app_manage_app_sc	Concede a um Campeão de segurança a capacidade de adicionar ou remover a si mesmo da lista relacionada de aplicações verificadas.	
sn_vul.app_pa_sc_view	Fornece uma exibição relevante para o Campeão de segurança específico.	
sn_vul.app_manage_app_vul_permissions	[interno] Usado por sn_vul.app_manage_applications.	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição	Contém as funções
sn_vul.app_manage_normalized_severity	Atualize o mapeamento para a gravidade normalizada.	sn_vul.app_read_norma
sn_vul.app_read_normalized_severity [Removido na v12.1. Não use.]	Exibir registros de gravidade normalizados.	
sn_vul.app_read_application_release	Exibir registros de versão da aplicação.	
sn_sec_int.admin	Fornece acesso a integrações.	
pa_power_user	Fornece acesso a relatórios	pa_viewer
sn_vul.app_sec_manager	Prioriza e gerencia itens vulneráveis da aplicação.	
sn_vul.app_developer	Desenvolvedor responsável por corrigir as vulnerabilidades da aplicação.	
sn_vul.app_create_watch_topic	Crie tópicos de observação para vulnerabilidades da aplicação.	
sn_vul.app_read_watch_topic	Leia os tópicos de observação para vulnerabilidades da aplicação.	
sn_vul.app_edit_watch_topic	Edite os tópicos de observação das vulnerabilidades da aplicação.	
sn_vul_blackduck.configure_integration	Configure integrações de terceiros.	sn_vul_blackduck.confi

Trabalhos agendados instalados

Para Resposta a vulnerabilidades trabalhos agendados compartilhados, consulte Componentes instalados com Resposta a vulnerabilidades.

Trabalho agendado	Descrição
Associar AVIs existentes à regra de exceção automática	Avalia itens vulneráveis da aplicação em busca de correspondências com regras de exceção.
Preencher entrada e CVE M2M	Torna os registros existentes consistentes com vários registros do CWE. Execute uma vez após o upgrade para preencher e desabilitar.
Sincronizar novamente o CWE primário	Para cálculos de CWE primários personalizados. Execute uma vez após o upgrade para sincronizar novamente e desabilitar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Acumular valores de item vulnerável da aplicação para vulnerabilidade e grupo	Calcula vulnerabilidades e acúmulos de grupo para itens vulneráveis da aplicação. **Nota:** A partir da v23.0 de Resposta a vulnerabilidades de aplicações, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de vários threads. Esse upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.
Integração da Lista de Projetos do Black Duck	Extrai e ingere dados na tabela de projetos do Black Duck.
Integração da lista de aplicações do Black Duck	Importa aplicações para a tabela de aplicações descobertas para todas as versões de projeto disponíveis com a Integração Black Duck na tabela de projetos.
Integração de item vulnerável da aplicação Black Duck	Ingere itens vulneráveis na aplicação ServiceNow com base nas vulnerabilidades detectadas por scanners para cada aplicação descoberta no sistema.

Tabelas instaladas

Tabela	Descrição
Versão da aplicação [sn_vul_app_release]	Contém informações da versão da aplicação.
Versão 13.0: Campeões de segurança da aplicação [sn_vul_app_m2m_app_sc]	Contém os Resposta a vulnerabilidades de aplicações registros do grupo do Campeão de segurança.
Entrada de vulnerabilidade da aplicação [sn_vul_app_vul_entry]	Contém entradas de vulnerabilidade da aplicação.
Integração de vulnerabilidade da aplicação [sn_vul_app_integration]	Contém Resposta a vulnerabilidades de aplicações registros de integração.
Localização de verificação de vulnerabilidades da aplicação	Contém informações do local de verificação de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_app_vul_scan_location]	
Resumo de verificação de vulnerabilidades da aplicação [sn_vul_app_vul_scan_summary]	Contém informações de resumo de verificação de terceiros.
Item vulnerável da aplicação [sn_vul_app_vulnerable_item]	Contém registros AVI. A partir da v19.0, as seguintes colunas foram adicionadas à lista de materiais de software: • sn_sbm_config_rule • sn_sbom_component • vex_justification • vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Aplicação escaneada [sn_vul_app_scanned_application]	Contém informações da aplicação.
Mapa de Estado [sn_vul_app_state_map]	Contém mapeamento de estado de integrações de terceiros para estados de item vulnerável da aplicação (IVA).
CWEs de vulnerabilidade [sn_vul_m2m_entry_cwe]	Vincula os dados de CVE a entradas vulneráveis da aplicação.
Manifesto de tarefa de correção da aplicação sn_vul_app_rt_manifest	Todas as atualizações na tarefa de correção são feitas usando esta tabela de manifesto por trabalhos agendados.
Tarefa de correção da aplicação sn_vul_app_vulnerability	Contém tarefas de correção da aplicação.
Item da Tarefa de correção da aplicação sn_vul_app_m2m_vul_group_item	Tabela M2M entre AVI e tarefas de correção de aplicação.
Versão 21.0: Itens vulneráveis da aplicação sn_vul_app_vulnerable_item	Contém registros AVI.
Versão 21.0:	Contém detalhes do pacote de aplicações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Pacote [sn_vul_app_package]	
Versão 21.0: Licenças sn_vul_app_license	Contém licenças de aplicações.
Versão 21.0: Tarefas de correção da aplicação sn_vul_app_vulnerability	Contém tarefas de correção da aplicação.
sn_vul_blackduck_config	Contém detalhes de configuração de integração do Black Duck.
sn_vul_blackduck_project	Contém detalhes dos projetos provenientes do Black Duck.
sn_vul_blackduck_project_import	Tabela de conjunto de importação para a ingestão do projeto Black Duck.
sn_vul_blackduck_app_import	Tabela de conjunto de importação para a ingestão da aplicação Black Duck.
sn_vul_blackduck_avit_import	Tabela de conjunto de importação para a ingestão de AVIT de Black Duck.

Estados de item vulnerável de aplicação (IVA)

Resposta a vulnerabilidades de aplicações oferece um modelo de estado para o status dos itens vulneráveis da aplicação (IVAs) a qualquer momento. Saber como cada estado se relaciona e afeta um ao outro ajuda a determinar quando e como corrigir seus IVAs.

Estados de item vulnerável da aplicação

Entender como os estados funcionam ajuda a criar ou editar regras de item vulnerável da aplicação (IVA). Os IVAs têm vários estados possíveis que são mapeados a partir do status de correção importado da integração de terceiros. Em um AVI, o campo **Estado** é somente leitura.

Resposta a vulnerabilidades de aplicações diagrama de fluxo de estado

Estado	Descrição
Aberto	Estado após a criação. A partir deste estado, você pode: V16: obter mais detalhes Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações diagrama de fluxo de estado

Estado	Descrição
	• Recomendação • Referências • Solicitação • Resposta V16: marcar como falso-positivo Marque um item como falso-positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas na verdade não há vulnerabilidade. V16: Solicitar exceção Solicite uma exceção, uma data de reabertura (Até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item até a data em que uma exceção é solicitada. V15: fechar Selecione o estado Fechado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Encerra o AVI. V15: Resolver Marque um AVI aberto como Resolvido para movê-lo para um estado resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação.
Adiado	**V15:** é acionado pela opção **Solicitar exceção**. Como parte do fluxo de trabalho de aprovação, o estado Adiado é Em revisão e não pode ser fechado até ser aprovado. A partir deste estado, você pode: V16: obter mais detalhes Obtenha as seguintes informações sobre um AVI importado do Fortify:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações diagrama de fluxo de estado

Estado	Descrição
	• Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta Reabrir Faz a transição de um AVI encerrado ou resolvido de volta para um estado Aberto. Fechar Selecione o estado Encerrado, um motivo e forneça informações adicionais. Encerra o AVI.
Sob Investigação	Selecione esta opção na lista **Estado**. A partir deste estado, você pode: V20.0 Faça a transição manual de uma tarefa de correção ou registro AVI para **Aguardando implementação**. V16: obter mais detalhes Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta V16: marcar como falso-positivo Marque um item como falso-positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas na verdade não há vulnerabilidade. V16: Solicitar exceção

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações diagrama de fluxo de estado

Estado	Descrição
	Solicite uma exceção, uma data de reabertura (Até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item até a data em que uma exceção é solicitada. V15: fechar Selecione o estado Fechado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Encerra o AVI. V15: Resolver Marque um AVI aberto como Resolvido para movê-lo para um estado resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação.
Aguardando Implementação	Você só pode fazer a transição de registros para este estado manualmente selecionando Aguardando implementação de AVI e registros de tarefa de correção no estado Sob investigação. A partir deste estado, você pode: Aberto Faz a transição do AVI de volta para um estado Aberto. Sob Investigação Obtenha mais informações para resolução. Transições para Sob investigação. Resolver Marque um AVI aberto como Resolvido para movê-lo para um estado resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação. Fechar Selecione o estado Fechado, um motivo na caixa de diálogo Fechar item vulnerável e

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades de aplicações diagrama de fluxo de estado

Estado	Descrição
	forneça informações adicionais. Encerra o AVI. Nesse estado, faça a transição de um registro para Aguardando implementação quando sua pesquisa e trabalho em uma tarefa estiverem concluídos e, embora uma correção esteja pronta para implementação, ela ainda não estará disponível. Defina a **data do compromisso** de correção e os campos do **plano** de correção. Após a implementação, você resolve ou fecha os registros.
Resolvido	Acionado a partir do botão Resolver. A partir deste estado, você pode: V16: obter mais detalhes Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta Reabrir Faz a transição de volta para um estado **Aberto**. Fechar Selecione o estado **Encerrado**, um motivo e forneça informações adicionais. Encerra o grupo. As informações de Anotações e Resolução aparecem na guia **Anotações**.
Encerrado	Acionado a partir do botão Fechar. A partir deste estado, você pode: Reabrir: faz a transição de volta para um estado Aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

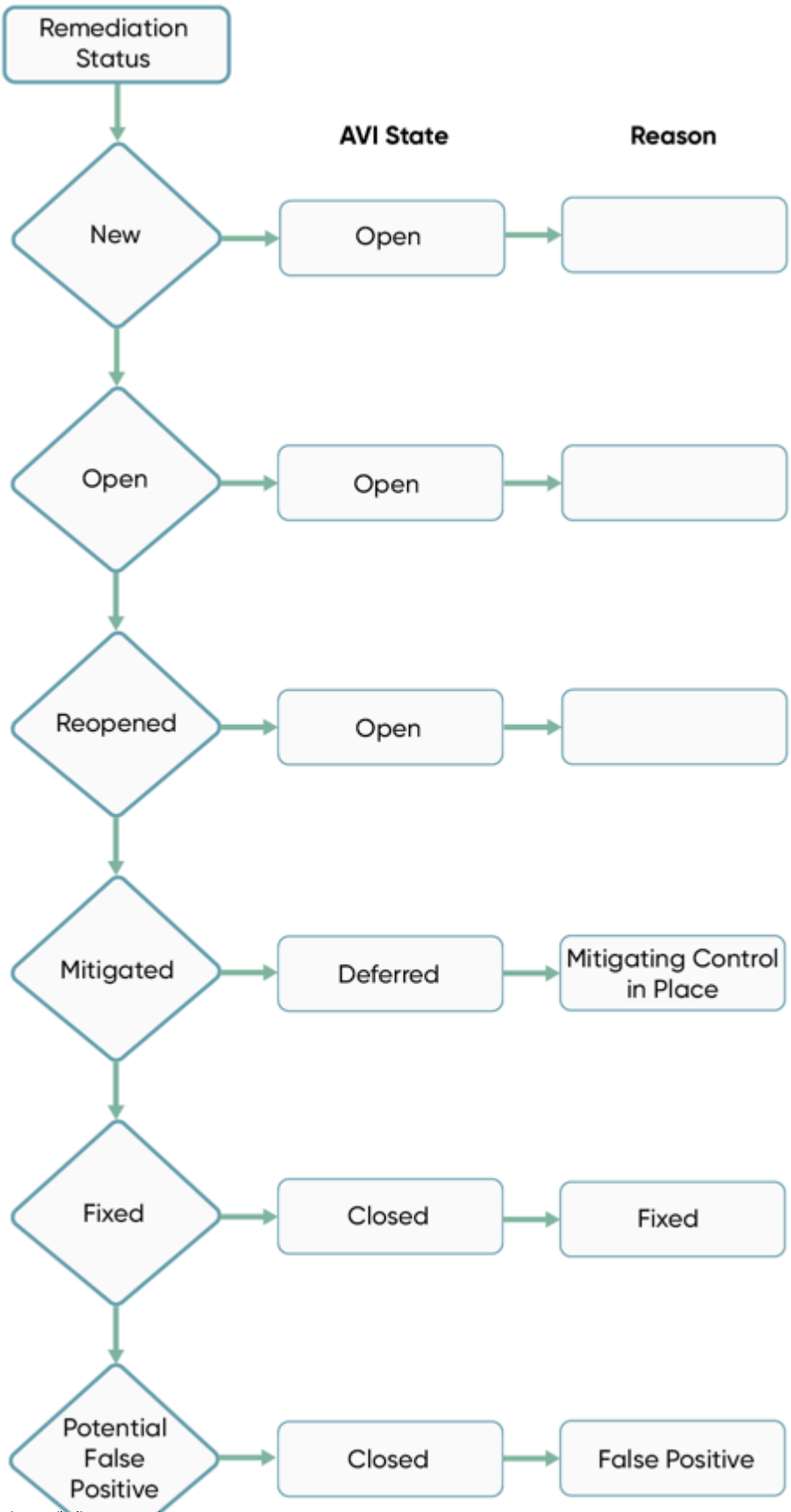
O mapeamento de estados por integração é mostrado da seguinte forma.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de estado para Veracode

Nota: Este mapeamento de estado é aplicável somente quando a opção de triagem em ServiceNow não está selecionada.

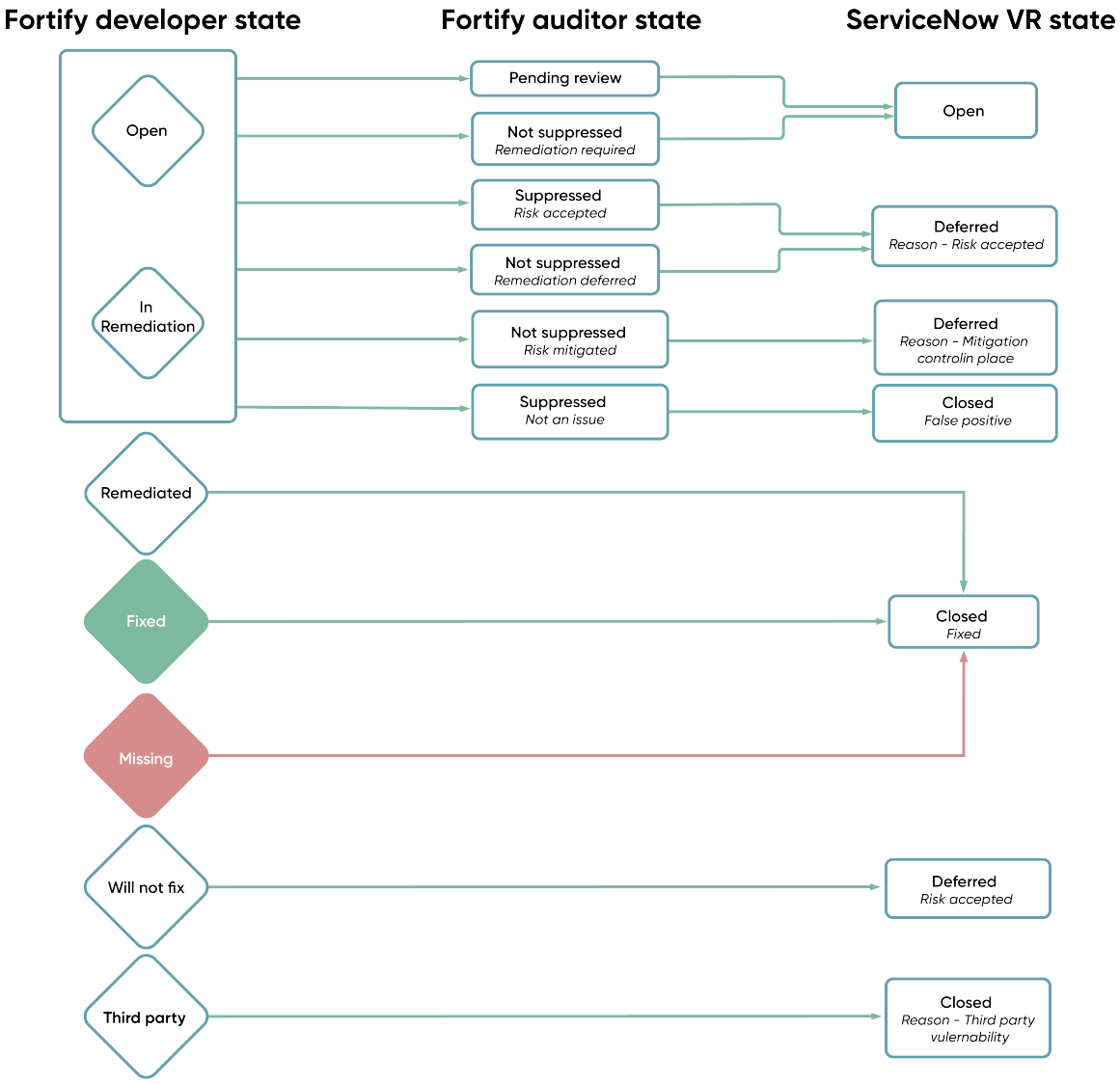


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de estado para Fortify

Nota: Este mapeamento de estado é aplicável somente quando a opção de triagem em ServiceNow não está selecionada.



Tradução automática

Resposta a vulnerabilidades de aplicações exemplos de regra de tarefa de correção

Um exemplo de regra de tarefa de correção usando o Construtor de condições.

Uma regra de tarefa de correção usando vulnerabilidade, modelo de produto, endereço IP e grupo de atribuição

1. No construtor de condições em um novo registro, defina a condição como **Vulnerabilidade** > **é** e insira uma vulnerabilidade conhecida.

   As vulnerabilidades são importadas das integrações do Nation Vulnerability Database (NVD) e do Common Weakness Enumeration (CWE), conforme descrito em Como configurar o Resposta a vulnerabilidades de aplicações.

2. Na seção Agrupar por, selecione o **item Vulnerável** da aplicação para o campo **Agrupar itens vulneráveis da aplicação de**.

3. No campo Usando, selecione **Grupo de atribuição**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use Regras de atribuição para definir automaticamente o campo **Grupo de atribuição** para uso em sua regra de tarefa de correção. Você pode usar uma regra fornecida com a aplicação ou configurar suas próprias regras de atribuição. Para obter mais informações, consulte Atribuir itens vulneráveis de aplicação em Resposta a vulnerabilidades de aplicações automaticamente.

4. Selecione outra condição, por exemplo, item de configuração de item **vulnerável da aplicação no campo Agrupar item vulnerável da aplicação** e endereço IP ou modelo de produto no campo **Usando**.
5. Na seção Atribuição, para Atribuir tarefa de correção campo a campo, selecione **Agrupar por campo**.
6. No campo Agrupar por, selecione **Grupo de atribuição**.

   Conforme descrito nesta seção, esta seleção atribui itens vulneráveis a vários grupos com base nas condições definidas na seção agrupar por. Embora os AVIs compartilhem a vulnerabilidade, eles são atribuídos a diferentes grupos com base no modelo de produto de IC ou por endereço IP.

7. Selecione **Enviar** para salvar sua regra.

Campos da aplicação verificados

As aplicações são armazenadas durante a importação em **Administração** > **Aplicações** in Resposta a vulnerabilidades de aplicações.

Campos da aplicação verificados

Os campos importados nesta tabela são somente leitura, a menos que seja especificado de outra forma. As entradas de**departamento** e **grupo de suporte** podem ser adicionadas ou editadas manualmente por um gerente do App-Sec.

Campo	Descrição
Nome	Nome importado da aplicação.
Versão	Versão importada da aplicação, quando aplicável.
Status operacional	Status operacional importado da aplicação.
Departamento	Departamento importado ao qual a aplicação pertence. Se estiver vazio, ele poderá ser adicionado manualmente.
Unidade de negócios	Unidade de negócios importada à qual o departamento pertence. Quando o campo **Departamento** é preenchido, este campo é preenchido automaticamente com a Unidade de negócios à qual o departamento pertence. Caso contrário, ele será deixado em branco e somente leitura.
Grupo de suporte	Grupo de suporte importado ao qual a aplicação pertence. Se estiver vazio, ele poderá ser adicionado manualmente.
Descrição	Descrição importada da aplicação.
Data da última verificação de conformidade com a política	Data em que a aplicação foi verificada pela última vez pelo Veracode quanto à conformidade com a política. É usado nas integrações encadeadas da integração da lista de aplicações, em que o suporte está disponível para ingestão delta para aplicações,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	comparando esta data com a hora de início delta das respectivas integrações. **Nota:** Os dados são recuperados para aplicações extraídas do Veracode, cujo valor de "Data da última verificação de conformidade com a política" é maior ou igual à "Hora de início" (delta_start_time) das integrações encadeadas.
Lista relacionada (visível somente para um gerente de App-Sec ou campeão de segurança)	
Campeão de segurança	Lista as aplicações associadas a um campeão de segurança. Os gerentes do App-Sec podem adicionar ou remover membros da lista.

Campos de item vulnerável da aplicação

Os itens vulneráveis da aplicação (IVAs) são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Campos de item vulnerável da aplicação

Com exceção dos campos **Grupo de atribuição**, **Atribuído a** e **Anotações**, todos os outros campos no AVI são somente leitura.

Campo	Descrição
Número	Identificador AVI gerado automaticamente para este registro.
Tipo de verificação	Tipo de scanner que encontrou este AVI. As opções são: • Dinâmico • Estático • SCA
Pontuação de risco	**Pontuação de risco** quantificado que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Calcular risco em Resposta a vulnerabilidades de aplicações automaticamente.
Pontuação de risco	Valor calculado de risco que o AVI representa para o seu ambiente. Para obter mais informações, consulte Calcular risco em Resposta a vulnerabilidades de aplicações automaticamente.
Data do compromisso de correção	Os AVIs de data devem ser corrigidos depois de serem movidos para **Sob investigação**. Este campo aparecerá somente se o IVA estiver em **Sob investigação**.
Meta de correção	Data em que os IVAs devem ser corrigidos, desde a primeira identificação. Aparece somente quando aplicável. Para obter mais informações sobre metas de correção, consulte Automatizar o acompanhamento da meta de correção no Resposta a vulnerabilidades de aplicações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status da Correção	Status da correção do AVI. É determinado pelo AVI com a data de vencimento mais próxima, quando aplicável. Os estados incluem: • Em andamento • Perto da meta • Destino anterior
Nome da categoria	Nome da categoria da vulnerabilidade.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável da aplicação.
Versão da aplicação	Versão da aplicação.
Módulo da aplicação	Aplicação afetada na verificação do DAST. Oculto para verificações SAST.
Local Versão 14.0: SAST	DAST: local da URL da vulnerabilidade na aplicação. SAST: caminho do arquivo e número da linha da vulnerabilidade na aplicação.
Estado	O padrão deste campo é **Aberto** quando criado. Consulte Estados de item vulnerável de aplicação (IVA) para obter mais informações sobre como os estados são mapeados.
Motivo	[Visível somente quando o AIV está no estado **Fechado**.] Explicação do estado.
Grupo de atribuição	Grupo selecionado para trabalhar neste AVI. Pode ser adicionado ou editado manualmente por um gerente do App-Sec.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha neste AVI. Pode ser adicionado ou editado manualmente por um gerente de App-Sec
Primeiro encontrado	Data em que a origem de terceiros encontrou o item vulnerável da aplicação pela primeira vez.
Último encontrado	Data em que a origem de terceiros encontrou o item vulnerável da aplicação pela última vez.
Encerrado	[Visível somente quando o AVI está no estado **Encerrado**.] Data em que o AVI foi encerrado.
Encerrado por	[Visível somente quando o AVI está no estado **Fechado**.] Entidade que fechou o AVI.
Resumo	Descrição importada da vulnerabilidade.
Descobertas Dados somente leitura importados da integração de terceiros.	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID de AVIT de origem	Identificador importado para o AVI de origem.
Gravidade de origem	Gravidade importada da aplicação de origem.
Data de correção de destino da origem	Data importada em que a origem espera que o IVA seja corrigido.
Status de mitigação da origem	Status de mitigação importado da aplicação de origem.
Status da correção da origem	Status de correção importado da aplicação de origem.
Status de descoberta da origem	[Visível somente quando preenchido] Status do problema importado da aplicação de origem.
Status SDLC	Status do ciclo de vida de desenvolvimento de software importado.
Está em conformidade com a política	Status de conformidade importado. Se nenhum status for fornecido, este campo será definido como **Não aplicável**.
Link de origem	URL para o AVI de origem.
Anotações de origem	Anotações importadas da origem.
Resumo da vulnerabilidade	Resumo importado da origem.
Explicação da vulnerabilidade	Explicação importada da origem.
Recomendação	Recomendação importada da origem.
Referências	Referências importadas da origem.
Solicitação/resposta HTTP (visível somente para verificações DAST)	
Solicitação de origem	Solicitação HTTP
Resposta de origem	Resposta HTTP
Anotações	
Plano de correção	Detalhes de como os IVAs serão corrigidos. O plano deve ser implementado até a **data do Compromisso**de correção . Este campo aparecerá somente se o IVA estiver em **Sob investigação**.
Comentários adicionais/ Anotações de trabalho	Qualquer informação relevante. Selecione a caixa de texto de Anotações de trabalho para adicionar informações. A partir da Resposta a vulnerabilidades v20.0, você pode adicionar anotações de trabalho na seção Anotações de um item vulnerável da aplicação adiado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados dos testes de invasão

Os proprietários de aplicações podem solicitar avaliação de teste de invasão para suas aplicações e monitorar o andamento da equipe de invasão ética até que a solicitação seja resolvida.

A solicitação de avaliação de teste de invasão passa pelos seguintes estados de transição até que seja resolvida.

Fases da solicitação de avaliação de teste de invasão

Campo	Descrição
Estados dos testes de invasão	
Aberto	Estado quando a solicitação de avaliação é criada pelo proprietário da aplicação.
Escopo	A equipe de invasão ética avalia a solicitação e o escopo da aplicação.
Preparação do ambiente	O proprietário da aplicação cria um ambiente com funções e outras informações e o fornece à equipe de invasão ética para testes.
Testando	A equipe de invasão ética testa manualmente a aplicação para identificar as descobertas do teste de invasão.
V16.1: Testes em andamento	A equipe de invasão ética indica que o teste está em andamento. Se este estado for selecionado, a opção **Testando em espera** se tornará disponível no formulário.
V16.1: Testes em espera	Este campo é exibido somente quando o estado Teste em andamento está selecionado. A equipe de invasão ética controla os acordos de nível de serviço (ANS) das solicitações de avaliação de teste de invasão selecionando este estado, se necessário. Isso garante que SLAs precisos sejam relatados.
V16.1: Testes em revisão	A equipe de invasão ética indica que o teste foi concluído e está sendo revisado por um especialista no assunto.
Encerrado	A equipe de invasão ética encerra as solicitações de avaliação de teste de invasão depois que as descobertas do teste de invasão são relatadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fases da solicitação de avaliação de teste de invasão

Campo	Descrição
	Nota: A partir da V16.1, você pode usar a opção **Copiar e criar solicitação** no formulário para replicar a solicitação no estado Encerrado e criar uma nova solicitação. Para obter detalhes, consulte Replicar uma solicitação de teste de invasão no estado fechado.
V16.1: Cancelado	O proprietário da aplicação cancela a solicitação de avaliação de teste de invasão.
V16.1: Rascunho	O proprietário da aplicação cria uma solicitação e a salva como rascunho antes de enviar a solicitação.
Estados de item vulnerável da aplicação	
Aberto	Quando a equipe de invasão ética identifica e cria as descobertas do teste de invasão, seu status é Aberto.
Resolvido	Quando a equipe de aplicações resolve as descobertas do teste de invasão, seu status é movido para Resolvido. **Nota:** Se a descoberta do teste de invasão tiver sido resolvida, mas ainda não tiver sido validada pela equipe de invasão ética, o subestado será *`Validation Pending`*.
Encerrado	A equipe de invasão ética valida que as descobertas do teste de invasão foram resolvidas e move o status para Encerrado.

Tradução automática

Como gerenciar o mapeamento de estado para adiamentos e falso-positivos no Resposta a vulnerabilidades de aplicações

Você pode gerenciar como os estados de **origem** nos itens vulneráveis da aplicação (IVAs) importados por Veracode Vulnerability Integration e Integrações de vulnerabilidade do Fortify são mapeados em sua instância após a importação.

A partir da v20.0 de Resposta a vulnerabilidades, você tem mais opções para fazer a triagem de seus AVIs importados com fluxos de trabalho ServiceNow.

Quando você Configure o Integrações de vulnerabilidade do Fortify ou o Configure o Veracode Vulnerability Integration, as páginas de configuração de integração fornecem duas opções para ajudá-lo a gerenciar exceções e falsos positivos em sua instância.

- Gerenciar exceções no ServiceNow
- Gerenciar falsos positivos no ServiceNow

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: gerente do App-Sec.

Caso de uso para gestão de exceções

IVAs são importados dessas integrações com estados de **origem**. Na importação, esses estados são mapeados para os estados **Destino** e **Motivo** de destino em sua instância porque, em alguns casos, não há correspondências exatas entre os estados de origem do scanner e os estados usados pela instância.

Por exemplo, estados de origem como **Não corrigirá**, **Correção adiada**, **Risco aceito**e **Risco mitigado** de Integrações de vulnerabilidade do Fortify são mapeados para o estado **Adiado** com um subestado de **Risco aceito** ou **Controle de mitigação em vigor** na sua instância.

Você tem as seguintes opções nas páginas de configuração dessas integrações:

Opção	Caixa de seleção selecionada	Descrição
Gerenciar exceções no ServiceNow	Y (por padrão)	Se você deixar esta opção selecionada, deverá solicitar exceções de registros AVI. AVIs importados marcados para o estado **Adiado** são triados com o fluxo de trabalho ServiceNow de gestão de exceções. AVIs com estados de **origem** que normalmente são mapeados para um estado **adiado** são mapeados para o estado de **triagem de destino no estadoaberto**.
	N	Se você desativar a caixa de seleção, preservará os estados de **origem** importados do scanner. Esses AVIs são mapeados para o **estado de destino** como **Adiado**e para um estado de **motivo de destino** em sua instância. Eles não são triados pelo fluxo de trabalho de exceção, porque não são mapeados para o estado de **triagem** de **destino e os estados de motivo da triagem** de destino. A ação de IU **Solicitar exceção** não está disponível no registro AVI porque o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Caixa de seleção selecionada	Descrição
		registro já está no estado Destino **adiado**.

Caso de uso para falso-positivo

Para falso-positivos de Veracode Vulnerability Integration como umexemplo, estados de origem como **Falso-positivo** ou Possível falso- **positivo** são mapeados para o **estado de destinofechado** com um subestado de **Falso-positivo**.

Opção	Caixa de seleção selecionada	Descrição
Gerenciar falsos positivos no ServiceNow	Y (por padrão)	Se você deixar esta opção selecionada, deverá solicitar um **falso-positivo** dos registros AVI. AVIs importados marcados para os estados **Falso-positivo** ou **Possível falso** -positivo são triados com o fluxo de trabalho ServiceNow Gestão de exceções. AVIs com estados de **origem** que normalmente são mapeados para um **estado de destinofechado** são mapeados para um estado de **triagem de destino** em **aberto**. A ação de IU **de falso-positivo** está disponível no registro AVI.
	N	Se você desativar a caixa de seleção, preservará os estados de **origem** importados do scanner. Esses AVIs são mapeados para o **estado de destino** como **encerrado** e um estado de **motivo de destino** em **falso-positivo** em sua instância. Eles não são triados pelo fluxo de trabalho de falso-positivo. A ação de IU **de falso-positivo** não está disponível no registro AVI porque o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Caixa de seleção selecionada	Descrição
		registro já está no estado de destino **fechado**.

referências de Resposta a vulnerabilidades de aplicações

Os termos a seguir são usados em Resposta a vulnerabilidades de aplicações.

Itens vulneráveis da aplicação (IVAs)

Pares de entradas de vulnerabilidade e aplicações potencialmente vulneráveis no ambiente da sua empresa.

Regras de atribuição

Regras usadas para atribuir AVIs com base nos critérios definidos.

Enumeração de plataforma comum (CPE)

Um esquema de nomenclatura estruturado do NIST NVD para sistemas, software e pacotes de tecnologia da informação.

Vulnerabilidades e Exposições Comuns (CVE)

Dicionário de vulnerabilidades e exposições de segurança da informação conhecidas publicamente.

Enumeração de pontos fracos comuns (CWE)

Lista de tipos de pontos fracos de software desenvolvidos pela comunidade.

Integrações

Trabalhos agendados que extraem dados de relatório do CWE ou de um sistema de terceiros, como Veracode, para recuperar dados de vulnerabilidade.

> **Nota:** Se a integração do banco de dados nacional de vulnerabilidades do NIST em Resposta a vulnerabilidades estiver ativada e configurada, o aprimoramento de CVE estará disponível para CWEs, mas não será obrigatório. Para obter informações sobre a integração do banco de dados nacional de vulnerabilidades do NIST, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Banco de dados nacional de vulnerabilidades (NVD)

Repositório do governo dos EUA de dados de gestão de vulnerabilidades baseados em padrões representados usando o Security Content Automation Protocol (SCAP).

Regras de destino de correção

Regras usadas para atribuir datas de destino de IVAs para correção com base nos critérios definidos.

Calculadoras de vulnerabilidade

Calculadoras usadas para priorizar e categorizar vulnerabilidades da aplicação com base nos critérios definidos.

Exemplo de regra de exceção para Resposta a vulnerabilidades de aplicações

Uma regra de exemplo com base em uma vulnerabilidade conhecida para uma regra de exceção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Um nome exclusivo para ajudá-lo a identificar sua finalidade e localizar a regra facilmente, por exemplo, `Veracode-1 cwe-22`.
Estado	Somente leitura: rascunho
Válido de	Data em que esta regra está ativa para adiar AVIs.
Ordem de execução	Ordem exclusiva para cada regra de exceção. Um valor mais baixo precede um mais alto.
Válido até	Data em que a tarefa de correção para de aceitar novos IVs.
Adiado até	Data até quando as tarefas de correção e os AVIs são adiados. Nesta data, o AVUL é encerrado, todos os AVIs são movidos para fora da tarefa e são reabertos. Regras de grupo são reaplicadas a esses AVIs.
Motivo	Motivo para criar esta regra de exceção. Selecione um na lista, por exemplo, **Correção indisponível**.
Grupo de atribuição	Grupo atribuído para rastrear os IVs adiados, por exemplo, APP Sec Manager.
Informação adicional	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção. Neste exemplo, `adie AVIs com a vulnerabilidade – Veracode-1-22`.
Condição	Condições de filtro para especificar quais AVIs correspondem a esta regra. Para este exemplo, `a vulnerabilidade é Veracode-1-22`.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada. Se você deixar esta opção desativada, sua regra será executada diariamente pelo trabalho agendado *`Associate existing AVIs with Auto Exception Rule`*, começando com novos dados. Se você habilitar a opção Executar em dados existentes, um trabalho agendado será executado uma vez nos dados existentes na data **Válido de**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de produto do Resposta a vulnerabilidades de aplicações

O produto Resposta a vulnerabilidades de aplicações (AVR) ingere as fraquezas e vulnerabilidades detectadas por suas ferramentas de teste de segurança de aplicações e fornece um único painel para entender a postura de segurança de todas as aplicações em seu ambiente.

O AVR permite que você reduza os riscos com os fluxos de trabalho de correção. O objetivo desta exibição de produto é ajudar você a entender como as entidades de chave AVR funcionam com a estrutura principal do CSDM.

Terminologia atualizada

A partir do AVR v19.0, a tabela de chaves e os nomes de coluna a seguir foram atualizados. Como resultado, você verá referências aos nomes mais antigos e mais recentes na documentação.

Lista atualizada de termos, tabelas e nomes de campo para AVR

Antes do AVR v19.0	A partir do AVR v19.0
Regras de pesquisa de IC	Regras de pesquisa
Formulário de regra de pesquisa de IC	Formulário de regra de pesquisa
Regra de correspondência de IC	Regra de correspondência
Pesquisar na tabela	Pesquisar na tabela de IC
Pesquisar no campo	Pesquisar no campo de IC
Versão da aplicação	Aplicações descobertas
Tabela de versão da aplicação	Tabela de aplicações descobertas
Criticalidade dos negócios	Criticalidade dos negócios de origem

Pré-requisitos

Instale as versões mais recentes das seguintes aplicações:

- Security Support Common
- Resposta a vulnerabilidades
- Estrutura de integração de segurança
- Orquestração de suporte de segurança
- Integrações de scanner, como Veracode e Fortify

AVR e CSDM 4.0

Antes do AVR v19.0, quando as vulnerabilidades da aplicação eram ingeridas, a aplicação para a qual as vulnerabilidades foram ingeridas era pesquisada usando as regras de pesquisa de IC, em relação às aplicações verificadas (sn_vul_app_scanned_application). Se o registro do nome da aplicação não estiver lá, será feita uma entrada.

A partir do AVR v19.0, para alinhar com a estrutura do CSDM 4.0, as tabelas de modelo de produto são usadas em vez da tabela de aplicações verificadas. Se a aplicação tiver a versão, a pesquisa será na tabela de modelo de software. Se não houver versão, a pesquisa será na tabela de modelo de aplicação. O modelo de aplicativo e o modelo de software

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são tabelas secundárias da tabela de modelo de produto, que é a tabela de base no CMDB. A seguinte captura de tela explica o modelo do produto.

Propriedade do sistema

Para usar o processo de pesquisa baseado em modelo de produto do CSDM 4.0, defina a propriedade do sistema *sn_vul.use_product_model* como *true*.

Considerações de propriedade do sistema

Nome da propriedade do sistema	Valor da propriedade do sistema	Pesquisar valor de destino	Considerações
sn_vul.use_product_model	verdadeiro	Selecione o valor do **modelo de produto**	Os novos usuários devem selecionar o valor **Modelo de produto** para usar as regras de pesquisa de modelo de produto da estrutura do CSDM 4.0.
	falso	Selecione o **item de configuração**de valor	Os usuários existentes podem continuar usando o processo de pesquisa de IC e as **regras de pesquisa de IC**existentes.

Nota: Para definir o valor de destino da pesquisa, navegue até a página **Regra de pesquisa** > **[Regra de pesquisa de integração AVR]** > **Pesquisar campo de destino**.

Regras de pesquisa no AVR

Na estrutura do CSDM 4.0, as regras de pesquisa baseadas em modelo de produto são usadas em vez de regras de pesquisa de IC para criar entradas nas respectivas classes de modelo de produto. Da mesma forma para scripts, você pode definir as regras de pesquisa na estrutura do modelo CSDM 4.0.

A partir do AVR v19.0, ao criar uma regra de pesquisa, você deve definir se deseja usar o item de configuração ou a abordagem de modelo de produto usando o campo de **destino de pesquisa**. Para obter mais informações, consulte Criar uma regra de pesquisa de IC.

Aplicações descobertas

Navegar até **Todos** > **Aplicações descobertas**. A tabela Aplicações descobertas exibe as aplicações ingeridas dos scanners. Se a propriedade do sistema *sn_vul.use_product_model* estiver definida como *true*, você poderá ver os modelos de produto correspondentes para as aplicações.

Considerações de AVR

Presença de registros duplicados de IC ou modelo de produto

Verifique se a propriedade do sistema *sn_vul.use_product_model* foi configurada corretamente para o processo de pesquisa. Certifique-se de selecionar o **item de**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configuração ou o **modelo de produto** como o destino de pesquisa ao configurar o formulário de regra de pesquisa.

Contêiner de Resposta a vulnerabilidades

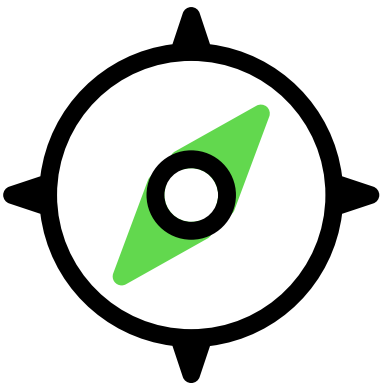
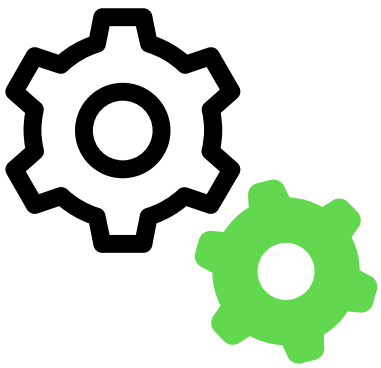
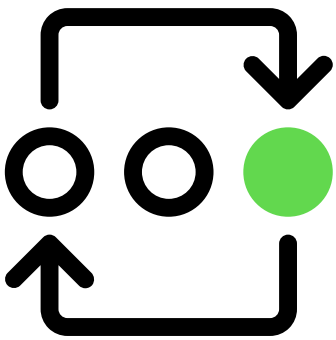
A aplicação ServiceNow® Contêiner de Resposta a vulnerabilidades importa itens vulneráveis de contêiner (CVITs) e, de acordo com as regras, permite que você corrija vulnerabilidades de contêiner. Os dados de vulnerabilidade são extraídos de fontes internas e externas, como o National Vulnerability Database (NVD) ou integrações de terceiros.

A partir da versão 18.0 do Resposta a vulnerabilidades, você pode monitorar e corrigir CVITs no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI, respectivamente. Para obter mais informações, consulte Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

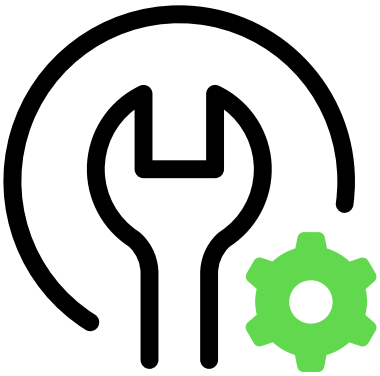
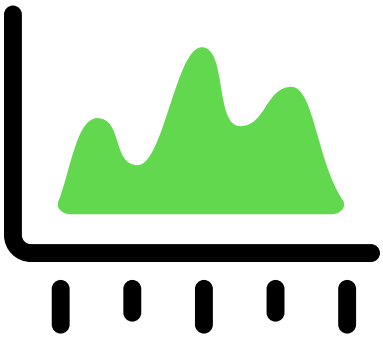
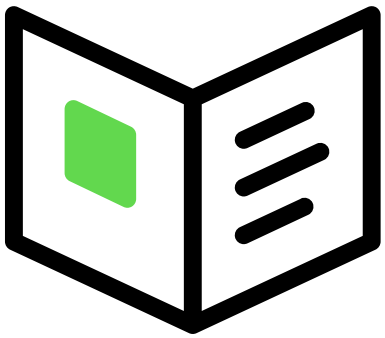
Contêiner de Resposta a vulnerabilidades

Explorar	Configurar	Integrar
		
Saiba mais sobre os conceitos e recursos da Resposta a vulnerabilidades do contêiner.	Configure a Resposta a vulnerabilidades do contêiner.	Amplie a Resposta a vulnerabilidades do contêiner integrando-o a outras aplicações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contêiner de Resposta a vulnerabilidades

Corrigir	Análise e Emissão de relatórios	Referência
		
Saiba como corrigir vulnerabilidades de contêiner.	Exibir análise da Resposta a vulnerabilidades do contêiner	Veja os detalhes sobre os componentes da Resposta a vulnerabilidades do contêiner, como campos, tabelas e propriedades.

Tradução automática

Benefícios

A aplicação Contêiner de Resposta a vulnerabilidades oferece os seguintes benefícios:

- Integra-se a produtos de segurança de contêiner de terceiros, como o Prisma Cloud Compute da Palo Alto Networks.
- Importa dados de vulnerabilidade para as imagens implantadas no tempo de execução e aprimora os dados de vulnerabilidade com informações contextuais de tempo de execução (hosts, clusters do Kubernetes, serviços e namespaces).
- Fornece uma lista das referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes no Configuration Management Database (CMDB) usando ServiceNow a Descoberta do Kubernetes.
- Oferece um painel de relatórios abrangente, fornecendo informações sobre as tendências de vulnerabilidade e correção.

Principais recursos

A aplicação Contêiner de Resposta a vulnerabilidades gerencia vulnerabilidades detectadas nos contêineres. Ele fornece os seguintes recursos:

- Aponte para a imagem do Docker de origem de CVITs em vez de executar contêineres.
- Configure a granularidade de CVITs para rastrear na imagem, no cluster do Kubernetes, no namespace ou no nível de serviço.
- Rastreie novas versões de imagem para identificar vulnerabilidades corrigidas. Todas as vulnerabilidades relatadas em versões mais antigas são resolvidas automaticamente em ServiceNow quando novas versões de imagem são implantadas no tempo de execução.
- Rastreie CVITs em imagens de base separadamente das imagens da aplicação para habilitar a correção independente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Gere solicitações de exceção ou solicitações de falso-positivo, que podem ser revisadas por meio de um processo de aprovador de vários níveis.
- Defina regras de exceção para adiar CVITs automaticamente.

Casos de uso

Os contêineres são uma ótima maneira de implantar e escalonar aplicações em vários ambientes com menos sobrecarga e maior portabilidade. No entanto, as vulnerabilidades nas imagens de contêiner podem representar risco para o host subjacente e, por fim, para a infraestrutura em que os contêineres foram iniciados a partir dessas imagens. Embora existam muitos produtos de segurança de contêiner que verificam imagens de contêiner em busca de vulnerabilidades, há algumas considerações e problemas associados à correção das vulnerabilidades. Contêiner de Resposta a vulnerabilidades pode ajudar a resolver vários problemas ou casos de uso envolvidos na correção de vulnerabilidades de imagem de contêiner. Explore maneiras de aproveitar o módulo Contêiner de Resposta a vulnerabilidades :

Contexto de tempo de execução

As vulnerabilidades em imagens de contêiner podem ser descobertas com a verificação da imagem nas seguintes fases do ciclo de vida da aplicação.

- Fase 1: quando as imagens estão sendo criadas no pipeline de IC/CD.
- Fase 2: quando as imagens são publicadas no registro
- Fase 3: quando as imagens são implantadas no tempo de execução.

Embora seja importante identificar vulnerabilidades o mais cedo possível na fase 1 e na fase 2, é igualmente importante executar uma verificação nas imagens implantadas em um ambiente de tempo de execução. Ele oferece os seguintes benefícios:

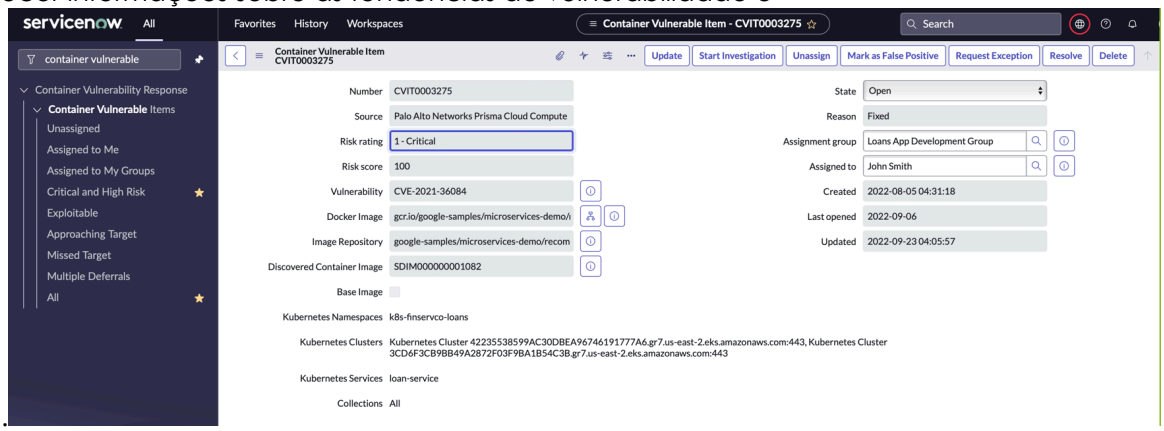
- Identificar novas vulnerabilidades e exposições comuns (CVEs) que foram publicadas.
- Fornecer visibilidade precisa sobre a postura de risco das aplicações implantadas.
- Priorização de vulnerabilidades que devem ser resolvidas. O contexto do tempo de execução em termos dos serviços de aplicações ou serviços de negócios afetados devido a uma vulnerabilidade pode ajudar na priorização.

Contêiner de Resposta a vulnerabilidades se integra a produtos de segurança de contêiner, como o Prisma Cloud Compute de Palo Alto Networks, para extrair os dados de vulnerabilidade das imagens implantadas no tempo de execução e aprimora os dados de vulnerabilidade com as informações contextuais do tempo de execução, como hosts, clusters do Kubernetes, serviços e namespaces em que essas imagens de contêiner estão implantadas. Os clientes que usam a ServiceNow descoberta do Kubernetes podem ver as referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes em seus Configuration Management Database (CMDB). Além de aprimorar os metadados, o ServiceNow também oferece um painel de relatórios abrangente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para fornecer informações sobre as tendências de vulnerabilidade e correção.



Identificar propriedade

Pré-requisitos

- **Metadados e referências do Kubernetes**: para que Contêiner de Resposta a vulnerabilidades preencha metadados do Kubernetes (namespace, cluster e assim por diante) e referências a Configuration Management Database (CMDB) entradas, você deve implementar a descoberta do Kubernetes de Information Technology Operations Management (ITOM). A descoberta do Kubernetes preenche a imagem do Docker, os contêineres do Docker em execução, pods, clusters do Kubernetes e assim por diante, no CMDB. Contêiner de Resposta a vulnerabilidades identifica a imagem do Docker em CMDB com base no ID da imagem e, em seguida, identifica as entidades do Kubernetes relacionadas e preenche as referências a essas entidades de itens vulneráveis.

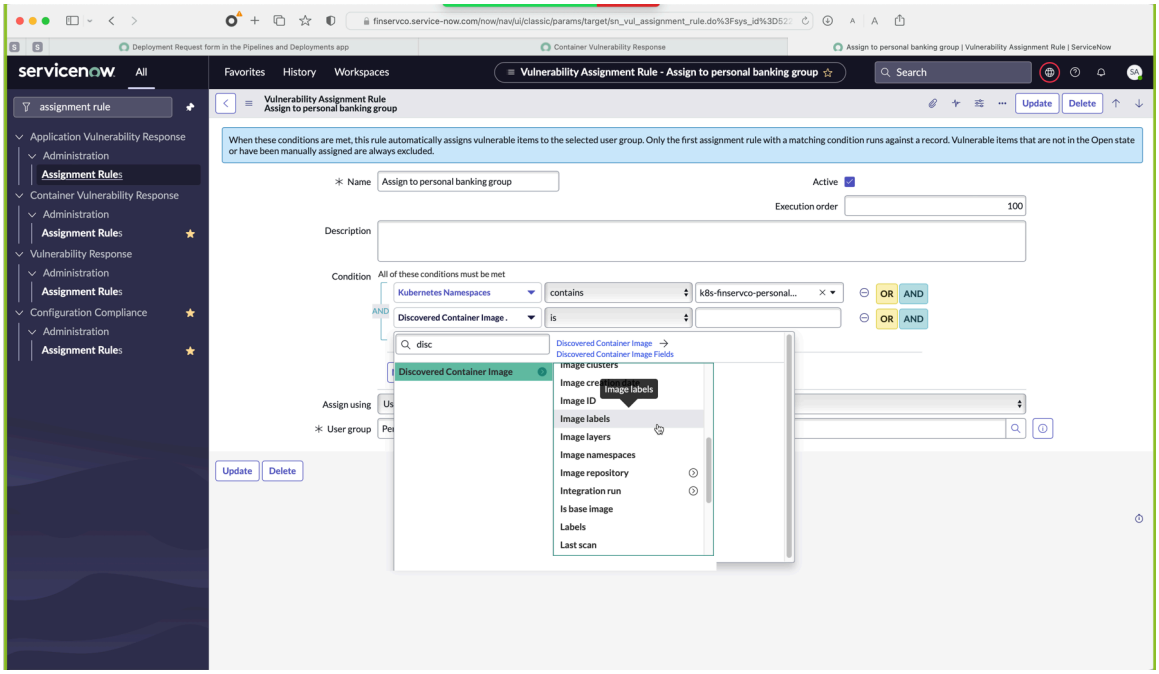
- **Metadados em nuvem e rótulos de imagem do Docker**: Contêiner de Resposta a vulnerabilidades também preenche rótulos de imagem do Docker, IDs de conta em nuvem, regiões onde uma imagem é implantada. Esses dados são mantidos no registro "Imagem de contêiner descoberta" associado ao item vulnerável. Não há pré-requisitos para que esses dados sejam preenchidos. Contêiner de Resposta a vulnerabilidades usa os dados retornados por produtos de segurança de contêiner (por exemplo, Palo Alto Prisma Cloud Compute) para preencher essas entradas.

A propriedade para corrigir uma vulnerabilidade em uma imagem de contêiner pode variar de organização para organização. Essas informações podem ser capturadas em locais diferentes. Algumas organizações usam rótulos de imagem do Docker como uma maneira de identificar as equipes de aplicações que possuem uma determinada imagem de contêiner, enquanto outras organizações podem usar o namespace do Kubernetes ou a conta de nuvem em que uma imagem de contêiner é implantada para identificar o proprietário correto.

Contêiner de Resposta a vulnerabilidades fornece os elementos de modelo de dados necessários para capturar e usar os rótulos de imagem do Docker, os metadados de cluster/serviço/namespace do Kubernetes ou os metadados da conta em nuvem (ID da conta na nuvem, região, provedor e assim por diante) nas "Regras de atribuição" módulo e atribua vulnerabilidades automaticamente à equipe de aplicações certa com base nos metadados da imagem ou no ambiente de tempo de execução.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



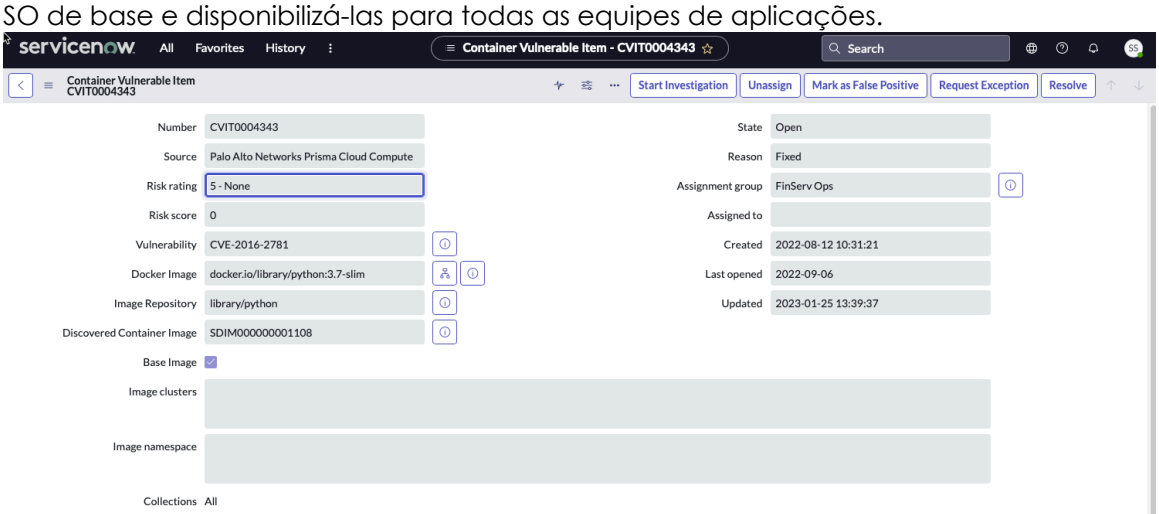
Rastrear vulnerabilidades nas imagens de base

Pré-requisitos

Para que a propriedade "Imagem de base" seja preenchida em Contêiner de Resposta a vulnerabilidades, as imagens de base devem ser configuradas explicitamente no console de Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute. Para obter mais informações sobre como configurar imagens de base no Prisma Cloud, consulte https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-calculate/vulnerability_management/base_images.

Contêiner de Resposta a vulnerabilidades permite a criação de registros de vulnerabilidade separados para uma camada base para que eles possam ser atribuídos a uma equipe diferente.

Rastreie as vulnerabilidades identificadas em uma imagem do SO de base, como o Alpine, a partir das vulnerabilidades detectadas em outras camadas da imagem do contêiner. Muitas organizações têm equipes dedicadas que são responsáveis por corrigir imagens do SO de base e disponibilizá-las para todas as equipes de aplicações.



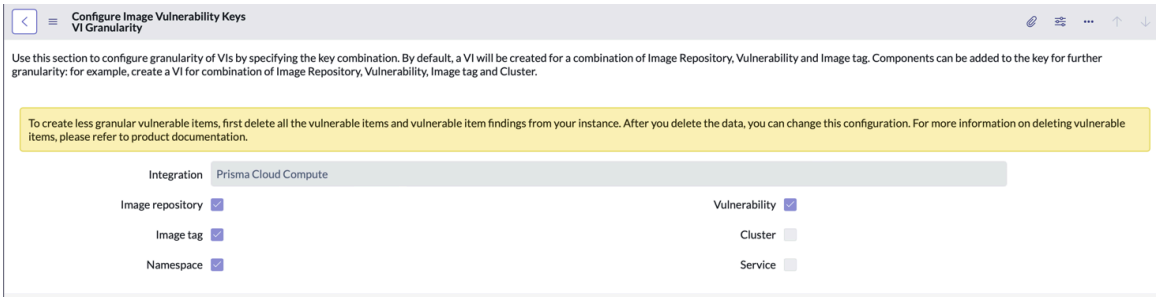
Definir granularidade para itens vulneráveis

Tradução automática

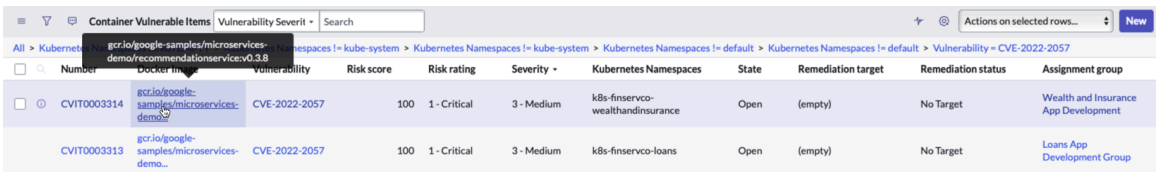
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

Configure a granularidade de CVITs navegando até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Configurar granularidade de IV**.



Por padrão, um item vulnerável é criado para cada combinação exclusiva de CVE e a versão da imagem do Docker (referência + marcador). No entanto, algumas imagens do Docker podem ser implantadas em mais de um namespace do Kubernetes e cada namespace pode pertencer a diferentes unidades de negócios ou equipes. Cada equipe pode seguir sua própria cadência para implantar novas versões de imagens de contêiner para corrigir vulnerabilidades. Para acomodar este cenário, Contêiner de Resposta a vulnerabilidades permite definir granularidade para itens vulneráveis: se um item vulnerável deve ser criado para cada namespace/cluster/serviço do Kubernetes, mesmo para cada combinação exclusiva de versão e vulnerabilidade da imagem do Docker.



No exemplo, você pode ver dois itens vulneráveis criados para a mesma combinação de imagem do Docker e CVE. Um para o namespace do Kubernetes 'k8s-finservco-loans' e outro para 'k8s-finservco-wealthandinsurance'.

Identifique os serviços afetados usando a identificação de serviço baseada em tag

Pré-requisitos

- Identifique vários serviços em sua aplicação e defina os pares de marcadores/chave-valor que representam esses serviços.
- Implante imagens do Docker e pods do Kubernetes com esses marcadores ou rótulos.
- Implantar ITOM Kubernetes Descoberta Defina "Serviços baseados em tag" com as tags ou rótulos corretos.
- Implantar ITOM Kubernetes Discovery
- Defina "Serviços baseados em tag" com as tags ou pares de chave-valor corretos.
- Importar dados de vulnerabilidade para ServiceNow usando Contêiner de Resposta a vulnerabilidades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O cálculo de risco para itens vulneráveis pode ser feito observando o IC (imagem do Docker) e a criticidade dos serviços associados em CMDB. No entanto, para facilitar a identificação de serviços afetados, Contêiner de Resposta a vulnerabilidades oferece identificação de serviço baseada em tag.

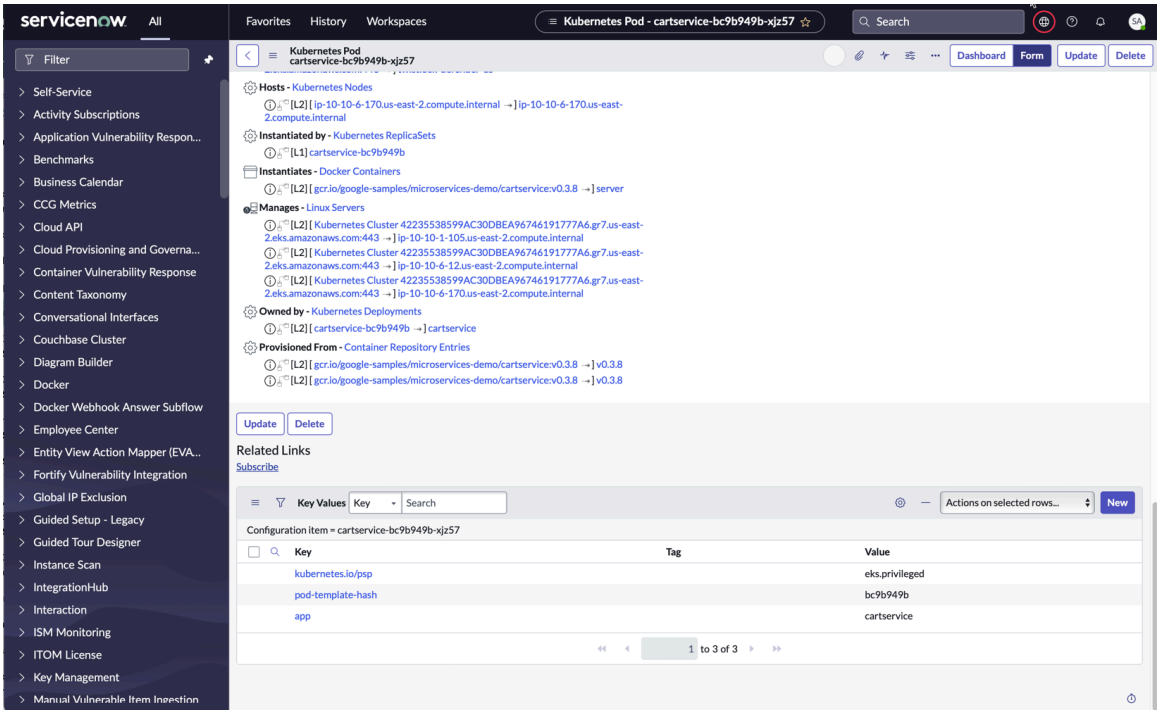
Quando pods ou entidades do Kubernetes são publicados com valores-chave ou rótulos correspondentes aos valores-chave definidos em qualquer "Serviço baseado em marcador" em ServiceNow, Contêiner de Resposta a vulnerabilidades estabelece automaticamente o relacionamento entre uma imagem do Docker e o serviço de aplicações afetado e usa o criticidade desse serviço de aplicações no cálculo de risco.

O fluxo é o seguinte:

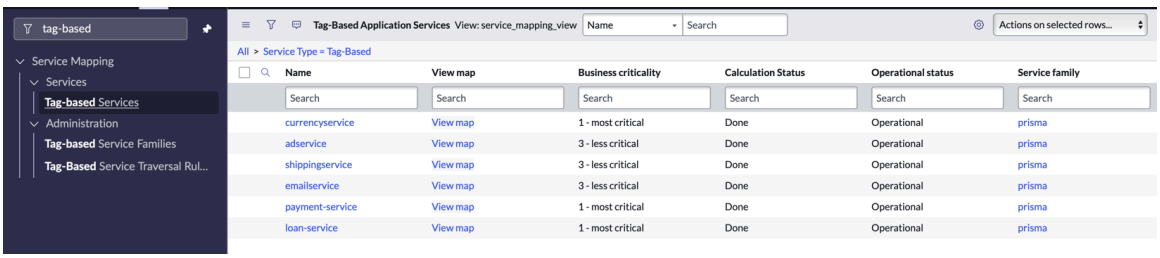
1. Contêiner de Resposta a vulnerabilidades importa dados de vulnerabilidade do produto de segurança de contêiner.
2. Para cada item vulnerável de contêiner, Contêiner de Resposta a vulnerabilidades preenche a imagem do Docker de CMDB que tem a vulnerabilidade.
3. Contêiner de Resposta a vulnerabilidades O analisa os rótulos de imagem do Docker ou os rótulos/valores-chave publicados com os pods do Kubernetes em que esta imagem está implantada. Esta imagem estará disponível em CMDB se você tiver a descoberta do Kubernetes em execução.
4. Contêiner de Resposta a vulnerabilidades pesquisa "Serviços baseados em marcador" em CMDB com os mesmos pares de chave-valor correspondentes definidos.

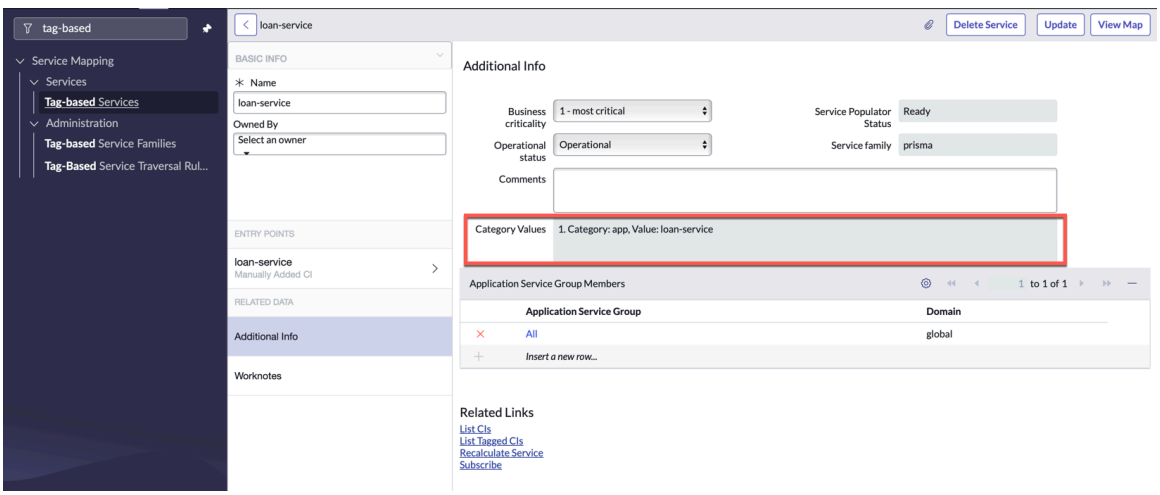
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Contêiner de Resposta a vulnerabilidades usa a "Criticidade dos negócios" do "Serviço baseado em marcador" correspondente (se houver algum encontrado) para calcular o risco de um item vulnerável de contêiner.





Rastreamento de vulnerabilidades

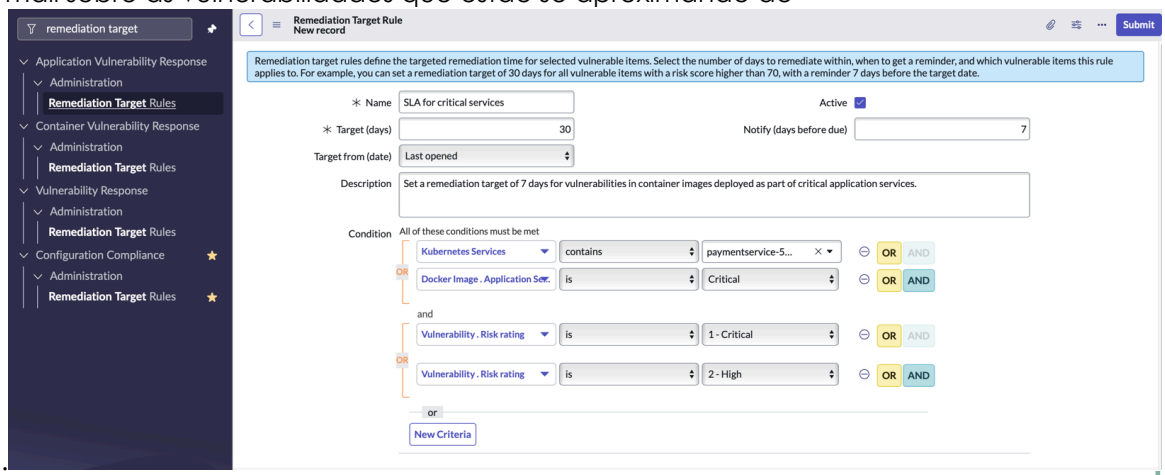
Definir metas de correção

ServiceNow permite que os gerentes de vulnerabilidade definam "Regras de meta de correção" para definir acordos de nível de serviço (ANS) para corrigir vulnerabilidades encontradas em imagens de contêiner.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A data de meta de correção pode ser definida com base em uma condição/critério em metadados de imagem ou informações de vulnerabilidade. Os responsáveis pela correção recebem comunicação por e-mail sobre as vulnerabilidades que estão se aproximando do prazo.



Identificação de vulnerabilidades corrigidas

Ao contrário das vulnerabilidades de host que podem ser corrigidas pela aplicação de um patch em um host, as vulnerabilidades de contêiner não podem ser corrigidas. Novas versões de imagens de contêiner devem ser criadas e implantadas para substituir as versões mais antigas. As novas versões têm um identificador diferente (ID de imagem) em comparação com as versões anteriores, o que torna um desafio acompanhar quais vulnerabilidades já foram corrigidas.

ServiceNow identifica vulnerabilidades que foram relatadas nas versões anteriores das imagens de contêiner, mas resolvidas na versão mais recente da imagem e move automaticamente essas vulnerabilidades para o estado "Fechado/Corrigido" para que as equipes de segurança sempre tenham visibilidade precisa da postura de risco mais recente.

Gerenciar exceções

As equipes de aplicações ou responsáveis pela correção das vulnerabilidades podem precisar da capacidade de solicitar uma exceção devido aos motivos a seguir.

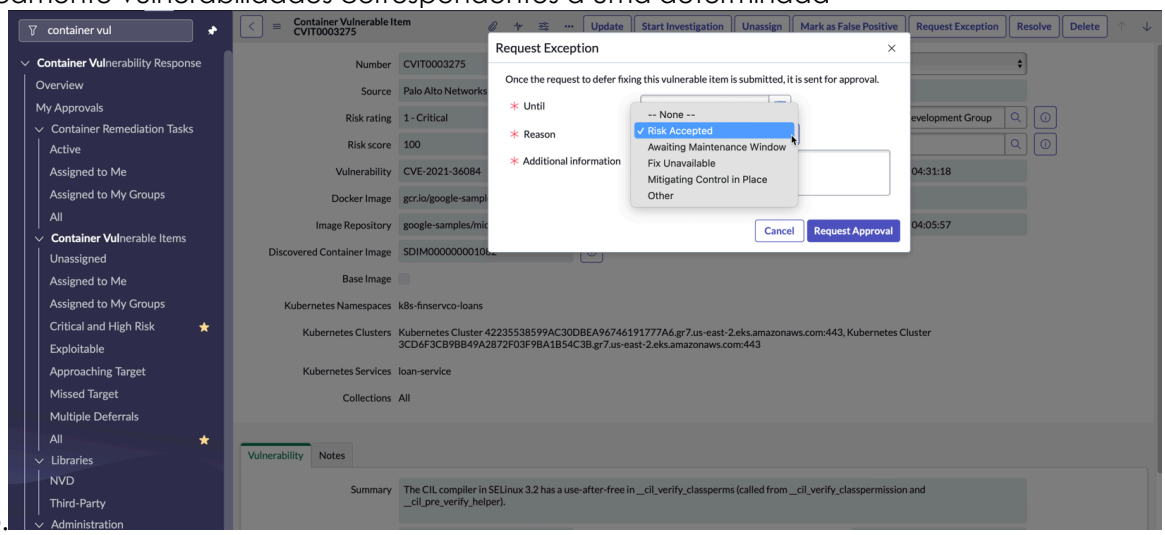
- Um controle de mitigação já está em vigor
- Risco aceito
- Aguardando janela de manutenção para enviar a correção.

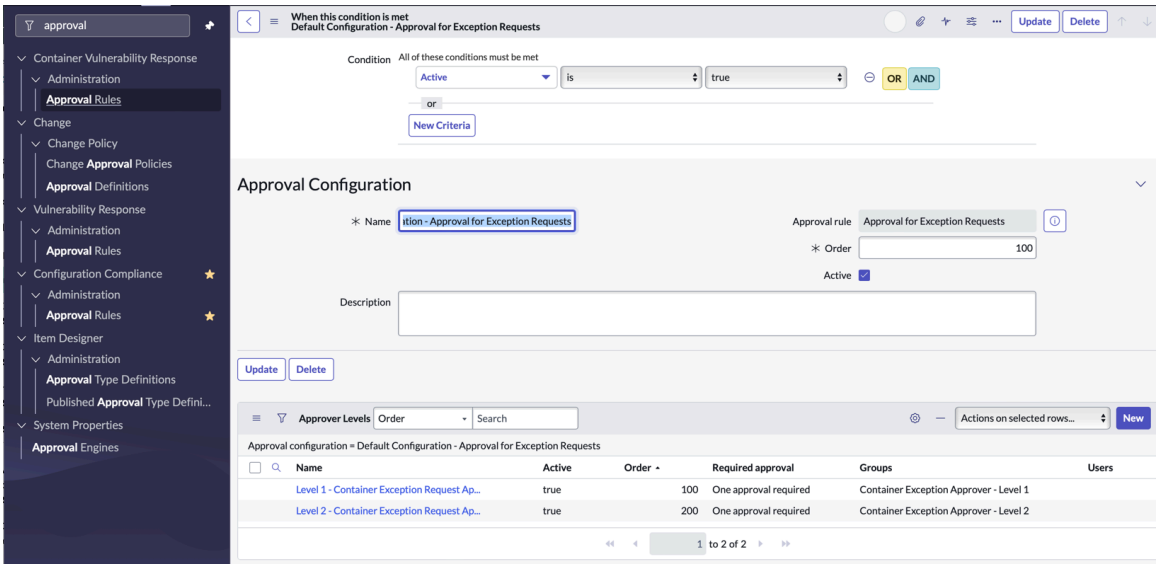
ServiceNow permite que os administradores de segurança definam vários níveis de aprovadores para solicitações de exceção. Você também pode definir regras de exceção automática que podem ser usadas para adiar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

automaticamente vulnerabilidades correspondentes a uma determinada condição.





Tradução automática

Novidades

Para saber mais sobre o que há de novo e o que mudou em Xanadu, consulte as Xanadu notas de versão.

Iniciar

- Para obter uma visão geral sobre Operações de segurança em sua instância Now Platform, consulte Noções básicas sobre Operações de segurança.
- Para obter informações sobre todas as aplicações Operações de segurança disponíveis para download em ServiceNow Store, consulte Operações de segurança e a ServiceNow Store.

Exploração do Contêiner de Resposta a vulnerabilidades

A aplicação Contêiner de Resposta a vulnerabilidades importa itens vulneráveis de contêiner (CVITs). De acordo com as regras, o recurso permite que você corrija as vulnerabilidades do contêiner. Contêiner de Resposta a vulnerabilidades está disponível por meio de uma assinatura separada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao contrário das aplicações tradicionais, os contêineres empacotam todos os códigos de origem da aplicação junto com suas dependências em um arquivo binário chamado imagem de contêiner. A imagem é publicada em um registro para fornecer uma opção para executar esta imagem como uma aplicação ou uma instância de contêiner em qualquer plataforma. As fases em um ciclo de vida de pré-implantação de contêiner são as seguintes:

1. Compor a imagem do contêiner: a imagem do contêiner é composta e apontada para um código de origem ou uma biblioteca dependente.
2. Criar a imagem do contêiner
3. Publicar a imagem do contêiner: o arquivo de imagem do contêiner é publicado em um registro. Cada imagem tem seu próprio ID exclusivo com base no conteúdo da imagem. Essas imagens são extraídas do registro para o ambiente de tempo de execução no modo de pós-implantação. As imagens são executadas como instâncias de contêiner no host no ambiente de produção.

Verificando imagens de contêiner

Uma imagem de contêiner pode ser verificada quanto a vulnerabilidades antes ou depois da implantação. Se as imagens de contêiner forem verificadas durante a fase de pré-implantação, você poderá receber muitos alertas de vulnerabilidade, que podem não precisar de sua atenção imediata. No entanto, a verificação de vulnerabilidades durante a fase de pós-implantação oferece benefícios maiores, como os seguintes:

- Fornecer visibilidade sobre o risco associado às aplicações implantadas.
- Fornecer uma exibição focada somente nas imagens no ambiente de produção.
- Identificar e priorizar as vulnerabilidades que devem ser tratadas imediatamente.
- Agrupamento e atribuição de vulnerabilidades com base nos metadados da imagem. Por exemplo, um repositório de imagens, um rótulo de imagem e outros atributos relacionados à imagem do contêiner podem ser usados para regras de agrupamento e atribuição.

Cada imagem de contêiner tem os seguintes componentes principais:

- Repositório de imagem ou contêiner: representa a imagem do Docker com um determinado repositório ou nome. Ele hospeda todas as versões da imagem.
- Imagem do Docker: representa uma versão específica da imagem do Docker de compilação.
- Contêiner do Docker: representa uma instância em execução da imagem do Docker. Cada versão tem um ID exclusivo e várias instâncias dos contêineres em execução no ambiente de produção.

Contêiner de Resposta a vulnerabilidades módulos

O módulo Contêiner de Resposta a vulnerabilidades fornece detalhes sobre o seguinte:

Itens vulneráveis de contêiner

Os itens vulneráveis de contêiner (CVITs) são agrupados e listados com base na atribuição, na criticalidade, na explorabilidade e no status de correção.

Bibliotecas

Obtenha acesso ao Banco de dados nacional de vulnerabilidades (NVD) e a bibliotecas de terceiros. Enquanto a biblioteca do NVD fornece informações limitadas ao ID do item de vulnerabilidade, a biblioteca de terceiros fornece a maioria dos detalhes sobre um item de vulnerabilidade. As informações na tela do NVD são preenchidas somente quando a integração do NVD é acionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Administração

O módulo Administração fornece informações sobre regras de atribuição de itens vulneráveis, regras de destino de correção e integrações de vulnerabilidade de contêiner. Além disso, você também pode configurar a duração após a qual um item vulnerável deve ser encerrado automaticamente. Você pode usar a seção Configurar granularidade de VI para configurar a granularidade de CVITs especificando as combinações de chaves. Por padrão, um CVIT é criado para uma combinação de um repositório de imagens, um marcador de imagem e uma vulnerabilidade. Você pode adicionar componentes adicionais à chave para obter mais granularidade. Por exemplo, você pode criar um CVIT para uma combinação de repositório de imagens, marcador de imagem, vulnerabilidade e cluster.

Versões disponíveis

Versão de lançamento	Notas de versão
Contêiner de Resposta a vulnerabilidades v2.1 Contêiner de Resposta a vulnerabilidades v2.06 Contêiner de Resposta a vulnerabilidades v2.0.4	

Contêiner de Resposta a vulnerabilidades estados de item vulnerável de contêiner e tarefa de correção

Com a aplicação Contêiner de Resposta a vulnerabilidades, você pode usar o modelo de estado para ver o status de uma tarefa de correção a qualquer momento. Saber como cada estado se relaciona e afeta um ao outro ajuda a determinar quando e como corrigir seus itens vulneráveis de contêiner (CVITs).

Estados da tarefa de correção

Casos de uso complexos às vezes podem fazer com que um item vulnerável de contêiner esteja em um estado diferente da sua tarefa de correção. Entender como os estados funcionam ajuda a explicar esse comportamento e pode ajudar na criação de tarefas de correção e na criação ou edição de regras de tarefa de correção.

As tarefas de correção têm muitos estados possíveis, conforme mostrado no diagrama a seguir.

Fluxo de estado da Resposta a vulnerabilidades do contêiner

Nota:

- Itens vulneráveis de contêiner não podem ser encerrados manualmente.
- Cada formulário de tarefa contém os botões **Seguir** e **Atualizar** que são padrão para tarefas ServiceNow.

Configuração da Contêiner de Resposta a vulnerabilidades

Antes de executar Contêiner de Resposta a vulnerabilidades em sua instância Now Platform, você deve configurá-la.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como instalar Resposta a vulnerabilidades e conformidade de configurações para contêineres

Antes de executar a aplicação Resposta a vulnerabilidades e conformidade de configurações para contêineres em sua instância Now Platform, você deve obter o direito e baixar a aplicação do ServiceNow Store. Instale a aplicação em sua instância Now Platform e conclua algumas etapas de instalação no Assistente de configuração.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tarefas de configuração	Descrição
Verifique se a aplicação está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Resposta a vulnerabilidades.
Verifique se você tem as funções ServiceNow necessárias atribuídas para sua instância.	A função de administrador é necessária para a instalação. Se ainda não estiver atribuído, o Administrador do sistema [admin] também atribuirá a função Administrador de vulnerabilidade, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleta)].

Função necessária: administrador

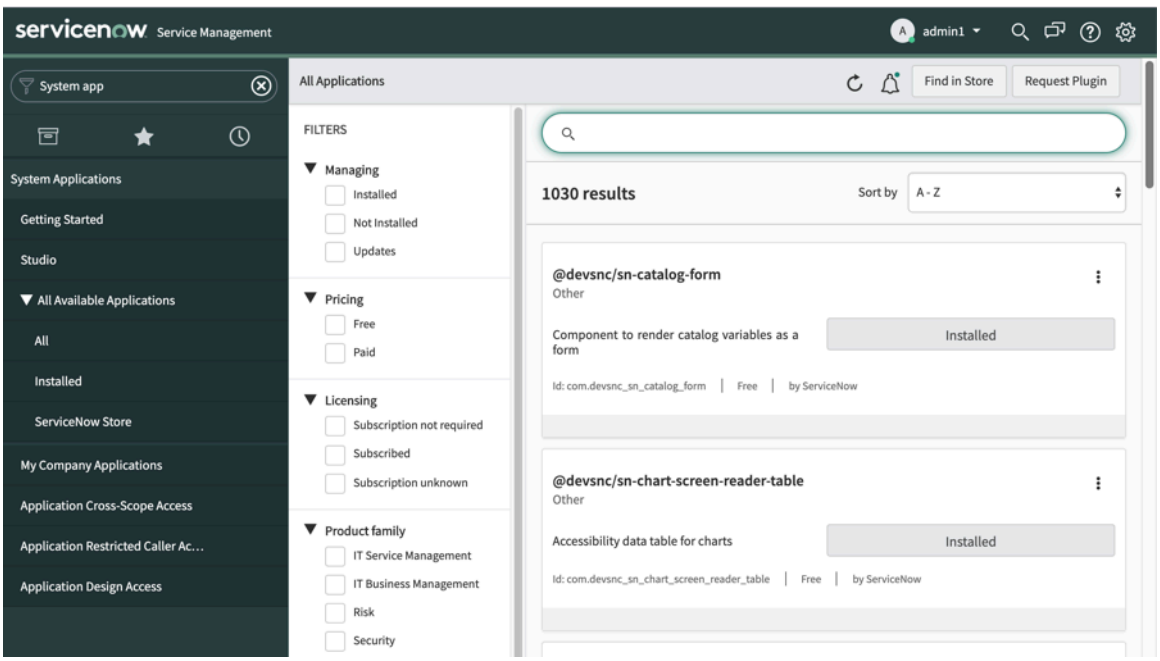
Procedimento

1. Para obter o direito e baixar a aplicação Resposta a vulnerabilidades e conformidade de configurações para contêineres, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Fazer login**.
3. Na barra de pesquisa, digite Resposta a vulnerabilidades e conformidade de configurações para contêineres.
4. Em Aplicações e soluções, clique no bloco Resposta a vulnerabilidades e conformidade de configurações para contêineres.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique **em Solicitar instalação**.
6. Faça login na instância da Now Platform em que você deseja instalar a aplicação Resposta a vulnerabilidades e conformidade de configurações para contêineres.
7. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



8. Nas aplicações listadas, localize a aplicação Resposta a vulnerabilidades e conformidade de configurações para contêineres, selecione uma versão na lista e clique em **Instalar**. A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências instaladas são exibidas.
9. Clique em **Fechar**.

Definir Contêiner de Resposta a vulnerabilidades notificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações de falso-positivos. Criar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Modelos de E-mail**.
2. Selecione **Novo**.

   Para obter instruções detalhadas sobre como criar notificações por e-mail, consulte Criar uma notificação por e-mail .

Resultados
A partir da v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos em Vulnerability Manager Workspace para usuários com as funções, sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin.
- Links abertos em Espaço de correção de problemas de TI para usuários com funções, sn_vul_container.remediation_owner.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Criar ou editar notificações de meta de correção

Os administradores de vulnerabilidade podem editar a notificação de meta de correção ou adicionar novas, especificando quando enviar a notificação, quem a recebe e qual conteúdo está na notificação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de meta de correção ou escolha **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultados
A partir da v21.0 de Resposta a vulnerabilidades, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos em Vulnerability Manager Workspace para os usuários com as funções, sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin.
- Links abertos em Espaço de correção de problemas de TI para os usuários com funções, sn_vul_container.remediation_owner.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configurar Gestão de exceções para Contêiner de Resposta a vulnerabilidades

Limite a duração de uma exceção solicitada e adicione um questionário à exceção ou à solicitação de falso-positivo usando o módulo Contêiner de Resposta a vulnerabilidades. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Contêiner de Resposta a vulnerabilidades. Você também pode solicitar uma exceção usando a integração GRC: Gestão de políticas e conformidade.

Antes de Iniciar

Função necessária: sn_vul_container.manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Contêiner de Resposta a vulnerabilidades estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Gestão de políticas e conformidade estiver instalado, você poderá selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica o objetivo de Política e Controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que gerou a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos. .

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Gestão de exceção**.
2. No formulário **Configuração de gestão de exceções**, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista **Gerenciar exceções usando**. Você pode selecionar Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade.
3. Se você selecionou a opção Resposta a vulnerabilidades, insira as seguintes informações:

Campos de Resposta a vulnerabilidades

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Exibe o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando você seleciona GRC: Gestão de políticas e conformidade, os campos Duração e Unidade desaparecem, pois Governança, risco e conformidade lida com esse fluxo.

4. Selecione **Salvar**.

Configurar regras de aprovação para Gestão de exceções

A partir da Resposta a vulnerabilidades v15.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Resposta a vulnerabilidades (VR) pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis de contêiner
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso-positivo para itens vulneráveis de contêiner

Você também pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Resposta a vulnerabilidades.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso-positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovaçãoy (dias) A partir da v2.5 de Contêiner de Resposta a vulnerabilidades	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v2.5 de Contêiner de Resposta a vulnerabilidades	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Criar configurações para uma regra de aprovação.

   Nota: Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para Gestão de exceções.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Testes de início rápido para Contêiner de Resposta a vulnerabilidades

Valide se Contêiner de Resposta a vulnerabilidades ainda funciona depois de fazer qualquer alteração na configuração, como aplicar um upgrade ou desenvolver um aplicativo. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

A propriedade de execução de testes está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se forem criados dados de demonstração ou contas de demonstração, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção. Consulte Executar o pacote de testes Automated Test Framework (ATF) para Resposta a vulnerabilidades para obter mais informações sobre como configurar e executar o pacote de testes para Contêiner de Resposta a vulnerabilidades.

Os testes de início rápido do Contêiner de Resposta a vulnerabilidades exigem a ativação da aplicação Contêiner de Resposta a vulnerabilidades (sn_vul_container).

Testes Contêiner de Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
CVR: Regras de atribuição	Determina se um conjunto de regras de atribuição pode atribuir automaticamente itens vulneráveis de contêiner a	Vancouver

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Contêiner de Resposta a vulnerabilidades

Teste	Descrição	Versão de lançamento
	um grupo de atribuição para correção.	
CVR: regra de exceção	Regras de exceção de teste.	Vancouver
CVR: marcar como fluxo falso-positivo	Teste se a opção de marcar como fluxo falso-positivo está funcionando no item vulnerável do contêiner.	Vancouver
CVR: regras de destino de correção	Crie regras de destino de correção.	Vancouver
CVR: fluxo de exceção de solicitação	Teste se o fluxo de exceção de solicitação está funcionando conforme o esperado.	Vancouver
CVR: Calculadoras de vulnerabilidade	Testa as calculadoras de vulnerabilidade do contêiner.	Vancouver

Informações relacionadas

Testes de início rápido

Executar o pacote de testes Automated Test Framework (ATF) para Contêiner de Resposta a vulnerabilidades

Execute o pacote de testes do Automated Test Framework (ATF) depois de instalar ou fazer upgrade da aplicação Contêiner de Resposta a vulnerabilidades.

Antes de Iniciar

Confirme uma instalação bem-sucedida e se sua instância funciona conforme projetado.

A propriedade de execução de testes está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras de não produção. Se forem criados dados de demonstração ou contas de demonstração, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção.

- Para habilitar o teste, siga estas etapas:
  1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Administração** > **Propriedades**.
  2. Se não estiver selecionado, marque a caixa de seleção **Habilitar execução de pacote de testes/teste**.
  3. Clique em **Salvar**.
  4. Se o escopo não estiver definido como **Resposta a vulnerabilidades do contêiner** no cabeçalho ou se o escopo não for exibido no cabeçalho, clique no ícone de configurações.
  5. Na janela Configurações do sistema, clique em **Desenvolvedor**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Se não estiver selecionado, clique em **Mostrar seletor de aplicações no cabeçalho** e feche a janela.
7. Na lista exibida ao lado de `Administrador do sistema`, clique em **Resposta a vulnerabilidades do contêiner** para o campo.

Função necessária: admin ou atf_test_admin

Procedimento

1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Testes**.
2. Na lista Pacote, localize **Resposta a vulnerabilidades e Conformidade de configurações para contêineres**.
3. Selecione um teste para abrir o registro.
4. No registro aberto, marque a caixa de seleção **Ativo**.
5. Na lista relacionada Etapas de teste, selecione verdadeiro na coluna Ativo.
6. Clique em **Atualizar**.
7. Abra o teste novamente e clique em **Habilitar execução de testes e pacote de testes aqui**.
8. Habilite Propriedades de teste/pacote de testes e Propriedades de depuração de teste.
9. Clique em **Salvar**.
10. Se o botão **Executar teste** não for exibido, atualize a tela, abra o registro novamente e clique em **Executar teste** para iniciar o teste.
    Depois de alguns momentos, a caixa de diálogo Executar teste indica um teste bem-sucedido. Clique **em Ir para o resultado** para obter mais informações.

O que Fazer Depois

Parabéns! Você pode continuar com a configuração de Contêiner de Resposta a vulnerabilidades.

Para obter mais informações sobre testes automatizados para Contêiner de Resposta a vulnerabilidades e testes automatizados, pacotes de testes e criação de testes automatizados, consulte Automated Test Framework (ATF) .

Integração do Contêiner de Resposta a vulnerabilidades a outras aplicações

Amplie os recursos de Contêiner de Resposta a vulnerabilidades integrando-os a outras aplicações.

Contêiner de Resposta a vulnerabilidades O integra-se a produtos de segurança de contêiner para extrair dados de vulnerabilidade das imagens implantadas no tempo de execução. Em seguida, ele aprimora os dados de vulnerabilidade com as informações contextuais do tempo de execução, como hosts, clusters do Kubernetes, serviços e namespaces em que essas imagens de contêiner são implantadas. Com a descoberta do Kubernetes da ServiceNow, você pode ver as referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes em seu Configuration Management Database (CMDB). Além de aprimorar os metadados, a ServiceNow também oferece um painel de relatórios abrangente para fornecer informações sobre as tendências de vulnerabilidade e correção.

Contêiner de Resposta a vulnerabilidades fornece integrações com as seguintes aplicações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração de Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute
- Noções básicas sobre a integração [Atlassian Jira com Resposta a vulnerabilidades

Importante: No Espaço do gerenciador de vulnerabilidades, você pode criar um problema ágil manualmente usando a ação de lista e a ação de formulário para rastrear a correção de CVITs e RTs.

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 2.1.2 do Contêiner de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Integração de Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute

A integração do Prisma Cloud Compute permite verificar imagens de contêiner para detectar vulnerabilidades.

A partir da versão 16.1 do Resposta a vulnerabilidades, você pode usar o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute na aplicação Contêiner de Resposta a vulnerabilidades para importar dados de vulnerabilidade de imagem de contêiner para contêineres implantados. Você pode exibir relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Resposta a vulnerabilidades. Essas vulnerabilidades podem ser priorizadas e corrigidas.

Se o produto Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server. Para obter mais informações, consulte Requisitos do sistema do MID Server .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição das integrações

Você pode exibir as integrações que fazem parte do Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute. Para exibir as integrações, navegue até **Todos** > **Integração do Prisma Cloud Compute** > **Integrações**.

As seguintes integrações estão disponíveis.

Sequência de execução	Programação	Integração	Descrição
1	Diariamente	Integração de imagens de base do Prisma Cloud Compute	Recupera as vulnerabilidades das imagens de base da API do Prisma e relata as vulnerabilidades das imagens de base separadamente. Ele também cria descobertas de imagem e itens vulneráveis, que apontam para as imagens de base.
2	Diariamente	Integração de vulnerabilidades do Prisma Cloud Compute	Recupera vulnerabilidades de contêiner. Cria descobertas, CVITs e imagens de contêiner descobertas.
3	Sob demanda	Integração de contagens de contêineres do Prisma Cloud Compute	Recupera contagens de contêiner para cada imagem não base.

Configuração de imagem base no Prisma

No console do Prisma, você pode configurar o registro e, em seguida, configurar as imagens de base desses registros. Se uma vulnerabilidade estiver presente na imagem de base, quando você executar a integração de imagens de base do Prisma Cloud Compute, a caixa de seleção **Imagem** de base será marcada, indicando que as vulnerabilidades estão presentes na imagem de base.

Configurar granularidade de IV

Para configurar a granularidade de CVITs, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Configurar granularidade de IV**e especificam as combinações de chaves. Por padrão, um CVIT é criado para uma combinação de repositório de imagens, marcador de imagem e vulnerabilidade. Você pode adicionar componentes adicionais à chave para obter mais granularidade. Por exemplo, você pode criar um CVIT para uma combinação de repositório de imagens, marcador de imagem, vulnerabilidade e cluster.

Processo de integração do Prisma

Quando o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute é executado, ele verifica se existe uma vulnerabilidade e exposição comum (CVE) na tabela do banco de dados nacional de vulnerabilidades (NVD). Se já estiver presente, as informações existentes serão usadas. No entanto, se o CVE não for encontrado, os registros de espaço reservado serão gerados na tabela do NVD. Ao criar esses registros do NVD de espaço reservado, inicialmente somente o CVE e seu nome são preenchidos. Outros detalhes não são preenchidos com a suposição de que a integração do NVD preenche esses detalhes posteriormente. Se o parâmetro de instância de integração

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

update_nvd estiver definido como verdadeiro, ele atualizará os registros do NVD do espaço reservado. Por padrão, o parâmetro de instância é definido como falso. No entanto, pelo menos até que a integração do NVD seja executada e preencha esses detalhes, é necessária alguma compreensão do CVE, como sua gravidade ou algumas informações básicas sobre o problema. Para atender a esse requisito, os campos **Exploração existe** e **Anotações** de correção são preenchidos com os detalhes obtidos do Prisma. Além disso, essa configuração é personalizável, permitindo que você especifique outros campos que deseja preencher na entrada do NVD com base nas informações fornecidas pelo Prisma.

Preparando para o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute

Você pode se preparar para Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute executando tarefas de configuração.

Antes de começar

Para instalar e configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute, você pode imprimir a check-list a seguir. Verifique se os itens listados estão concluídos antes de instalar a aplicação e importar os dados de vulnerabilidade para a instância Now Platform®.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL base da API • Nome de usuário e senha. Essas credenciais são usadas para extrair as vulnerabilidades da integração do Prisma Cloud Compute. Para obter mais informações, consulte https://pan.dev/compute/api/ . **Nota:** O MID Server é opcional. A credencial do usuário usada para a integração do Prisma Cloud Compute precisa de permissão para monitorar as imagens. Consulte o seguinte código: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Se ainda não estiver instalado e ativado, instale a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 16.1 de Resposta a vulnerabilidades ou posterior.
☐	Obtenha direitos e baixe a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute em sua instância Now Platform®.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow Suporte técnico.
☐	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e corrigir os itens vulneráveis: administrador Instale o aplicativo Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades do contêiner (sn_vul_container.vulnerability_admin) e outras funções. sn_vul_container.vulnerability_admin Conclui a configuração da integração do Prisma Cloud Compute. Esta função tem acesso completo à aplicação Contêiner de Resposta a vulnerabilidades (CVR) e seus registros. Este administrador configura integrações e regras em Contêiner de Resposta a vulnerabilidades. Grupo de resposta a vulnerabilidades Por padrão, o grupo de Resposta a vulnerabilidades está disponível. Os usuários atribuídos ao grupo de Resposta a vulnerabilidades herdam sn_vul.read_all, sn_vul_container.read_all. Grupo responsável pela correção de contêiner Por padrão, o grupo de responsáveis pela correção de contêiner está disponível. Os usuários atribuídos a este grupo herdam o sn_vul_container.remediation_owner. O proprietário de correção de contêiner corrige vulnerabilidades de contêiner atribuídas a ele ou a um grupo ao qual pertence. Analista de vulnerabilidade Os usuários atribuídos ao grupo Analista de vulnerabilidade de contêiner herdam sn_vul.vulnerability_analyst. O Analista de vulnerabilidade monitora a correção de todos os itens vulneráveis. Se ainda não tiver sido criado, talvez você prefira criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância. Para obter mais informações, consulte Criar um grupo de usuários .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Instale a integração Resposta a vulnerabilidades com o NVD e execute a API NIST National Vulnerability Database Integration (somente CVE).

Você está pronto para Configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute.

Instalar o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que o produto Prisma Cloud Compute se integre corretamente a Contêiner de Resposta a vulnerabilidades. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute.
2. Navegue até o ServiceNow Store.
3. Na aplicação ServiceNow Store, pesquise a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute.
4. Clique no bloco da aplicação.
   São exibidas informações detalhadas sobre a aplicação que você está instalando.

   Nota: Leia as seções **Outros Requisitos** e **Dependências**, se necessário.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique em **Obter**.
7. Atualize o **Nome da instância** e **o Motivo dos campos da instância** e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Aplicações**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.

Resultados

Sua aplicação é instalada automaticamente em sua instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Configure o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute para o seu ambiente. Consulte Configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute.

Configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute

Instale e configure a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute. Importar dados do Prisma Cloud Compute. Você pode usar os dados importados para priorizar e corrigir vulnerabilidades das imagens do Docker.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Abra o e-mail de ServiceNow que você recebeu sobre a integração.
2. Faça login na sua instância como um administrador.
3. Siga as instruções no e-mail para obter o Integração de Resposta a vulnerabilidades com Palo Alto Networks Prisma Cloud Compute.
4. Navegar até **Todos** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.
   No formulário de configuração do Prisma Cloud Compute, preencha os campos. Para obter mais informações, consulte Formulário de configuração do Prisma Cloud Compute.
5. Na lista Projetos, selecione **Todos os projetos** ou **Projetos específicos** para configurar todos os projetos ou projetos selecionados, respectivamente.
   Se você selecionar **Projetos específicos**, poderá selecionar os projetos na lista Disponível.
6. Conclua a configuração clicando em **Concluir** ou em **Salvar e testar credenciais**.
   - Se você configurou um projeto, clique em **Concluir**.
   - Se você não configurou um projeto, clique em **Salvar e testar credenciais**
7. Exiba a instância recém-criada navegando até **Integração do Prisma Cloud Compute** > **Administração** > **Instâncias de Integração**.
8. Exiba os projetos configurados anteriormente clicando em **Parâmetros de instância de integração**.
9. Execute a instância de integração recém-criada para importar os seguintes dados:
   - Imagens do Docker: lista as imagens do Docker, que são criadas usando um mecanismo de identificação e reconciliação (IRE). Cada imagem do Docker também fornece informações sobre o relacionamento entre os repositórios e as versões instaladas.
   - Imagens de contêiner descobertas: o módulo Imagens de contêiner descobertas fornece informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens. Ele também armazena as informações da camada e as associa à imagem descoberta. Você também pode exibir os projetos e a contagem de contêineres aqui. Para uma imagem de contêiner descoberta, você pode exibir metadados de nuvem, como provedor de nuvem, região de nuvem, ID de conta de nuvem e IDs de recurso de nuvem.
   - Pacotes de imagem do contêiner: fornece informações sobre os pacotes em que existem vulnerabilidades. Os detalhes do pacote binário também são fornecidos como um valor separado por vírgula.
   - Camadas de imagem do contêiner: esta tela exibe o registro de cada camada de imagem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Descobertas de imagem do contêiner: esta tela exibe a lista de descobertas junto com informações sobre vulnerabilidades associadas, camada de imagem, imagem do Docker, repositório de imagens e imagem descoberta. Atualmente, as informações de vulnerabilidade estão limitadas apenas ao ID. As informações adicionais são preenchidas quando a integração do NVD é acionada.
- Itens vulneráveis de contêiner: cada descoberta tem uma vulnerabilidade correspondente. Os CVITs são criados com base na granularidade.

10. Configure a granularidade de um item vulnerável.

a. Navegar até **Integração do Prisma Cloud Compute** > **Configurar chaves de vulnerabilidade de imagem**

b. Configure a granularidade dos CVITs marcando as caixas de seleção necessárias. Os itens vulneráveis são criados com base nas chaves selecionadas durante a próxima importação.

Nota: Por padrão, um CVIT é criado para uma combinação de Repositório de imagem, Vulnerabilidade e Marcador de imagem. Você pode adicionar componentes à chave para obter mais granularidade. Por exemplo, você pode criar um CVIT para uma combinação de Repositório de imagens, Vulnerabilidade, Marcador de imagem e Cluster. Depois que os itens vulneráveis ou as descobertas de itens vulneráveis são criados, as caixas de seleção não são mais editáveis.

Correção de vulnerabilidades de contêiner

O monitoramento da correção é um processo que começa com a revisão do status e termina com o fechamento de itens vulneráveis de contêiner (CVITs). Contêiner de Resposta a vulnerabilidades oferece ferramentas e procedimentos para tornar esse processo mais produtivo e eficiente.

Contêiner de Resposta a vulnerabilidades regras da calculadora

As calculadoras de vulnerabilidade automatizam o cálculo de valores iniciais para os campos em itens vulneráveis de contêiner. A condição de cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

Para exibir e criar calculadoras de vulnerabilidade, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Calculadoras de vulnerabilidade**.

O sistema de base Contêiner de Resposta a vulnerabilidades inclui duas calculadoras de vulnerabilidade que definem a pontuação de risco base no item vulnerável do contêiner. Os seguintes grupos de calculadoras estão disponíveis no sistema de base:

- Gravidade da vulnerabilidade: calcula a pontuação de risco dos itens vulneráveis usando a gravidade da vulnerabilidade normalizada.
- Calculadora de risco padrão: é baseada na regra de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da versão 2.10 de Contêiner de Resposta a vulnerabilidades, no caso de:

- Regra da**calculadora de risco padrão** : sempre que a pontuação de risco em um item vulnerável de contêiner (CVIT) muda, os seguintes detalhes são documentados na seção Anotações do CVIT:
  - Nome do grupo de calculadoras
  - Nome da calculadora
  - Valores de campo que têm um peso maior que 1 e sua contribuição de pontuação de risco.
  - Pontuação de risco final
- Regra de risco de**gravidade de vulnerabilidade** : sempre que a pontuação de risco é atualizada em um CVIT, a seção **Anotações** é atualizada com os seguintes detalhes:
  - Nome do grupo de calculadoras
  - Nome da calculadora: dependendo se a regra da calculadora é baseada em um modelo ou em um script, o nome é acrescentado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e marque a caixa de seleção **Exibição avançada**. Na caixa suspensa **Tipo de valor**, selecione a opção necessária. Se o **modelo** for selecionado, a pontuação de risco será atualizada de acordo com a condição especificada na regra. Se **Script** estiver selecionado, você poderá adicionar ou atualizar o script existente.

Ponderações de pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação e classificação de risco com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio *`Update Risk Rating from Risk Score`* na tabela de itens vulneráveis do contêiner é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis do contêiner. Antes da versão 17.1 da aplicação Resposta a vulnerabilidades (VR), as seguintes classificações de risco eram fornecidas como parte da inclusão de script `VulnerabilityUtils`, que era codificada.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

A partir da versão 18.0 de Resposta a vulnerabilidades,

- Os tipos de classificação de risco são enviados na tabela base Ponderações de pontuação de risco [sn_sec_cmn_risk_scorew_weights] como cvr_risk_rating. Esses tipos são passados como parte das regras de negócio ou inclusões de script em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e regras de negócio relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as vulnerabilidades e exposições comuns associadas (CVEs) ou entradas de terceiros (TPEs) nos itens de vulnerabilidade (VIs) estão vinculadas a uma vulnerabilidade de exploração conhecida (KEV) de CVE.

Para obter mais informações, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Contêiner de Resposta a vulnerabilidades regras de atribuição

Defina os critérios pelos quais os itens vulneráveis de contêiner (CVITs) são atribuídos automaticamente a um grupo de atribuição para correção.

Para criar e exibir regras de atribuição para itens vulneráveis de contêiner. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de atribuição**. Ao criar uma regra de atribuição, você pode definir as condições. Quando essas condições são atendidas, a regra atribui automaticamente os itens vulneráveis do contêiner ao grupo de usuários selecionado. Somente a primeira regra de atribuição com uma condição correspondente é executada em relação a um registro.

Nota: Os itens vulneráveis de contêiner que não estão no estado Aberto ou que foram atribuídos manualmente são sempre excluídos.

Para obter mais informações, consulte Resposta a vulnerabilidades visão geral das regras de atribuição.

Importante: Como administrador e analista de vulnerabilidades, você pode obter as atribuições mais recentes para CVITs selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que reaplicar as Regras de atribuição para todos os CVITs na IU clássico, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Contêiner de Resposta a vulnerabilidades regras de destino de correção

As regras de destino de correção definem o intervalo de tempo esperado para corrigir um item vulnerável de contêiner (CVIT). Essas regras são semelhantes à forma como os SLAs fornecem um intervalo de tempo para corrigir a própria vulnerabilidade.

Para criar e exibir regras de destino de correção para vulnerabilidades de contêiner, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de destino de correção**.

As regras de destino de correção definem o tempo de correção de destino para itens vulneráveis de contêiner (CVITs) selecionados. Defina um prazo para corrigir a vulnerabilidade selecionando o número de dias para a correção. Defina um lembrete para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

correção e defina os itens vulneráveis de contêiner aos quais a regra se aplica. Você pode definir uma meta de correção para os dias em que ela precisa ser corrigida e também definir um lembrete antes de se aproximar da data de meta. Para obter mais informações, consulte Resposta a vulnerabilidades regras de destino de correção.

Importante: Como administrador e analista de vulnerabilidades, você pode obter a data da meta de correção mais recente para CVITs selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que executar as Regras de destino de correção para todos os CVITs na IU clássico, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Gestão de exceções no Contêiner de Resposta a vulnerabilidades

Quando sua organização não pode cumprir uma política de segurança ou gestão de vulnerabilidades, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável de contêiner (CVIT) que não pode ser corrigido de acordo com a política.

Algumas vulnerabilidades de contêiner (CVIT) podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade.

Ciclo de vida de uma exceção

Definição de uma exceção

Uma exceção é uma solicitação para adiar a correção de um CVIT ou RT por um período especificado. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Como solicitar uma exceção

Como responsável pela correção, você pode solicitar uma isenção para um CVIT ou RT usando o processo de gestão de exceções. Depois que o aprovador de exceção aprova esta solicitação, o **CVIT** ou RT passa para um estado Adiado.

Como aprovar uma solicitação de exceção

CVIT ou RTs que não podem ser corrigidos imediatamente são revisados por analistas de vulnerabilidade, avaliados quanto ao risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se apenas o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir da Resposta a vulnerabilidades v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Depois que uma solicitação de exceção para um CVIT ou RT for aprovada, você poderá executar as seguintes ações:

- Reabrir
- Excluir
- Atualizar os campos **Atribuição a** ou **Grupos** de atribuição

Acompanhamento de uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** do CVIT ou RT. Se uma ação for realizada em um RT, você não poderá rastrear o status dos CVITs individuais nesse RT.

Expiração de uma solicitação de exceção

Quando uma solicitação de exceção para um CVIT ou RT específico expira, o CVIT ou RT afetado é revertido para o estado **Aberto**.

Se um único CVIT ou todos os CVITs em um RT forem aprovados na próxima verificação, os CVITs e, quando aplicável, o campo **Estado** do RT mudarão para **Encerrado** com o subestado **Fixo**.

Configurar regras de aprovação

Exibir e configurar regras de aprovação navegando até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de aprovação**. Solicite uma exceção para os CVITs que não podem ser corrigidos ou adiados imediatamente, identificando as vulnerabilidades, itens de configuração (ICs) ou CVITs afetados. Automatizar o processo de adiamento de CVIT. Adie os CVITs correspondentes com base nessas regras quando o sistema identificar esses CVITs.

As seguintes regras de aprovação são enviadas por padrão:

- Aprovação para solicitações de exceção: uma configuração padrão com dois níveis de aprovação é fornecida no sistema de base. Sempre que houver uma solicitação de exceção em um item vulnerável, a solicitação de aprovação será enviada aos usuários ou grupos presentes no nível 1. Depois de aprovada pelos aprovadores de nível 1, ela é enviada aos aprovadores de nível 2.

Nota: Você pode alterar os níveis padrão e editar conforme necessário. A partir da Contêiner de Resposta a vulnerabilidades v2.0.6, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de falso-positivo ou exceção é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *sn_vul_container.container_exception_approver_L1*, *sn_vul_container.container_exception_approver_L2*ou *sn_vul_container.container_false_positive_approver_group* para alterar o valor da propriedade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Aprovação para regras de exceção: não tem configuração, mas dois níveis de aprovação.
- Aprovação para falsos positivos: tem uma configuração com um nível de aprovação.

Nota: A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Como solicitar e aprovar uma exceção no Contêiner de Resposta a vulnerabilidades

Você pode solicitar o adiamento da correção de um item vulnerável de contêiner (CVIT) por um período especificado. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Para solicitar ou aprovar uma exceção, consulte:

- Solicitar uma exceção para um item vulnerável de contêiner
- Solicitar uma exceção para vulnerabilidades de contêiner usando GRC: Gestão de políticas e conformidade

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada. A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Solicitar uma exceção para um item vulnerável de contêiner

Solicite uma exceção para um item vulnerável de contêiner (CVIT) que não pode ser corrigido imediatamente. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar

Função necessária: grupo de desenvolvedores

Por Que e Quando Desempenhar Esta Tarefa

Você pode solicitar uma exceção para vários CVITs simultaneamente usando o recurso de edição em massa no Vulnerability Manager Workspace. Para obter mais informações, consulte Solicitar exceção em massa no Espaço do gerenciador de vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** > **Todos**.
2. Selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto ou Sob investigação.
3. No formulário Item vulnerável do contêiner, clique em **Solicitar exceção**.

4.a. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada em **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado Aberto. **Nota:** A partir da versão 1.2 do Contêiner de Resposta a vulnerabilidades, se um item vulnerável tiver sido adiado para correção usando o recurso de gestão de exceções, caso ele seja reaberto pelo scanner, a data de adiamento definida na vulnerabilidade ainda persistirá. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema *sn_vul.container.auto_defer_cvit_in_active_e* como verdadeiro. Além disso, a data adiada até persiste mesmo depois que o CVIT é encerrado ou a exceção expira. A função necessária é sn_vul_container.manage_exception_configuration para leitura e gravação.
Motivo	Motivo da exceção. Estas são as opções: ▪ Risco aceito ▪ Aguardando janela de manutenção ▪ Correção indisponível ▪ Redução do controle no local ▪ Outro Para ver como adicionar novas opções de motivo, consulte Definir um mapeamento de motivo da política.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Solicitar aprovação**.
O estado do item vulnerável do contêiner muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma exceção para uma tarefa de correção de contêiner

Solicite uma exceção para adiar uma tarefa de correção de contêiner por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções nos espaços Resposta a vulnerabilidades. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Função necessária:

sn_vul.remediation_owner, sn_vul.app_security_Champion ou sn_vul_container.remediation_owner.

Você também pode solicitar exceções para tarefas de correção de contêiner no ambiente clássico.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Tarefas de correção** > **Todos**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No registro da tarefa de correção de contêiner, selecione **Solicitar exceção**.
4. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar uma exceção para vulnerabilidades de contêiner usando GRC: Gestão de políticas e conformidade

Solicite exceções de política usando a capacidade de gestão de exceções de política GRCGestão de políticas e conformidade na aplicação [] de dentro de Contêiner de Resposta a vulnerabilidades.

Antes de Iniciar

Antes de poder usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Gestão de políticas e conformidade do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.

   Nota: Se GRC: Gestão de políticas e conformidade for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção. Para mais informações sobre campos de formulário, consulte Formulário Solicitar exceção.

   a. Envie a solicitação de exceção clicando em **Solicitar aprovação**.
   O estado dos itens vulneráveis muda para Em revisão e uma exceção à política é criada. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

   b. Exiba a exceção à política clicando na lista relacionada Exceções às políticas.

   c. Clique no número da exceção à política.

   d. No campo **Aprovador**, selecione o nome do aprovador.

   e. Clique na guia Origem e selecione um objetivo de **controle no campo Objetivo** de controle.

   f. Clique na guia Avaliação de risco e selecione a classificação de **risco** no campo Classificação de risco.

   g. Salve o formulário.

   h. Clique na guia **Controles afetados**.

   i. Adicione os controles clicando em **Adicionar**.

   j. Salve o formulário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode gerar uma revisão de conformidade clicando em **Solicitar revisão de conformidade**.

O formulário de aprovação é enviado ao aprovador.

O aprovador pode aprovar a solicitação clicando em **Aprovar** ou solicitar aprovação adicional clicando em **Solicitar aprovação adicional**.

O estado do registro muda para Adiado. O motivo declarado é aquele que você selecionou ao gerar a solicitação de exceção. A guia **Adiamento** fornece anotações adicionais sobre o registro.

Nota: Se a solicitação for rejeitada, o registro será movido para o estado anterior.

3. Clique em **Enviar**.
   Para obter mais informações sobre a integração de exceção à política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Definir um mapeamento de motivo da política

Defina as opções de motivo a serem disponibilizadas a qualquer usuário que solicite uma exceção.

Antes de Iniciar

Função necessária: sn_vul.compliance.manager e sn_vul_container.manage_exception_configuration

Procedimento

1. Navegar até **Todos** > **Políticas e conformidade** > **Exceções às políticas** > **Registro de Integração**.

   Nota: Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Escolhas de motivo ou adicionar um novo motivo.

2. Clique no registro de integração do Container Vulnerability Response - CVIT.
3. Na lista Escolhas de motivo, clique em **Novo**.
4. Clique no ícone de lupa.
5. Adicione uma opção de motivo existente para criar uma nova.
   - Se você quiser adicionar uma opção de motivo existente, selecione um motivo.
   - Se você quiser adicionar uma nova opção de motivo à tabela Escolhas de motivo, clique em **Novo** e preencha os campos no formulário.

Formulário Lista de seleção de motivo

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamento do motivo da política para as respectivas aplicações. Para navegar até esta tabela, insira `sn_vul_policy_reason_mapping.LIST` no navegador de filtros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	Ordem para esta opção. Os motivos são ordenados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção à política sob demanda for solicitada. Se o registro de integração não contiver nenhuma opção específica da aplicação, todas as opções de motivo com o campo **Padrão** selecionado estarão disponíveis.
Ativo	Opção para exibir a opção na lista de opções de motivo.

6. Clique em **Enviar**.

Resultados
A opção de motivo é adicionada. A opção de motivo estará disponível no campo **Motivo** do formulário de solicitação de exceção à política para a aplicação selecionada.

Aprovar uma solicitação de exceção no Contêiner de Resposta a vulnerabilidades

Aprove solicitações de exceção para itens vulneráveis de contêiner ou tarefas de correção que não podem ser corrigidas imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Você pode aprovar a exceção e as solicitações de falso-positivo no Vulnerability Manager Workspace. Consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Você também pode aprovar solicitações de exceção no ambiente clássico:

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Adiar um item vulnerável de contêiner em Contêiner de Resposta a vulnerabilidades

Se você determinar que o problema associado a um item vulnerável de contêiner (CVIT) é de baixo risco e pode ser adiado imediatamente sem análise adicional, você pode usar o recurso **Adiar**.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)
Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Por Que e Quando Desempenhar Esta Tarefa
Um trabalho agendado é executado todos os dias, verificando se há itens vulneráveis adiados que atingiram a data de reabertura. No dia em que o adiamento do CVIT estiver definido para expirar, o registro será reaberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner**.
2. Abra um item vulnerável.
3. Clique **em Solicitar exceção**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada. **Nota:** A partir da versão 18.0 de Contêiner de Resposta a vulnerabilidades, se um item vulnerável de contêiner adiado (CVIT) for fechado e reaberto por um scanner antes que a janela de exceção expire, o estado do CVIT será revertido para o estado adiado, respeitando a janela de exceção ativa. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema *sn_vul.container.auto_defer_cvit_in_active_ex* como verdadeiro. Além disso, a data adiada Até persiste mesmo depois que o item vulnerável é fechado ou a exceção expira. A função necessária é sn_vul_container.manage_exception_configuration para leitura e gravação. Depois que o registro for enviado, se as notificações por e-mail estiverem definidas, os membros do grupo Contêiner de Resposta a vulnerabilidades receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como Aberto e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Falso positivo ◦ Correção indisponível ◦ Risco aceito

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Clique em **Enviar**.
   O grupo está marcado como **Em revisão**. Um link relacionado a **Reabrir** é exibido. A data e o motivo da reabertura aparecem nas anotações de trabalho na guia **Aprovações de mudança de estado**.

   A partir da Contêiner de Resposta a vulnerabilidades v2.3, você pode adicionar informações relevantes no campo Anotações de trabalho na seção Anotações de um item vulnerável de contêiner adiado.

Solicitar uma extensão para um item vulnerável de contêiner adiado

Solicite uma extensão para um item vulnerável de contêiner adiado antes que ele atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner**.
2. Abra um item vulnerável de contêiner adiado.
3. Selecione **Solicitar extensão**.

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável do contêiner é Adiado.

4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável do contêiner adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

   Nota:
   - A solicitação passa por dois níveis de aprovação.
   - Se um item vulnerável de contêiner adiado for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Como trabalhar com uma regra de exceção no Contêiner de Resposta a vulnerabilidades

Você pode solicitar uma exceção para itens vulneráveis de contêiner (CVITs) que não podem ser corrigidos ou adiados imediatamente. Ao automatizar o processo de adiamento de VI, você pode adiar os CVITs correspondentes com base na regra quando o sistema os identifica.

Você pode executar as seguintes tarefas para uma regra de exceção:

- Criar uma regra de exceção no Contêiner de Resposta a vulnerabilidades
- #unique_626
- Como ativar uma regra de exceção no Contêiner de Resposta a vulnerabilidades
- Reabrir uma regra de exceção no Contêiner de Resposta a vulnerabilidades
- Atualizar uma regra de exceção aprovada no Contêiner de Resposta a vulnerabilidades
- Excluir uma regra de exceção no Contêiner de Resposta a vulnerabilidades
- Adiar um item vulnerável de contêiner em Contêiner de Resposta a vulnerabilidades

Nota: A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Criar uma regra de exceção no Contêiner de Resposta a vulnerabilidades

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica de um grupo de itens vulneráveis de contêiner (CVITs), como uma regra com uma condição que se baseia na gravidade da vulnerabilidade desses CVITs. Com esta regra, você pode adiar CVITs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A regra é aplicada a partir da data "Válido de" até a data "Válido até". A tarefa de correção (VUL) é criada quando a regra é aprovada. O método de agrupamento para esta VUL é conhecido como regras de exceção. A VUL é criada no estado Adiado. Você não pode fechar, reabrir ou excluir esta VUL. CVITs novos e reabertos são adiados e adicionados a esta VUL a partir da data "Válido a partir de" até que o grupo expire na data "Válido até".

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Nota: Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Na página de registro Novo regra de exceção, clique em **Novo** para criar uma regra.
3. No formulário Regra de exceção, preencha os campos.

   Nota: Para mais informações sobre campos de formulário, consulte Formulário Regra de exceção.

4. Adicione o grupo de atribuição ao criar a regra.
5. Envie o formulário para aprovação.
   O status da solicitação muda para Em revisão. Até que você envie a regra de exceção, ela permanecerá no estado Rascunho.
6. Para exibir e criar um grupo para gerenciar regras de exceção:

   a. Navegar até **Todos** > **Administração de usuários** > **Grupos**.

   b. Em uma regra de exceção, clique na guia **Aprovações solicitadas** para exibir o status da solicitação.
   Um trabalho agendado é executado diariamente, o que executa as regras de exceção nos dados existentes. Todos os itens vulneráveis que correspondem à condição são movidos para o estado Adiado. Se uma regra de exceção aprovada for excluída, todos os itens vulneráveis adiados serão revertidos para o estado anterior. Para obter mais informações, consulte Como trabalhar com uma regra de exceção.

Como ativar uma regra de exceção no Contêiner de Resposta a vulnerabilidades

Uma regra é ativada na data "Válida a partir de". Após a ativação, ele automatiza o processo de exceção para itens vulneráveis de contêiner (CVITs).

A regra de exceção segue este ciclo de vida:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Os novos CVITs que você cria ou reabre e que atendem à condição especificada são adiados. Se você habilitar a opção Executar em dados existentes ao executar a regra de exceção pela primeira vez, todos os CVITs ativos e não adiados que corresponderem à condição da regra de exceção serão movidos para a tarefa de correção (RT) recém-criada e seu estado será alterado para Adiado.
2. Se um CVIT recém-criado corresponder à condição da regra de exceção, ele será movido para o RT adiado que está associado à regra e a regra do grupo não será executada nele.
3. Na data "Válido a partir de", os CVITs existentes serão adicionados se você habilitar a opção Executar nos dados existentes.
4. O RT para de aceitar novos CVITs quando a regra expira na data "Válido até". O RT permanece até a data "Adiado até".
5. A regra de exceção expira na data "Válido até".

Reabrir uma regra de exceção no Contêiner de Resposta a vulnerabilidades

Reabra uma regra de exceção que foi rejeitada, mas você deseja reenviar. A reabertura da regra a move para o estado Rascunho.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode atualizar e reenviar a regra para aprovação.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Encontre a regra que deseja reabrir e clique em **Reabrir**.
3. Atualize o formulário e reenvie-o para aprovação.

Atualizar uma regra de exceção aprovada no Contêiner de Resposta a vulnerabilidades

Cancele uma regra aprovada para poder atualizá-la. Por exemplo, antes de poder modificar quaisquer datas ou adicionar uma condição a uma regra aprovada, você deve cancelá-la para que a tarefa de correção (VUL) seja excluída e os itens vulneráveis de contêiner (CVITs) sejam movidos para o estado Aberto.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
As regras de grupo são reaplicadas a esses CVITs. Envie a regra depois de fazer as mudanças para que ela passe pelo processo de aprovação mais uma vez.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja cancelar e clique em **Cancelar**.
3. Na caixa de diálogo Cancelar regra, clique em **Cancelar regra**.
   A regra retorna para o estado Rascunho e a VUL associada é excluída. Os CVITs relacionados são reabertos e as regras de grupo são aplicadas aos CVITs individuais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Excluir uma regra de exceção no Contêiner de Resposta a vulnerabilidades

Exclua uma regra de exceção que não é mais necessária. Por exemplo, você pode excluir uma regra se não quiser adiar um item vulnerável de contêiner (CVIT) durante a ingestão.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A exclusão de uma regra cancela a tarefa de correção associada (VUL). Os CVITs relacionados são reabertos e as regras de grupo são aplicadas aos CVITs individuais.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo Excluir regra, clique em **Excluir regra** para excluir a regra selecionada.
   A tarefa de correção associada também é excluída. Os CVITs relacionados são reabertos e as regras de grupo são aplicadas aos CVITs individuais.

Solicitar uma extensão para uma tarefa de correção adiada no Contêiner de Resposta a vulnerabilidades

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento adiada. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento
1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiado expira e o item vulnerável do contêiner é reativado.
Motivo	Insira o motivo para adiar o problema. As opções incluem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Com a aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis do contêiner, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis de contêiner devem estar no estado adiado e seus dados atuais até precedem a data atualizada até. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para uma regra de exceção no Contêiner de Resposta a vulnerabilidades

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Regras de exceção**.
2. Selecione uma regra de exceção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ◦ Risco aceito ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nos itens vulneráveis do contêiner. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Marcar e aprovar um item de vulnerabilidade de contêiner com falso-positivo

Itens vulneráveis de contêiner (CVITs) e tarefas de correção (VULs) podem ser marcados como falso-positivos. Aprovadores com acesso de gravação podem aprovar essas solicitações de outros usuários.

- Marcar como falso-positivo em Contêiner de Resposta a vulnerabilidades
- Aprovar um falso-positivo

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho de falso-positivo, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando um CVIT ou tarefa de correção é marcado como falso-positivo, o solicitante recebe um e-mail de confirmação. Simultaneamente, o aprovador recebe um e-mail informando que um CVIT ou tarefa de correção foi marcado como falso-positivo. A partir da v2.5 de Contêiner de Resposta a vulnerabilidades, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Como analista de vulnerabilidade e proprietário de correção, você pode solicitar e aprovar falsos positivos no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI, respectivamente.

Marcar como falso-positivo em Contêiner de Resposta a vulnerabilidades

Marque um item vulnerável de contêiner (CVIT) ou tarefa de correção como falso-positivo se o aviso fornecido pelo scanner não for realmente um problema. Por exemplo, se um CVIT tiver sido desativado, mas o scanner ainda estiver levantando um problema relacionado a ele, marque-o como um falso-positivo.

Importante: Como analista de vulnerabilidade e proprietário de correção, você pode solicitar falsos positivos no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI, respectivamente.

Antes de Iniciar

Função necessária: responsável pela correção

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner (ou Tarefas de correção)** > **Todos**.
2. Abra o CVIT que você deseja marcar como falso-positivo e clique em **Marcar como falso-positivo**.
   O CVIT deve estar em um estado **Aberto**.
3. No formulário Falso-positivo, insira os detalhes em **Informações adicionais** e clique em **Solicitar aprovação**.
   A solicitação é enviada para aprovação e o Estado do CVIT muda para **Em revisão**. O solicitante e o aprovador são notificados por e-mail.

Aprovar um falso-positivo

Como aprovador de falso-positivo, você pode aprovar solicitações de falso-positivo de outros usuários.

Importante: Você pode aprovar ou rejeitar solicitações de falso-positivo no Vulnerability Manager Workspace. Para obter mais informações, consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Antes de Iniciar

Função necessária: false_positive_approver
Você também pode aprovar solicitações de exceção e falso-positivo no ambiente clássico:

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Nota: Um falso-positivo pode ter limite de tempo. Somente o aprovador pode definir a data de término.

Tarefas de correção e regras de tarefa da Resposta a vulnerabilidades do contêiner

Configure tarefas de correção (CVULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis de contêiner (CVIT) e analisá-los em massa. Os critérios pelos quais as tarefas de correção são formadas são configurados para que os CVITs sejam

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atribuídos automaticamente às tarefas de correção. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Acompanhamento de contagens de adiamento para itens vulneráveis de contêiner e tarefas de correção

Rastreie o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou tarefa de correção foi adiado. O trabalho agendado definir contagens de adiamento é executado diariamente para publicar contagens dos registros que foram adiados mais de uma vez na coluna Contagem de adiamento. Os registros são exibidos nos módulos de vários adiamentos para VR, AVR e CVR.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem definir como os itens vulneráveis de contêiner são agrupados e atribuídos automaticamente. Uma **vulnerabilidade** de regra padrão está incluída no sistema de base que reúne CVITs com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis no CVIT. Esses valores podem incluir item de configuração (IC), entrada de vulnerabilidade e assim por diante.

Há regras de tarefa para Resposta a vulnerabilidades de contêiner que estão incluídas com a aplicação Resposta a vulnerabilidades que está disponível quando você a ativa.

Você pode criar várias condições com o Construtor de condições. Na seção Agrupar por, depois de definir um par de campos, outra linha será exibida. Você pode ter até seis seleções **de Agrupar por**. Você também pode automatizar a atribuição de grupo.

Por exemplo, você pode agrupar seus itens vulneráveis de contêiner pelo item de configuração ou pelo modelo de produto. Você pode ter uma regra de tarefa para vulnerabilidades de baixa gravidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades que expõem a empresa a mais riscos. Consulte Criar, editar e excluir regras de tarefa de correção da Resposta a vulnerabilidades do contêiner para obter mais informações sobre as opções disponíveis.

Um conjunto diferente de regras pode ser usado para itens vulneráveis de contêiner que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado aos valores **Agrupar por** da regra da tarefa de correção para fazer a descrição resumida do novo registro.

Quando um novo item vulnerável de contêiner é criado, importado ou reaberto após ser fechado, as regras são avaliadas em relação a ele. Um CVIT só é avaliado uma vez, automaticamente, a menos que seja reaberto após ser fechado ou as regras sejam reaplicadas manualmente.

O processo a seguir é usado para cada CVIT novo ou reaberto:

- Para cada regra de tarefa de correção, o CVIT é comparado ao filtro de regra de tarefa de correção.
- Para cada regra em que a condição da regra da tarefa de correção corresponde, a regra extrai os dados das seleções **Agrupar por** no CVIT. Ele cria um nome de grupo e um campo. Neste caso, **Alto risco: QID-32342: Resumo de QID-3242** (Nome: ID da vulnerabilidade: resumo da vulnerabilidade).

  Nota: O campo de descrição resumida está limitado a 160 caracteres. Resumos de vulnerabilidade mais longos são truncados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A regra verifica se há uma tarefa de correção **aberta** correspondente que esteja atribuída ao mesmo grupo de atribuição que o CVIT.

- Se a tarefa for encontrada, o CVIT será adicionado à tarefa existente no estado **Aberto**.
- Se nenhuma tarefa no estado **Aberto** for encontrada, a regra criará uma tarefa **de alto risco: QID-32342**, a atribuirá ao mesmo grupo de atribuição que o CVIT e colocará o CVIT na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições da regra da tarefa de correção antes de ser colocada em uma tarefa de correção, muitas regras podem afetar o desempenho. Configure suas regras de tarefa para que as condições ajudem a evitar a criação de tarefas de correção duplicadas.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelas **Regras de atribuição** no CVIT ao agrupar os itens e atribui a tarefa de correção para corresponder aos CVITs.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras no módulo **Regras de atribuição**. Para obter mais informações sobre regras de atribuição, consulte Visão geral das regras de atribuição da Resposta a vulnerabilidades.

Quando uma regra de tarefa é excluída do formulário ou da exibição de lista, você tem a opção de excluir todas as tarefas Abertas criadas por essa regra. As tarefas que não estão no estado **Aberto** são excluídas.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use o botão **Reaplicar** na página de regra de tarefa de correção para executar novamente a regra alterada em todas as tarefas de correção em **aberto** ativas criadas por essa regra. Ele exclui e recria automaticamente as tarefas de correção com base na regra alterada.

A reaplicação verifica somente as tarefas de correção existentes.

Depois de selecionar **Reaplicar**, a seguinte mensagem será exibida: A reaplicação desta regra de tarefa de correção excluirá e recriará as tarefas de correção para esta regra. As tarefas de correção que não estão no estado Aberto não são excluídas.

Importante: Como administrador e analista de vulnerabilidades, você pode avaliar as regras de tarefa de correção para itens vulneráveis selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que reaplicar as Regras de tarefa de correção na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Regras de tarefa de correção e criação e atualização de CVIT

Se um IC de uma verificação estiver associado a uma vulnerabilidade conhecida, um CVIT será criado. Depois de criado, o CVIT é avaliado em relação às condições das regras de tarefa de correção para uma correspondência. Se houver uma correspondência com uma tarefa de correção existente, o CVIT será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o CVIT.

Se alguma propriedade capturada nas condições de filtragem da tarefa de correção for atualizada ou alterada em um CVIT, o IVA atualizado também será avaliado em relação às regras de tarefa de correção para uma correspondência. Se houver uma correspondência

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

com uma tarefa de correção existente, o CVIT será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o CVIT.

Rollup e rolldown de estado

Se você atualizar uma tarefa de correção para Aberto ou de Aberto para Sob investigação, o novo estado será revertido para todos os CVITs associados. A rolagem de estado ocorre imediatamente após a mudança do estado.

O acúmulo de estado de CVITs para a tarefa de correção ocorrerá somente se todos os **CVITs** na tarefa estiverem nos estados Adiado ou Encerrado- **fixo**. O acúmulo é feito com o Acúmulo de valores de item vulnerável do contêiner para a vulnerabilidade e um trabalho agendado em grupo, que é executado a cada 15 minutos. O estado não é acumulado até que o trabalho seja executado. Para que um estado seja acumulado dos CVITs para a tarefa de correção, todos os CVITs devem estar no mesmo estado.

Criar, editar e excluir regras de tarefa de correção da Resposta a vulnerabilidades do contêiner

Você pode criar regras para agrupar automaticamente itens vulneráveis de contêiner (CVIT) em tarefas de correção (CVUL) com base nas condições do filtro. Essas regras agrupam CVITs automaticamente conforme são importados ou criados manualmente.

Antes de Iniciar

Se você criar uma nova regra, ela não se aplicará aos dados existentes. Depois de enviá-lo, ele é executado em relação às novas importações.

Função necessária: gerente de App-Sec

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras da tarefa de correção.**.
2. Abra a regra ou selecione **Novo**.
3. Preencha os campos no formulário ou edite-os.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra de tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condição	Condições de filtro opcionais para a regra. Por padrão, (caixa de seleção que**diferencia maiúsculas de minúsculas** não marcada), o texto de pesquisa que você insere no construtor de condições em

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefas. Um exemplo de condição é **Vulnerabilidade** > **é** > **VULNENT123451** (uma vulnerabilidade importada conhecida). Qualquer CVIT que tenha esta vulnerabilidade corresponde a esta condição.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis de contêiner de	A tabela que a regra usa para agrupar CVITs. Selecione os elementos da árvore: ◦ Item vulnerável do contêiner [sn_vuln_vulnerable_item] ◦ Item vulnerável do contêiner - Imagem do Docker ◦ Item vulnerável do contêiner – Vulnerabilidade do contêiner **Nota:** Se você escolher uma tabela estendida, o **campo Usando** será aplicado somente para itens vulneráveis de aplicação que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar CVITs. Selecione as condições na árvore.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir automaticamente tarefas de correção, a opção Atribuição é usada além das opções **Agrupar por** para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para que cada CVIT seja colocado em uma tarefa com um conjunto de grupo de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ◦ Agrupar por campo: se você selecionou qualquer campo de grupo de usuários nos valores de **campo Usando** na seção

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Agrupar por, eles serão exibidos no menu suspenso. ◦ Grupo de usuários: use a lista de pesquisa para selecionar um grupo de usuários estático.

Nota: Se você excluir uma regra do formulário ou da exibição de lista, terá a opção de excluir todas as tarefas de correção em aberto criadas por essa regra. Grupos que não estão no estado Aberto são excluídos.

4. Selecione **Enviar** para novas regras.
   Depois de selecionar **Enviar**, sua regra será exibida na lista Regras da tarefa de correção [sn_vul_grouping_rule]. As situações a seguir iniciam sua regra.
   - Quando novos CVITs são criados.
   - Quando você seleciona **Reaplicar**. Selecione **Reaplicar** para avaliar regras de tarefa somente em tarefas de correção existentes.
   - Quando os CVITs são atualizados, por você ou pelo sistema.

     Se um CVIT for atualizado, as regras de tarefa serão avaliadas quanto a correspondências com as tarefas de correção existentes. Algumas atualizações comuns que iniciam uma verificação de regras são:
     - Quando o Estado muda de Encerrado para Aberto ou de Encerrado para Sob investigação.
     - O item de configuração (IC) foi alterado.
     - A vulnerabilidade foi alterada.

   O sistema verifica se todas as regras de tarefa correspondem ao CVIT atualizado. Se as condições de uma regra corresponderem às condições de uma tarefa de correção, os CVITs correspondentes serão atribuídos a ela.

   Se nenhuma correspondência for encontrada, uma nova tarefa de correção será criada.

   Para obter mais informações sobre a distribuição de estado de CVITs para tarefas de correção e a distribuição de estado de tarefas de correção para CVITs, consulte Visão geral de tarefas e regras de tarefa da Resposta a vulnerabilidades do contêiner.

   Para obter um exemplo de uma regra de tarefa de correção, consulte Exemplos de regra de tarefa de correção da Resposta a vulnerabilidades da aplicação.

5. Para excluir uma regra de tarefa, selecione a regra na lista Regras da tarefa de correção e clique em Excluir.
   A seguinte mensagem é exibida: `A regra de tarefa de correção selecionada criou n tarefas de correção. Das tarefas de correção, n estão no estado Aberto.`

Opção	Descrição
Caixa de seleção desativada (padrão).	Exclua somente a regra. As tarefas que não estão no estado Aberto são excluídas.
Caixa de seleção selecionada.	Inclua as tarefas de correção no estado Aberto ao excluir a regra da tarefa de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	correção. Exclua a regra e todas as tarefas de correção no estado Aberto.

6. Escolha uma opção e selecione **Excluir**.

Criar regras de fechamento automático

Use regras de fechamento automático para fechar CVITs mais antigos automaticamente com base nas condições de filtro que você definir.

Antes de Iniciar

Função necessária: sn_vul.app_manage_auto_close_rules

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de fechamento automático**.

   O sistema base fornece as seguintes regras de fechamento automático: **Última verificação de vulnerabilidades de contêiner**: vulnerabilidades não relatadas nos últimos 90 dias são transferidas para o estado obsoleto.

2. Selecione **Novo** para criar uma regra de fechamento automático.
3. No formulário, preencha os campos.

Campo	Valor
Nome	Nome da regra de fechamento automático.
Ativo	Opção para ativar a regra. Se ativado, ele fechará automaticamente todas as detecções que correspondam aos critérios de filtro.
Ordem de execução	Valor exclusivo para a execução da regra de fechamento automático. Este valor determina a ordem de execução. O valor padrão é 100.
Tipo de integração	Integração de vulnerabilidade da aplicação
Descrição	Descrição da regra de fechamento automático.
Condição	Condições de filtro usadas para identificar detecções que devem ser encerradas.

4. Selecione **Enviar**.
   Os trabalhos agendados de regras **de fechamento automático são** executados à noite. Ele identifica CVITs com base nas condições especificadas e faz a transição das condições correspondentes para o estado **Obsoleto**. Nos casos em que há CVITs com status "Encerrado" e "Obsoleto", o CVIT é encerrado com o subestado definido como "Fixo".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fechar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção de aplicação pode ser encerrado imediatamente sem análise adicional, poderá usar o recurso **Fechar**. A partir da v2.10 de Contêiner de Resposta a vulnerabilidades, o botão **Fechar** foi removido para uma tarefa de correção de contêiner.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Nos espaços Resposta a vulnerabilidades, uma tarefa de correção passa pelos mesmos estados que uma tarefa de correção anterior tinha nas versões anteriores do Resposta a vulnerabilidades. Quando todos os itens vulneráveis (VITs) em uma tarefa de correção são encerrados, a tarefa de correção faz a transição para o estado Inativo.

Importante: Você pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou o remove de uma tarefa de correção , a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados `Encerrado` ou `Adiado`.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Selecione o botão **Fechar**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Estado	Selecione o estado como *Encerrado*.
Motivo	Insira o motivo para fechar o problema.
Informação adicional	Insira outras informações relevantes.

4. Selecione **Enviar**.
   A tarefa de correção é marcada como **Encerrada**.

IT Operations Management e descoberta de padrões

Quando a descoberta está habilitada, as informações são recebidas da equipe Information Technology Operations Management (ITOM). Se a ITOM Descoberta estiver habilitada, você poderá ver Namespaces do Kubernetes, Clusters do Kubernetes e Serviços do Kubernetes ao abrir um item vulnerável de contêiner (CVIT). Do contrário, você pode ver as informações de carga do Prisma.

Os rótulos de imagem das cargas do Prisma são armazenados como pares de valores de chave na imagem do Docker. Os rótulos em uma carga do Prisma são armazenados na tabela cmdb_key_value. Para habilitar este recurso, uma regra de identificação é enviada para cmdb_ci_docker_image pela equipe de ITOM. Abra a imagem do Docker para exibir a lista de itens relacionados. A maioria dos itens é preenchida pela equipe ITOM. A entrada de identificação de uma imagem do Docker é enviada para mostrar os valores como pares de valores de chave.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A criticalidade dos negócios é determinada com base nas informações de criticalidade do serviço recebidas da equipe ITOM. Um trabalho agendado é executado para extrair dados de todos os serviços associados a uma imagem. Ele calcula a criticidade dos negócios com base no mapeamento de serviços. Como a pontuação de risco pode depender da criticalidade dos negócios, a pontuação de risco também é calculada com base nela.

Soluções de análise e emissão de relatórios para Contêiner de Resposta a vulnerabilidades

Este Solução Performance Analytics e relatórios contém conteúdo Análise da plataforma] pré-empacotado para uso com outros produtos Now Platform. Este Solução Performance Analytics e relatórios fornece uma exposição sobre como as vulnerabilidades são gerenciadas por meio de vários gráficos.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta Solução:

- Now Platform administrador (admin): instale e ative esta solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Análise da plataforma administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Informações relacionadas

Soluções de análise e relatório

Painel do Contêiner de Resposta a vulnerabilidades

As soluções de análise e emissão de relatórios contêm conteúdo Performance Analytics e Emissão de relatórios pré-empacotado para uso com outros produtos Now Platform. Este Solução Performance Analytics e relatórios permite que você rastreie o volume, o desempenho e o andamento das vulnerabilidades desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado.

Funções necessárias de Now Platform

- Now Platform administrador (admin): instale e ative esta solução de análise e emissão de relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Acessar os painéis de Contêiner de Resposta a vulnerabilidades

Para abrir o painel, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Visão geral**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

A partir da versão 2.2 do Contêiner de Resposta a vulnerabilidades, este painel também pode ser exibido na IU Next Experience. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e selecione o ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, selecione a lista suspensa ao lado do nome do painel. Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace e Visão geral dos painéis.

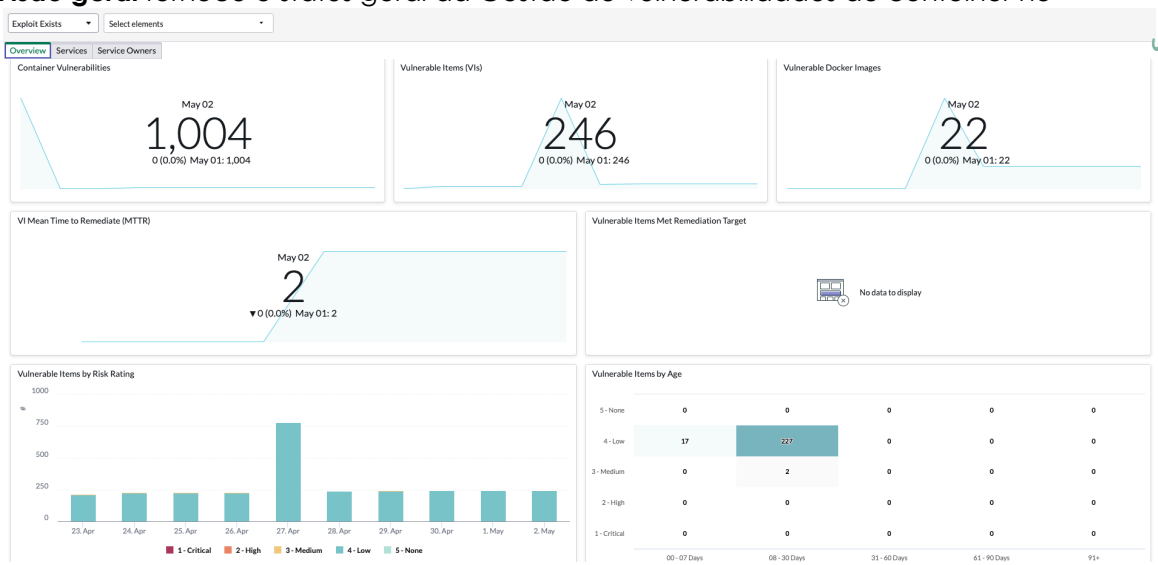
Nota:

- Se você for um novo usuário, poderá exibir os painéis somente nos espaços.
- Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Guias da Gestão de vulnerabilidades de contêiner

Este painel permite que você veja as vulnerabilidades que estão presentes nos contêineres. Você pode exibir as vulnerabilidades e os dados relacionados por região, idade, serviços e outros detalhamentos.

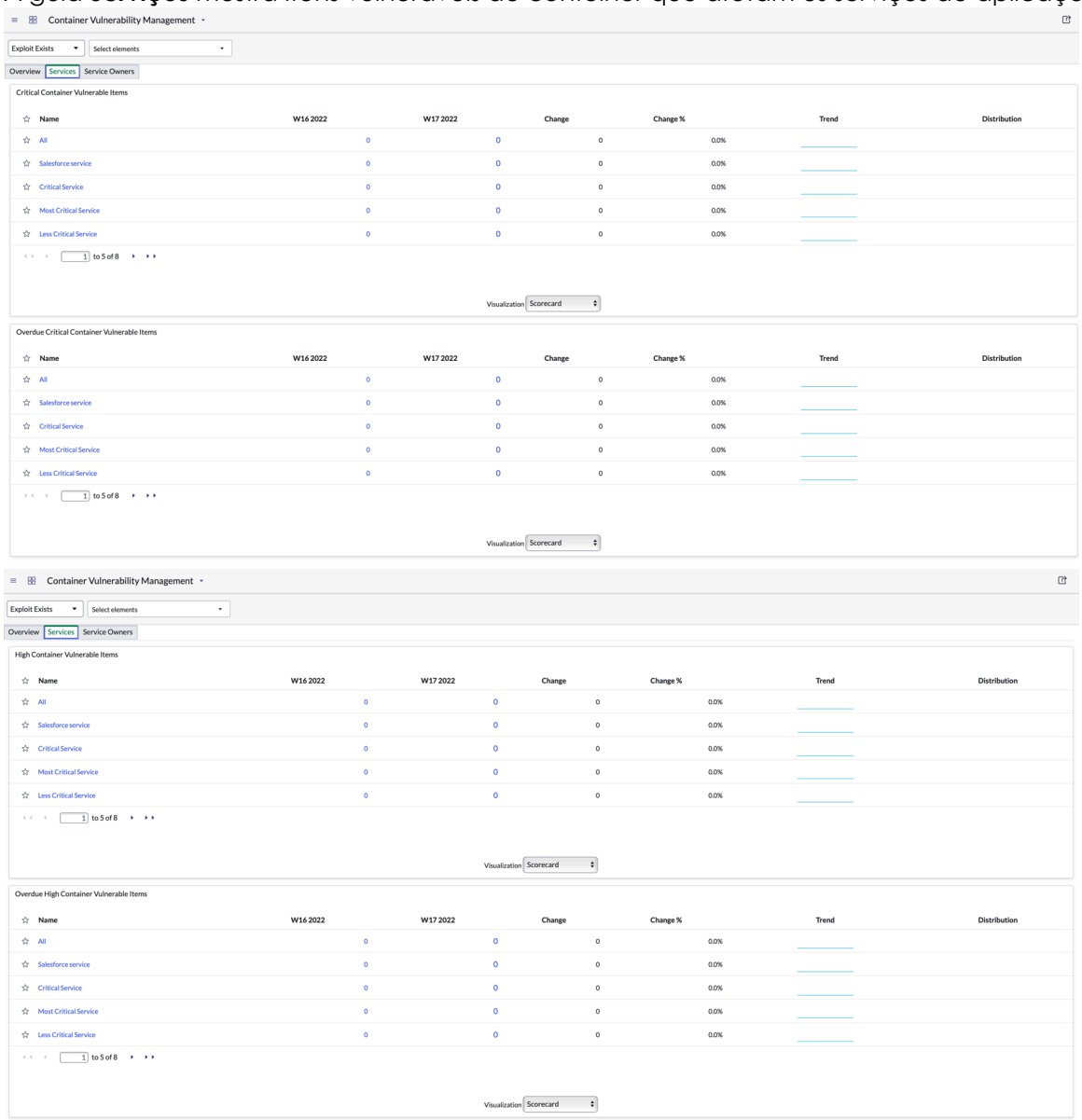
A guia **Visão geral** fornece o status geral da Gestão de vulnerabilidades de contêiner no sistema.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

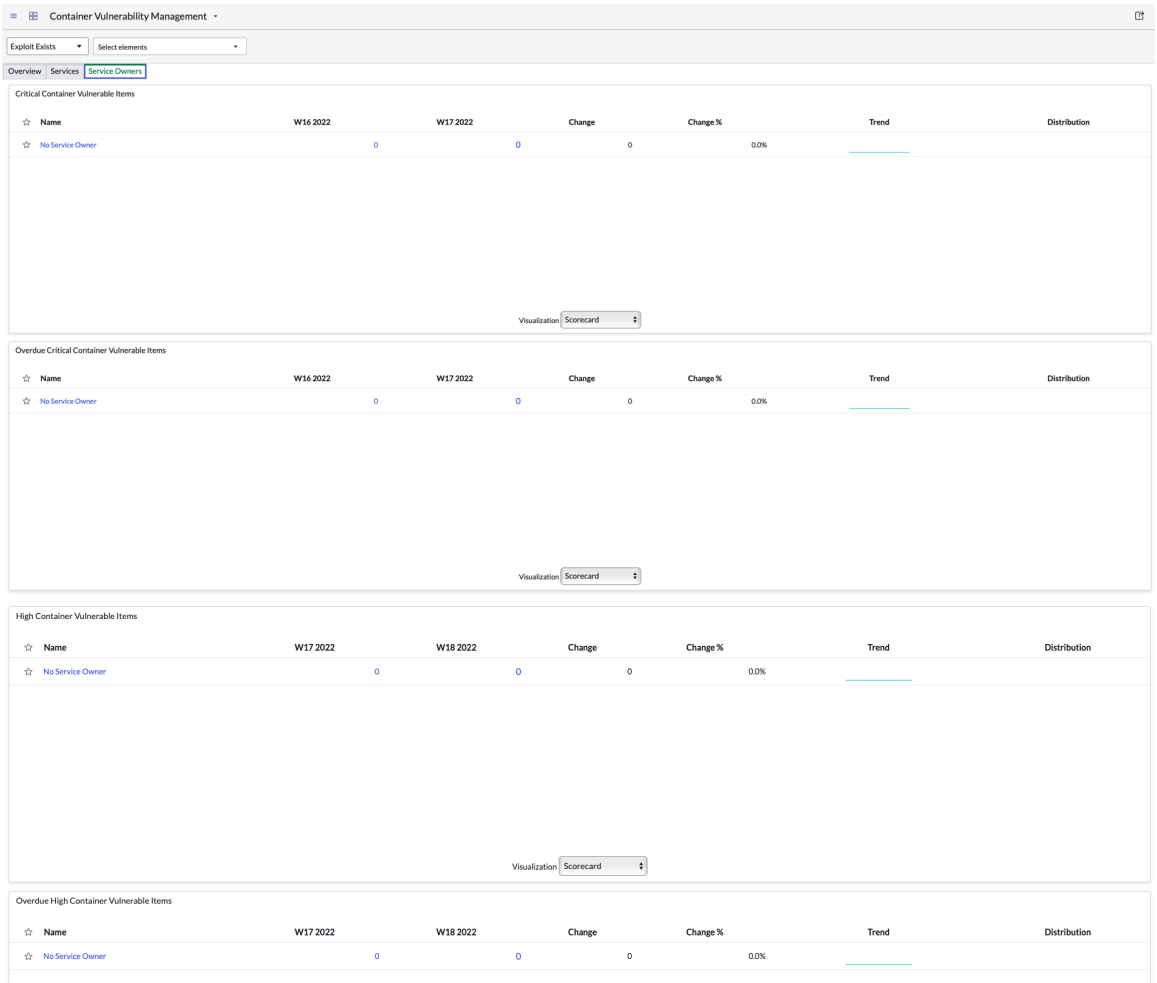
A guia **Serviços** mostra itens vulneráveis de contêiner que afetam os serviços de aplicações.



A guia **Responsáveis pelo serviço** mostra itens vulneráveis de contêiner que afetam os responsáveis pelo serviço.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Detalhamentos

- Explorar Itens Existentes
- Explorar Vetor de Ataque
- Explorar Nível de Habilidade
- Status da meta de correção
- Pontuação de risco
- Estado
- Grupo de atribuição

Tradução automática

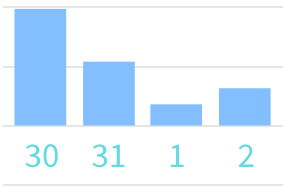
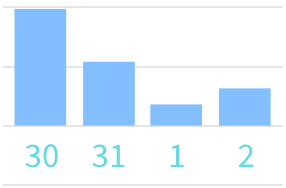
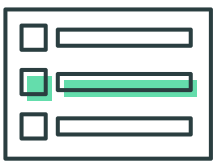
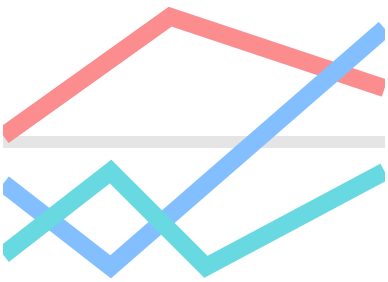
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Nome	Tipo	Descrição
Vulnerabilidades do contêiner	Pontuação única	Número de vulnerabilidades de contêiner associadas a um ou mais itens vulneráveis de contêiner ativos.
Itens vulneráveis (IVs)	Pontuação única	Número de itens vulneráveis do contêiner ativos (não encerrados).
Imagens do Docker vulneráveis	Pontuação única	Número de imagens do docker associadas aos itens vulneráveis de contêiner ativos.
Tempo médio de correção (MTTR) de VI	Pontuação única	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução.
Itens vulneráveis que atenderam à meta de correção	Pontuação única	Percentual de itens vulneráveis de contêiner encerrados que atenderam às datas de meta de correção nos trimestres atual e anterior. As metas de correção são calculadas a partir da data da Última

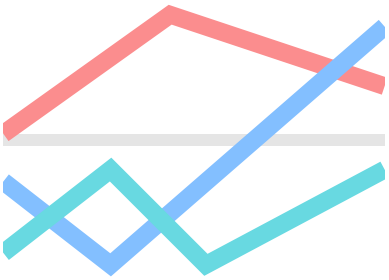
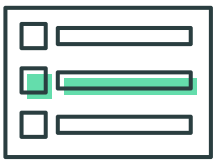
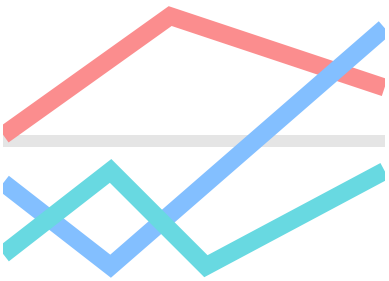
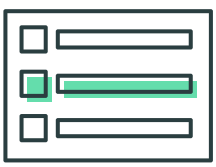
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		abertura mais o número de dias.
Itens vulneráveis por classificação de risco	Barra 	Número de itens vulneráveis de contêiner ativo, agrupados por classificação de risco no período selecionado.
Itens vulneráveis conforme o tempo decorrido	Barra 	Número de itens vulneráveis de contêiner ativos agrupados por classificação de risco e idade (em dias).
Itens vulneráveis de contêineres críticos	  de lista e linha	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica, agrupados por serviço.

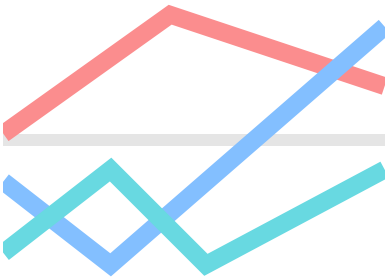
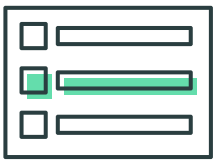
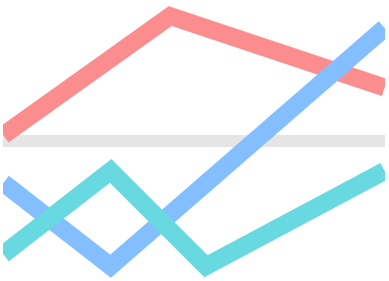
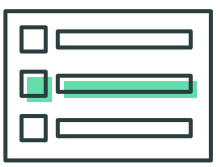
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica e após suas datas de meta de correção, agrupados por serviço.
Itens de alta vulnerabilidade de contêineres	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco alta, agrupados por serviço.

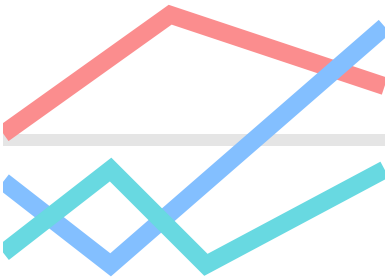
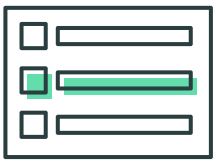
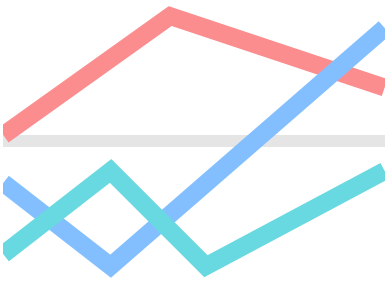
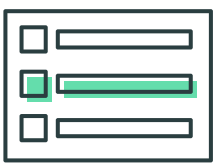
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis ativos com uma classificação de risco alta e após suas datas de meta de correção, agrupados por serviço.
Itens vulneráveis de contêineres críticos	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica, agrupados por responsável pelo serviço.

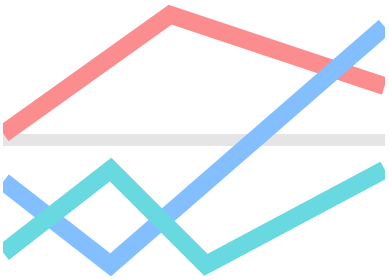
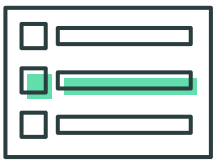
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica e após suas datas de meta de correção, agrupados por responsável pelo serviço.
Itens de alta vulnerabilidade de contêineres	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco alta, agrupados por responsável pelo serviço.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis ativos com uma classificação de risco alta e após as datas de meta de correção, agrupados por responsável pelo serviço.

Referência do Contêiner de Resposta a vulnerabilidades

Tópicos de referência que contêm informações sobre tabelas, funções e propriedades instaladas com o Contêiner de Resposta a vulnerabilidades.

Componentes instalados com Contêiner de Resposta a vulnerabilidades

Vários tipos de componentes são instalados com a ativação da aplicação Contêiner de Resposta a vulnerabilidades, incluindo tabelas, funções de usuário e trabalhos agendados.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas com Contêiner de Resposta a vulnerabilidades

As funções são adicionadas com a ativação de Contêiner de Resposta a vulnerabilidades.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Resposta a vulnerabilidades. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se você for um cliente de upgrade, o acesso dos usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write anteriores à v10.3 não foi alterado. Usuários e grupos permanecem atribuídos a essas funções até que você os altere. No entanto, a partir da v10.3, você pode preferir atribuir funções granulares para obter mais controle sobre o que usuários e grupos podem fazer e ver na aplicação Resposta a vulnerabilidades. Para obter uma visão geral e mais informações sobre como gerenciar essas funções, consulte Resposta a vulnerabilidades personas e funções granulares e Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Título da função [name]	Descrição
V2.10: sn_vul_container.delete	Exclui registros de origem. C as funções sn_vul_cmn.dele sn_vul_container.delete_vi.
sn_vul_container.ci_manager	Gerencia a reclassificação configuração (ICs) incomp
sn_vul_container.configure_integrations	Configura integrações de c
sn_vul_container.configure_vi_granularity	Configura a granularidade vulnerável do contêiner.
sn_vul_container.create_vi	Pode criar itens vulneráveis manualmente.
sn_vul_container.delete_vi	Pode excluir itens vulnerável contêiner criados manualm
sn_vul_container.exception_approver	Aprova exceções, adiamen fechamentos de itens vulne contêiner. A partir da v2.3, a função g sn_vul_container.read_all, f desta função para que voc acessar os itens vulneráveis e as tarefas de correção at você e seu grupo em vez d itens vulneráveis de contêin de correção.
sn_vul_container.false_positive_approver	Aprova ou rejeita itens vuln contêiner de fechamento c positivos.
sn_vul_container.manage_assignment_rules	Define e atualiza regras de de itens vulneráveis de con
sn_vul_container.manage_auto_close_stale_vi	Configurar os itens vulnerável contêiner obsoleto de fech automático
sn_vul_container.manage_auto_exception_rule	Gerenciar (criar/ler/atualiza regras de exceção
sn_vul_container.manage_normalized_severity	Pode atualizar o mapeame normalizar a gravidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição
sn_vul_container.manage_permissions	Pode atribuir funções de res vulnerabilidades de contêin
sn_vul_container.manage_remediation_targ…	Define e atualiza regras de correção de contêiner.
sn_vul_container.manage_risk_score_confi...	Define e atualiza calculado pontuação de risco, regras e calculadoras de acúmulo vulnerabilidade para itens v de contêiner.
sn_vul_container.read_all	Pode exibir todos os itens vu contêiner e informações rel
sn_vul_container.read_assigned	Pode exibir itens vulneráveis contêiner atribuídos a mim grupos.
sn_vul_container.read_assignment_rules	Pode exibir Regras de atribu vulneráveis de contêiner.
sn_vul_container.read_auto_exception_rule	Regras de exceção de leitu
sn_vul_container.read_discovered_image	Pode exibir itens descoberto
sn_vul_container.read_integrations	Pode exibir resultados de ex integração.
sn_vul_container.read_normalized_severity	Pode exibir o mapeamento gravidade normalizado.
sn_vul_container.read_remediation_target...	Pode exibir Regras de destin correção.
sn_vul_container.read_risk_score_configu...	Pode exibir calculadoras de de risco, regras de risco e c de acúmulo de vulnerabilid itens vulneráveis de contêin
sn_vul_container.remediation_owner	Lê e grava itens vulneráveis atribuídos a eles. Os registro vulnerabilidade também po lidos por um usuário com es
sn_vul_container.update_assigned_to	Pode atualizar a atribuição vulneráveis de contêiner. Requer sn_vul_container.wr sn_vul_container.write_assig
sn_vul_container.update_assignment_group	Pode atualizar o grupo de a para itens vulneráveis de co Requer sn_vul_container.wr sn_vul_container.write_assig
sn_vul_container.update_state	Pode atualizar estados de i vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [name]	Descrição
	Requer sn_vul_container.wr sn_vul_container.write_assig
sn_vul_container.vulnerability_admin	Configura todas as regras, integrações e assim por dia o produto Contêiner de Res vulnerabilidades.
sn_vul_container.vulnerability_analyst	Monitora a correção de toc vulneráveis de contêiner.
sn_vul_container.write_all	Pode atualizar todos os iten de contêiner e tarefas de c
sn_vul_container.write_assigned	Pode atualizar itens vulnerá contêiner ou tarefas de cor atribuídas a mim ou aos me
sn_vul_container.read_watch_topic	Pode ler tópicos de observa vulnerabilidades de contêir
sn_vul_container.create_watch_topic	Pode criar tópicos de obser vulnerabilidades de contêir
sn_vul_container.edit_watch_topic	Pode editar tópicos de obs para vulnerabilidades de c
sn_vul_container.manage_exception_configuration	Pode gerenciar configuraç gestão de exceções.

Tabelas instaladas com Contêiner de Resposta a vulnerabilidades

As tabelas são adicionadas com a ativação de Contêiner de Resposta a vulnerabilidades (CVR).

Tabela	Descrição
Descoberta de imagem do contêiner sn_vul_container_image_findings	Armazena informações sobre as vulnerabilidades associadas, camada de imagem, imagem do Docker, repositório de imagens e imagem descoberta.
Camada da imagem do contêiner sn_vul_container_image_lay	Contém as informações de cada camada de imagem. Uma imagem é um arquivo estático com código executável que pode criar um contêiner em um sistema de computação.
Pacote de imagem do contêiner sn_vul_container_image_package	Fornece informações sobre os pacotes em que existem vulnerabilidades. Os detalhes do pacote binário também são fornecidos como um valor separado por vírgulas.
Item vulnerável de contêiner sn_vul_container_image_vulnerable_item	Contém detalhes de cada descoberta e a vulnerabilidade correspondente.
Imagem de contêiner descoberta sn_vul_container_image	Fornece informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens. Ele também armazena as

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	informações da camada e as associa à imagem descoberta.
Mapeamentos de descoberta sn_vul_container_finding_m2m_vul_item	Relacionamento M2M das descobertas da imagem do contêiner e dos itens vulneráveis do contêiner (CVITs).
Fechar automaticamente itens vulneráveis sn_vul_container_image_auto_close_config	Contém as informações sobre como fechar as descobertas de imagem de contêiner obsoletas e acumular o estado para os CVITs.
Chaves de vulnerabilidade da imagem do contêiner sn_vul_container_image_vulnerability_keys	Contém a configuração de granularidade para criação de CVITs a partir das descobertas de imagem do contêiner.
Serviços relacionados ao Docker sn_vul_container_m2m_ci_services	Contém todos os serviços de negócio relacionados a uma imagem de contêiner.
Contagens de contêineres de VR sn_vul_container_vr_container_counts	Contém a média móvel de instâncias de contêiner geradas a partir de uma imagem de contêiner nos últimos 90 dias.
Item de Tarefa de correção de contêiner sn_vul_container_m2m_vul_group_item	Tabela M2M entre CVIT e tarefas de correção de contêiner.
Tarefa de correção de contêiner sn_vul_container_vulnerability	Contém tarefas de correção de contêiner.
Manifesto de tarefa de correção de contêiner sn_vul_container_rt_manifest	Todas as atualizações na tarefa de correção serão feitas usando esta tabela de manifesto por trabalhos agendados.

Trabalhos agendados instalados com Contêiner de Resposta a vulnerabilidades

Trabalhos agendados são adicionados com a ativação de Contêiner de Resposta a vulnerabilidades.

Trabalho agendado	Descrição
Associar VIs de contêiner existentes à regra de exceção automática	Associa automaticamente a regra de exceção automática aos itens vulneráveis de contêiner (CVITs) existentes.
Expiração do adiamento do item vulnerável do contêiner de verificação	Envia notificações se os itens vulneráveis de contêiner ou as vulnerabilidades de contêiner expirarem (e se expirarem em uma semana).
Contagem de contêineres de Resposta a	É executado diariamente para preencher a tabela sn_vul_container_vr_container_counts que calcula a média móvel de 90 dias para contêineres.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
vulnerabilidades (aplicação - Resposta a vulnerabilidades e Conformidade de configurações para contêineres)	
CVITs de fechamento automático	Encerra automaticamente os itens de vulnerabilidade do contêiner que correspondem à condição definida na configuração de fechamento automático. Seu status é alterado para "fixo".
Calcular a criticalidade dos negócios para CVIT	Processa todos os CVITs ativos e atualiza o campo de Criticidade dos negócios com base nos serviços afetados da imagem do Docker do CVIT.
Fechar CVITs de cancelamento que não têm uma imagem do Docker associada	Expira automaticamente CVITs que não têm um IC associado a. Seu estado é definido como Encerrado e o subestado como Cancelado.
Calcular contagens de IV relacionadas à tarefa de correção de contêiner	Calcula as contagens nos registros da Tarefa de correção de contêiner.
Acumular valores de item vulnerável de contêiner para vulnerabilidade e grupo	Calcula vulnerabilidades e acúmulos de grupo para itens vulneráveis de contêiner. **Nota:** A partir da v2.10 de Contêiner de Resposta a vulnerabilidades, o trabalho agendado foi aprimorado para criar trabalhos em segundo plano com recursos de vários threads. Esse upgrade envolve a segmentação do trabalho em vários trabalhos secundários menores, que são executados em paralelo ou simultaneamente. Esta modificação permite o processamento de vários registros simultaneamente, acelerando significativamente a tarefa geral.

Tradução automática

Contêiner de Resposta a vulnerabilidades Glossário

Saiba mais sobre termos e conceitos exclusivos de Contêiner de Resposta a vulnerabilidades.

Termos principais

Contêiner

Uma unidade de software que empacota o código e todas as suas dependências para que a aplicação seja executada de forma contínua e confiável de um ambiente de computação para outro.

Imagem do contêiner

Um arquivo estático com código executável que pode criar um contêiner em um sistema de computação. Uma imagem de contêiner não pode ser alterada e, portanto, pode ser implantada de forma consistente em qualquer ambiente.

Cluster

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um conjunto de máquinas de trabalho, chamadas de nós, que executam aplicações em contêineres.

Docker

Software para criar, implantar e gerenciar contêineres de aplicações em servidores e na nuvem.

Imagem do Docker

Um arquivo de modelo que contém código, bibliotecas necessárias, configurações e assim por diante. O arquivo é usado para iniciar instâncias de contêiner. Ele consiste em uma união de sistemas de arquivos em camadas.

Dockerfile

Um arquivo de texto que contém instruções para criar imagens de contêiner adicionando várias camadas. Por exemplo, camadas de código do aplicativo, Nginx e Ubuntu de base.

Docker Compose

Uma ferramenta para definir e executar aplicações complexas com o Docker. Com o Compose, você pode definir uma aplicação de vários contêineres em um único arquivo.

Contêiner do Docker

Um contêiner do Docker é uma instância de tempo de execução iniciada a partir de uma imagem do Docker.

Camada de imagem

Uma camada é uma modificação em uma imagem. É representado por uma instrução no Dockerfile. As camadas são aplicadas em sequência à imagem base para criar a imagem final.

Repositório de imagem

Uma coleção de imagens do Docker com diferentes marcadores ou versões.

Rótulos de imagem

Um conjunto de pares de chave-valor armazenados com a imagem como metadados.

Namespace

Uma abstração usada pelo Kubernetes para oferecer suporte ao isolamento de grupos de recursos em um único cluster.

Pod

Um conjunto de contêineres em execução (outra abstração sobre um contêiner).

Registro

Um serviço hospedado que contém repositórios de imagens.

Serviço

Uma maneira abstrata de expor uma aplicação em execução em um conjunto de pods como um serviço de rede.

Marcador

Um marcador é um rótulo aplicado a uma imagem do Docker em um determinado repositório de imagens. Os marcadores são como várias imagens em um repositório são diferenciadas umas das outras.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de configuração do Prisma Cloud Compute

O formulário de configuração do Prisma Cloud Compute é acessado de dentro do módulo Prisma Cloud Compute Integration.

Para exibir o formulário de configuração do Prisma Cloud Compute, navegue até **Todos** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.

Configuração do Prisma Cloud Compute

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL Base da API	URL para integração com o Prisma Cloud Compute.
Nome de usuário	Nome de usuário para acessar o Prisma Cloud Compute.
Senha	Senha para acessar o Prisma Cloud Compute.
MID Server	Uma aplicação Java que é executada como um serviço do Windows ou daemon do UNIX em um servidor em sua rede local. O MID Server permite a comunicação e a movimentação de dados entre uma instância ServiceNow e aplicações, fontes de dados e serviços externos.
Usar projetos	Opção para configurar os projetos. Ao marcar a caixa de seleção, você pode selecionar projetos na página de configuração e executar as integrações com base nos projetos configurados para preencher detalhes específicos do projeto. **Nota:** Se esta caixa de seleção estiver marcada, a guia **Configurar projetos** será habilitada. Clique em **Avançar** para prosseguir com a configuração dos projetos.

Formulário Solicitar exceção

Solicite exceções de política usando a capacidade de gestão de exceções de política GRCGestão de políticas e conformidade na aplicação [] de dentro de Contêiner de Resposta a vulnerabilidades.

Para exibir o formulário de configuração do Prisma Cloud Compute, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Itens vulneráveis de contêiner** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não estiver selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e quando o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

Formulário Regra de exceção

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica de um grupo de itens vulneráveis de contêiner (CVITs), como uma regra com uma condição que se baseia na gravidade da vulnerabilidade desses CVITs. Com esta regra, você pode adiar CVITs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Para exibir o formulário Regra de exceção, navegue até **Todos** > **Resposta a vulnerabilidades do contêiner** > **Administração** > **Regras de exceção**.

Formulário Regra de exceção

Campo	Descrição
Nome	Nome da regra de exceção.
Válido de	Data a partir da qual esta regra está ativa para adiar os CVITs.
Válido até	Data a partir da qual a tarefa de correção para de aceitar novos CVITs.
Motivo	Motivo para criar esta regra de exceção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de exceção

Campo	Descrição
Grupo de atribuição	Grupo ao qual a tarefa de correção criada para rastrear os CVITs adiados está atribuída.
Informação adicional	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condição de filtro para os CVITs que podem ser definidos durante o processamento dos CVITs.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.
Fase do fluxo de trabalho	Status de aprovação atual da regra de exceção.
Estado	Estado da regra de exceção.
Ordem de execução	Ordem exclusiva para cada regra de exceção.
Adiado até	Data até quando as VULs e CVITs são adiadas. Nesta data, a VUL criada é fechada, todos os CVITs são movidos para fora do grupo e as regras do grupo são reaplicadas.

Conformidade de configurações

A aplicação ServiceNow® Conformidade de configurações é uma aplicação de avaliação de configuração segura (SCA) que agrega resultados de verificação de integrações com aplicações de verificação de configuração de terceiros. Você pode priorizar problemas de conformidade de configuração usando seu Configuration Management Database (CMDB). Conformidade de configurações se integra totalmente ao processo de gestão de mudanças de TI para corrigir suas configurações fora de conformidade.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

A partir da versão 18.0 do Resposta a vulnerabilidades, você pode monitorar e corrigir problemas de configuração em Vulnerability Manager Workspace e Espaço de correção

Tradução automática

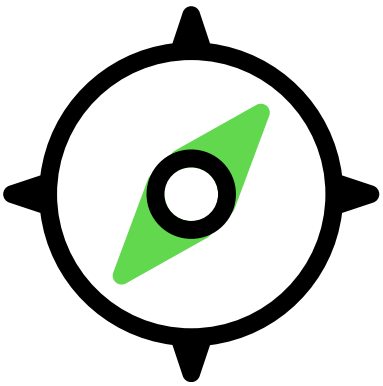
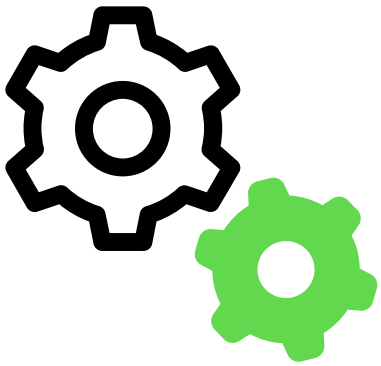
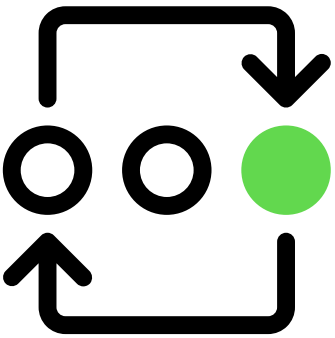
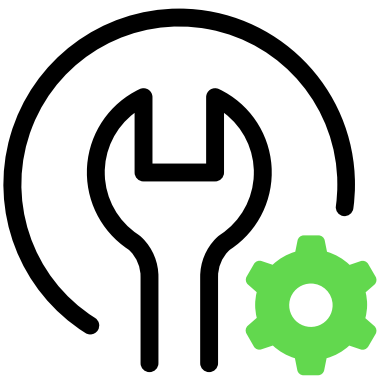
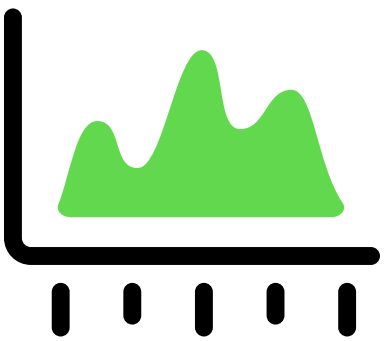
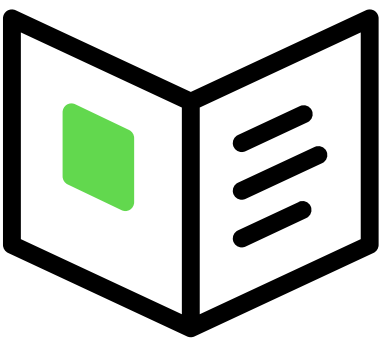
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de problemas de TI, respectivamente. Para obter mais informações, consulte Vulnerability Manager Workspace e Espaço de correção de problemas de TI.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Conformidade de configurações

Explorar	Configurar	Integrar
		
Saiba mais sobre os conceitos e recursos de Conformidade de configurações	Configurar Conformidade de configuração	Estenda a Conformidade de configuração integrando-a a outras aplicações
Corrigir	**Análise e relatórios**	**Referência**
		
Saiba como corrigir seus ativos fora de conformidade com a Conformidade de configuração	Exibir relatórios e painéis no Configuration Compliance	Veja os detalhes sobre componentes de Conformidade de configuração, como campos, tabelas e propriedades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorando Conformidade de configurações

Use os resultados de testes obtidos de integrações de avaliação de configuração segura (SCA) de terceiros para verificar a conformidade com as políticas corporativas ou de segurança. Identifique, priorize e corrija itens de configuração fora de conformidade.

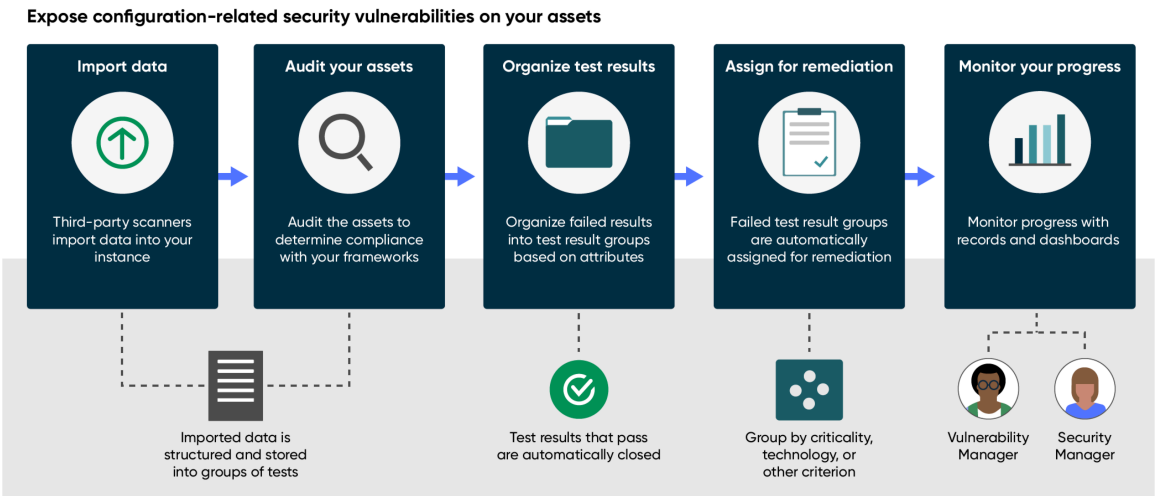
Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

O que é Conformidade de configurações

A aplicação ServiceNow® Conformidade de configurações permite priorizar e corrigir as vulnerabilidades mais críticas relacionadas à configuração em seu ambiente de forma rápida e eficiente. Conformidade de configurações está disponível por assinatura no ServiceNow® Store.



Principais recursos do Conformidade de configurações

Use o Configuration Management Database (CMDB) em seu Now Platform® para ajudá-lo a expor e corrigir suas vulnerabilidades de segurança mais críticas relacionadas à configuração. Concentre seus recursos de correção em atividades com a maior redução de risco. Simplifique o processo de correção na segurança, na TI e nas partes interessadas do processo de negócios. A aplicação Conformidade de configurações inclui os seguintes recursos principais:

- Com integrações de terceiros compatíveis, importe automaticamente políticas, testes, fontes autorizadas e tecnologias. Consulte Integrações do Conformidade de configurações para obter mais informações sobre integrações compatíveis.
- Correlacione políticas e testes com itens de configuração (ativos) para identificar vulnerabilidades relacionadas à configuração e ajudá-lo a verificar se seus ativos estão em conformidade com suas políticas e controles.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Unifique a avaliação, a atribuição e a correção de configuração em todos os seus ativos.
- O conteúdo de verificação de configuração pode ser importado das principais aplicações de integração do ecossistema de avaliação de configuração segura (SCA).
- As descobertas de configuração e falhas de teste podem ser agrupadas e roteadas automaticamente com base nos conjuntos de habilidades e áreas de responsabilidade do especialista em correção. Fluxos de trabalho inteligentes e integração estreita com a gestão de mudanças fornecem transferências de tarefas suaves entre grupos.
- Quando usados com a aplicação ServiceNow Governança, risco e conformidade (GRC), os testes de configuração em Conformidade de configurações podem ser acumulados em seus controles GRC correspondentes.
- Com a gestão de mudanças aprimorada, crie solicitações de mudança preenchidas previamente para TI diretamente do Conformidade de configurações para ajudá-lo nas tarefas de correção que exigem recursos adicionais.
- Com painéis, exiba as métricas de status de correção na tarefa de correção, teste de conformidade e registros de política.

Quem usa Conformidade de configurações

Conformidade de configurações As atividades do podem envolver muitos níveis de gestão.

- Administradores do sistema
- Administradores de vulnerabilidade
- Gerentes de vulnerabilidade
- Analistas de vulnerabilidade
- Administradores de conformidade

Conformidade de configurações tarefas envolvem as funções a seguir.

- sn_vulc.admin — pode ler, gravar e excluir
- sn_vulc.write — pode ler e gravar
- sn_vulc.remediation_owner — Pode ler e atualizar registros atribuídos

  Nota: A função sn_vulc.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a qualquer usuário.

- sn_vulc.read — pode ler

Conformidade de configurações e Operações de segurança

Quando o Qualys Vulnerability Integration e o Integrações de vulnerabilidade da Tenable estão instalados, o acesso a Resposta a vulnerabilidades se torna disponível. Você pode ter várias implantações dessas integrações. Os dados obtidos de cada implantação são identificados e estão disponíveis em uma única instância de GRC.

Versões disponíveis para Xanadu

Versão de lançamento	Notas de versão
Conformidade de configurações v14.7, v14.8, v14.9, v14.10, v14.11, v14.12	Para obter informações de compatibilidade, consulte KB0856498 Matriz de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão de lançamento	Notas de versão
	compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Conformidade de configurações dados importados

A aplicação Conformidade de configurações importa políticas, testes, fontes autorizadas e resultados de testes de integrações de terceiros e os armazena em módulos para exibição.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Integrações compatíveis

As integrações de terceiros importam descobertas de avaliação de configuração, grupos de testes, testes, tecnologias, fontes autorizadas e resultados de testes para a aplicação Conformidade de configurações. Os gerentes de vulnerabilidade ou analistas de vulnerabilidade podem usar esses dados para identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos.

Para obter mais informações sobre integrações compatíveis, consulte Integrações do Conformidade de configurações.

Grupos de teste

Grupos de teste estão relacionados a documentos oficiais e registros de teste. Um grupo de testes de configuração define Grupos de Teste. Os grupos de teste normalmente se alinham a uma classe de tecnologia, por exemplo, Windows, bancos de dados Oracle, Cisco IOS e geralmente são derivados do padrão primário do setor. Os grupos de teste podem ser modificados para atender às necessidades da organização. Um único teste de configuração pode pertencer a vários grupos de teste.

Integração	Descrição
Qualys Vulnerability Integration	Os grupos de teste são recuperados e os IDs de controle são preenchidos pelo trabalho agendado, **Políticas de PC da Qualys** à 1h. Você pode exibir o trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Políticas de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute as **Políticas de PC da Qualys** primeiro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io de integração de resultados de conformidade importa políticas. Se você optar por executar as integrações manualmente, execute-as na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Para exibir o registro da política, navegue até **Todos** > **Conformidade de configurações** > **Grupos de teste**. Para identificar e criar corretamente os registros do grupo de teste, as informações de auditoria dos grupos de teste são importadas e exibidas no campo **Descrição resumida**.

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser controlada.

Um teste Conformidade de configurações é o mecanismo que as aplicações de integração de terceiros usam para agrupar ativos por tipo de vulnerabilidade. Algumas soluções de verificação de VA de terceiros, como a Qualys, têm bibliotecas muito grandes de testes (até 8.000) que são mapeadas para políticas e "estruturas" de fontes autorizadas.

Um Teste pode ter muitos valores, um para muitos, esperado versus real e assim por diante. Um teste é qualquer coisa que possa ser usada para identificar uma classe de ativo de software ou hardware que está fora de conformidade. Por exemplo, uma versão ou número de hardware.

Integração	Descrição
Qualys Vulnerability Integration	O trabalho agendado, **Qualys PC Controls**, recupera os testes. Você pode exibir o trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Controles de PC da Qualys**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	Nota: Se você optar por executar a integração manualmente, execute **Controles de PC** da **Qualys após Políticas de PC**da Qualys .
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io A integração de resultados de conformidade importa testes de configuração (Testes). Se você optar por executar as integrações manualmente, execute-as na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Para exibir o registro de Teste de configuração, navegue até **Conformidade de configurações** > **Testes**. No registro, os dados importados são exibidos no campo **Descrição resumida** e nas guias Status da correção, Descrição e Correção. Os dados também são exibidos nos links relacionados **Citações**, **Políticas**e **Resultados de testes**.

Tecnologias

Uma das técnicas usadas por scanners de vulnerabilidade de terceiros para criar grupos de teste de itens de configuração de software e hardware para análise é organizá-los por tecnologia. As tecnologias são uma biblioteca importada de sistemas operacionais, dispositivos de rede, bancos de dados e aplicativos associados a políticas. Os testes têm várias implementações para diferentes tecnologias. A correção também é específica da tecnologia.

Você pode exibir as tecnologias aplicáveis a um teste para entender melhor a quais tipos de ativos de software ou hardware o controle pode ser aplicado. Exemplos de tecnologias que podem ser aplicadas a controles incluem CentOS 7.x, Windows 8.1, Windows 2016 Server e assim por diante. A lista de tecnologias é somente leitura e corresponde às tecnologias definidas na aplicação Qualys Cloud Platform.

As tecnologias são importadas somente para avaliações de configuração relacionadas ao banco de dados. O *db_type* (se não estiver vazio) na importação é usado para criar uma tecnologia. Exibir tecnologias preenchidas na seção Tecnologias em registros de teste de configuração, registros de resultado de testes, registros de política e em **Conformidade de configurações** > **Dados de suporte** > **Tecnologias**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fontes autorizadas

Conformidade de configurações usa citações e fontes autorizadas ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente mapeiam para seções de padrões publicados do setor, como "NIST 800-53 versão 3 (2009) 3: 2009, SA-4".

Nota: No Qualys Vulnerability Integration, essa combinação é chamada de estrutura.

Fontes autorizadas e citações (também conhecidas como mandatos) são importadas dos scanners de vulnerabilidade de terceiros.

Os registros de origem autorizada contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas na área de segurança de computadores. Eles definem requisitos para políticas e procedimentos de segurança. Os testes de configuração podem fazer referência a várias fontes autorizadas por meio de citações. Fontes autorizadas podem relatar a conformidade de um determinado padrão na preparação para uma auditoria.

Integração	Descrição
Qualys Vulnerability Integration	O trabalho agendado, **Detalhe de políticas de PC da Qualys**, recupera as fontes autorizadas e as citações. Você pode exibir este trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Detalhe das políticas de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Qualys PC Policies Detail** após **Qualys PC Policies**.
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io Integração de resultados de conformidade importa fontes autorizadas como parte dos dados de citações. Se você optar por executar as integrações manualmente, execute-as na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	Os dados são exibidos no link relacionado a **Citações** nos registros de teste de configuração.

Resultados de testes

Conformidade de configurações não calcula os resultados de testes, mas os importa como parte de uma integração de terceiros. Depois que podem ser exibidos em Conformidade de configurações, eles são corrigidos usando **Tarefas**de correção. Para obter mais informações, consulte Conformidade de configurações correlação.

Integração	Descrição
Qualys Vulnerability Integration	Você pode recuperar os resultados de testes de uma das seguintes maneiras: • O trabalho agendado, **Resultados de PC da Qualys**, recupera os resultados de testes. Você pode exibir este trabalho agendado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Resultados de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute os **Resultados de PC** da **Qualys após as Políticas de PC** da **Qualys e o Detalhe**das políticas de PC da Qualys . A importação de **resultados de PC da Qualys** usa o parâmetro *Start Time* na guia **Detalhes da integração**. Todas as outras Conformidade de configurações importações apresentam todos os dados disponíveis, independentemente de *Start Time*. Quando a importação de **resultados de PC da Qualys** é concluída, um evento é disparado para acionar os cálculos de fim de importação. Para obter mais informações, consulte Conformidade de configurações estados. • Como alternativa, a partir da V14.5, você também pode executar as seguintes integrações para recuperar os resultados de testes:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	Integração: nome / **Descrição** Qualys Integração de host de política de PCRS: Recupera os IDs de host de cada política. Para exibir este trabalho agendado, navegue até: Qualys Vulnerability Integration > Integrações primárias > Qualys PCRS Policy Host Integration. **Nota:** Se você optar por executar a integração manualmente, execute Qualys PCRS Policy Host Integration após Qualys PC Policies e Qualys PC Policies Detail. Depois que este trabalho agendado é concluído, ele aciona automaticamente a integração de resultados de testes do Qualys PCRS. Qualys Integração de resultados de testes de PCRS: Recupera os resultados de testes para cada ID de host. Para exibir este trabalho agendado, navegue até Qualys Vulnerability Integration > Integrações primárias > Integração de resultados de testes de PCRS da Qualys.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	<table><tr><th>Integração: nome</th><th>Descrição</th></tr><tr><td></td><td>**Nota:** Se você optar por executar a integração manualmente, execute a integração de resultados de testes da Qualys PCRS após a integração de políticas de PC da Qualys, detalhe de políticas de PC da Qualys e integração de host de política da Qualys PCRS. Esta integração usa o parâmetro Hora de início na guia Detalhes da integração.</td></tr></table>
Integrações de vulnerabilidade da Tenable	O trabalho agendado Tenable.io de integração de resultados de conformidade importa resultados de testes. Se você optar por executar as integrações manualmente, execute-as na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Integração de preenchimento de resultados de conformidade • Tenable.io Integração de ativos • Tenable.io Integração de preenchimento de resultados de conformidade Para exibir o registro de Teste de configuração, navegue até **Conformidade de configurações** > **Resultados de testes**. No

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	registro, os dados importados são exibidos nos campos**Teste**e **Item de configuração**. Os dados também são exibidos nas guias **Valores esperados, Valoresreais**e **Correção**. Os links relacionados a **Tarefas** de correção e **Histórico de resultados de testes** são preenchidos.

Descoberta de Conformidade de configurações

Conformidade de configurações os dados são importados de aplicações de scanner SCA de terceiros. Eles estruturam grupos de testes de software e hardware em registros de dados para agilizar a realização de avaliações.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Quando uma importação é concluída, um evento é enviado para indicar ações de fim de importação. Para cada tarefa de correção ativa, as seguintes ações são realizadas:

- Grupos resolvidos com resultados com falha retornam ao estado **Aguardando implementação**.
- As tarefas de correção em que todos os resultados foram aprovados são **Encerradas**.
- O estado dos resultados de testes que estão em tarefas de correção ativas é atualizado.
- O sinalizador que indica se um resultado faz parte de uma tarefa de correção ativa é atualizado.

Conformidade de configurações correlação

Conformidade de configurações O fornece priorização e agrupamento de resultados de testes (na tarefa de correção) para ajudar na correção de problemas de não conformidade.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Priorização centrada em ativos

As verificações de configuração podem produzir um grande número de descobertas. Priorize as descobertas para obter a maior redução de risco. A prioridade inclui a criticalidade do teste de configuração e a criticalidade do ativo. A prioridade do resultado de testes de configuração é expressa como uma pontuação de risco na escala de 0 a 100. A calculadora agrupa a pontuação de risco de cálculo e pode ser personalizada.

Quando a importação de terceiros é concluída, Conformidade de configurações envia um evento para indicar ações de fim de importação. Para cada grupo de resultados ativo, as seguintes ações são realizadas:

- As tarefas de correção resolvidas com resultados com falha retornam para o estado **Aguardando implementação**.
- Tarefas de correção em que todos os resultados aprovados são **Encerrados**.
- O estado dos resultados de testes que estão em tarefas de correção ativas é atualizado.
- O sinalizador que indica se um resultado faz parte de uma tarefa de correção ativa é atualizado.

Ordem de precedência das Tarefas de correção

Quando os resultados de testes pertencem a mais de uma tarefa de correção, o **Estado** de um resultado de testes é derivado de acordo com uma ordem de precedência.

Os campos **Estado** e **Resolução** no formulário **Teste de configuração** e o campo **Resultado** no formulário Resultado de **testes** são calculados seguindo esta ordem de precedência.

Nota:

A precedência de associação de grupo se aplica somente a itens em que o item não passou no teste de configuração. Os itens**aprovados** estão sempre no estado **Closed-Fixed**.

O valor de **Resultado** determina o estado. Ignoramos as tarefas de correção no estado **Encerrado-Corrigido** e **Encerrado-Cancelado**. O estado do item é calculado a partir dos estados de todas as outras tarefas de correção às quais ele pertence ou está definido como **Aberto**, se não existir nenhuma outra tarefa de correção para o item.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Criação de Tarefas de correção

Conformidade de configurações As Tarefas de correção são criadas manualmente.

Existem duas maneiras de criar e preencher **Tarefas**de correção .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- No módulo **Tarefas** de correção e usando filtros que preenchem automaticamente a guia **Resultados de testes**.

  Essa maneira é boa para quando você sabe qual filtragem deseja usar. Por exemplo, capturar todos os resultados de testes com falha que são de criticalidade moderada e alta, afetam a infraestrutura baseada no Windows e se aplicam somente à aplicação de cadeia de suprimentos do SAP.

- Ao selecionar resultados de testes na lista **Resultados** de testes e criar uma tarefa de correção no menu **Ações em linhas selecionadas...**

  Este método é bom para resultados que não são facilmente filtrados ou situações em que você deseja especificar resultados de testes para correção. Por exemplo, exceções que não têm nada em comum.

Nota: Se você criar uma tarefa de correção na lista **Resultados de testes** e posteriormente decidir usar um filtro para essa tarefa de correção, suas entradas originais serão removidas e substituídas pelos resultados do filtro.

Resultados de testes não agrupados

Os resultados de testes não agrupados contêm todos os resultados de testes não aprovados que não são membros de uma tarefa de correção ativa (não**encerrada**). Este módulo é atualizado após cada importação e sempre que os resultados de testes são adicionados ou removidos de uma tarefa de correção.

Itens Descobertos para Conformidade de configurações

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) usando regras de pesquisa de IC, quando são importados usando as integrações de host e resultados de testes. Os itens descobertos fornecem visibilidade sobre como a identificação de ativos é mapeada para ICs no CMDB.

Os Itens Descobertos são considerados **Correspondidos**, **Não Correspondidos**ou **Reclassificados**. Os ICs identificados estão no estado **Correspondido**.

Para facilitar a localização de possíveis problemas de correspondência, a regra de pesquisa de IC que correspondeu ao IC aparece no campo **de regra de correspondência de IC**.

Nota: O suporte ao campo**de regra de correspondência de IC** está disponível somente para a integração Qualys.

Se uma correspondência não for encontrada, um IC será criado na classe de *IC*`incompatível [sn_sec_cmn_unmatched_ci]`, `[cmdb_ci_unclassed_hardware]`ou `[cmdb_ci_incomplete_ip]` do CMDB. Se o IC incompatível original tiver sido reclassificado, os registros de itens descobertos serão atualizados para refletir esse estado. Para obter mais informações, consulte ICs incompatíveis e Exibir e reclassificar itens de configuração incompatíveis para obter mais informações.

Por padrão, o **Operações de segurança** > **CMDB** > **Itens Descobertos** O módulo lista itens de configuração incompatíveis. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter uma descrição dos campos em Itens Descobertos, consulte Campos de formulário de Itens Descobertos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mudanças de IC para itens descobertos para Conformidade de configurações

O valor padrão da propriedade `sn_sec_cmn.update_on_ci_change` é `verdadeiro`. Portanto, quando o item de configuração (IC) de um item descoberto é atualizado, os resultados de testes também são atualizados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

O ID externo do resultado de testes é atualizado e a pontuação de risco, as regras de atribuição, as regras de tarefa de correção e a regra de meta de correção são reavaliadas. Se houver um resultado de testes com o mesmo teste e IC, os resultados de testes serão atualizados com o resultado de testes existente e o resultado de testes atual será encerrado com o subestado `invalidCI`. As anotações de trabalho são adicionadas de acordo.

Se você não quiser atualizar o IC do resultado de testes existente, defina a propriedade como falsa. Nesse caso, se um IC mudar, um novo resultado de teste será criado e o existente será encerrado como um `IC inválido`.

Reconciliar itens descobertos sem correspondência para Conformidade de configurações

Crie um trabalho de programação para reconciliar itens descobertos incompatíveis. Quando um resultado de testes é criado, o item de configuração (IC) adicionado a ele no momento da criação pode estar desatualizado.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se as informações no CMDB mudarem, as informações de IC incompatíveis não serão reconciliadas. Para reconciliar, aplique regras de pesquisa de IC nos resultados de testes que estão em um estado incompatível quando o CMDB é atualizado com os ICs mais recentes.
Um trabalho de programação é executado sob demanda para reaplicar a regra de correspondência de IC para os itens descobertos em um estado incompatível. Se o IC mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Os resultados de testes afetados também são atualizados. Para obter detalhes, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Procedimento
1. Navegar até **Todos** > **Operações de segurança > Reconciliar itens descobertos incompatíveis**.
2. Na página Trabalhos em segundo plano, clique em **Criar trabalho de reconciliação**.
3. No formulário, preencha os campos.

Nota: Você só pode editar o campo Parâmetros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho em segundo plano

Campo	Descrição
Número	Número de trabalho exclusivo.
Criado(a) por	Usuário que criou o trabalho.
Parâmetros	Parâmetros para reconciliar os itens descobertos incompatíveis: ◦ limite: número máximo de itens descobertos a serem reconciliados. Se você não inserir um valor, 10.000 itens descobertos serão reconciliados. ◦ firstDiscovereditem: primeiro item descoberto que deve ser reconciliado. Se você não inserir um valor, o processo de reconciliação será iniciado a partir do primeiro item descoberto.
Estado	Estado atual do trabalho em segundo plano.
Descrição do estado	Descrição do estado atual do trabalho em segundo plano.
Tipo de trabalho	Tipo de trabalho. O valor é **Reconciliar itens descobertos incompatíveis**.
Iniciada em	Hora em que o trabalho foi iniciado.
Finalizado às	Hora em que o trabalho foi concluído.
Duração do trabalho	Tempo total necessário para concluir o trabalho.
Subestado	Subestado do estado selecionado.
Anotações	Número de registros processados.

4. Clique em **Enviar**.

Nota:

- Para interromper a execução do trabalho, clique em **Cancelar**.
- Você não pode reconciliar ICs incompatíveis ou reaplicar regras de pesquisa de IC ao importar hosts ou resultados de testes.

Reaplicar regras de pesquisa de IC em itens descobertos selecionados para Conformidade de configurações

Reaplicar regras de pesquisa de item de configuração (IC) em itens descobertos selecionados nas ações de seleção da exibição de lista de itens descobertos. O administrador pode precisar editar ou atualizar uma regra de pesquisa por vários motivos. Se a regra de pesquisa mudar, eles poderão reaplicá-la aos itens descobertos.

Antes de Iniciar
Funções necessárias:

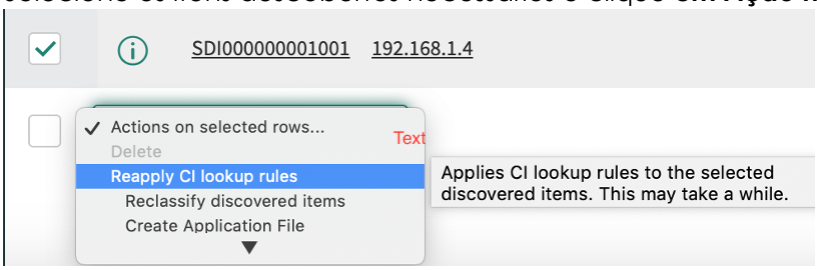
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Se o IC mudar após a reaplicação das regras de pesquisa de IC, os itens descobertos serão atualizados com o novo IC e os resultados de testes. Para obter mais informações, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **CMDB** > **Itens Descobertos**.
2. Selecione os itens descobertos necessários e clique **em Ação nas linhas selecionadas**.



3. Selecione **Reaplicar regras de pesquisa de IC** na lista.

   As regras são reaplicadas nesses itens descobertos.

O Integrações de vulnerabilidade da Tenable com Conformidade de configurações

O produto Tenable.io da Integrações de vulnerabilidade da Tenable importa políticas, controles (resultados de testes) e testes de configuração para processamento na aplicação Conformidade de configurações.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tenable.io

O Integrações de vulnerabilidade da Tenable é compatível.

Você pode usar dados importados para:

- Identifique vulnerabilidades relacionadas à configuração em seus ativos listados em Configuration Management Database (CMDB)
- Verifique se seus ativos estão em conformidade com suas políticas e controles.

Dados de ativos, políticas, controles (resultados de testes) e testes de configuração são importados com as seguintes integrações:

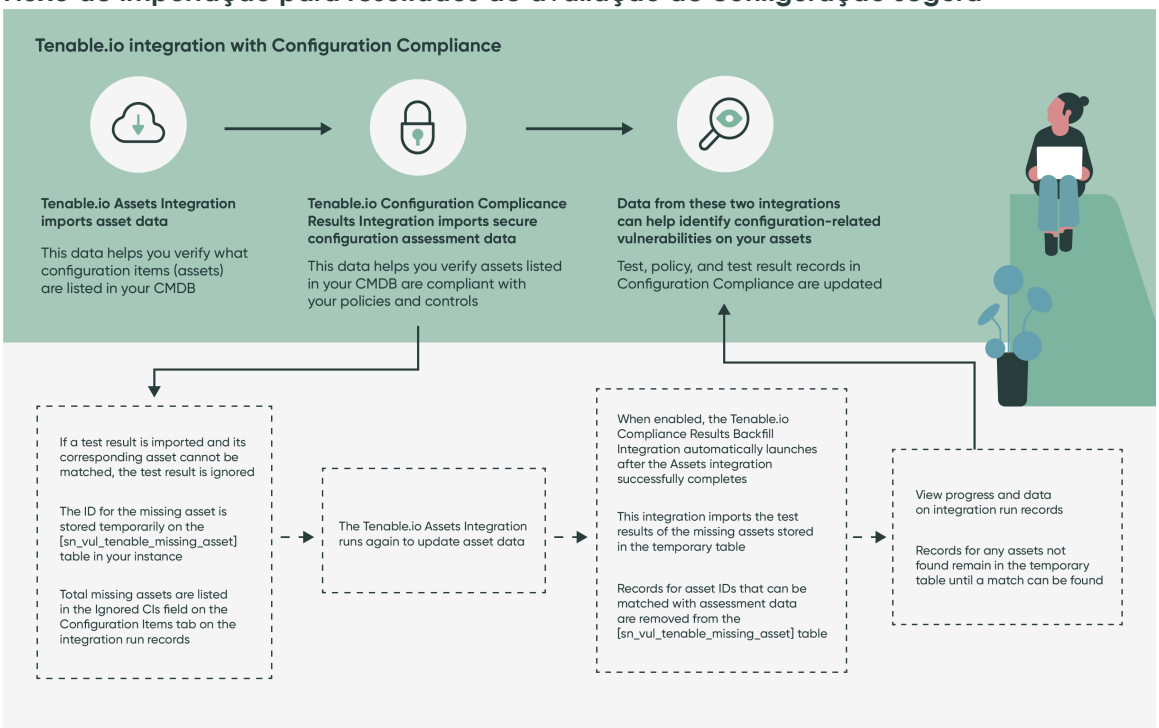
- Tenable.io Integração de ativos
- Tenable.io Integração de resultados de conformidade
- Tenable.io Integração de preenchimento de resultados de conformidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A imagem a seguir ilustra como as integrações funcionam juntas para importar dados de avaliação de ativos e configuração e reconciliar todos os ICs ignorados durante uma importação.

Fluxo de importação para resultados de avaliação de configuração segura



Os dados são importados, atualizados e exibidos no resultado de testes, na política e nos registros de teste de configuração na aplicação Conformidade de configurações.

Em alguns casos, o número de itens de configuração (ICs) importados é diferente para a Tenable.io integração de ativos e a Tenable.io integração de resultados de conformidade. Quando isso ocorre, registros temporários são criados e armazenados para os IDs de ativo ignorados. Esses registros podem ser correspondidos posteriormente com dados de avaliação importados por importações da integração de preenchimento de resultados de conformidade.

Por exemplo, digamos que a integração de ativos importe 80 ativos em uma execução de integração, mas a integração de resultados de conformidade importe 100.

Nota: Você pode verificar o número de ICs ignorados nas execuções de integração navegando até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**. Clique no nome de uma integração para abrir o registro. No link relacionado **Execuções de integração de vulnerabilidade**, abra um registro de execução de integração e selecione a guia **Itens** para ver o valor no campo **ICs ignorados**. Este campo rastreia o total de ativos ignorados (ausentes) na importação.

Ao comparar os valores nos campos de **ICs ignorados** em cada registro de execução de integração, há uma diferença de 20 ICs ignorados. Como resultado, a integração de aterramento é executada automaticamente, conforme mostrado na imagem anterior. Esta integração importa as informações de avaliação de configuração dos 20 ativos extras encontrados pela Integração de resultados de conformidade, mas perdidos pela Integração de ativos. Como os dados de avaliação de ativos ausentes não são importados, a Tenable.io Integração de preenchimento de resultados de conformidade importa até 200 IDs de ativo por execução de integração para reconciliar os ativos ausentes com os dados de avaliação correspondentes. Todos os registros criados para ativos ausentes ou ignorados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e listados na tabela temporária são excluídos depois que esses ativos e seus dados são correspondidos.

Nota: Pode levar várias execuções dessas integrações para importar todos os ativos ignorados.

Para obter mais informações sobre como habilitar e configurar a Tenable.io Asset Integration, consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração. Consulte Noções básicas sobre a integração de vulnerabilidade da Tenable para obter mais informações sobre a integração.

A Tenable.io Integração de resultados de conformidade e a Tenable.io Integração de aterramento de resultados de conformidade estão inativas por padrão.

Para ativá-los:

1. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações da Tenable, clique no nome de uma integração para abrir o registro e marque a caixa de seleção **Ativo** para habilitá-lo. Você pode preferir deixar as configurações de programação em seus valores padrão para que essas integrações sejam iniciadas.

Regras de Pesquisa de IC para identificar itens de configuração a partir de integrações de vulnerabilidade de terceiros do Conformidade de configurações

Quando os dados são importados de uma integração de terceiros, o Conformidade de configurações usa automaticamente os dados do host para pesquisar correspondências no Configuration Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras são usadas para identificar itens de configuração (ICs) e adicioná-los ao registro de resultados de testes para ajudar na correção.

Conforme os ativos são importados, uma pesquisa é realizada primeiro na lista de **itens descobertos** usando IDs de terceiros para encontrar correspondências com os itens de configuração (ICs) de importações anteriores. Quando uma correspondência de ID de host é encontrada, ela é usada como o campo **Item de configuração** no registro de resultado de testes.

Você pode ver como os ativos importados são mapeados para ICs usando a lista de **Itens descobertos**. Se uma correspondência não for encontrada ou o campo cmdb_ci estiver vazio, as regras usarão as informações de outro host para tentar identificar corretamente o IC. Se uma correspondência ainda não for encontrada, um IC de espaço reservado será criado e designado como **IC incompatível**. Consulte ICs incompatíveis para obter mais informações sobre como esses ICs são tratados.

Um novo item descoberto é criado e mapeado para este IC.

Nota: As regras de pesquisa de IC estão disponíveis somente para a Integração Qualys do para Operações de segurança.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Cada origem pode ter várias implantações. A Qualys pode ter várias implantações da Integração da Qualys. Cada implantação tem seu próprio conjunto de regras de pesquisa de IC.

Nota: As regras de pesquisa de IC são compartilhadas por todas as implantações da integração de vulnerabilidade. Se uma regra for excluída ou modificada, a exclusão ou as mudanças afetarão todas as implantações da integração de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao tentar uma correspondência, a primeira etapa é uma pesquisa de ID de fornecedor para uma correspondência exata entre origem, source_instance e ID de fornecedor. Em seguida, as regras de pesquisa são executadas em ordem, da menor para a maior, e param quando uma regra retorna apenas um único IC como uma correspondência. Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Nota: Para evitar a correspondência em elementos de network de baixo nível, se um IC correspondente for `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic` ou `cmdb_ci_ip_address`, o IC primário será retornado.

Uma propriedade do sistema para excluir classes de IC está disponível. Esta propriedade não está disponível com atualização. Consulte Ignorar classes de IC para obter informações de atualização e instruções sobre como definir a propriedade.

Para facilitar a localização de problemas de correspondência, quando uma correspondência for encontrada, a regra de pesquisa de IC usada para localizá-la será adicionada ao registro de item descoberto no campo **Regra de correspondência de IC**. As regras de pesquisa são avaliadas primeiro pelo menor valor de **Pedido**.

Algumas das regras de pesquisa de IC Qualys enviadas com o sistema de base são:

- ID DE HOST DA QUALYS
- FQDN
- NetBIOS
- DNS
- IP

Algumas das regras de pesquisa de IC do Microsoft Defender enviadas com o sistema base são:

- Bucket S3
- Nome
- ID de recurso

Algumas das regras de pesquisa de IC do Palo Alto Prisma Cloud enviadas com o sistema base são:

- Bucket S3
- Nome
- ID de recurso

A importação de dados de resultados de testes pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem criadas com cuidado. A lógica usada para iterar e executar a correspondência dentro do CMDB pode resultar em longos tempos de processamento. Para evitar qualquer degradação potencial de recursos ou complicações de desempenho, teste todas as regras de pesquisa de IC personalizadas ou modificações nas **regras de pesquisa de IC** predefinidas. Consulte Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Resposta a vulnerabilidades regras de pesquisa de IC para obter mais informações sobre como evitar registros órfãos duplicados, excluir dados e limpar dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicar novamente as regras de pesquisa de IC atualizadas

Ao alterar uma regra de pesquisa de IC, clique em **Aplicar mudanças** na página da lista Regras de pesquisa de IC para executar novamente todas as regras nos itens descobertos que:

- Foram correspondidos pelas regras atualizadas
- Não são correspondidos por nenhuma regra

Se o item de configuração (IC) mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Os resultados de testes também são atualizados. Para obter mais informações, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Desduplicação de itens de configuração existentes para Conformidade de configurações

O Remediador de ICs duplicados para tarefas de desduplicação é atualizado com a propriedade `sn_sec_cmn_src_ci.cmdb_ci`.

Sempre que uma tarefa de desduplicação é usada para atualizar os itens de configuração (ICs), ela também atualiza os itens descobertos relacionados a esses ICs. Portanto, os resultados de testes são atualizados com o IC. Para obter detalhes, consulte Mudanças de IC para itens descobertos para Conformidade de configurações.

Criando ICs para Conformidade de configurações usando o Mecanismo de Identificação e Reconciliação

A partir de Conformidade de configurações 11.1, você pode criar itens de configuração (ICs) no Configuration Management Database (CMDB) usando a API do Mecanismo de identificação e reconciliação (IRE). Ao usar a API do IRE para criar ICs, você pode impedir a criação de ICs duplicados e reconciliar atributos de IC permitindo que somente fontes de dados autorizadas gravem em CMDB.

Uma classe de IC (tabela) é o nome da tabela original no banco de dados da instância. CMDB contém classes do sistema de base que armazenam dados sobre ICs.

Como usar o IRE para criação de IC

Antes da versão 11.1, se um IC correspondente não fosse encontrado na lista Itens descobertos ou CMDB, um IC era criado na classe de IC incompatível (`sn_sec_cmn_unmatched_ci`).

Para obter mais informações, consulte ICs incompatíveis.

A partir da versão 11.1, você pode usar a API IRE para criar ICs em CMDB. Em vez de usar a classe de IC incompatível, um IC é criado na classe Hardware sem classe ou na classe Dispositivo identificado com IP incompleto.

Classes de IC do CMDB

Nota: Para usar as novas classes, ative o plug-in CMDB CI Class Models. Caso contrário, os ICs serão criados na classe de IC incompatível.

A partir da versão 11.1, se o host que você importou de um scanner de terceiros não puder ser encontrado na lista de itens descobertos ou CMDB, ele será armazenado em uma das seguintes novas CMDB classes de IC.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Classes de IC do CMDB

CMDB **Classe de IC**	**Descrição**
Dispositivo identificado com IP incompleto (`cmdb_ci_incomplete_ip`)	O IC será criado nesta tabela se somente o endereço IP estiver disponível nas informações de host que são recebidas do scanner.
Hardware não classificado (`cmdb_unclassed_hardware_ci`)	O IC será criado nesta tabela se qualquer uma das seguintes informações estiver disponível nas informações de host que são recebidas do scanner: • Nome do host • Endereço IP • DNS • NETBIOS • Endereço MAC **Nota:** Se o endereço MAC estiver disponível, a entrada do adaptador de rede será criada e relacionada ao IC de hardware não classificado. Se os endereços IP e MAC estiverem disponíveis, o IC do endereço IP também será criado e relacionado ao IC de hardware não classificado.

O sistema usará automaticamente uma classe de IC incompatível se ocorrer uma das seguintes situações:

- O plug-in CMDB de classe de IC não está ativado.
- O IRE gera uma exceção ao criar um novo IC.

Informações relacionadas

Aplicação da Store dos Modelos de classe de IC do CMDB

Mecanismo de Identificação e Reconciliação (IRE)

Conformidade de configurações visão geral das regras de atribuição

Defina os critérios pelos quais os resultados de testes são atribuídos automaticamente a um grupo de atribuição para correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Uma regra de atribuição padrão, **Atribuir ao grupo de suporte de IC**, está incluída no sistema de base que atribui resultados de testes ao **grupo de suporte de IC**. Inativo por padrão.

Os grupos de atribuição definidos pelas Regras de atribuição são usados pelas **Regras de tarefa** de correção para atribuir proprietários a tarefas de correção (RTs).

Atribuindo resultados de testes automaticamente

Existem três maneiras diferentes de atribuir resultados de testes usando **Atribuir usando**:

- Grupo de atribuição: esta opção permite selecionar qualquer um dos Now Platform® grupos de usuários existentes.
- Campo de grupo de atribuição: esta opção permite que você escolha qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir:
  - Nenhum: indica que não há valor padrão para este campo obrigatório
  - Item de configuração: grupo de aprovação
  - Item de configuração: grupo de atribuição
  - Item de configuração: grupo de suporte
- Script: esta opção permite definir as condições usando um script. Esta opção requer codificação ou conhecimento avançado ServiceNow®.

Consulte Criar ou editar Conformidade de configurações regras de atribuição para obter mais informações sobre como criar regras de atribuição.

Com a função sn_vulc.remediation_owner, você pode exibir e atualizar resultados de testes e tarefas de correção atribuídos a eles ou a seus grupos de atribuição. Para exibir os módulos, navegue até **Todos** > **Conformidade de configurações** > **Resultados de testes** > **Meus Resultados de testes em Aberto**, ou **Conformidade de configurações** > **Tarefas de correção** > **Minhas Tarefas em Aberto**.

A função sn_vulc.remediation_owner pode ser atribuída diretamente a um usuário ou é atribuída automaticamente quando você atribui a função itil a um usuário.

Processo de avaliação da regra de atribuição

Quando um novo resultado de testes é importado ou reaberto após ser fechado, as regras de atribuição são avaliadas em relação a ele. As regras de atribuição são avaliadas após a correspondência de IC e os cálculos de pontuação de risco. Um resultado de teste só é avaliado automaticamente na importação inicial e quando uma regra é alterada, a menos que seja reaberto após ser fechado. Você pode reaplicar as regras manualmente após as mudanças.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O processo a seguir é usado para cada resultado de teste novo ou reaberto:

- Para cada regra de atribuição de resultado de testes, o resultado do teste é comparado ao filtro de atribuição, a regra de ordem mais baixa primeiro.
- Quando a condição corresponde, o resultado do teste é atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Onde as condições não encontrarem uma correspondência entre todas as regras, o resultado do teste permanecerá não atribuído.

Reaplicando regras de atribuição

Ao alterar uma regra de atribuição, use o botão **Aplicar mudanças** na página da lista Regras de atribuição para executar novamente todas as regras alteradas em todos os resultados de testes abertos ativos, exceto aqueles que foram atribuídos manualmente.

Nota: As regras de atribuição não reavaliam atribuições criadas manualmente.

O trabalho agendado [*Reapply all assignment rules*] está inativo, por padrão. Quando ativado, ele avalia todos os resultados de testes abertos em relação a todas as regras ativas, exceto aquelas atribuídas manualmente. Ele pode ser executado diariamente, semanalmente, mensalmente, periodicamente, uma vez ou sob demanda.

Importante: Como administrador e analista, você pode obter as atribuições mais recentes dos resultados de testes selecionados no Vulnerability Manager Workspace. Este método é mais eficiente do que reaplicar as Regras de atribuição para todos os resultados de testes na IU clássico, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Regras de atribuição e atribuição de tarefa de correção

Normalmente, você atribuiria sua tarefa de correção (RT) ao mesmo grupo de atribuição que os resultados de testes nele. É isso que as regras de tarefa de correção fazem, por padrão.

Por exemplo, se o RT agrupar por classe de item de configuração, a tarefa de correção criada poderá ser dividida pelos diferentes grupos de atribuição. Um Oracle Database TRG pode ser atribuído ao Grupo 1 e um Oracle Database TRG atribuído ao Grupo 2.

Quando o grupo de atribuição é alterado no nível da tarefa de correção, todos os resultados de testes nessa tarefa de correção que têm o mesmo grupo de atribuição são atualizados para o novo grupo de atribuição. Os resultados de testes são marcados como atribuídos manualmente e não estão qualificados para avaliação de regra adicional.

Removendo atribuições de Conformidade de configurações tarefas de correção

Você pode limpar os campos **Atribuído a** e **Grupo de atribuição** nas tarefas de correção (RT) e os resultados de testes associados diretamente dos registros de TRG que você determina que podem estar atribuídos incorretamente a você ou a seus grupos.

Visão geral

A partir da aplicação v14.3 da Conformidade de configurações, os responsáveis pela correção podem atualizar registros para reatribuição com o botão Cancelar **atribuição**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso de uso para sn_vulc.remediation_owner

Se você determinar que os RTs e os resultados de testes associados não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou a seus grupos, convém remover a si mesmo ou seus grupos de **Atribuído a** e Campos de **grupo de atribuição** nesses registros de tarefa de correção.

Cancelar atribuição do módulo

O botão **Cancelar atribuição** é exibido nos registros de RT em qualquer estado diferente de Encerrado ou Resolvido.

Se você selecionar **Cancelar atribuição**, será solicitado que todos os resultados de testes associados ao grupo sejam reatribuídos e façam a transição para o tipo de atribuição **Não atribuído**.

Todos os registros atualizados com o botão de IU ou manualmente são exibidos no módulo Não atribuído em Conformidade de configurações.

Para saber como reatribuir registros usando a ação de IU *Unassigned*, consulte Remover atribuições de tarefas de correção para você ou seus grupos.

Propriedades e notificações do sistema

Se você for um administrador com a função **sn_vulc.vulnerability_admin**, ao selecionar Cancelar atribuição em um registro, por padrão, a propriedade do sistema, *sn_vulc.unassign_test_result_group.approval_required* aciona o registro de Aprovação de mudança de estado e o registro de Aprovação solicitada. Além disso, a solicitação é exibida na lista Minhas aprovações do aprovador.

Nota: Como administrador de vulnerabilidades, você pode definir a propriedade do sistema *sn_vulc.unassign_test_result_group.approval_required* como **falsa** para desabilitar o processo de aprovação.

- Se o aprovador aprovar sua solicitação, por padrão, a propriedade do sistema *sn_vulc.default_assignment_group* limpará os campos Atribuído a e Grupo de atribuição e preencherá o campo Tipo de atribuição com **Não atribuído**. Como administrador de vulnerabilidades, você pode alterar o valor na propriedade do sistema *sn_vulc.default_assignment_group* para que os campos de atribuição sejam limpos e um grupo específico seja atribuído. Por exemplo, se um usuário selecionar **Cancelar atribuição** em um registro e você quiser redirecioná-lo para um grupo específico para revisão, você poderá adicionar um ID de sistema para o grupo de sua escolha no campo de valor da propriedade do sistema.
- Se o aprovador rejeitar sua solicitação, o motivo da rejeição será exibido na guia **Anotações**.

Como alternativa, se *sn_vulc.default_assignment_group* não estiver configurado para um grupo específico, por padrão, os usuários que você adicionar ao grupo de usuários de notificação de cancelamento de atribuição serão alertados quando os registros forem não atribuídos. A propriedade do sistema, *sn_vulc.default_notification_group* determina as notificações para este grupo.

O tipo de atribuição, seja **Manual**, **Regra**ou **Não atribuído**, está disponível nos registros RT e na exibição de lista. O tipo de atribuição **Não atribuído** é exibido depois que os campos **Atribuído a** e **Grupo de atribuição** são limpos pela propriedade do sistema do recurso.

Tradução automática

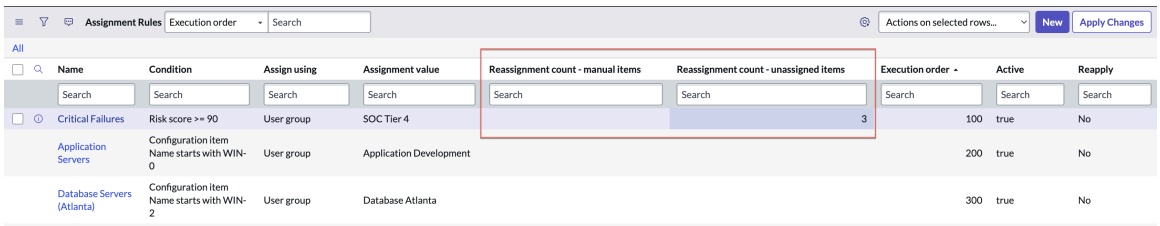
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Monitorando suas regras de atribuição com o trabalho agendado para este recurso

Um trabalho agendado diário conta os registros quando eles fazem a transição para o tipo de atribuição **Não atribuído**. Com essa contagem, os analistas de vulnerabilidade podem monitorar e ajustar regras de atribuição que possam não estar funcionando bem com base em regras de atribuição que tenham contagens mais altas de RTs não atribuídos.

O trabalho agendado *`Reassignment count for assignment rules`* é executado diariamente e publica o número total de RTs não atribuídos por este recurso para uma regra de atribuição específica.

O trabalho também conta todos os registros que não foram atribuídos manualmente. As contagens manuais e as contagens coletadas por este recurso são publicadas na lista Regras de atribuição de vulnerabilidade em duas colunas: *`Reassignment count - manual items`* e *`Reassignment count - unassigned items`*.



1. Como administrador de vulnerabilidades, você pode exibir essas contagens navegando até **Conformidade de configurações** > **Administração** > **Regras de atribuição**.
2. Selecione o ícone de engrenagem no canto superior direito da lista e selecione **Contagem de reatribuições - itens manuais**e **Contagem de reatribuições - itens não atribuídos** para exibição.
3. Qualquer RT que foi atribuído originalmente por uma regra, mas posteriormente foi reatribuído automática ou manualmente, contém uma referência à regra original na exibição de lista.

Conformidade de configurações tarefas de correção e regras de tarefa de correção visão geral

Crie automaticamente Tarefas de correção (RTs) para analisar os resultados em massa usando regras de tarefa de correção. Os critérios pelos quais os grupos são formados são configurados para que você não precise atribuir manualmente os resultados de testes em grupos.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre tarefas de correção

As tarefas de correção representam um conjunto de resultados de testes a serem corrigidos. O agrupamento de resultados de testes tem muitas vantagens. Você pode mover os resultados de testes por meio dos estados de correção, marcá-los como sob investigação, adiá-los e marcá-los como resolvidos em massa usando grupos. Você pode criar condições para agrupar automaticamente todos os resultados com resultados, tecnologias, pontuações de risco e quaisquer outros dados especificados relacionados aos resultados de testes. Os resultados de testes podem pertencer a mais de uma tarefa de correção, dando a você a flexibilidade de trabalhar ativamente com uma tarefa de correção e monitorar outra. Tudo depende das suas necessidades organizacionais. Por exemplo, você pode agrupar por atribuição e também criar uma tarefa de correção contendo tecnologias.

As tarefas de correção são criadas da seguinte forma.

- Manualmente, usando uma de duas opções, para adicionar resultados de testes à tarefa de correção.
  - **Manual**: cria uma tarefa de correção sem entradas. Os resultados de testes devem ser adicionados manualmente.
  - **Filtro**: cria uma tarefa de correção e usa condições para adicionar automaticamente resultados de testes a essa tarefa de correção.

  Nota: Os resultados de testes adicionados manualmente não são removidos automaticamente das tarefas de correção por regras de tarefa de correção ou condições da tarefa de correção.

- Automaticamente, usando regras de tarefa de correção. Esta é a opção mais fácil. Depois de configurada, as regras de tarefa de correção criam todas as tarefas de correção desejadas.

Em uma tarefa de correção, o grupo de resultados de testes pode ser atribuído a um usuário, adiado para mais tarde, usado para criar uma **solicitação de mudança**e assim por diante.

Nota:

Com a função sn_vulc.remediation_owner, você pode exibir e atualizar resultados de testes e tarefas de correção atribuídos a você ou aos seus grupos de atribuição. Para exibir os módulos, navegue até **Todos** > **Conformidade de configurações** > **Resultados de testes** > **Meus Resultados de testes em Aberto**, ou **Conformidade de configurações** > **Tarefas de correção** > **Minhas Tarefas em Aberto**.

Quando é determinado que um novo resultado de testes pode ser adicionado a uma tarefa de correção, o resultado do teste é incluído na lista relacionada **Resultados de testes** da tarefa de correção.

Ao atualizar o estado de uma tarefa de correção, os resultados de testes associados podem ter seu estado atualizado para corresponder a essa tarefa de correção. Para obter mais informações sobre mudanças de estado, consulte Conformidade de configurações estados.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem definir como os resultados de testes são agrupados e atribuídos automaticamente. Uma regra padrão, **Grupo de atribuição, Teste**, está incluída no sistema de base que agrupa os resultados de testes com base em um **grupo de atribuição** de resultados de testes e no campo **Teste**. Esta regra está desabilitada por padrão. Você pode agrupar por qualquer outro conjunto de valores em colunas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

acessíveis a partir do resultado de testes. Você pode usar até seis chaves e qualquer número de condições. Para obter mais informações, consulte Criar ou editar Conformidade de configurações regras de tarefa de correção.

Importante: Como administrador e analista, você pode avaliar as regras de tarefa de correção para resultados de testes selecionados no Espaço do gerenciador de vulnerabilidades. Este método é mais eficiente do que reaplicar as regras de tarefa de correção na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Por exemplo, você pode agrupar seus resultados de testes por grupo de atribuição ou tecnologia e item de configuração (IC). Um conjunto diferente de regras pode ser usado para resultados de testes que expõem a empresa a mais riscos. Você pode ter uma regra de tarefa de correção para ICs de baixa severidade ou baixo risco. Consulte Campos de Resultados de testes para obter mais informações sobre os campos disponíveis.

Quando um novo resultado de testes é importado ou reaberto após ser fechado, as regras de tarefa de correção são avaliadas em relação a ele. Um resultado de teste é avaliado apenas uma vez, a menos que seja reaberto após ser fechado.

As regras de tarefa de correção são avaliadas após a correspondência de IC, os cálculos de pontuação de risco e as regras de atribuição.

O processo a seguir é usado para cada resultado de teste novo ou reaberto:

- Para cada regra de tarefa de correção, o resultado do teste é comparado ao filtro de condição.
- Para cada regra em que a condição da regra corresponde, ele extrai os dados das colunas de chave do grupo no resultado do teste. A regra verifica se há uma tarefa de correção **aberta** correspondente que esteja atribuída ao mesmo grupo de atribuição que o resultado do teste.

  Se a tarefa de correção for encontrada, o resultado do teste será adicionado à tarefa de correção existente no estado **Aberto**.

- Se nenhuma tarefa de correção no estado **Aberto** for encontrada, a regra criará uma tarefa de correção, a atribuirá com base no **grupo de usuários** ou no valor de **chave** na regra e colocará o resultado do teste nela.

Mais de uma regra de resultado de testes pode ser definida para agrupar diferentes tipos de resultados. Como cada resultado é comparado com as condições da regra antes de ser colocado em uma tarefa de correção, muitas regras podem afetar o desempenho.

Quando uma regra de tarefa de correção é excluída, você tem a opção de excluir todas as tarefas de correção em aberto criadas pela regra. Isso se aplica à exibição do formulário de regra e à exibição de lista.

Quando uma atribuição de tarefa de correção é feita ou alterada, os campos **Grupo de atribuição** e **Atribuído a** são acumulados para todos os resultados de testes, exceto aqueles em que o resultado de testes tem um grupo de atribuição diferente do RT. Para obter mais informações sobre regras de atribuição, consulte Conformidade de configurações visão geral das regras de atribuição. Essas atribuições são usadas automaticamente para este grupo na próxima importação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acompanhar contagens de adiamento para resultados de testes e tarefas de correção

A partir da v14.3, rastreie o número de vezes que um resultado de testes ou uma tarefa de correção é adiado no módulo Vários adiamentos. Um trabalho agendado, **definir contagens de adiamento**, é executado diariamente para publicar contagens de registros que foram adiados mais de uma vez na coluna Contagem de adiamento nos registros listados no módulo Vários adiamentos.

Configuração de grupos de calculadoras e calculadoras para Conformidade de configurações

As calculadoras de Conformidade de configuração são usadas para atualizar valores de registro quando condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Calculadoras de Conformidade de configuração

A aplicação Conformidade de configuração inclui dois tipos de calculadoras, Calculadoras de risco e Calculadoras de acúmulo de pontuação de risco. Esses grupos de calculadoras são habilitados por padrão.

O grupo de calculadoras de pontuação de risco foi renomeado para Calculadoras de risco.

As calculadoras de acúmulo de pontuação de risco incluem calculadoras de acúmulo para testes de configuração e tarefas de correção.

A configuração de calculadoras de risco e acúmulo para correção de resultados de testes e tarefas de correção inclui as seguintes tarefas:

- Criar uma calculadora de risco
- Criar uma calculadora de acúmulo de pontuação de risco

Depois de criar uma calculadora de risco, ela fica disponível para cálculos com a próxima ingestão de dados. Depois de criá-lo, você também pode preferir aplicá-lo sob demanda.

Para obter mais informações sobre calculadoras e grupos de calculadoras, consulte Conformidade de configurações grupos de calculadoras.

Conformidade de configurações Visão geral da Gestão de exceções

Quando sua organização não pode cumprir uma política de segurança ou gestão de vulnerabilidades, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções para uma tarefa de correção que não pode ser corrigida de acordo com a política.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade relacionada à configuração.

Ciclo de vida de uma exceção

Uma exceção é uma solicitação para adiar a correção de uma tarefa de correção por um período especificado.

O ciclo de vida de uma exceção é o seguinte:

- Como solicitar uma exceção
- Como aprovar uma solicitação de exceção
- Acompanhamento de uma solicitação de exceção
- Expiração de uma solicitação de exceção

Como solicitar uma exceção

Como responsável pela correção, você pode solicitar uma isenção para uma tarefa de correção usando o processo de gestão de exceções. Durante o processo de aprovação, a tarefa de correção permanece no estado **Em revisão**. Depois que o aprovador de exceção aprova esta solicitação, a tarefa de correção é movida para um estado **Adiado**.

Como aprovar uma solicitação de exceção

As tarefas de correção que não podem ser corrigidas imediatamente são revisadas, avaliadas quanto ao risco e aprovadas para adiamento até que possam ser corrigidas. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se apenas o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção para Conformidade de configurações.

Nota:

A partir da Conformidade de configurações v13.0, se você estiver implantando a aplicação CC pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho.

Depois que uma solicitação de exceção para uma tarefa de correção for aprovada, você poderá executar as seguintes ações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Reabrir
- Fechar
- Excluir

Nota: Os comentários de rejeição são mostrados nas Anotações de trabalho de uma tarefa de correção. Se uma solicitação de exceção for rejeitada, esta tarefa de correção será revertida para o estado anterior.

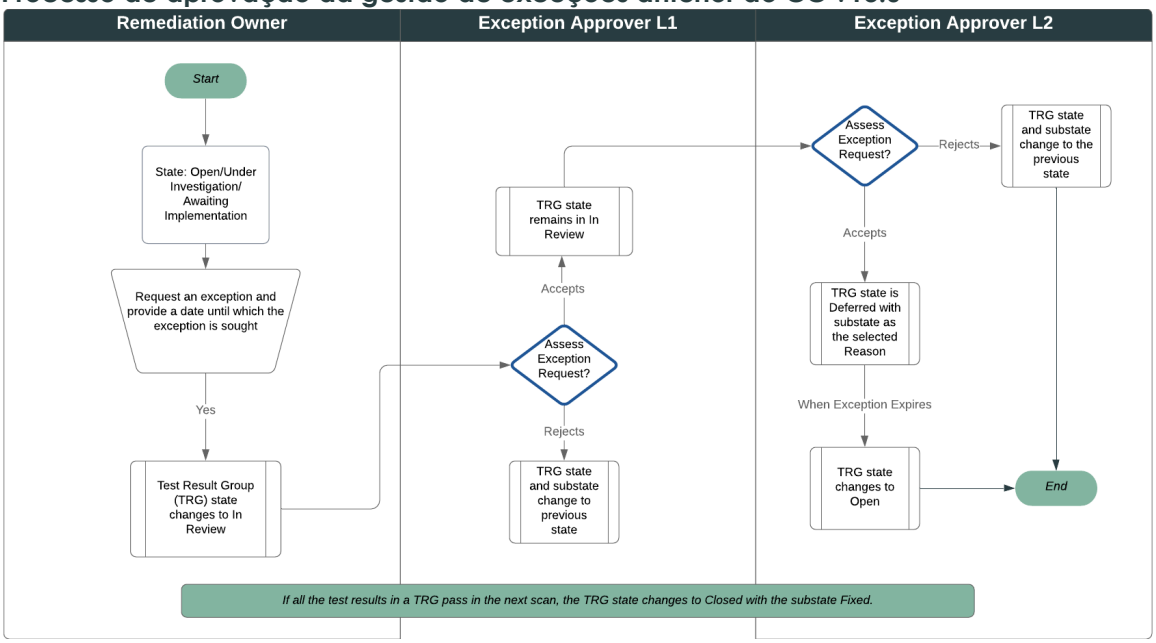
Acompanhamento de uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** da tarefa de correção. Se uma ação for realizada em uma tarefa de correção, você não poderá rastrear o status dos resultados de testes individuais nessa tarefa de correção.

Expiração de uma solicitação de exceção

Quando uma solicitação de exceção para uma tarefa de correção expira, a tarefa de correção é revertida para o estado **Aberto**.

Processo de aprovação da gestão de exceções anterior ao CC v13.0



Conformidade de configurações gestão de mudanças

Como proprietário de correção de TI, você pode criar e gerenciar solicitações de mudança (CHG) diretamente de tarefas de correção (RTs) na aplicação Conformidade de configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Solicitações de mudança e o fluxo de trabalho Conformidade de configurações

As solicitações de mudança e a gestão de mudanças fazem parte do processo de correção do fluxo de trabalho Conformidade de configurações. Durante esta fase de correção, você pode usar solicitações de mudança para ajudá-lo a priorizar, rastrear e corrigir resultados de testes.

A aplicação Conformidade de configurações funciona com o Now Platform® processo de gestão de mudanças de TI para ajudá-lo a corrigir software e tecnologias fora de conformidade em seu ambiente.

Com a gestão de mudanças na aplicação Conformidade de configurações, você pode associar resultados de testes a solicitações de mudança existentes ou dividir uma tarefa de correção e criar uma nova tarefa de correção somente para os resultados de testes selecionados.

Para obter mais informações, consulte Como criar uma solicitação de mudança no Conformidade de configurações.

Termos principais

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser controlada. Um teste é qualquer coisa que possa ser usada para identificar uma classe de software ou um ativo de hardware que está fora de conformidade.

Resultados de testes

Os resultados de testes são importados por integrações de terceiros. Depois que podem ser exibidos em Conformidade de configurações, eles são corrigidos usando **Tarefas**de correção. Os grupos são atribuídos para correção de acordo com as regras de atribuição.

Nota: A partir da versão 14.9 do Conformidade de configurações, o resultado do teste é rotulado como Descoberta.

Tarefa de correção

Os resultados de testes são agrupados em tarefas de correção de acordo com as regras de atribuição e atribuídos automaticamente aos proprietários de correção para correção.

Nota: A partir da versão 14.9 da Conformidade de configurações, o resultado de testes é rotulado como Tarefade correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupos de teste

Os grupos de teste estão relacionados a documentos oficiais e registros de teste. Um grupo de testes de configuração define um grupo de teste.

Solicitações de mudança

As solicitações de mudança ajudam a implementar processos controlados para correção. Você pode usar solicitações de mudança com tarefas de correção em Conformidade de configurações para ajudá-lo a identificar, rastrear e resolver ativos fora de conformidade (itens de configuração) que exigem recursos adicionais ou que você pode ter como destino o adiamento.

Para obter mais informações sobre resultados de testes e tarefas de correção, consulte Conformidade de configurações tarefas de correção e regras de tarefa de correção visão geral.

Quando usar solicitações de mudança no Conformidade de configurações

As solicitações de mudança ajudam a iniciar e rastrear atividades de correção nos resultados de testes. Quando os proprietários de correção têm um grande número de resultados de testes não corrigidos ou itens de configuração, eles podem usar solicitações de mudança para identificar resultados de testes para adiamento. Como alternativa, eles podem identificar e reagrupar resultados de testes e itens de configuração que exigem mais recursos do que os identificados inicialmente na tarefa de correção original.

Criar solicitações de mudança a partir de uma tarefa de correção

Crie uma solicitação de mudança diretamente de uma tarefa de correção para todos os resultados de testes na tarefa de correção ou use a filtragem para identificar somente os resultados de testes que correspondem a critérios específicos. Crie uma solicitação de mudança com informações preenchidas previamente para agilizar sua investigação de resultados de testes que exigem intervenção manual.

Dividir uma tarefa de correção

Em uma tarefa de correção existente, identifique um subconjunto de resultados de testes que você deseja mover para uma nova tarefa de correção. Ao criar um novo TRG, você pode trabalhar com um grupo específico de resultados de testes sem afetar a tarefa de correção original.

Associar resultados de testes a uma solicitação de mudança existente

Associe resultados de testes a tarefas existentes para evitar a criação de solicitações de mudança duplicadas enquanto você trabalha para resolver suas tarefas de correção. Ao associar uma tarefa de correção a uma solicitação de mudança que já está disponível em sua instância, você pode usar listas de tarefas existentes.

Tipos de solicitações de mudança para uma tarefa de correção

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente das tarefas de correção atribuídas a você. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente de uma tarefa de correção:

- Padrão. Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento ou instrução de trabalho especificado.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.
- Emergência. Uma mudança para resolver um incidente grave.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalação, instalação e configuração da aplicação Conformidade de configurações

Antes de executar a aplicação em sua instância Now Platform®, você deve primeiro baixar e instalar a aplicação Conformidade de configurações do ServiceNow® Store. Esta aplicação está disponível como uma assinatura separada.

Conclua as seguintes etapas da check-list de configuração listadas na tabela a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Para obter mais informações sobre as versões lançadas da aplicação Conformidade de configurações, bem como aplicações de terceiros e ServiceNow, consulte o artigo Matriz de compatibilidade de resposta a vulnerabilidades e mudanças de esquema de versão [KB0856498] na Base de conhecimento HI.

Para obter mais informações sobre como obter direitos para aplicações da loja, consulte .

Configurar tarefas de check-list

Tarefas de configuração	Descrição
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá a função Administrador de conformidade de configuração [sn_vulc.admin]. • O administrador de Conformidade de configuração [sn_vulc.admin] supervisiona a configuração e verifica os resultados esperados. • O responsável pela correção [sn_vulc.remediation_owner] lê e atualiza os registros atribuídos. A função sn_vulc.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a qualquer usuário.
Integrações compatíveis	Antes de poder usar Conformidade de configurações para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede. Verifique se a aplicação Resposta a vulnerabilidades está instalada e ativada antes de configurar as integrações de terceiros compatíveis. Consulte Como instalar Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar tarefas de check-list

Tarefas de configuração	Descrição
	Para verificar se as aplicações de integração estão instaladas e ativadas, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre integrações de terceiros e uma lista de produtos compatíveis, consulte Integrações do Conformidade de configurações.

Qualys Vulnerability Integration

- Se o Qualys Vulnerability Integration já estiver instalado no seu sistema e suas credenciais de API forem diferentes daquelas que você deseja usar para Conformidade de configurações, vá para o Assistente de configuração (em Resposta a vulnerabilidades) e atribua-as a cada integração de **PC da Qualys**.
- Navegar até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** e edite o campo **Credenciais de API** da **Qualys na guia Detalhes de REST** da Qualys.

Para obter informações mais detalhadas sobre o Qualys Vulnerability Integration, consulte Noções básicas sobre Qualys Vulnerability Integration.

Agora você está pronto para instalar a aplicação Conformidade de configurações. Consulte Como instalar Conformidade de configurações.

Como instalar Conformidade de configurações

Antes de executar Conformidade de configurações em sua instância Now Platform®, você deve primeiro baixar e instalar a aplicação Conformidade de configurações do ServiceNow Store. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Consulte Instalação, instalação e configuração da aplicação Conformidade de configurações para tarefas de configuração. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

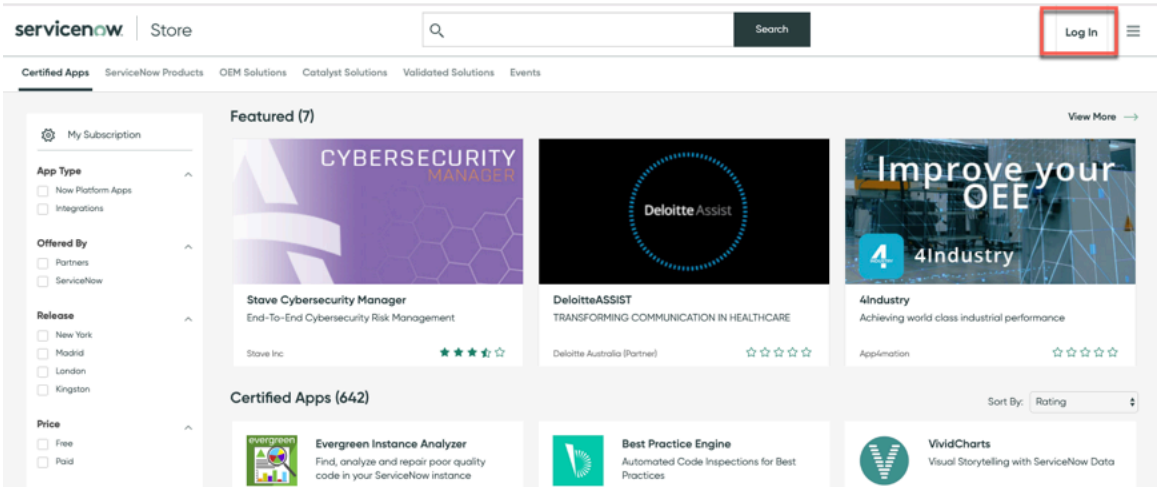
Função necessária: administrador

Procedimento

1. Para obter o direito e baixar a aplicação principal Conformidade de configurações, navegue até o ServiceNow Store.
2. No canto superior direito da página, clique em **Fazer login**.

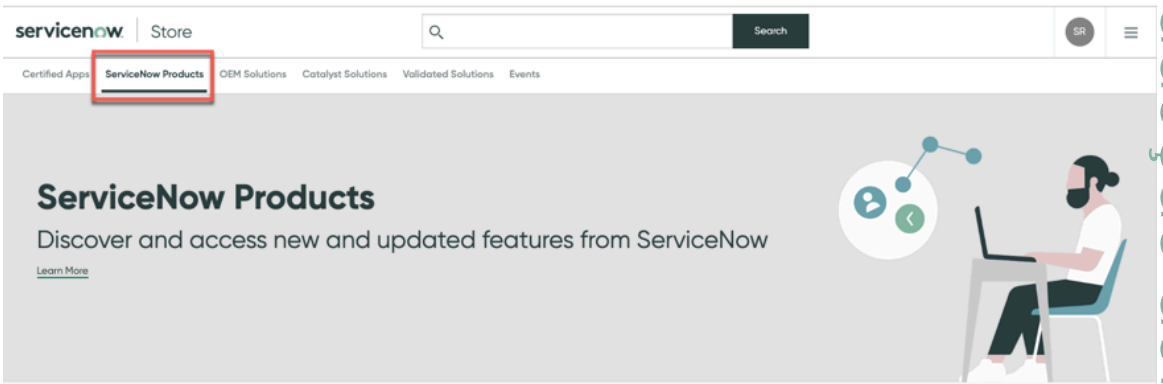
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login**.

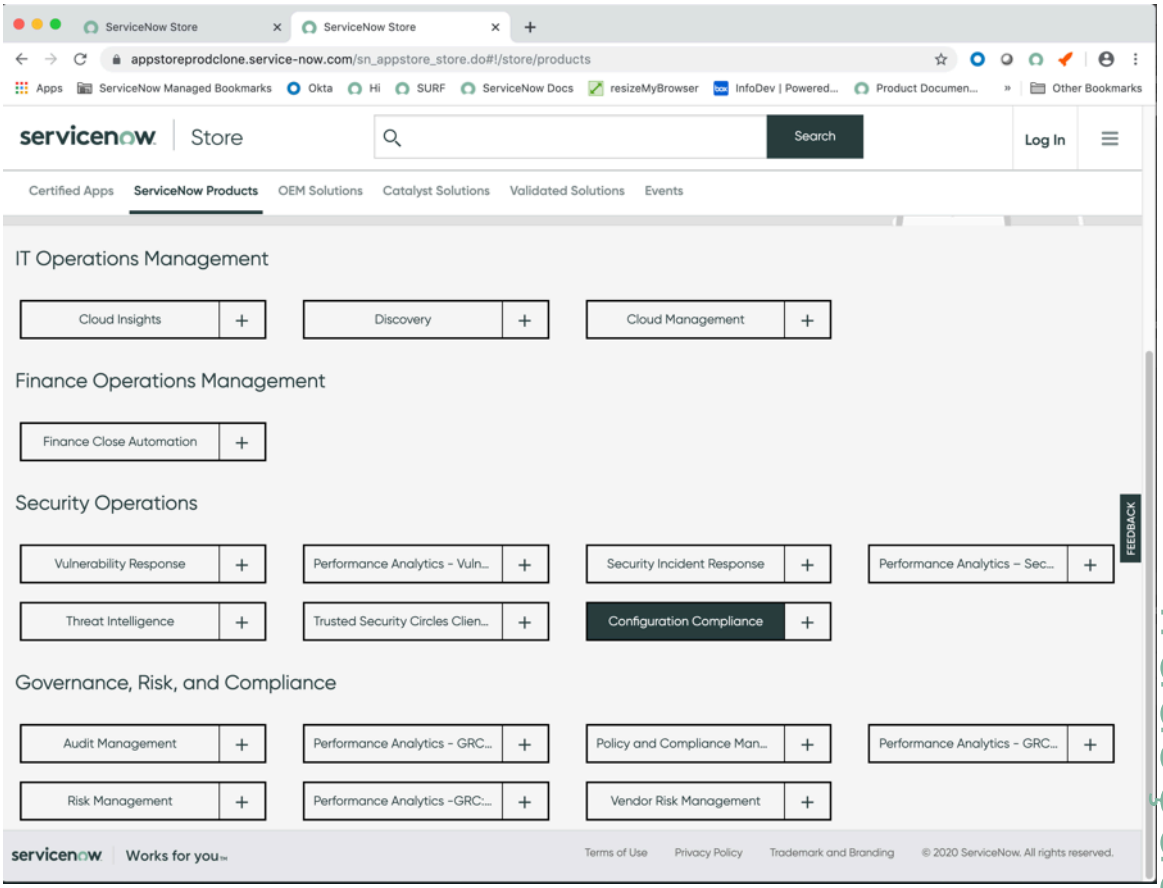
4. Na página exibida, se não estiver selecionado, clique na guia **Produtos da ServiceNow**.



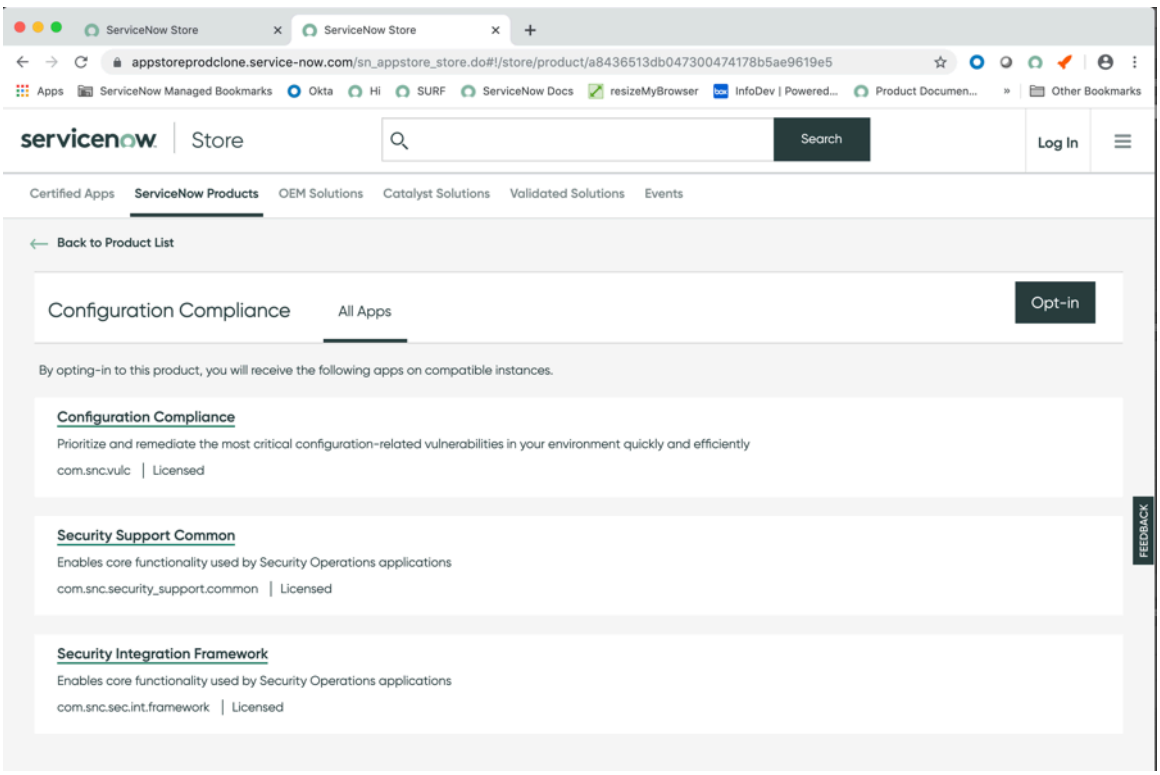
5. Para exibir as aplicações associadas para as quais você está qualificado com a aplicação Conformidade de configurações, na página da lista de produtos, clique no produto **Conformidade de configurações**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A página exibida lista todas as aplicações para as quais você está qualificado se aceitar. Para obter mais informações sobre uma aplicação, clique em um link.

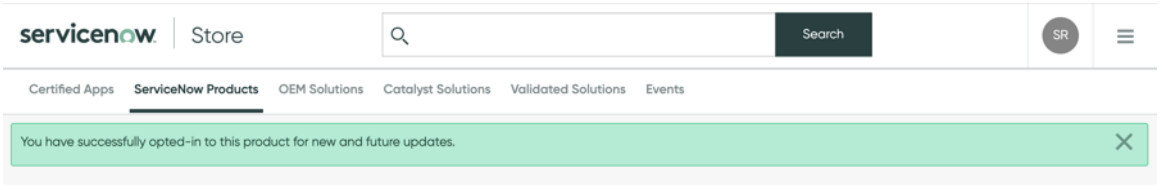


6. Para obter a aplicação Conformidade de configurações, clique em **Aceitar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.
   Uma mensagem é exibida indicando que você aceitou com sucesso a aplicação.



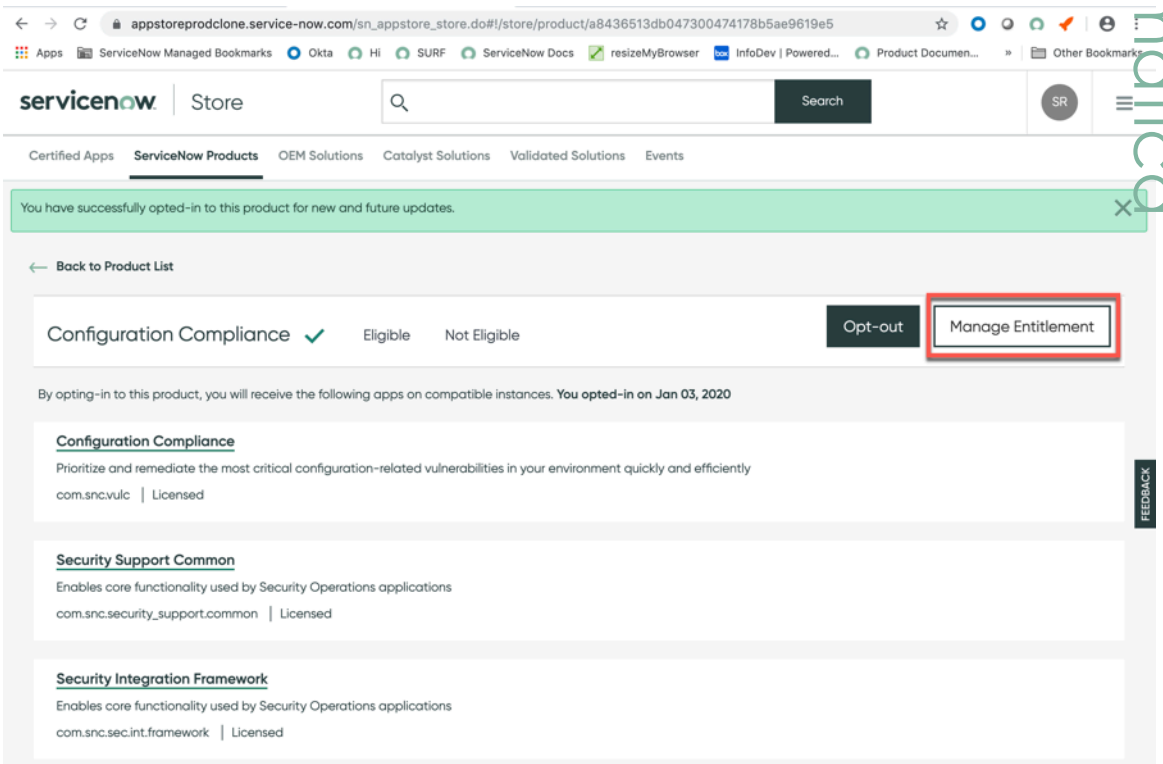
Com a guia Produtos ServiceNow selecionada na Lista de produtos, uma marca de seleção verde substitui o sinal de adição à direita da aplicação Conformidade de configurações, conforme mostrado na figura a seguir.

Depois de aceitar os termos e condições e direitos gerenciados de qualquer uma das aplicações na guia **Produtos da ServiceNow**, na página Lista de produtos, você pode clicar no sinal de mais (+) para obter direitos e aceitar outras aplicações nesta página com um único clique.

8. Pule para a etapa 10 para instalar a aplicação em sua instância Now Platform.
9. Opcional: Como alternativa, se você quiser gerenciar seu direito da aplicação Conformidade de configurações em outras instâncias Now Platform, siga estas etapas.

   a. Se o botão Gerenciar direito não for exibido, clique na aplicação Conformidade de configurações na lista de produtos para exibi-la.

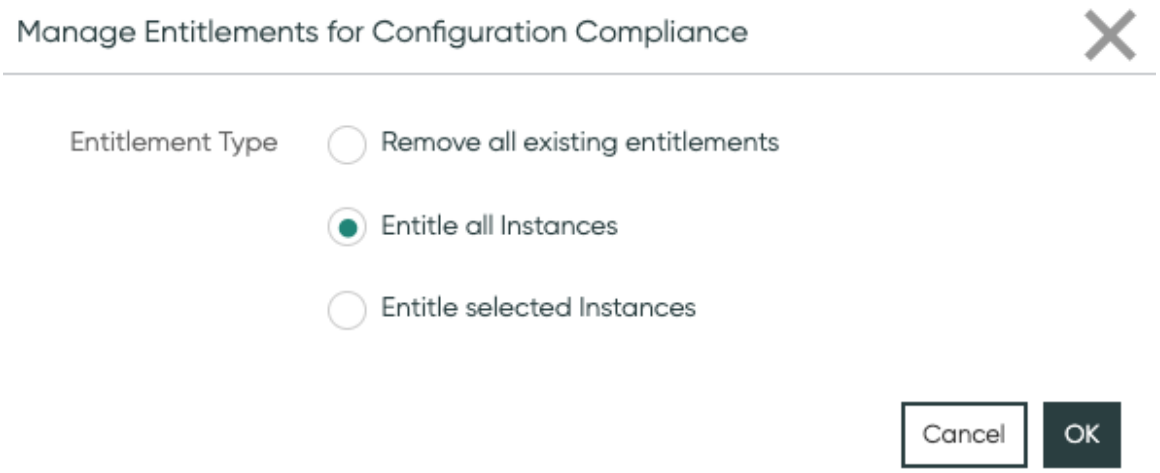
   b. Clique **em Gerenciar direito**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na caixa de diálogo Gerenciar direitos para Conformidade de configurações que é exibida, escolha uma:

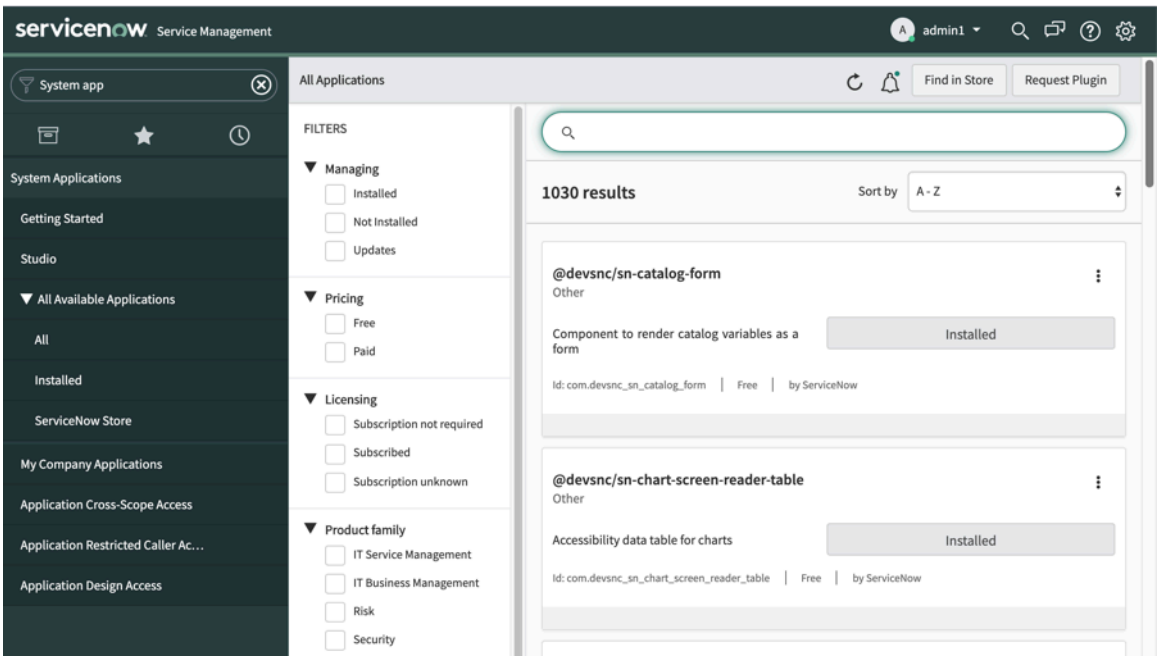


d. Clique em **OK** ou em **Cancelar** para continuar.

Você está pronto para ativar plug-ins e instalar a aplicação em sua(s) Now Platform instância(s).

10. Faça login na instância Now Platform na qual você deseja instalar a aplicação Conformidade de configurações.

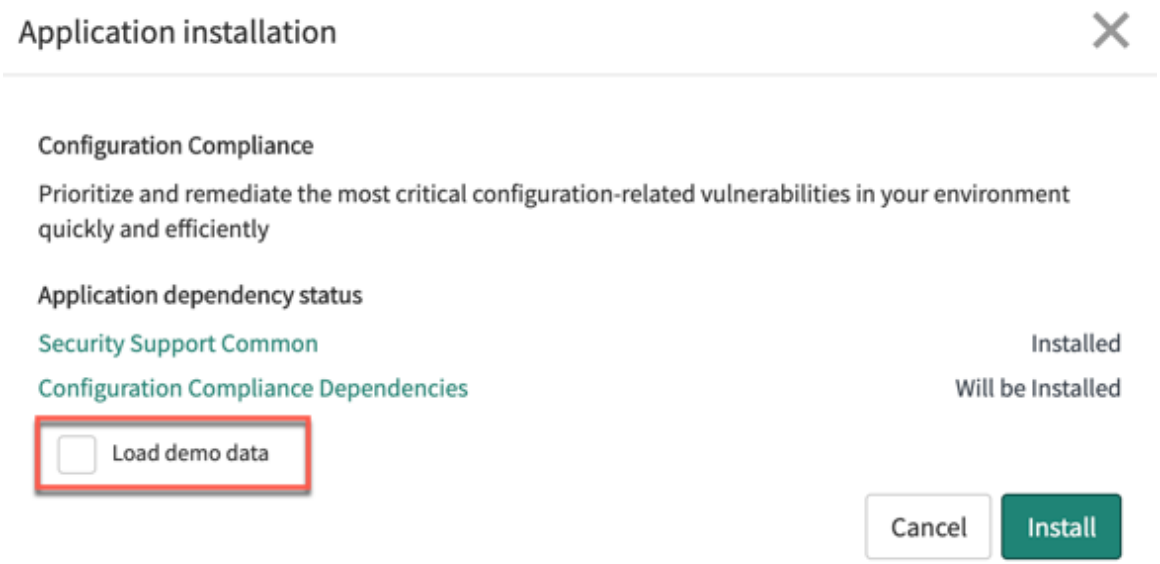
11. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



12. Nas aplicações listadas, localize a aplicação Conformidade de configurações (sn_vulc) e clique em **Instalar**.
A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas são exibidas.

Tradução automática

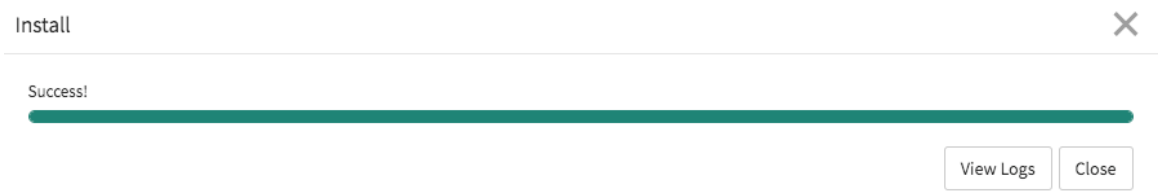
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



13. Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar**.

    Nota: Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não estarão disponíveis para instalação posterior no **Gerenciador de aplicações**. Para obter informações sobre como instalar ou reinstalar dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.

    Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.



14. Clique em **Fechar**.

    Plug-ins SCA de terceiros separados adquirem e transformam dados em Conformidade de configurações. Antes de poder usar Conformidade de configurações para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede.

    Para obter informações sobre como instalar integrações de terceiros para Conformidade de configurações, consulte Integrações do Conformidade de configurações.

Componentes instalados com Conformidade de configurações

Vários tipos de componentes são instalados com a ativação do plug-in Conformidade de configurações, incluindo tabelas e funções do usuário.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dados de demonstração estão disponíveis para este recurso.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos agendados e as tabelas instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.
3. No Construtor de condições, para adicionar um segundo filtro, selecione **AND e**, em seguida, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, Trabalho **agendado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de Conformidade de configurações [sn_vulc.admin]	Capaz de modificar a propriedade da aplicação, configuração, regras de atualização, integrações da aplicação Conformidade de configurações. A partir da v15.0, um usuário administrador não pode excluir registros de origem,	sn_vulc.write **Nota:** Herda as funções necessárias para a administração dos registros da aplicação Conformidade de configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	como Expliots, CVEs etc.	
ler [sn_vulc.read]	Leia listas e registros em Conformidade de configurações.	sn_sec_cmn.calcul_read
gravar [sn_vulc.write]	Escreva listas e registros em Conformidade de configuração.	• sn_vulc.read • sn_vulc.remediation_owner
atribuição de gravação [sn_vulc.write_assignment]	Gravar nos campos de atribuição de resultado de testes.	Contido na função sn_vulc.remediation_owner.
responsável pela correção sn_vulc.remediation_owner	Exiba e atualize a permissão para resultados de testes atribuídos a você ou ao seu grupo.	Contido na função itil. Contém: • sn_sec_cmn.read • sn_vulc.write_assignment
CC.Sistema sn_vulc.import_admin	Executa todos os trabalhos agendados na aplicação de conformidade de configuração. **Nota:** Este usuário é o padrão executar como usuário para cada trabalho agendado em conformidade de configuração.	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration
VRCommon.Sistema sn_vul_cmn.admin	Usuário padrão de execução para todos os trabalhos agendados na aplicação comum de Resposta a vulnerabilidades.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.Sistema sn_sec_cmn.admin	Usuário padrão de execução para todos os trabalhos agendados que	• sn_sec_cmn.int_write • sn_sec_cmn.write

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	são usados para a capacidade de trabalhos em segundo plano na aplicação comum de suporte de segurança	• workflow_admin • sn_sec_cmn.calcul_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7: sn_vulc.edit_watch_topic	Editar tópicos de observação para Conformidade de configuração.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	Leia os tópicos de observação de Conformidade de configuração.	cmdb_read
V14.7: sn_vulc.create_watch_topic	Crie tópicos de observação para Conformidade de configurações.	sn_vulc.read_watch_topic
sn_vulc.auditor	Permitir leitura para todos os módulos de conformidade de configuração	sn_vulc.read sn_vulc.advanced_read
sn_vulc.advanced_read	Permitir leitura de todos os módulos de administração de conformidade de configuração	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	Permitir leitura para mapeamento de	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	criticalidade de teste	
sn_vulc.read_task_rules	Permitir leitura de regras de tarefa de correção	
sn_vulc.read_assignment_rules	Permitir leitura para regras de atribuição	
sn_vulc.read_risk_score_configuration	Permitir leitura para configuração de pontuação de risco	
sn_vulc.read_auto_close_rules	Permitir leitura para configuração de fechamento automático	
sn_vulc.false_positive_approver	Permite aprovar/ rejeitar tarefas de correção de fechamento como falso-positivo	
V15.0: sn_vulc.delete	Exclui registros de origem.	

Trabalhos agendados instalados

Trabalho agendado	Descrição
V15.0: atualizar grupo de teste em testes de configuração	Atualiza o grupo de teste em testes para a origem da Tenable e do Microsoft Defender. Este é um trabalho único.
V15.0: preenchimento de campos de resultado de testes existentes	Atualiza valores em colunas recém-adicionadas (como Idade, Idade encerrada, Ativo etc.) na tabela de resultados de testes, filtros e módulos salvos. Este é um trabalho único.
V15.0: Preencher tabela de ICs vulneráveis - Excluir e preencher novamente para resultados de testes	Preenche o total de registros na tabela de ICs vulneráveis. Este é um trabalho único.
Versão 12.0 Calcular métricas de correção para todos os grupos de resultados de testes	Calcula e atualiza valores para métricas de status em registros de tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Versão 12.0: Calcular métricas de correção para todos os resultados de testes	Calcula e atualiza valores para métricas de status em registros de resultados de testes.
Versão 12.0: Sincronização de estado da solicitação de mudança	Trabalho sob demanda que sincroniza os estados de todas as tarefas de correção (RTs) existentes com as solicitações de mudança (CHGs). Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também move os estados de todas as tarefas de correção relacionadas automaticamente. Habilita a sincronização de estado daqui para frente.
Versão 11.1: Verificar adiamento de grupos de resultados de testes Vencimento	Envia notificações se as tarefas de correção expirarem (e se expirarem em uma semana).
Contagem de IC de Conformidade de configuração	Preenche a contagem de itens de configuração (IC) distintos e a média de 90 dias consecutivos na tabela Contagem de itens de configuração [sn_vulc_cc_configuration_item_count].
Versão 11.1: Avaliar e notificar metas de correção	Define ou atualiza datas de meta de correção em todos os resultados de testes. Determina o status das datas de meta de correção em relação às regras. Envia notificações
V14.7: Inserir grupos de resultados de testes na tarefa de correção unificada	Trabalho agendado único para inserir todas as tarefas de correção criadas na IU clássica na tarefa de correção unificada (sn_vul_remediation_task).
Versão 12.0: Preencher CR-TRG m2m para CR e CR-Primário	Preenche solicitações de mudança em tarefas de correção.
Removido na v11.1: reabrir grupos de resultados de testes adiados **Nota:** Descontinuado para versões anteriores à 11.1. Não use.	Reabre grupos adiados quando a data de vencimento tiver passado.
Reaplicar todas as regras de atribuição	Reaplica todas as regras de atribuição.
Versão 14.3: contagem de reatribuições para regras de atribuição	É executado diariamente e publica o número total de resultados de testes e tarefas de correção não atribuídos por este recurso para uma regra de atribuição específica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
Reavaliar o estado dos grupos de resultados de testes	Reavalia o estado das tarefas de correção para entradas em que **assessment_state** é falso. É executado a cada 15 minutos.
Acumular pontuação de risco do resultado de testes para testar o grupo de resultados e o teste de configuração	É executado por hora e calcula as pontuações de acúmulo para os testes de configuração alterados e tarefas de correção. • Calcula a pontuação de risco de acúmulo para todos os testes em sn_vulc_test_manifest e exclui o registro de manifesto após a conclusão. • Calcula a pontuação de risco de acúmulo para todos os testes em sn_vulc_result_group_manifest e exclui o manifesto após a conclusão.
Versão 12.0: Atualizar métricas de correção de política	A partir da v15.0 de Conformidade de configurações, este trabalho agendado foi renomeado para Atualizar métricas de correção. • Calcula e atualiza valores para métricas de status em registros de apólice. • Calcula o percentual de conformidade do resultado de testes de um IC no item descoberto.
Versão 14.3: definir contagens de adiamento	Coleta o número de vezes que um resultado de testes ou uma tarefa de correção foi adiado.
Atualizar classificação de risco para resultados de testes	Atualiza a classificação de risco dos resultados de testes.
Pontuação de risco de acúmulo de atualizações para todos os grupos de resultados não encerrados e testes de configuração.	Atualiza a pontuação de risco de acúmulo para todos os grupos de resultados não encerrados e testes Conformidade de configurações.

Tabelas instaladas

Tabela	Descrição
Regra de atribuição [sn_vulc_assignment_rule]	Contém o conjunto de regras avaliadas para definir o grupo de atribuição nos resultados de testes.
Fonte Autorizada [sn_vulc_auth_src]	Armazene fontes autorizadas importadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Calculadora [sn_vulc_calculator_risk_score]	Contém a calculadora que define determinados campos de resultado de testes quando determinadas condições são atendidas.
Contagem de Itens de Configuração do CC [sn_vulc_cc_configuration_item_count]	Contém o número total de itens de configuração.
Versão 12.0: associação de solicitação de mudança [sn_vulc_action_associate_cr]	Tabela de preparação usada para associar solicitações de mudança a tarefas de correção.
Versão 12.0: criação de solicitação de mudança [sn_vulc_action_create_cr]	Tabela de preparação usada para criar formulários de solicitação de mudança.
Versão 12.0: formulário de solicitação de mudança [sn_vulc_cr_form]	Tabela base para gestão de solicitações de mudança.
Citação [sn_vulc_citation]	Contém citações importadas
Teste de configuração [sn_vulc_test]	Contém dados de teste de configuração importados.
Manifesto de teste de configuração [sn_vulc_test_manifest]	Contém os testes de configuração para os quais a pontuação de risco de acúmulo precisa ser calculada.
Tabela de ativos ausentes da versão 12.2 [sn_vul_missing_asset]	Contém registros de ativos temporários para dados de avaliação de conformidade de configuração importados com ativos incompatíveis.
Tecnologia de Teste de Configuração [sn_vulc_test_tecnologia]	Contém tecnologias de teste de configuração importadas.
Regra de grupo [sn_vulc_grouping_rule]	Contém as regras que definem os critérios com os quais os grupos são criados automaticamente para um conjunto de resultados de testes.
Política [sn_vulc_policy]	Contém políticas importadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Teste de Configuração de Política [sn_vulc_policy_test]	Contém dados de teste de configuração de política importados.
Regra de meta de correção [sn_vulc_ttr_rule]	Define o intervalo de tempo esperado para corrigir um resultado de testes.
Calculadoras de Risco [sn_vulc_calculator_group]	Contém o agrupamento de calculadoras Conformidade de configurações. A ordem do grupo de calculadoras determina qual grupo é avaliado primeiro e, em cada grupo, uma calculadora é usada no máximo.
Calculadora de acúmulo de pontuação de risco [sn_vulc_risk_score_rollup]	Contém configurações da calculadora de acúmulo.
Grupo de resultados do teste de divisão [sn_vulc_action_split_trg]	Tabela de preparação usada para dividir tarefas de correção.
Aprovação de mudança de estado [sn_vulc_state_change_approval]	Contém dados do processo de estado de aprovação.
Tecnologia [sn_vulc_tecnologia]	Contém tecnologias importadas.
Mapa de Criticidade de Teste [sn_vulc_test_criticality_map]	Contém dados do mapa de criticalidade.
Resultado do Teste [sn_vulc_result]	Contém resultados de testes importados.
Grupo de resultados de testes [sn_vulc_result_group]	Contém tarefas de correção importadas.
Versão 12.0: Solicitações de mudança do grupo de resultados de testes	Contém solicitações de mudança para tarefas de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Manifesto do grupo de resultados de testes [sn_vulc_result_group_manifest]	Contém as tarefas de correção para as quais a pontuação de risco de acúmulo precisa ser calculada.
Grupos de resultados de testes [sn_vulc_m2m_result_result_group]	Contém dados da tarefa de correção.
Histórico de Resultado de testes [sn_vulc_result_history]	Contém o histórico de resultados de testes importados.
Status de correção do resultado de testes	Status do resultado de testes em relação à regra de meta de correção aplicada mais próxima.
V14.7: Contagens de testes de tópico de observação [sn_vulc_wt_test_counts]	Tabela de cache da guia Testes de configuração distinta no espaço do Gerenciador de vulnerabilidades.

Criar ou editar Conformidade de configurações regras de atribuição

Crie regras para atribuir automaticamente resultados de testes com base nas condições do filtro. Essas regras atribuem resultados de testes conforme são importados.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

O sistema base é fornecido com uma Conformidade de configurações regra de atribuição, **Atribuir ao grupo de suporte de IC**, que atribui resultados de testes ao mesmo grupo de atribuição que o grupo de suporte de IC. Esta regra está inativa por padrão. Você pode modificar usando condições de filtro. Com regras de atribuição, você define uma ou mais condições de atribuição e a ordem de execução. Quando um resultado de teste corresponde a uma condição de regra, a pesquisa de atribuição é interrompida.

Nota: Regras novas ou atualizadas são avaliadas automaticamente na próxima importação ou manualmente usando o botão **Aplicar mudanças** na lista Regras de atribuição.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de atribuição**.
2. Abra a regra **Atribuir ao grupo de suporte de IC** ou clique em **Novo**.
3. Edite a regra **Atribuir ao grupo de suporte de IC** ou, se for **Novo**, preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regra de atribuição da Conformidade de configurações

Campo	Descrição
Nome	Nome da regra de grupo.
Ordem de execução	Ordem na qual as regras são avaliadas. O número mais baixo é avaliado primeiro. Regras de alta prioridade, resultados de testes que precisam de tratamento especial, onde o risco é crítico ou um resultado de testes que deve ser tratado pela conformidade regulatória, devem ser executados primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir resultados de testes ao grupo que descobre a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Ativo	Indica se a regra de atribuição está ativa.
Condição	
Campos de condição	Condições que devem ser atendidas. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.
Novos critérios	Adiciona mais campos de filtro de condição para escolher.
Descrição	Texto que descreve a regra de atribuição.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ◦ Grupo de usuários: selecione um grupo de usuários na tabela de pesquisa ◦ Campo de grupo de usuários: selecione um campo de grupo de usuários no menu suspenso. ◦ Script: crie ou edite um script. **Nota:** Criar ou editar um script requer ServiceNow conhecimento.
Campo de grupo de usuários	Selecione o grupo de usuários responsável pela correção dos testes que correspondam às condições das regras de atribuição.

4. Clique em **Enviar**.

Conformidade de configurações regras de destino de correção

Com as regras de destino de correção, você pode definir os intervalos de tempo esperados para corrigir os resultados de testes. Você pode enviar notificações para usuários e grupos quando as datas de destino estiverem se aproximando e quando elas estiverem vencidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias: administrador de Conformidade de configuração (sn_vulc_admin) ou um gerente com a função sn_vulc.manage_remediation_target_rules.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

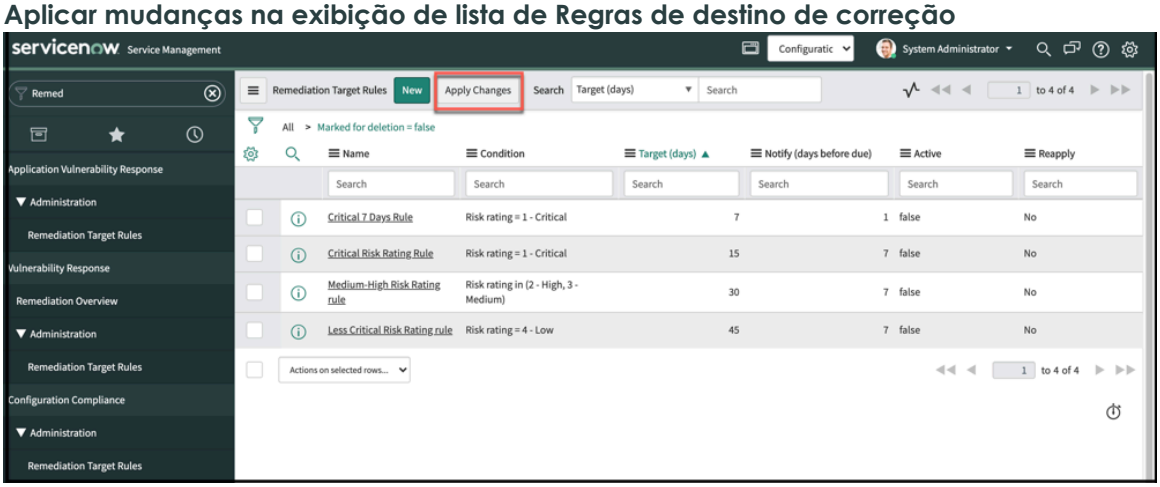
Regras de destino de correção

Um trabalho agendado, *Evaluate and notify remediation targets*, é executado diariamente e usa regras de destino de correção ativas para avaliar registros de resultados de testes ativos. Sempre que registros de resultados de testes associados a tarefas de correção são atualizados ou alterados, os valores modificados são avaliados pelas regras de destino e as mudanças são acumuladas e exibidas nas tarefas de correção associadas.

Você pode editar, desabilitar ou excluir regras de destino de correção existentes e criar novas. Ao alterar, desabilitar ou criar uma nova regra, você tem a opção de clicar em **Aplicar mudanças** na exibição de lista Regras de destino de correção e aplicar manualmente as mudanças introduzidas antes do próximo trabalho agendado. Com esta opção, você pode reavaliar seus registros de resultados de testes sem precisar esperar. Se você optar por não aplicar suas mudanças manualmente, o próximo trabalho agendado diário selecionará suas mudanças e as aplicará.

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de destino de correção** para exibir regras de destino de correção.

Aplicar mudanças na exibição de lista de Regras de destino de correção



2. Clique em uma regra na coluna Nome para abrir seu registro.
3. Marque a caixa de seleção **Ativo** no registro Regra de destino de correção para habilitar (`verdadeiro`) quaisquer regras desabilitadas (`falso`).

Sempre que você alterar ou adicionar uma regra de destino, independentemente de optar por aplicar as mudanças manualmente ou aguardar o próximo trabalho agendado,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

suas mudanças serão usadas para avaliar todos os resultados de testes ativos junto com quaisquer outras regras de destino que sejam afetadas por suas mudanças. Quando você opta por aplicar manualmente as mudanças, essa avaliação pode levar algum tempo se você tiver um grande volume de resultados de testes ativos, porque todas as regras afetadas por suas mudanças são usadas para uma avaliação.

Por exemplo, o valor padrão para dias de correção direcionados é 30. Se você criar uma nova regra que também tenha 30 para Dias de correção direcionados, esta regra e todas as regras de destino com 30 dias ou mais como datas de destino serão aplicadas aos resultados de testes.

Regras de destino desativadas e excluídas

Quando uma regra está ativa, `verdadeiro` é exibido na coluna Ativo na exibição de lista de Regras de destino de correção. Depois que uma regra é desativada (`falso`), ela não é mais aplicada a novos resultados de testes. No entanto, o trabalho agendado continua rastreando todos os resultados de testes existentes aos quais a regra foi aplicada. Se a regra ou as regras desativadas forem reativadas posteriormente, qualquer resultado de testes com um campo **Data de meta de correção** vazio será avaliado em relação às regras reativadas. Isso inclui resultados de testes criados enquanto as regras estavam desativadas.

Quando as regras são excluídas, a **Data de meta** de correção e os campos relacionados nos resultados de testes encerrados são preservados. A **data de meta** de correção e os campos relacionados nos resultados de testes não encerrados são limpos e todas as regras dependentes são reaplicadas.

Para desativar uma regra, no registro da regra de destino de correção, desmarque a caixa de seleção ativa e clique em **Atualizar**. `Falso` é exibido na coluna Ativo na exibição de lista de Regras de destino de correção.

Para excluir uma regra, clique em **Excluir** no formulário ou, como alternativa, na exibição de lista, selecione a regra ou as regras e clique em **Excluir** na lista **Ações nas linhas**. A regra não é mais exibida na lista e a próxima regra na ordem de operação substitui a regra excluída.

Se você desativar ou excluir uma regra e optar por aplicar as mudanças antes do próximo trabalho agendado, a referência da regra será apagada do campo, mas a data de correção e os dados de status serão preservados. Se você não aplicar as mudanças manualmente, a referência de regra será apagada do campo com o próximo trabalho agendado.

Sobre as regras de destino e o trabalho programado Avaliar e notificar metas de correção

O trabalho agendado *`Evaluate and notify remediation targets`* é executado uma vez às 4:30:00 diariamente. Ele seleciona todas as regras de destino de correção ativas e avalia todos os resultados de testes ativos, começando com os resultados de testes com a data de meta de correção mais antiga. Ele avalia todos os resultados de testes que atendem aos seguintes critérios:

- Não estão em um estado **Fechado**.
- Não têm data de meta de correção.
- Ter datas de meta de correção posteriores às datas nas regras de meta de correção.
- São criados após a conclusão de uma importação de scanner. O trabalho agendado seleciona e avalia todos os novos resultados de testes criados como resultado de uma importação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que uma regra de meta é definida, as datas de meta de correção são calculadas pelo trabalho agendado *Evaluate and notify remediation targets*. O trabalho agendado adiciona uma data de meta de correção, se não houver uma, ou, se esta regra contiver uma data anterior à do registro, ele atualizará a data de meta existente.

Todos os registros expirados e datas de lembrete que correspondam às regras de destino são selecionados pelo trabalho e as notificações são enviadas. Para regras desabilitadas, o trabalho limpa os campos de correção nos registros de resultado de testes e para de enviar notificações.

Exibição de datas de destino e status nas exibições de lista e formulário

Conformidade de configurações Os gerentes podem ver a data da meta de correção no formulário de resultados de testes e nas exibições de lista. As regras de destino de correção também são executadas após a importação de um scanner e executadas novamente se um resultado de testes for reaberto.

O trabalho agendado atualiza a **Meta** de correção e o **Status** de correção na exibição de lista de resultados de testes e os campos **Regra de metade correção**, Meta de **correção e Status** de correção no formulário de resultados de testes.

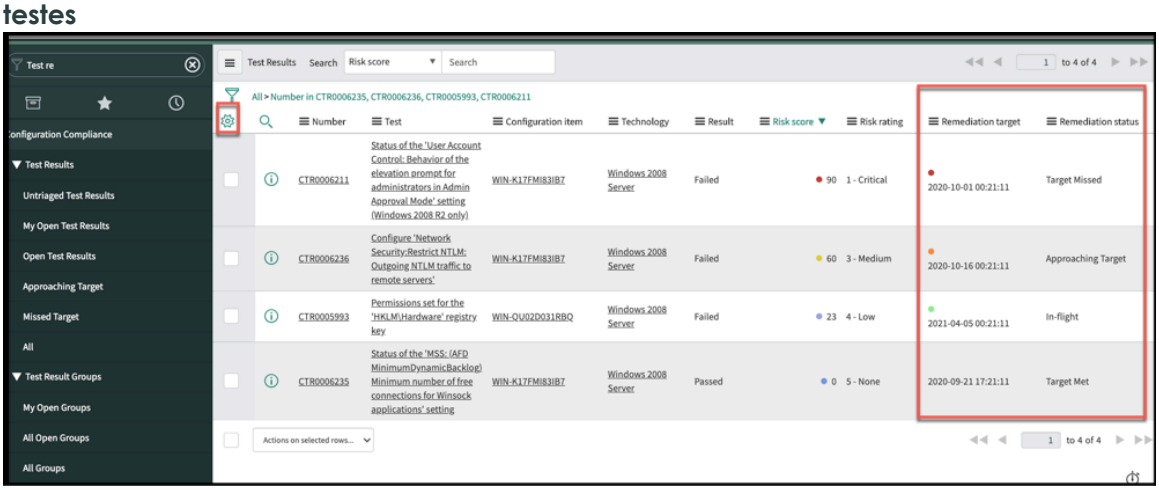
Nota: Por padrão, as colunas **Meta** de **correção e Status** da correção não são exibidas na exibição de lista de Resultados de testes. Para exibir essas colunas, você também deve adicioná-las à exibição de lista. Da mesma forma, adicione os campos **Regra de metade correção**, Meta de **correção e Status** da correção ao formulário de resultados de testes.

Use os slushbuckets nos menus Configurações e Ação adicional, respectivamente, conforme mostrado nas imagens a seguir para exibir essas colunas e campos. Para o menu Ação adicional no registro de resultado de testes, clique no ícone do menu e, em seguida, em **Configurar** e **Layout do formulário** para exibir o slushbucket e mover os campos de **Disponível** para **Selecionado**.

A data da meta de correção é codificada na exibição de lista de Resultados de testes como pontos coloridos:

- Os resultados de testes que não atingiram a data de notificação são mostrados em verde.
- Os resultados de testes que se aproximam da data de meta de correção são mostrados em laranja.
- Os resultados de testes após a data de meta de correção são mostrados em vermelho.

Meta de correção e colunas de status na exibição de lista de Resultados de testes

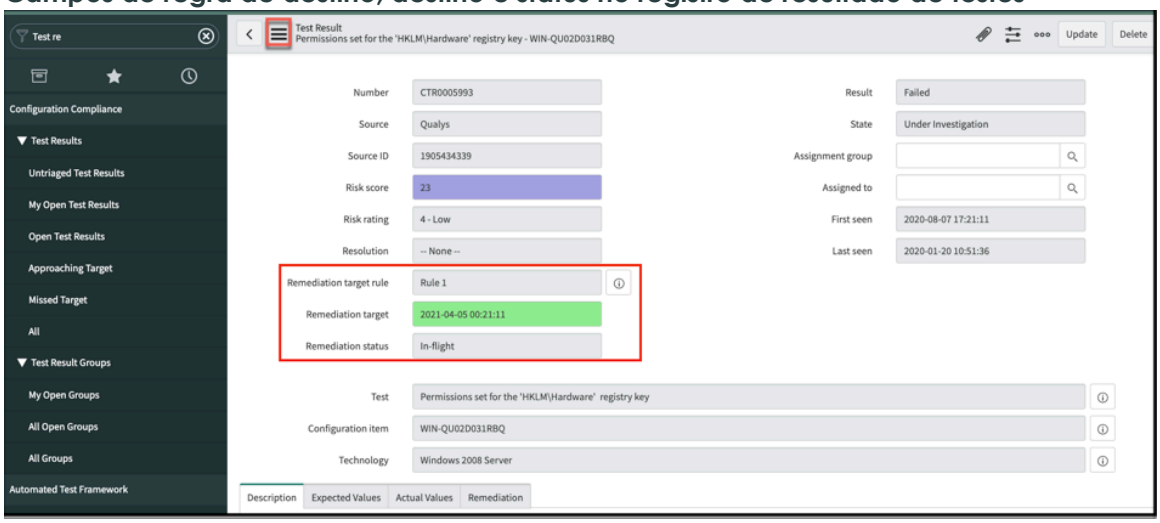


© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

- `Meta não atingida`: a data de meta está vencida
- `Em`andamento : o resultado do teste está em andamento

Campos de regra de destino, destino e status no registro de resultado de testes



Os registros de resultados de testes também são exibidos visualmente no painel Conformidade de configurações. Navegar até **Todos** > **Conformidade de configurações** > **Visão geral** e verifique o painel quanto ao status. A visão geral inclui widgets existentes e status de correção. As cores dos gráficos correspondem às cores exibidas na exibição de lista de Resultados de testes e no registro de Resultado de testes.

Cenário da regra de meta de correção

Quando várias regras de destino de correção são aplicadas ao mesmo resultado de testes, a regra mais restritiva é aplicada.

Por exemplo, se um resultado de testes identificado pela primeira vez em 01/03/2018 atender às condições para duas regras de meta de correção:

- Regra de meta de correção 1: definida em 03/07/2018; a meta de correção é de 15 dias desde a primeira vez; A data da meta de correção calculada é 16/03/2018 10:00:00.
- Regra de meta de correção 2: definida em 10/03/2018; a meta de correção é de 10 dias desde a primeira vez; A data da meta de correção calculada é 11/03/2018 10:00:00.

Nota:

As metas de correção são calculadas a partir da data da **última visita** mais o número de dias (medidos como incrementos de 24 horas).

A partir da V14.5, as metas de correção são calculadas a partir da **meta de (data)**. O valor padrão permanece **Última Visto**. A partir da v14.12, o valor padrão é **Last pass**.

Neste cenário, a Regra de meta de correção 2 se aplica ao resultado de testes, porque ele tem a data mais restritiva: 10 dias desde que o resultado do teste foi identificado pela primeira vez versus 15 dias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ou modificar regras de destino e reaplicar mudanças

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de destino de correção** para exibir, editar e criar novas regras de destino de correção.
2. Na coluna Nome, clique em uma regra para abrir uma regra de destino e editar o registro ou, como alternativa, clique em **Novo** para criar uma nova regra de destino.
3. Preencha o formulário para definir o intervalo de tempo de correção esperado, especifique a quais resultados de testes esta regra se aplica com condições e determine quando enviar lembretes para usuários ou grupos, ou ambos.

Campo	Descrição
Nome	Nome da regra.
Ativo	Habilite ou desabilite a regra. A regra é habilitada automaticamente (verdadeira) por padrão e será aplicada aos resultados de testes se você optar por aplicar as mudanças manualmente ou após o próximo trabalho agendado.
Meta (dias)	Defina a data do prazo de meta para correção em número de dias. O valor padrão para dias de correção direcionados é 30. Por exemplo, se você criar uma nova regra que também tenha 30 como valor de destino, a nova regra e quaisquer outras regras existentes que também tenham 30 dias ou mais como datas de destino serão aplicadas aos resultados de testes.
V14.5: destino de (data)	Data a partir do momento em que as datas de destino são calculadas. Você pode especificar somente a data ou os campos de tipo de data e hora. A partir da v14.12, o valor padrão é *Last pass*. Selecione uma das seguintes opções: ◦ Visto pela última vez ◦ Visto pela primeira vez ◦ Criação ◦ Última aprovação Se a última aprovação estiver vazia, a data de criação será considerada para o cálculo da meta de correção. Para personalizar os valores deste campo, consulte KB1642413 .
Notificar (dias antes do vencimento)	Defina um número de dias antes da data limite para lembrar usuários e grupos.
Descrição	Descrição resumida da regra.
Condição	Use o construtor de condições para especificar os resultados de testes aos quais esta

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	regra se aplica. Por exemplo, defina uma data de meta de correção de 30 dias para todos os resultados de testes com pontuações de risco superiores a 70. Envie lembretes para usuários ou grupos, ou ambos, sete dias antes da data de correção. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário. Antes da versão 12.0, a diferenciação de maiúsculas e minúsculas era compatível com o texto de pesquisa inserido no Construtor de condições.
Usuário e grupos de usuários ou ambos	Selecione usuários ou grupos, ou ambos, para enviar notificações sobre as datas de destino próximas e atrasadas que você definiu.

4. Clique em **Enviar**. Como alternativa, para salvar regras editadas, clique em **Atualizar**.

   A exibição de lista é exibida com a regra atualizada ou nova. As regras na lista são ordenadas e executadas começando com a regra com a data de meta de correção mais baixa. Se você desabilitar ou excluir uma regra, a próxima regra na sequência de ordem substituirá a regra inativa ou excluída.

5. Para aplicar as novas mudanças agora, clique em **Aplicar mudanças**.

Importante: Como administrador ou analista, você pode obter a data da meta de correção mais recente para os resultados de testes selecionados no Espaço do gerenciador de vulnerabilidades. Este método é mais eficiente do que executar as Regras de destino de correção para todos os resultados de testes na IU clássica, que é um processo demorado. Para obter mais informações, consulte Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace.

Conformidade de configurações grupos de calculadoras

Conformidade de configurações calculadoras são usadas para atualizar valores de registro quando condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações grupos de calculadoras

No registro da Calculadora de risco padrão, as regras da calculadora podem ser aplicadas a todos os resultados de testes afetados e coleções sob demanda. Os gerentes de vulnerabilidade podem usar este recurso para ajustar a configuração da calculadora de risco. Eles podem experimentar vários esquemas de priorização no início da implantação e aplicar essas mudanças sob demanda para ver como elas afetam as descobertas de importação.

O grupo de calculadoras de pontuação de risco foi renomeado para Calculadoras de risco.

As calculadoras de acúmulo de pontuação de risco estão incluídas com Conformidade de configurações. Existem dois tipos de calculadoras de acúmulo individuais:

Acúmulo de risco de teste de configuração

Calculadoras que acumulam pontuações de risco para todos os Resultados de testes com o mesmo Teste de configuração para fornecer uma pontuação de risco geral para o Teste de configuração. O valor acumulado é exibido nos campos de pontuação de risco.

Acúmulo de pontuação de risco da tarefa de correção

Essas calculadoras acumulam pontuações de risco para todos os Resultados de testes em uma Tarefa de correção para fornecer uma pontuação de risco geral para essa tarefa de correção. O valor acumulado é exibido nos campos de pontuação de risco.

O grupo de calculadoras de pontuação de risco e o grupo de calculadoras de acúmulo de pontuação de risco estão habilitados por padrão.

Para obter mais informações, revise os seguintes termos-chave para calculadoras Conformidade de configurações :

Resultado do teste

Um resultado de teste é o resultado do teste de configuração em um item de configuração (IC) e a tecnologia associada. Os resultados de testes nos estados Falha, erro e Desconhecido identificam hardware, software e ativos que estão fora de conformidade com suas políticas.

Tarefa de correção

Os resultados de testes são agrupados no momento da importação de dados com base nas regras de tarefa de correção predefinidas. Essas tarefas de correção são semelhantes aos grupos de vulnerabilidades em Resposta a vulnerabilidades. As Tarefas de correção organizam os resultados de testes em grupos para análise em massa e representam um conjunto de itens a serem corrigidos.

Pontuação de risco em um resultado de teste

Um valor calculado por calculadoras de pontuação de risco que se baseia no contexto de negócios de um ativo e na severidade do teste associado. É a média da criticalidade dos negócios do ativo afetado, conforme definido no CMDB, e a severidade do teste conforme comunicado pelo scanner.

Cada ativo pode ter vários serviços associados a ele. A criticalidade de um ativo para os negócios é determinada pelo serviço com a criticalidade mais alta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor calculado é exibido nos campos Pontuação de risco dos resultados de testes. As pontuações exibem valores que variam de 0 a 100. Os campos também são codificados por cores para fornecer a você uma visão geral da gravidade.

Pontuação de risco na tarefa de correção

Essa pontuação é exibida no registro da Tarefa de correção e é o valor acumulado das pontuações de risco para todos os resultados de testes ativos em uma Tarefa de correção. Essa pontuação muda conforme os resultados de testes são corrigidos na Tarefa de correção.

Pontuação de risco no teste de configuração

Essa pontuação é exibida em testes de configuração e é o valor acumulado das pontuações de risco para todos os resultados de testes ativos com esse teste de configuração. Essa pontuação muda conforme os resultados de testes associados a este teste de configuração são corrigidos.

Pontuação de risco

A quantidade de risco que um resultado de teste com falha representa para o seu sistema. Ele se baseia em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica os riscos como Críticos (1) a Nenhum (5). A pontuação é baseada em um intervalo de pontuações de risco e é exibida nos campos de classificação de risco.

Intervalos de classificação de risco

Pontuação de risco	Pontuação de risco
1- Crítica	90 a 100
2- Alto	70 a 89
3- Médio	40 a 69
4- Baixo	1 a 39
5- Nenhum	0

Calculadoras de acúmulo de pontuação de risco

Existem dois tipos de calculadoras de acúmulo:

- Acúmulo de risco de teste de configuração: essas calculadoras acumulam pontuações de risco para todos os resultados de testes com o mesmo teste de configuração para fornecer uma pontuação de risco geral para o teste de configuração. O valor acumulado é exibido nos campos de pontuação de risco. Você pode editar os valores de script para peso e pontuação dessas calculadoras.
- Acúmulo de pontuação de risco da tarefa de correção: essas calculadoras acumulam pontuações de risco para todos os resultados de testes em uma tarefa de correção para fornecer uma pontuação de risco geral para essa tarefa de correção. O valor acumulado é exibido nos campos de pontuação de risco. Você pode editar os valores de script para peso e pontuação dessas calculadoras. Para obter um exemplo de uma calculadora de acúmulo de pontuação de risco e como ela calcula as pontuações, consulte Exemplo de cálculo de acúmulo de risco para Conformidade de configurações (anterior à v15.0).

Pontuação de risco histórico

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A pontuação de risco inerente em todos os resultados de testes aprovados em uma tarefa de correção. Este campo exibe a quantidade de risco que foi corrigida por um grupo de teste e só é exibido depois que um grupo de teste está no estado "Encerrado" e a pontuação de risco é zero.

As pontuações são calculadas sempre que a pontuação de risco muda ou quando os resultados de testes são adicionados ou removidos de uma tarefa de correção.

Nota: Para funcionar corretamente, este script requer o plug-in Mapeamento de serviços. Mapeamento de serviços está disponível como uma assinatura separada e requer ativação pela equipe de ServiceNow.

Criar um grupo de calculadoras Conformidade de configurações

Conformidade de configurações grupos de calculadoras são usados para agrupar calculadoras com base em como você deseja usá-las.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
O sistema de base Conformidade de configurações inclui um grupo de calculadoras: **Pontuação de risco**. Ao criar outras calculadoras, você pode adicioná-las a este grupo ou criar outros grupos e calculadoras. Em cada grupo, a primeira calculadora que corresponde ao resultado do teste é executada.

Há dois grupos de calculadoras incluídos com a aplicação Conformidade de configuração:

- Calculadoras de Risco
- Calculadoras de acúmulo de pontuação de risco

As Calculadoras de risco calculam a pontuação e a classificação de risco de um Resultado de testes.

As calculadoras de acúmulo de pontuação de risco acumulam pontuações de risco para todos os resultados de testes e tarefas de correção com o mesmo teste de configuração para fornecer uma pontuação de risco geral.

Você também cria novas calculadoras diretamente desses grupos.

Procedimento

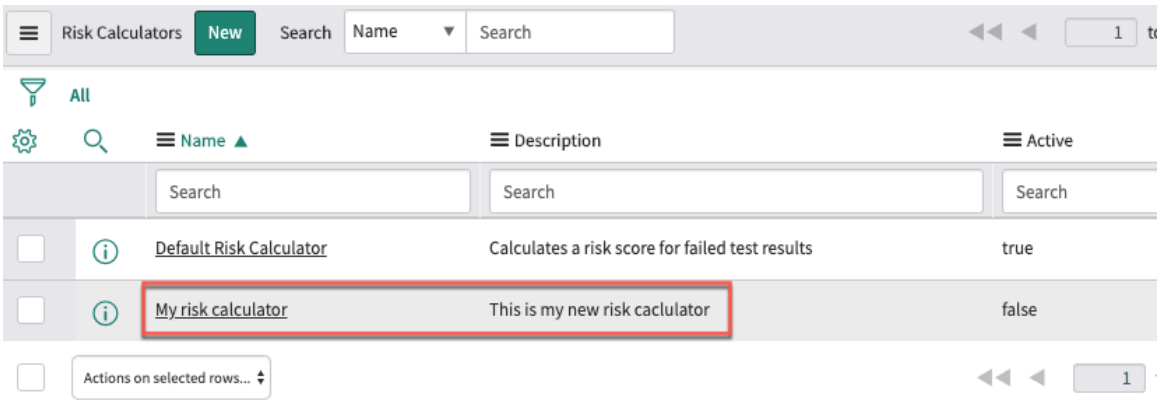
1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Grupos de Calculadoras**.
2. Navegar até **Todos** > **Conformidade de configurações** > **Administração** e selecione Calculadoras de risco ou **Calculadoras** de acúmulo de **pontuação**de risco .
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da calculadora.
Descrição	Uma descrição deste grupo de calculadoras.
Ativo	Habilite ou desabilite o grupo de calculadoras.

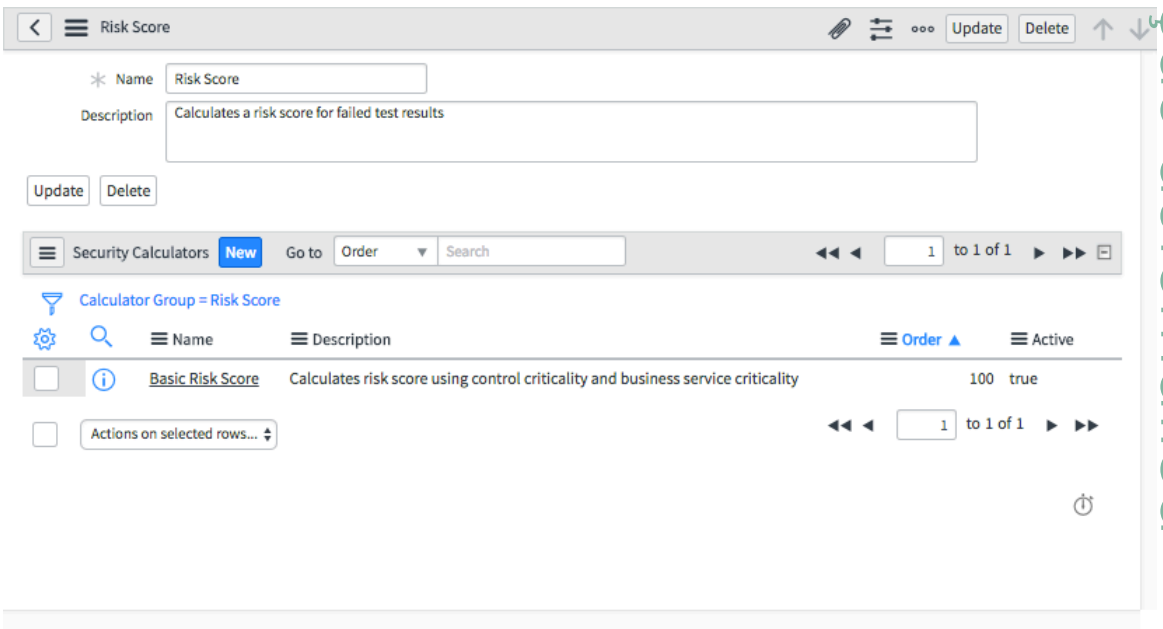
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique com o botão direito do mouse em **Salvar** no cabeçalho do formulário ou clique em **Enviar**.
   O novo grupo de calculadoras é exibido em na lista de grupos com as outras calculadoras. Clique no nome do novo grupo de calculadoras para abrir o registro. Consulte Criar, editar e reaplicar calculadoras de risco para Conformidade de configurações para obter mais informações sobre como definir condições e valores exibidos e reaplicar calculadoras.



   A lista relacionada **Calculadoras de segurança** é exibida.



6. Clique em **Novo** para adicionar calculadoras junto com suas condições ao grupo.

   A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no Construtor de condições não é compatível com este registro ou formulário.

Conformidade de configurações calculadoras e regras de calculadora

Conformidade de configurações automatizar o cálculo de valores iniciais para os campos nos resultados de testes. A condição de cada calculadora é avaliada em ordem e a primeira calculadora correspondente é usada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações calculadoras

O sistema de base da Conformidade de configuração inclui uma calculadora de conformidade de configuração (**Calculadora de risco padrão**) que define a **pontuação de risco** básica no resultado do teste. As calculadoras de Conformidade de configuração podem ser criadas para priorizar e classificar o impacto dos resultados de testes com base em qualquer critério usando filtros de condição. Seja o impacto nos negócios da vulnerabilidade, a classe do item de configuração (IC), você pode criar calculadoras de conformidade de configuração adicionais para definir outros campos nos resultados de testes ou personalizar as calculadoras de conformidade de configuração existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades.

Cada calculadora contém uma lista de regras de calculadora, com uma condição que determina quando aplicá-la. Quando a calculadora é executada, a condição de cada regra de calculadora é avaliada na ordem e a primeira regra de calculadora correspondente é usada.

Todas as calculadoras de conformidade de configuração habilitadas definem os campos selecionados sempre que um resultado de testes é criado, quando um IC associado ou Teste de configuração muda ou quando o link relacionado **Calcular pontuação de risco** em um resultado de testes é usado. Por exemplo, a Pontuação de risco é atualizada automaticamente nos registros de resultados de testes quando o valor de control.criticality é atualizado em um resultado de testes importado. Depois que uma importação de resultado de testes tiver atualizado uma pontuação de resultado de testes, você poderá recalcular a pontuação de risco dos resultados de testes selecionando o botão **Reaplicar calculadora**.

Em um resultado de testes existente, se você selecionar o link relacionado **Calcular pontuação de risco** e uma das calculadoras estiver habilitada, o campo Pontuação de risco no resultado de testes será atualizado.

Nota:

- O link relacionado **Calcular pontuação de risco** só fica visível quando pelo menos uma calculadora de conformidade de configuração está habilitada.
- A partir da v22.0 de Resposta a vulnerabilidades, você pode atualizar a pontuação de risco de um resultado de testes no Espaço do gerenciador de vulnerabilidades e no Espaço de correção de TI selecionando o botão **Calcular pontuação de risco** na exibição de registro.
- A partir da versão 14.13 de Conformidade de configurações, sempre que a pontuação de risco em um resultado de testes muda, os seguintes detalhes são documentados na seção Anotações do resultado de testes:
  - Nome do grupo de calculadoras
  - Nome da calculadora: dependendo se a regra da calculadora é baseada em um modelo ou em um script, o nome é acrescentado com os detalhes entre colchetes. Para modificar ou exibir a base da regra da calculadora, selecione qualquer regra e marque a caixa de seleção **Exibição avançada**. Na caixa suspensa **Tipo de valor**, selecione a opção necessária. Se o **modelo** for selecionado, a pontuação de risco será atualizada de acordo com a condição especificada na regra. Se **Script** estiver selecionado, você poderá adicionar ou atualizar o script existente.
  - Valores de campo com sua ponderação e contribuição de pontuação de risco
  - Pontuação de risco final

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações regras da calculadora

Por padrão, uma **Calculadora de risco padrão** do sistema base é fornecida. Se você quiser criar uma regra de risco para esta calculadora, deverá definir o campo de destino da **Calculadora de risco padrão** como **Pontuação**de risco . Selecione o botão **Nova regra de risco** para criar uma nova regra de risco . Este cria uma regra de calculadora de resultado de testes especializada chamada **Regra de risco**que, por sua vez, calcula a **pontuação de risco** com base em vários valores. Por padrão, os seguintes valores para calcular a pontuação de risco são considerados:

- Criticidade dos negócios
- Criticidade

Você pode ajustar os valores a serem usados na **Regra de risco padrão** e quanto peso atribuir a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a **pontuação de risco**base.

A partir da Conformidade de configurações versão 13.0, você pode personalizar os critérios para a regra de risco padrão. Para obter mais informações, consulte Definir campos e pesos para a regra de risco.

Atribuindo uma porcentagem de ponderação

Você também pode atribuir porcentagem de ponderação (0-100) no nível do valor do campo. Por exemplo, você pode atribuir um percentual de ponderação a cada nível de gravidade (de Nenhum a Crítico). Se o peso de criticalidade for 50 para a regra de risco, e os seguintes valores de peso forem atribuídos para o nível de criticalidade:

Atribuir percentual de ponderação

Criticidade	Pontuação de risco
Crítico	100
Alto(a)	50
Médio	20
Nenhum(a)	0

Se a criticalidade for crítica, o peso correspondente será 50. Se a criticidade for alta, o peso será 25 e, se for média, o peso será 10. Se a criticalidade for nenhuma, o peso correspondente será 0. Para obter mais informações, consulte o exemplo de cálculo de pontuação de risco para Conformidade de configuração.

Cada regra tem uma configuração de **Ordem**, no entanto, a primeira a corresponder às condições atualiza o campo **Pontuação de risco** no resultado do teste. Regras de calculadora sem script normalmente criam menos impacto no desempenho do que as regras de calculadora com script.

A calculadora do sistema base Conformidade de configurações contém regras de calculadora que atribuem a cada nível de criticidade (Nenhum a Crítico) um valor (0-100) para **Pontuação de Risco** com base na gravidade. A gravidade desconhecida é atribuída automaticamente a uma pontuação de risco de 100. Esses valores podem ser ajustados, como a Calculadora de risco padrão, novas regras de calculadora ou novas regras de risco podem ser criadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ponderações de pontuação de risco de vulnerabilidade

Todas as vulnerabilidades recebem uma pontuação e classificação de risco com base em fatores como gravidade, criticidade, informações de exploração e assim por diante. A regra de negócio *Update Risk Rating from Risk Score* na tabela de itens vulneráveis é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Antes da versão 17.1 da aplicação Resposta a vulnerabilidades (VR), as seguintes classificações de risco eram fornecidas como parte da inclusão de script `VulnerabilityUtils`, que era codificada.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

A partir da versão 18.0 de Resposta a vulnerabilidades,

- Os tipos de classificação de risco são enviados na tabela base como cc_risk_rating. Esses tipos são passados como parte da regra de negócio em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e regras de negócio relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as vulnerabilidades e exposições comuns associadas (CVEs) ou entradas de terceiros (TPEs) nos itens de vulnerabilidade (VIs) estão vinculadas a uma vulnerabilidade de exploração conhecida (KEV) de CVE.

Definir campos e pesos para a regra de risco

Personalize os parâmetros e pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de teste e ativo exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Função necessária: sn_vulc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Calculadoras de Risco**.
2. Clique **em Calculadora de risco padrão**.
3. Selecione o campo de destino como **Pontuação de risco**.
   O botão **Nova regra de risco é** exibido na tabela Regra da calculadora.
4. Clique no botão **Nova regra de risco** para navegar até o formulário **Regra de risco de conformidade de configuração**.
5. Na seção Critérios da calculadora de risco, defina o peso de cada critério de acordo com sua importância no cálculo de pontuação de risco geral.
6. Desmarque a caixa de seleção **Ativo** para desativar a regra.
7. Clique em **Adicionar critérios** para adicionar campos de regra de risco aos critérios da calculadora de risco.
8. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	A tabela que você usa para definir a ponderação da pontuação de risco. Selecione uma das seguintes opções: ◦ Resultado de testes: adicione campos para os quais é possível acessar diretamente a referência com pontos a partir do Resultado de testes (TR). ◦ Resultado de testes - Item de configuração: adicione campos de referência com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela cmdb_ci base. ◦ Resultado de testes - Teste: adicione campos de referência com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, Entrada de terceiros. Esses campos não fazem parte da tabela base de Teste de configuração. ◦ Tabela de referência do resultado de testes: adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao resultado de testes. Esses campos não podem ser percorridos com pontos diretamente a partir do Resultado de testes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Tabela de referência do item de configuração: adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não são passíveis de referência com pontos diretamente do TR. ◦ Tabela de referência de teste: adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vulc_test ou tabelas que têm uma referência a sn_vulc_test. Esses campos não são passíveis de referência com pontos diretamente do TR. ◦ Condições personalizadas: use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Campo	O campo usado para o cálculo de pontuação de risco para esta regra.
Ponderação	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Tabela	◦ Resultado de testes > Item de configuração ◦ Resultado de testes > Teste ◦ Tabela de referência do resultado de testes ◦ Tabela de referência do item de configuração ◦ Tabela de referência do teste Este campo aparece somente quando qualquer uma das opções listadas é selecionada no campo Escolher tabela de referência.
Agregação	Selecione o valor mínimo ou máximo a ser considerado para cálculos quando o campo for selecionado nas Tabelas relacionadas (m2m). Este campo aparece somente quando uma tabela de referência é selecionada no campo Escolher tabela de referência.
Definir ponderação de valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	defina os valores de campo como um intervalo (por exemplo, 1–5). O valor deve ser um número inteiro entre 0 e 100. Este campo não aparecerá se a opção Condições personalizadas for selecionada no campo Escolher tabela de referência.
Tabela de condição	Selecione uma condição na lista. Este campo aparece somente quando a opção Condições personalizadas é selecionada no campo Escolher tabela de referência.
Nome do campo	Insira um nome para os critérios de risco. Este campo aparece somente quando Condições personalizadas são selecionadas no campo Escolher tabela de referência.
Condição	Visualize os itens nesta tabela que correspondem às condições definidas. Este campo aparece somente quando Condições personalizadas são selecionadas no campo Escolher tabela de referência.

9. Clique em **Enviar**.

O que Fazer Depois
Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco no resultado de testes ativos.

Editar calculadoras de acúmulo de risco para Conformidade de configurações

Edite uma calculadora de acúmulo de risco existente.

Antes de Iniciar
Função necessária: Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** e selecione **Calculadoras de acúmulo de pontuação de risco**.
2. Com a lista de Calculadoras de Acúmulo de Pontuação de Risco exibida, clique em uma calculadora para abrir o registro e editar o formulário.

Campo	Descrição
Nome	O nome da calculadora de acúmulo de teste de configuração ou tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Uma descrição da calculadora de acúmulo de risco.
Tabela	Tabela na qual a calculadora de acúmulo é aplicada.
Incluir adiamento	Inclui resultados de testes adiados durante o acúmulo da pontuação de risco.

3. Defina as ponderações de uma das seguintes maneiras:
   - Na seção Pesos de Rollup, atribua ponderações para o seguinte:

     Ponderações de Rollup

Campo	Descrição	Ponderação padrão
Pontuação de risco máximo	Pontuação de risco máximo dos resultados de testes considerados.	85
Pontuação de risco médio	Agregado das pontuações de risco de todos os resultados de testes considerados.	0
Contagem de resultados de testes	Número de resultados de testes.	15

   - Marque a caixa de seleção **Exibição avançada** e, no Editor de **valores de script**, edite os valores no script conforme necessário.

     Nota: A edição de scripts requer conhecimento avançado das aplicações Now Platform e Conformidade de configurações.

4. Clique em **Atualizar** para salvar suas edições.

   Calculadoras de acúmulo são trabalhos agendados que são executados por hora para selecionar mudanças. Esses trabalhos agendados também têm pontuações de risco gerais para testes de configuração e tarefa de correção. Os valores acumulados são exibidos nos campos de pontuação de risco.

   Para obter um exemplo de como uma calculadora de acúmulo de risco determina pontuações, consulte Exemplo de cálculo de acúmulo de risco para Conformidade de configurações (anterior à v15.0).

Criar, editar e reaplicar calculadoras de risco para Conformidade de configurações

As regras da calculadora podem ser aplicadas a todos os resultados de testes afetados e coleções sob demanda. Os gerentes de vulnerabilidade podem usar este recurso para ajustar a configuração da calculadora de risco e aplicar mudanças sob demanda para importar descobertas.

Antes de Iniciar
Função necessária: sn_vulc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

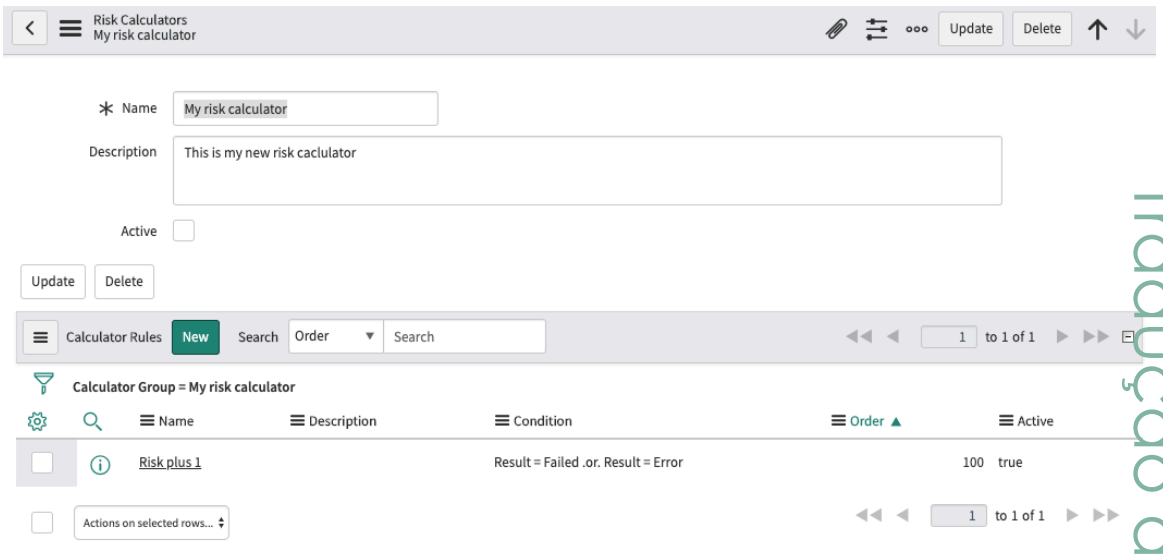
Procedimento

1. Para criar uma nova calculadora de risco, siga estas etapas.

   a. Navegar até **Todos** > **Conformidade de configurações** > **Administração** e selecione **Calculadoras de risco**.

   b. Na lista Calculadora de risco, clique em **Novo**.

   c. Insira um nome e uma descrição para sua nova calculadora e clique em **Enviar**.
   A nova calculadora é exibida na lista Calculadora de risco.



   d. Na lista, clique na nova calculadora para criar as condições sob as quais a calculadora é executada e especifique os campos e valores que você deseja exibir nos registros de resultados de testes e nas tarefas de correção.

   e. No registro exibido, clique em **Novo**.

   f. Preencha os campos nas guias conforme apropriado.

Guia	Descrição
Quando esta condição for atendida	Use o construtor de condições para criar as condições sob as quais a calculadora é executada. Um exemplo é: `Result is Failed ou Result is Error`.
Definir estes valores	Use o modelo para selecionar os campos e valores que você deseja exibir.

   g. Clique em **Enviar**.
   O registro é exibido com as novas regras da calculadora e o grupo ao qual pertence.

2. Para reaplicar uma calculadora existente para testar resultados ou editar as regras e os valores exibidos para uma calculadora de risco existente, siga estas etapas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Nas listas Calculadoras de risco ou Calculadora de acúmulo de risco, selecione a calculadora que deseja editar.

b. Para reaplicar uma calculadora de risco aos dados de resultado de testes existentes do registro, clique em **Reaplicar calculadora**.
Todos os resultados de testes que atendem às condições da calculadora são atualizados.

> **Nota:** Dependendo do número de resultados de testes, esta atualização pode demorar.

c. Para editar as condições e os valores, no canto inferior esquerdo da coluna Nome, clique no nome da calculadora.
Para calculadoras de risco, o registro e as guias **Quando esta condição for atendida** e **Definir estes valores** são exibidos.

d. Preencha o formulário conforme apropriado.

Guia	Descrição do Campo
Quando esta condição for atendida	Use o construtor de condições de filtro para criar as condições sob as quais você deseja que a calculadora seja executada.
Definir estes valores	Escolha um para continuar. ▪ Tipo de valor - Modelo. Escolha os campos na lista e os valores correspondentes. ▪ Script - insira suas mudanças usando o editor. **Nota:** A edição de scripts requer conhecimento avançado das aplicações Now Platform e Conformidade de configurações.

3. Opcional: Para aplicar as novas regras sob demanda aos dados de resultado de testes existentes, siga estas etapas.

a. Com a lista de Calculadoras de risco exibida, clique na calculadora que deseja aplicar. O registro é exibido.

b. Clique em **Reaplicar calculadora** para testar e aplicar suas mudanças sob demanda às descobertas de importação.

4. Exiba suas mudanças nos resultados de testes e continue a editar suas calculadoras conforme necessário.

Exemplos de cálculo de pontuação de risco Conformidade de configurações

A partir da v13.0 de Conformidade de configurações, você pode personalizar os critérios para a regra de risco padrão. Use pontuações de risco fornecidas por fornecedores terceirizados, como Qualys e Tenable, para cálculos de pontuação de risco.

Fornecedores de terceiros, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo Criticidade na tabela sn_vulc_test. Use este

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

campo para cálculos de pontuação de risco. Para usar esta pontuação para calcular a pontuação de risco, siga o procedimento:

Adicionar criticalidade de origem como um critério para uma regra de risco

Use pontuações com base na criticidade fornecida por fornecedores terceirizados para calcular pontuações de risco.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

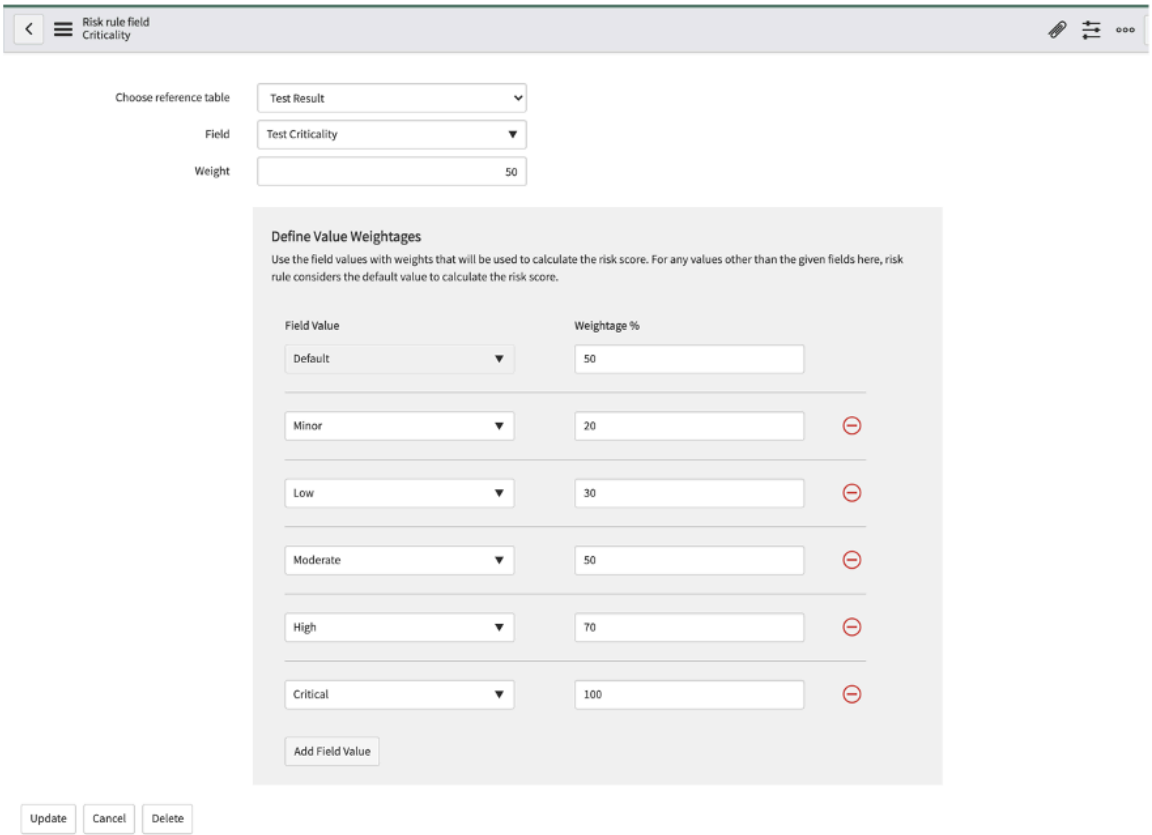
Fornecedores de terceiros, como Qualys e Tenable, fornecem suas próprias pontuações de risco. Essas pontuações são preenchidas no campo Criticidade na tabela sn_vulc_test. Use este campo para cálculos de pontuação de risco e cálculo da pontuação de risco.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Calculadoras de Risco**.
2. Navegue até o formulário Regra de risco.
3. Desmarque a caixa de seleção **Ativo** para desativar a regra.
4. Clique **em Adicionar critérios**.
5. Na lista **Escolher tabela de referência**, selecione **Resultado de teste**.
6. Na lista **Campo**, selecione **Test.Criticality**.
7. No campo **Peso**, especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
8. Na seção **Definir ponderações de valor**, adicione valores de campos e atribua uma porcentagem de ponderação aos campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Clique em **Enviar**.

Adicionar criticalidade dos negócios como critério para uma regra de risco

Especifique um valor de criticalidade para serviços de negócio e use a criticalidade de negócio para calcular as pontuações de risco.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Supondo que sua organização tenha muitos serviços de negócio e um item de configuração (IC) esteja sendo usado pelos seguintes serviços:

Criticidade dos serviços de negócio

Serviço de negócio	Criticidade
Gestão de nuvem	1 - Mais crítico
Comércio eletrônico	2 - Um pouco crítico
Serviços de cliente	3 - Menos crítico
Viagem e despesas	4 - Não crítico

O mapeamento entre o IC e os serviços é armazenado na tabela Serviços [cmdb_ci_services]. Quando um IC não passa em um teste de configuração, um resultado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de teste (TR) é criado. Você pode usar o valor da criticalidade dos serviços afetados para calcular a pontuação de risco para este TR. Siga o procedimento para usar o valor de criticalidade desses serviços para calcular a pontuação de risco.

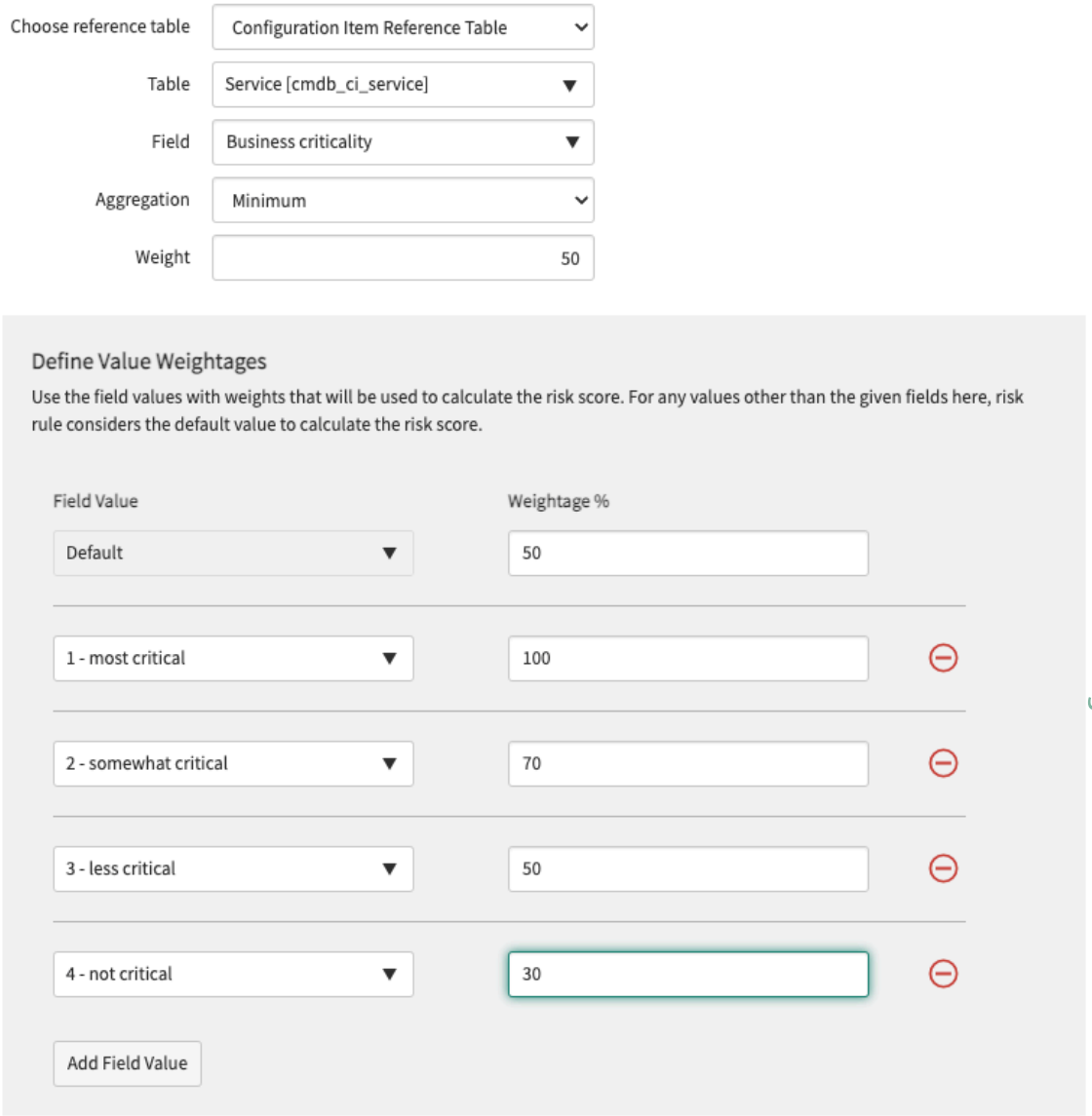
Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Calculadoras de Risco**.
2. Navegue até o formulário Regra de risco na seção **Regras da calculadora**.
3. Desmarque a caixa de seleção **Ativo** para desativar a regra.
4. Clique **em Adicionar critérios**.
5. Na lista **Escolher tabela de referência**, selecione **Tabela de referência do item de configuração**.
6. Na lista **Tabela**, selecione **Serviço [cmdb_ci_service]**.
7. Na lista **Campo**, selecione **Criticidade dos negócios**.
8. No campo **Agregação**, selecione **Mínimo** para recuperar o serviço mais crítico deste caso de uso (1 – Valor mais crítico) ou **Máximo** para recuperar o serviço menos crítico deste caso de uso (4 – Valor não crítico).
9. No campo **Peso**, especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
10. Na seção **Definir ponderações de valor**, adicione valores de campo e atribua ponderações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Peso da regra de risco de criticalidade de negócio personalizada



Tradução automática

11. Clique em **Enviar**.

Adicionar critério condicional à calculadora de risco

Use condições personalizadas para a regra de risco para cálculo de pontuação de risco.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Supondo que sua organização tenha vários itens de configuração (ICs), dos quais apenas alguns podem ser acessados por um usuário externo. Os usuários podem adicionar ponderações de pontuação de risco para esses ICs externos.

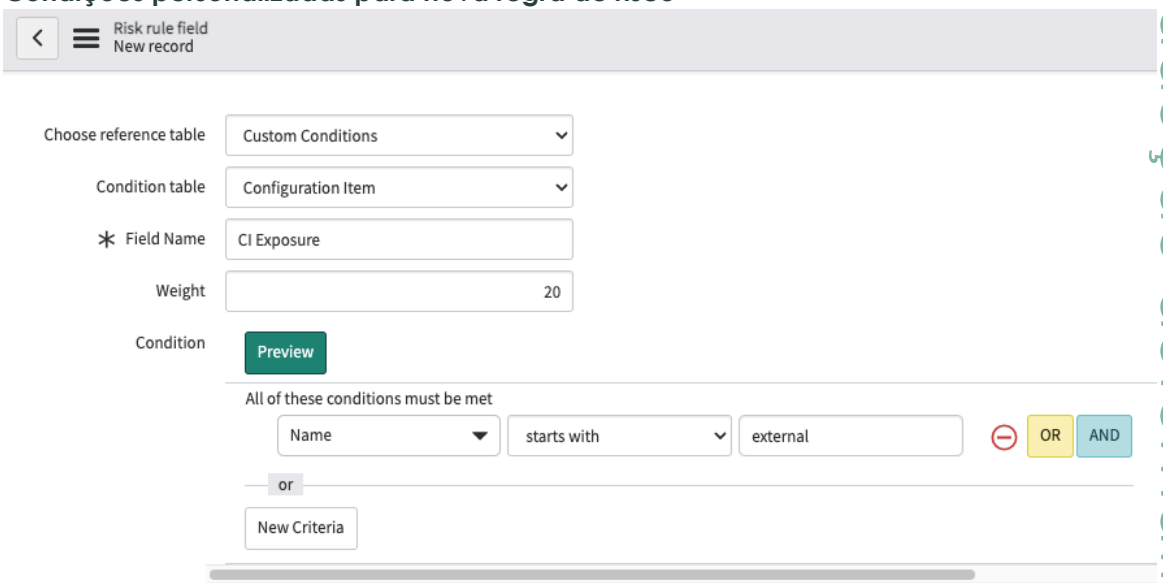
Nota: Você pode identificar esses ICs pelo nome. Os nomes começam com "externo".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Calculadoras de Risco**.
2. Navegue até o formulário Regra de risco.
3. Desmarque a caixa de seleção **Ativo** para desativar a regra.
4. Clique **em Adicionar critérios**.
5. Na lista **Escolher tabela de referência**, selecione **Condições personalizadas**.
6. Na lista **Tabela de condições**, selecione **Item de configuração**.
7. No **campo Nome do** campo, insira `Exposição de IC`.
8. No campo **Peso**, especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
9. No campo **Condição**, selecione **Nome > começa com**, especifique o valor como `externo`.

Condições personalizadas para nova regra de risco



10. Clique em **Enviar**.

Informações relacionadas

Grupos de calculadoras de Conformidade de configuração

Exemplo de cálculo de pontuação de risco para Conformidade de configurações

Determine as calculadoras de pontuação de risco para gerar pontuações de risco que usam os dados de teste e ativo específicos para sua organização.

Exemplo de determinação de pontuações de calculadoras de regra de risco

O exemplo a seguir demonstra como as pontuações das calculadoras de regra de risco são determinadas. Suponha que uma calculadora de regra de risco esteja configurada com os campos nesta tabela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Determinar pontuações da calculadora de regra de risco

Campo	Ponderação	Detalhamento de peso
Controle.Criticalidade	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 50 Alto: 70 Crítico: 100
Criticidade_do_Negócio	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 50 Altura: 70 Crítico: 100

Suponha que os Resultados de testes mostrados nesta tabela estejam presentes no sistema.

Mapeamento de resultados de testes

ID	Criticidade dos negócios	Criticidade de controle
CTR0000001	1 – Mais crítico	Secundário(a)
CTR0000002	1 – Mais crítico	Baixo
CTR0000003	2 – Um pouco crítico	Secundário(a)
CTR0000004	2 – Um pouco crítico	Moderado(a)
CTR0000005	3 – Menos crítico	Baixo

O cálculo da pontuação de risco para o resultado de testes é calculado com base na fórmula:

Pontuação de risco = (W (control.criticality) * FV (control.criticality). + W (business_criticality) * FV (business_criticality)) / 100 em que W é o peso e FV é a porcentagem de peso do valor do campo.

A pontuação de risco resultante para esses resultados de testes é conforme descrito nesta tabela:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontuação de risco com base nos resultados de testes

ID	Criticidade dos negócios (50%)	Criticidade de controle (50%)	Pontuação de risco resultante
CTR0000001	1 - Mais crítico (50% x100)	Secundário (50% x 20)	60
CTR0000002	1 - Mais crítico (50% x100)	Baixo (50% x 30)	65
CTR0000003	2 – Razoavelmente crítico (50% x 70)	Secundário (50% x 30)	45
CTR0000004	2 – Razoavelmente crítico (50% x 70)	Moderado (50% x 50)	60
CTR0000005	3 – Menos crítico (50% x 50)	Baixo (50% x 30)	40

Se a porcentagem de ponderação for alterada para um dos valores de campo, consulte esta tabela para obter os resultados:

Resultados para percentual de ponderação alterado

Campo	Ponderação	Detalhamento de peso
Controle.Criticalidade	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 60 Altura: 70 Crítico: 100
Criticidade_do_Negócio	50	Padrão: 50 1 – Mais crítico: 100 2 – Razoavelmente crítico: 70 3 – Menos crítico: 20 4 – Não crítico: 30

A pontuação de risco dos resultados de testes após a reaplicação da calculadora é mostrada nesta tabela:

Pontuação de risco para TR ao reaplicar a calculadora

ID	Criticidade dos negócios (50%)	Criticidade de controle (50%)	Pontuação de risco resultante
CTR0000001	1 - Mais crítico (50% x100)	Secundário (50% x 20)	60

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontuação de risco para TR ao reaplicar a calculadora

ID	Criticidade dos negócios (50%)	Criticidade de controle (50%)	Pontuação de risco resultante
CTR0000002	1 - Mais crítico (50% x100)	Baixo (50% x 30)	65
CTR0000003	2 – Razoavelmente crítico (50% x 70)	Secundário (50% x 30)	45
CTR0000004	2 – Razoavelmente crítico (50% x 70)	Moderado (50% x 60) *Valor revisado	65 *Valor revisado
CTR0000005	3 – Menos crítico (50% x 20) *Valor revisado	Baixo (50% x 30)	25 *Valor revisado

Exemplo de cálculo de acúmulo de risco para Conformidade de configurações (anterior à v15.0)

O exemplo a seguir demonstra como as pontuações das calculadoras de acúmulo de risco são determinadas.

Para a calculadora de acúmulo de tarefa de correção a seguir, a fórmula para calcular a pontuação de risco da tarefa de correção é:

(Pontuação de risco máximo/100) * 85 + (fator * 15).

O fator na equação anterior é determinado pelo número de resultados de testes, conforme mostrado na tabela a seguir.

Contagem de Resultado de testes	Fator
< 10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
> 1000	1

Para a Tarefa de correção a seguir, TRG0003066, com três pontuações de risco de resultados de testes, a pontuação máxima é 90.

Número	Pontuação de risco	Tarefa de correção	Resultado	Status
CTR000123	90	TRG0003066	Reprovado	Aberto
CTR000124	70	TRG0003066	Reprovado	Aberto
CTR000125	40	TRG0003066	Reprovado	Aberto

Para a Tarefa de correção, TRG0003066:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A pontuação de risco é 79, (90/100) * 85 + 0,2 * 15 = Piso matemático (76,5 +3) = 79.

A pontuação de risco histórico é nula porque a Tarefa de correção ainda está "Aberta".

Após a ingestão de dados, os resultados de testes são "Aprovados" e a Tarefa de correção muda para "Encerrada", conforme mostrado na tabela a seguir.

Número	Pontuação de risco (anterior à v15.0)	Tarefa de correção	Resultado	Status
CTR000123	0	TRG0003066	Aprovado	Encerrado
CTR000124	0	TRG0003066	Aprovado	Encerrado
CTR000125	0	TRG0003066	Aprovado	Encerrado

O histórico de resultados de testes é exibido na tabela a seguir.

Número	Pontuação de risco	Último resultado	Resultado
CTRH000111	90	CTR000123	Reprovado
CTRH000112	70	CTR000124	Reprovado
CTRH000113	40	CTR000125	Reprovado

A pontuação de risco é zero porque não há resultados de testes ativos na Tarefa de correção.

Para a Tarefa de correção, TRG0003066:

A pontuação de risco histórico é 79: (90/100) * 85 + 0,2 * 15 = Piso matemático (76,5 +3) =79.

Exemplo de cálculo de acúmulo de risco para Conformidade de configurações (v15.0 e posterior)

O exemplo a seguir demonstra como as pontuações das calculadoras de acúmulo de risco são determinadas.

Para a calculadora de acúmulo de tarefa de correção a seguir, a fórmula para calcular a pontuação de risco da tarefa de correção é:

(Pontuação de risco máximo* 80/100) + (Pontuação de risco médio* 5/100) + (Fator * 15)

Em que, os pesos são os seguintes:

- Pontuação de risco máximo: 80
- Pontuação de risco médio: 5
- Fator: 15

O peso padrão da pontuação de risco médio é 0. Para obter mais informações sobre como definir os pesos, consulte Editar calculadoras de acúmulo de risco para Conformidade de configurações.

O fator na equação anterior é determinado pelo número de resultados de testes, conforme mostrado na tabela a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contagem de Resultado de testes	Fator
< 10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
> 10.000	1

Para a Tarefa de correção a seguir, TRG0003066, com três pontuações de risco de resultados de testes, a pontuação de risco máxima é 90 e a pontuação de risco média é 66,67.

Número	Pontuação de risco	Tarefa de correção	Resultado	Status
CTR000123	90	TRG0003066	Reprovado	Aberto
CTR000124	70	TRG0003066	Reprovado	Aberto
CTR000125	40	TRG0003066	Reprovado	Aberto

Para a Tarefa de correção, TRG0003066:

A pontuação de risco é 81, (90 * 80/100) + (66,67 * 5/100) + (0,2 * 15) = Piso-matemático (78,3 +3) = 81.

A pontuação de risco histórico é nula porque a tarefa de correção ainda está "Aberta".

Após a ingestão de dados, os resultados de testes são "Aprovados" e a Tarefa de correção muda para "Encerrada", conforme mostrado na tabela a seguir. A partir da v15.0 de Conformidade de configurações, a pontuação de risco de um resultado de testes aprovado é preenchida para determinar o risco reduzido.

Número	Pontuação de risco	Tarefa de correção	Resultado	Status
CTR000123	90	TRG0003066	Aprovado	Encerrado
CTR000124	70	TRG0003066	Aprovado	Encerrado
CTR000125	40	TRG0003066	Aprovado	Encerrado

O histórico de resultados de testes é exibido na tabela a seguir.

Número	Pontuação de risco	Último resultado	Resultado
CTRH000111	90	CTR000123	Reprovado
CTRH000112	70	CTR000124	Reprovado
CTRH000113	40	CTR000125	Reprovado

A pontuação de risco da Tarefa de correção é zero porque não há resultados de testes ativos na Tarefa de correção.

Para a Tarefa de correção, TRG0003066:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Pontuação de risco histórico é 81: (90 * 80/100) + (66,67 * 5/100) + (0,2 * 15) = Piso matemático (78,3 +3) = 81.

Criar ou editar Conformidade de configurações regras de tarefa de correção

Você pode criar regras para agrupar automaticamente os resultados de testes com base nas condições do filtro. Essas regras agrupam automaticamente os resultados de testes à medida que são importados. Use o filtro para limitar os resultados de testes agrupados por esta regra, como selecionar todos os resultados de testes com explorações.

Antes de Iniciar
Função necessária: sn_vulc.admin

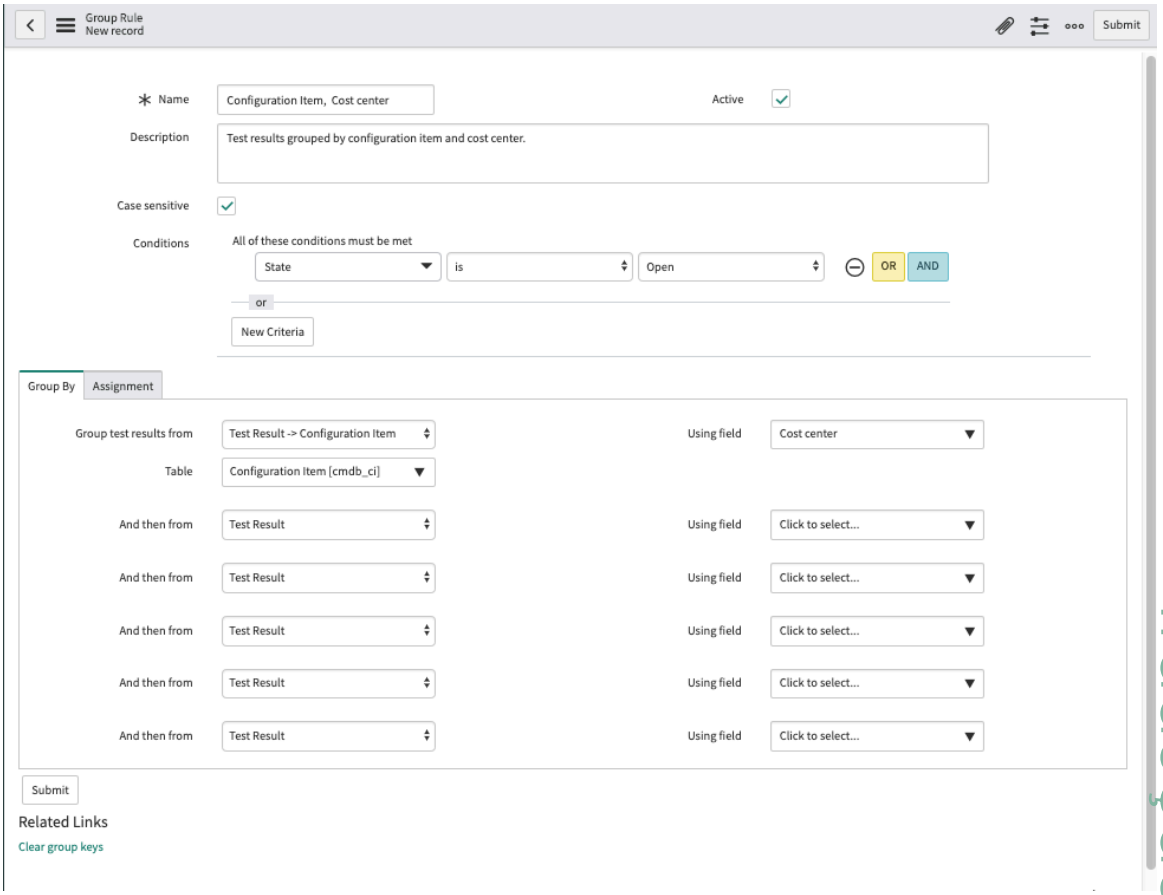
Por Que e Quando Desempenhar Esta Tarefa
O sistema base é fornecido com uma regra de tarefa de correção, **Grupo de atribuição, Teste**, que agrupa resultados de testes por grupo de atribuição (preenchido previamente a partir de **Regras de atribuição**) e o campo **Teste** de resultado de testes. Esta regra pode ser modificada usando condições de filtro e chaves de grupo. As chaves de grupo são colunas na tabela de resultados de testes. Selecione até seis chaves para indicar quais valores devem ser usados para agrupar os resultados de testes.

A partir da versão 14.7 de Conformidade de configurações, a regra da tarefa de correção **de teste do grupo de atribuição** foi desativada para novas implementações.

Nota: Regras novas ou atualizadas são avaliadas automaticamente na próxima importação ou manualmente usando o botão **Reaplicar** no formulário Regra de grupo.

Procedimento
1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de tarefa de correção**.
2. Abra o **Grupo de atribuição, Regra de teste** ou clique em **Novo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Se for **Novo**, preencha os campos no formulário, conforme apropriado.

Conformidade de configurações Regra da tarefa de correção

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se o grupo está ativo.
Descrição	Descrição de texto desta regra de tarefa de correção.
Diferenciação entre maiúsculas e minúsculas	Determina se a correspondência de regra faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não diferencia maiúsculas de minúsculas.
Condições	Condições que devem ser atendidas. Por padrão, (caixa de seleção que**diferencia maiúsculas de minúsculas** desabilitada), o texto de pesquisa que você insere no construtor de condições em registros e formulários de regras de grupo não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de grupo.
Agrupar por	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Agrupar resultados de testes de	Automatize a criação de grupos com base nesta regra. Escolha uma das opções disponíveis. ◦ Resultado de testes | Usando campo ◦ Resultado de testes->Item de configuração | Tabela | Usando campo Se um campo **de tabela** estendida for selecionado, os resultados de testes que não usam a tabela estendida correspondente serão agrupados em uma tarefa de correção separada.
Atribuição	
Atribuir grupos de resultados de testes por	Automatize a atribuição de grupos criados com base nesta regra. Escolha uma das opções disponíveis. ◦ Chave do grupo Quando selecionado, um campo de Valor de chave é exibido, os campos disponíveis são listados em um menu suspenso. ◦ Grupo de usuários Quando selecionado, um campo de pesquisa de grupo de usuários é exibido.

4. Clique em **Enviar**.

Nota: **O link relacionado Limpar Agrupar por Chaves** remove as chaves de grupo da guia Agrupar por no formulário.

Especifique a duração de uma exceção solicitada para uma tarefa de correção

Use as propriedades do sistema para limitar a duração pela qual uma exceção é solicitada para uma tarefa de correção. A correção da tarefa de correção foi adiada pelo período especificado.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
A propriedade `sn_vulc.exception_max_request_days` é usada para especificar o número máximo de dias para os quais uma exceção para uma tarefa de correção pode ser solicitada. O valor padrão é 365 dias.

Nota: Você pode usar a propriedade `sn_vulc.exception_approval_required` para desabilitar o fluxo de trabalho de aprovação de exceção para a tarefa de correção se ela não for necessária. Por padrão, esta propriedade está habilitada e seu valor é `verdadeiro`.

Procedimento

1. Navegar até **Todos** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Na página Propriedades do sistema, pesquise por `sn_vulc.exception_max_request_days`.
3. Clique no nome da propriedade para abrir o registro de Propriedade do sistema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para poder editar este registro, certifique-se de que Conformidade de configurações esteja selecionado como a aplicação atual.
5. Insira um **Valor** positivo e clique em **Atualizar**.
   O registro é atualizado e salvo.

Configurar Gestão de exceções para Conformidade de configurações

Limite a duração de uma exceção solicitada e adicione um questionário à exceção usando o módulo Conformidade de configurações. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Resposta a vulnerabilidades. Você também pode solicitar uma exceção usando a integração GRC: Gestão de políticas e conformidade.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Se Resposta a vulnerabilidades estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Gestão de políticas e conformidade estiver instalado, você poderá selecionar GRC: Gestão de políticas e conformidade na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica o objetivo de Política e Controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que está levantando a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista Gerenciar exceções usando.
   - Resposta a vulnerabilidades

     Nota: A partir da versão 22.0 de Resposta a vulnerabilidades, você também pode configurar o questionário para solicitações de falso-positivo para a opção Resposta a vulnerabilidades.

   - GRC: Gestão de políticas e conformidade

     Nota: Você deve ativar o plug-in GRC para usar GRC: Gestão de políticas e conformidade para solicitar uma exceção.

   Nota: Alterar a configuração não afeta os dados existentes.
3. Preencha os campos no formulário.

Configurações do formulário Gestão de exceções de CC

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Opção para exibir o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso-positivo. O questionário para uma solicitação de falso-positivo é exibido por padrão.

4. Selecione **Salvar**.

Adicionar um aprovador de exceção para Conformidade de configurações

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção para uma tarefa de correção em Conformidade de configurações.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Uma solicitação de exceção para uma tarefa de correção é aprovada usando o fluxo de trabalho de aprovação padrão em dois níveis. A adição de usuários ao grupo de primeiro nível é obrigatória. Se não houver usuários no segundo nível, a solicitação será aprovada automaticamente após a aprovação de primeiro nível.

Nota: Se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada.

Nota: Até Conformidade de configurações v13.0, se não houver um aprovador de primeiro nível, uma exceção não poderá ser solicitada. No entanto, a partir da Conformidade de configurações v13.0, se você estiver implantando a aplicação CC pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo novamente para fluxo de trabalho.

Procedimento

1. Navegar até **Todos** > **Segurança do sistema** > **Usuários e Grupos** > **Grupos**.
2. Na coluna Nome, pesquise por **Exceção**e clique em **Aprovador de exceção - Nível 1 CC**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir de Conformidade de configurações v14.7.5, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de exceção é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *sn_vulc.exception_approver_L1_CC* ou *sn_vulc.exception_approver_L2_CC* para mudar o valor da propriedade.

3. No formulário Aprovador de exceção de grupo - CC de nível 1, navegue até **Membros do Grupo** > **Novo** (ou **Editar**).
4. No formulário, preencha os campos.

Formulário do usuário

Campo	Descrição
ID do Usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear o usuário fora da instância e encerrar todas as sessões ativas do usuário. O sistema evita que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ◦ Listas de usuários ◦ Lista de seleção em campos de referência (ícone de lupa) ◦ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço Web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário para o local deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...**.

5. Clique em **Enviar**.
6. Opcional: Repita as etapas 1 a 5 para criar um Aprovador de exceção - Nível 2 CC.

   Nota: Ao criar um aprovador de segundo nível, selecione **Aprovador de exceção - CC de nível 2**

7. Opcional: Se você selecionar **Editar**, mova os usuários da **Coleção** para o painel **Membros do grupo** e clique em **Salvar**.
   O aprovador deve navegar até **Todos** > **Conformidade de configurações** > **Minhas aprovações** e aprovar solicitações.

Criar um mapa de criticalidade Conformidade de configurações

O mapeamento de criticalidadeConformidade de configurações fornece um mapa de transformação para campos de criticalidade de origem de terceiros em campos reconhecíveis na gravidade Conformidade de configurações.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Mapeamento de Criticalidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Mapeamento de campo

Campo	Descrição
Origem	O nome da origem do mapeamento de criticalidade.
Valor de origem	O valor de criticalidade de origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Valor de meta	O valor de meta. As opções são: Crítico O problema de configuração associado ao controle está causando uma interrupção em um ou mais ICs críticos para os negócios. Alto(a) O problema de configuração associado ao controle é uma ameaça, mas não está causando o desligamento de recursos de rede críticos. Moderado(a) O problema de configuração associado ao controle é um risco, mas não é uma ameaça imediata. Baixo O problema de configuração associado ao controle é uma ameaça de baixo nível e pode ser ignorado em favor dos ICs que estão em maior risco. Secundário(a) O problema de configuração associado ao controle é um risco menor e pode ser ignorado se necessário.

4. Clique em **Enviar**.

Criar notificações por e-mail

Os administradores de vulnerabilidade podem editar a notificação ou adicionar novas, especificando quando enviar a notificação, quem a recebe e qual conteúdo está na notificação.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode criar modelos de e-mail para diferentes tipos de notificações por e-mail. Para obter mais informações sobre como criar modelos de e-mail, consulte Definir Resposta a vulnerabilidades modelos de e-mail.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de meta de correção ou escolha **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.
   Para mais informações sobre campos de formulário, consulte Criar uma notificação por e-mail .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultados
A partir da v14.11 de Conformidade de configurações, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Links abertos em Vulnerability Manager Workspace para os usuários com a função sn_vulc.admin.
- Links abertos em Espaço de correção de problemas de TI para os usuários com a função sn_vulc.remediation_owner.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configurar regras de aprovação para Gestão de exceções no Conformidade de configurações

A partir da Conformidade de configurações v13.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções e regras de exceção. Se você estiver implantando o CC pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Se você for um usuário Conformidade de configurações existente, a opção padrão será fluxo de trabalho.

Se você implantou Conformidade de configurações v13.0 ou posterior, o valor da propriedade do sistema *sn_vulc.flow_designer_activation* será definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Conformidade de configurações antes da v13.0, o valor desta propriedade do sistema será definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota: Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer no Conformidade de configurações.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Regras de aprovação de exceção para grupos de resultados de testes
- Regra de aprovação para regras de exceção automática

Nota: Você também pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para a Gestão de exceções no Conformidade de configurações.

Procedimento
1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de aprovação** > **Regras de aprovação de exceção para grupo de resultados de testes**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Conformidade de configurações.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovaçãoy (dias) A partir da v14.11 de Conformidade de configurações	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v14.11 de Conformidade de configurações	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Criar configurações para uma regra de aprovação no Conformidade de configurações.

   Nota: Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para a Gestão de exceções no Conformidade de configurações.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para os mesmos resultados de testes encontrados em diferentes tarefas de correção.

Criar configurações para uma regra de aprovação no Conformidade de configurações

Defina as condições para filtrar tarefas de correção correspondentes para um nível de aprovação.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
No módulo Configurações de aprovação, você pode configurar vários níveis de aprovação para diferentes configurações. Defina regras baseadas em condição, com cada regra contendo vários níveis de aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Use o módulo Regras de aprovação para configurar regras de aprovação para os fluxos de trabalho de gestão de exceções. Para obter informações sobre como configurar regras de aprovação, consulte Criar níveis de aprovação para a Gestão de exceções no Conformidade de configurações.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. No formulário, preencha os campos.

Formulário Configuração de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Ativo	Habilitado por padrão, o que significa que a configuração de aprovação está em uso.
Descrição	Descrição resumida dos níveis de configuração de aprovação.

5. Defina uma condição para os resultados de testes ou tarefas de correção de uma das seguintes maneiras:

Campo	Descrição
Condição	Identifica os resultados de testes correspondentes ou as tarefas de correção.
Condição avançada	Script que define a condição para os resultados de testes ou tarefas de correção. **Nota:** Este campo aparece quando você marca a caixa de seleção **Avançado**.

6. Selecione **Atualizar**.

Você pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para a Gestão de exceções no Conformidade de configurações.

Example:
Você pode definir diferentes caminhos de aprovação para diferentes tipos de tarefas de correção.

Criar níveis de aprovação para a Gestão de exceções no Conformidade de configurações

Defina os níveis de usuários e grupos de usuários que aprovarão as solicitações de exceção.

Antes de Iniciar
Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. Na seção **Níveis** de aprovador, selecione um nível de aprovador.
5. No formulário, preencha os campos.

Formulário Nível do aprovador

Campo	Descrição
Nome	Nome do nível de aprovação.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ◦ Um aprovador necessário ◦ Todos os usuários devem aprovar
Ativo	Habilitado por padrão, o que significa que o nível de aprovação está em uso.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação. Este campo é somente leitura.
Configuração de aprovação	Contém as configurações de aprovação. Este campo é somente leitura.
Atribuir usando	Selecione uma opção de: ◦ Usuário e grupo de usuários ◦ Campo da tabela de aprovação ◦ Script

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções para gestão de exceções e regras de exceção: ◦ sn_vulc.exception_approver ◦ sn_vulc.read ◦ sn_vulc.read_auto_exception_rule
Usuários	Edite os usuários listados nos grupos.

6. Para salvar as mudanças, selecione **Atualizar**.

Nota: Antes da v13.0, o processo de fluxo de trabalho era funcional se houvesse usuários somente no nível de exceção 1. No entanto, a partir da v13.0, deve haver pelo menos um usuário em cada nível.

Antes da v13.0, no fluxo de trabalho, se não houvesse usuário no segundo nível, a tarefa de correção era adiada. No entanto, da v13.0 em diante, se não houver usuário no segundo nível, a solicitação de aprovação será rejeitada automaticamente.

Example:
Pode haver diferentes níveis de aprovação para tarefas de correção para servidores Linux e Windows.

Fluxo de trabalho de gestão de exceções versus Flow Designer no Conformidade de configurações

A partir de Conformidade de configurações (CC) v13.0, se você estiver implantando o CC pela primeira vez, o Flow Designer para aprovar solicitações de exceção na gestão de exceções será habilitado por padrão. Se você já for um usuário de CC, a opção padrão será fluxo de trabalho.

Fluxo de trabalho versus Flow Designer

Considerações	Fluxo de trabalho	Flow Designer
Versão	Antes da v13.0 do CC.	A partir da v13.0 do CC.
Opção padrão	Opção padrão se você for um usuário de CC existente.	Opção padrão para novos usuários de CC a partir da v13.0.
Como definir o processo de aprovação	A gestão de exceções inclui solicitações de exceção junto com regras de exceção.	Inclui a definição de vários níveis e a adição de diferentes aprovadores para diferentes casos de uso. Mais fácil de implementar do que o fluxo de trabalho. A gestão de exceções inclui solicitações de exceção junto com regras de exceção.
Atualizando para o Flow Designer	Você pode fazer upgrade para o Flow Designer a partir	O Flow Designer está habilitado por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho versus Flow Designer

Considerações	Fluxo de trabalho	Flow Designer
	do fluxo de trabalho. No entanto, as solicitações existentes só podem ser aprovadas usando o fluxo de trabalho.	
Propriedade do sistema *sn_vulc.flow_designer_activation*	Se você estiver usando o fluxo de trabalho para gestão de exceções antes da v13.0, a propriedade do sistema será definida como falsa. Para ativar o Flow Designer, defina esta propriedade como verdadeira. **Nota:** Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer.	Se você estiver usando CC pela primeira vez para v13.0 ou posterior, o valor da propriedade do sistema será definido como verdadeiro por padrão.
Módulo de regras de aprovação	Depois de definir a propriedade do sistema como verdadeira, o trabalho agendado **Habilitar regras de aprovação do módulo** é executado em 24 horas. Este trabalho agendado habilita o módulo **Regras de aprovação**. Para ativar este módulo instantaneamente, execute este trabalho manualmente.	Se você implantou o CC pela primeira vez a partir do CC v13.0, este módulo estará disponível por padrão.
Níveis de aprovação	Fornece a opção de definir apenas dois níveis de aprovadores.	Fornece várias opções, como definir qualquer número de configurações, níveis de aprovador e adicionar dinamicamente aprovadores para cada regra.

Integrações do Conformidade de configurações

As integrações de terceiros importam descobertas de avaliação de configuração, políticas, testes, tecnologias, fontes autorizadas, resultados de testes junto com outros dados de vulnerabilidade para a aplicação Conformidade de configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

A aplicação Conformidade de configurações é compatível com as seguintes integrações de terceiros:

- A partir da v14.11, conduza a correção de lacunas de segurança em seus ativos empresariais identificados pela aplicação Controle de posturas de segurança publicando descobertas como resultados de testes na aplicação Conformidade de configurações. A aplicação Controle de posturas de segurança e suas aplicações compatíveis estão disponíveis com assinaturas separadas do ServiceNow® Store. Para obter mais informações, consulte Controle de posturas de segurança.
- Microsoft Defender for Cloud Integration para Operações de segurança
- Palo Alto Prisma Cloud Vulnerability Integration
- Qualys integração com Conformidade de configurações
- O produto Tenable.io da integração de vulnerabilidade da Tenable

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 14.8.5 do Conformidade de configurações, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Defender for Cloud Integration para Operações de segurança

O produto Microsoft Defender for Cloud Integration é um sistema de gestão de segurança de infraestrutura que aprimora a postura de segurança de seus ambientes de nuvem.

Microsoft Defender for Cloud Integration para Operações de segurança se integra com a aplicação Conformidade de configurações para mapear testes para itens de configuração (ICs) para criar resultados de testes. Ele descobre continuamente novos recursos de nuvem implantados em cargas de trabalho e determina se eles estão configurados de acordo com padrões de segurança, como o Center for Internet Security (CIS).

A partir da versão 2.2, a Central de segurança do Microsoft Azure foi renomeada para Microsoft Defender for Cloud Integration para Operações de segurança.

Versões disponíveis

Aplicação	Versão
Microsoft Defender for Cloud Integration para Operações de segurança	2,3
Conformidade de configurações	14.3
Security Support Common	13.2
Resposta a vulnerabilidades	16,2

Várias implantações da plataforma Microsoft Defender for Cloud

Se você tiver várias implantações da aplicação da plataforma Microsoft Defender for Cloud, poderá adicionar uma integração para cada implantação. Os recursos identificados por várias implantações de terceiros são consolidados e reconciliados com seu Configuration Management Database (CMDB). Essa consolidação ocorre mesmo quando os processos de verificação se sobrepõem entre as várias implantações.

ServiceNow Microsoft Defender for Cloud Integrações

O Microsoft Defender for Cloud Integration para Operações de segurança aprimora os dados de conformidade em sua instância recuperando dados de Microsoft Defender for Cloud. Uma série de trabalhos agendados invoca as integrações automaticamente. Você também pode executar esses trabalhos agendados manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção dos resultados de testes, mantendo a instância sincronizada com Microsoft Defender for Cloud.

Há um usuário executar como configurado para cada registro de integração, com o valor padrão **VR.System**. Este valor deve permanecer o mesmo.

Nota: Se você não definir um usuário executar como válido, anexos de recuperação de dados duplicados ou múltiplos serão criados para os registros de fonte de dados. O número de anexos aumenta cada vez que a integração é executada. Isso aumenta o tempo de processamento, resultando em resultados de transformação inconsistentes.

Microsoft Defender for Cloud As tarefas de integração de plataforma envolvem as funções a seguir.

- sn_vul_asc.configure_integration: capacidade de ler, gravar e excluir registros.
- sn_vul_asc.read_integration: capacidade de ler registros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição das Microsoft Defender for Cloud integrações

Exiba as integrações navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Integrações**.

As seguintes integrações estão incluídas no sistema de base.

Integração	Descrição
Integração de definição de política	Recupera políticas e cria entradas de política em sua instância.
Integração de metadados de avaliação	Recupera metadados de avaliação e cria testes em sua instância.
Integração de controles e padrões de conformidade	Recupera padrões e controles e cria a origem de autorização e as citações. Em seguida, ele os vincula aos testes criados.
Integração de avaliação	Recupera avaliações e as processa em sua instância. A saída desta integração são os resultados de testes.

Criar ICs usando o Mecanismo de identificação e reconciliação

Use o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs quando um IC existente não puder ser correspondido com um host importado de um scanner de terceiros.

Se um IC não for correspondido no CMDB, um IC será criado na classe *cmdb_ci_cmp_resource*. Posteriormente, quando uma descoberta encontrar o mesmo IC, ela aprimorará o IC ou criará outro.

Nota: A reconciliação automática não acontece para recursos de nuvem.

Instalar e configurar Microsoft Defender for Cloud Integration para Operações de segurança

Instale e configure o Microsoft Defender for Cloud Integration para Operações de segurança, para que você possa usar os dados importados de Microsoft Defender for Cloud para priorizar e corrigir quaisquer erros de configuração em seus ativos.

Antes de Iniciar

Crie um novo registro de app no Azure Active Directory. Para obter mais informações sobre como registrar uma nova aplicação no Azure Active Directory, pesquise `Registrar uma aplicação cliente no Azure Active Directory` no site de documentação da Microsoft . Atribua a função de **leitor de segurança** para o registro do app recém-criado no escopo relevante com o qual você deseja se conectar a ServiceNow. Pode estar em um grupo de gerenciamento ou no nível de assinatura.

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Plug-ins**.
2. Na barra de pesquisa, pesquise por `Microsoft Defender para Cloud Integration for Security Operations`.
3. Selecione **Instalar**.

   Todas as dependências que serão instaladas são exibidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Navegar até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Administração** > **Configuração** > **Configuração do Microsoft Defender para Nuvem**.
5. No formulário, preencha os campos.

Microsoft Defender for Cloud Formulário de configuração

Campo	Descrição
URL da API	URL do recurso da instância. Exemplo: https://management.azure.com (nuvem pública do Azure)
ID de locatário	Identidade do locatário da sua organização.
Instância de integração	Instância padrão. Você também pode criar uma instância para trazer os dados de vários locatários ou assinaturas do Microsoft Defender.
ID de cliente	Identidade do cliente gerada depois que a aplicação Microsoft Defender for Cloud Integration é registrada.
Segredo do cliente	Segredo do cliente gerado depois que a aplicação Microsoft Defender for Cloud Integration é registrada.
Importar descobertas de	Recursos e avaliações que correspondem aos IDs de grupo de gerenciamento e IDs de assinatura selecionados que serão recuperados.
IDs do grupo de gestão	Recursos e avaliações que correspondem às IDs de grupo de gestão que serão recuperadas. **Nota:** Este campo aparece somente quando você seleciona **Grupos de gestão específicos** no campo **Importar descobertas de**.
IDs de Assinatura	Números de identificação das assinaturas para as quais os recursos e avaliações serão recuperados. **Nota:** Este campo aparece somente quando você seleciona **Assinaturas específicas** no campo **Importar descobertas de**.
Status de validação	Se as credenciais e o ID de assinatura fornecidos são válidos.

6. Configure ou execute as integrações selecionando **Salvar e testar**.

Conformidade de configurações dados importados para Microsoft Defender for Cloud Integration

Conformidade de configurações O importa políticas, testes, fontes autorizadas e resultados de testes de integrações de terceiros e os armazena em módulos para exibição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Grupos de teste

Um grupo de testes de configuração constitui um grupo de teste. Os grupos de teste estão relacionados a documentos oficiais e registros de teste e podem ser modificados para atender às necessidades da sua organização. Um teste de configuração pode pertencer a vários grupos de teste.

Se o Microsoft Defender for Cloud Integration estiver instalado, os grupos de teste serão recuperados e preenchidos pelo trabalho agendado, **Integração de definições de política**. Você pode exibir o trabalho agendado navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Administração** > **Integrações** > **Integração de definições de política**.

Nota: Se você optar por executar a integração manualmente, execute primeiro a **Integração de definições de política**.

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como os ativos devem ser regidos.

Um teste Conformidade de configurações é o mecanismo que as aplicações de integração de terceiros usam para agrupar ativos por tipo de resultados de testes.

Se o Microsoft Defender for Cloud Integration estiver instalado, o trabalho agendado, **Avaliação de integração de metadados**, recuperará os testes. Você pode exibir o trabalho agendado navegando até **Integração** > **Integrações Primárias** > **Integração de metadados de avaliação**.

Nota: Se você optar por executar a integração manualmente, execute a integração de **metadados de avaliação** após a **integração de definições de política**.

A partir da v15.0 de Conformidade de configurações, o grupo de teste ao qual um teste pertence é preenchido na coluna **Grupos de teste** da lista de testes.

Fontes autorizadas

Conformidade de configurações usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente mapeiam para seções de padrões publicados do setor, como **ISO 27001** e **PCI DSS 3.2.1**.

Esses registros de origem contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas na área de segurança de computadores. Eles definem requisitos para políticas e procedimentos de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o Microsoft Defender for Cloud Integration estiver instalado, o trabalho agendado, **Padrões e controles**de conformidade, recuperará as fontes autorizadas e as citações. Você pode exibir este trabalho agendado navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Integrações** > **Integração de controles e padrões de conformidade**.

Nota: Se você optar por executar a integração manualmente, execute a **Integração de controles e padrões de conformidade** após a **Integração de metadados de avaliação**.

Ativos

A **integração de avaliação** fornece informações vitais, como marcadores de recursos e atributos de nuvem. Essas informações são exibidas no formulário Item descoberto. É usado principalmente para filtragem em Conformidade de configurações Regras de atribuição e tarefa de correção.

- Marcadores de recursos: todos os marcadores de recursos de nuvem são importados como marcadores de host como parte da **integração de avaliação**. Os marcadores de nuvem para qualquer tipo de recurso de nuvem são armazenados aqui, seja o recurso um host ou não.
  - O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Se um marcador de Tokyo for criado, um marcador de **TOKYO**não poderá ser armazenado na tabela de marcadores de host. **Tokyo** e **TOKYO** são considerados a mesma marca de host. O marcador que foi importado primeiro vence.
  - Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Atributos de nuvem para ativos: a seguir estão os atributos de nuvem que as integrações recuperam de Microsoft Defender for Cloud:
  - Conta de nuvem
  - Região da nuvem
  - Tipo de Recurso de Nuvem
  - Provedor de serviço de nuvem

Resultados de testes

Conformidade de configurações não calcula os resultados de testes, mas os importa como parte de uma integração de terceiros. Depois que podem ser exibidos em Conformidade de configurações, eles são corrigidos usando **Tarefas**de correção.

Se a integração Microsoft Defender for Cloud estiver instalada, o trabalho agendado, **Integração de avaliação**, recuperará os resultados de testes. Você pode exibir este trabalho agendado navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Integrações** > **Integração de avaliação**.

A importação **de integração de avaliação** é a única integração que usa o parâmetro *`Start Time`* na guia **Detalhes da integração**. Todas as outras Conformidade de configurações importações apresentam todos os dados disponíveis, independentemente de *`Start Time`*.

Quando a importação da **integração de avaliação** é concluída, um evento é iniciado para acionar cálculos de fim de importação.

A **integração de avaliação** extrai as avaliações de dados somente se houver uma mudança de status da última execução de integração bem-sucedida para o último dia

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

por padrão. Portanto, se a avaliação falhar continuamente nos últimos dias, a integração não buscará a avaliação, pois não há mudança de status para a avaliação. Para manter os resultados de testes atualizados com as avaliações do Defender, uma nova **integração de avaliação abrangente** foi adicionada e extrai os dados dos últimos sete dias. Ele é executado semanalmente e extrai todos os resultados de testes, que não são aprovados.

Regras de pesquisa de IC para identificar ICs de Microsoft Defender for Cloud integrações

Quando os dados são importados de uma integração de terceiros, Conformidade de configurações usa automaticamente os dados de recursos para pesquisar correspondências em Configuration Management Database (CMDB), usando Regras de pesquisa de IC. Essas regras são usadas para identificar os itens de configuração (ICs) e adicioná-los ao registro de resultados de testes para ajudar na correção. As regras de pesquisa de IC do sistema base estão disponíveis para ID de recurso, Nome e Bucket S3. Para obter mais informações sobre regras de pesquisa de IC, consulte Regras de bloqueio de IC para Microsoft Defender for Cloud Integration for Security Operations.

Noções básicas sobre Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud

O Prisma Cloud é uma solução de segurança de infraestrutura em nuvem baseada em API. Ele se conecta ao seu ambiente de nuvem e monitora os recursos implantados nos ambientes de nuvem pública, como Amazon Web Services (AWS), Microsoft Azuree assim por diante. Você obtém visibilidade e controle completos sobre os riscos em sua infraestrutura de nuvem pública.

A aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud facilita a ingestão de políticas e alertas do Prisma Cloud, como testes e resultados de testes, respectivamente, na aplicação Conformidade de configurações. Com a configuração correta, os resultados de testes podem ser gerenciados perfeitamente, atribuindo-se pontuações de risco apropriadas e agrupando-as e atribuindo-as a usuários e grupos relevantes.

Versões disponíveis

A tabela lista as aplicações das quais Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud depende, junto com a versão da aplicação.

Aplicação	Versão
Prisma Cloud integration for Security Operations	2,3
Conformidade de configurações	14.7
Security Support Common	13,5
Resposta a vulnerabilidades	18,0

ServiceNow Integrações do Prisma Cloud

A aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud ajuda a importar os dados do Prisma para a instância ServiceNow para aprimorar a gestão da instância. Uma série de trabalhos agendados invoca as integrações automaticamente. Você também pode executar esses trabalhos agendados manualmente. Os trabalhos agendados simplificam o ciclo de vida de correção dos resultados de testes, mantendo a instância atualizada, recuperando dados periodicamente do Prisma Cloud.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As tarefas de integração do Prisma Cloud envolvem as funções a seguir.

- sn_vul_prismacloud.configure_integration: capacidade de ler, gravar e excluir registros.
- sn_vul_prismacloud.read_integration: capacidade de ler registros.

Exibição das integrações

Você pode exibir as integrações que fazem parte de Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud navegando até **Integração na nuvem do Prisma** > **Integrações**.

As seguintes integrações estão disponíveis no sistema de base.

Sequência de execução	Programação	Integração	Descrição
1	Semanalmente	Prisma Policy Integration	• Recupera políticas do Prisma Cloud e cria entradas de teste em sua instância. • Ele não fornece suporte incremental. Se você executar a integração nos últimos 10 dias, ele também mostrará o resultado das execuções de integração anteriores.
2	Diariamente	Prisma Alerts Integration	• Recupera alertas do Prisma Cloud e cria entradas de resultados de testes em sua instância. • Fornece suporte incremental. A integração é executada diariamente após o último tempo de execução de integração.

Preparando para instalar o Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud

Prepare-se para instalar o Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud executando as tarefas de configuração.

Antes de começar

Para integrar a Resposta a vulnerabilidades ao Palo Alto Prisma Cloud, você deve ser atribuído a um grupo de permissões no Prisma que forneça acesso somente leitura aos dados de políticas e alertas. Você pode encontrar mais informações sobre grupos de permissões em Funções de administrador do Prisma Cloud .

Para obter informações detalhadas sobre as funções atribuídas a diferentes grupos de permissões, consulte a página Prisma Cloud Administrator Permissões .

Além disso, as chaves de acesso devem ser criadas para habilitar a leitura dos alertas. Para obter mais informações sobre como criar chaves de acesso, consulte Criar e gerenciar chaves de acesso .

Para instalar e configurar o Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud, use a check-list a seguir. Antes de instalar a aplicação, verifique se os itens listados estão concluídos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL base da API • ID da chave de acesso • Chave secreta • Nome de usuário e senha para acessar o Prisma Cloud. Essas credenciais são usadas para se conectar à instância do Prisma Cloud a partir da instância Now Platform®. O ID da chave de acesso e a chave secreta devem ser gerados no portal do Prisma Cloud após o registro.
☐	Se ainda não estiver instalado e ativado, instale a aplicação Resposta a vulnerabilidades antes de instalar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 15.2.0 de Resposta a vulnerabilidades ou posterior.
☐	Se você ainda não tiver a aplicação em sua instância, obtenha direitos e baixe a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud para sua instância Now Platform®. Consulte .
☐	Certifique-se de ter instalado os seguintes plug-ins para uma execução de integração sem problemas: • Resposta a vulnerabilidades • Conformidade de configurações • Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud Os plug-ins a seguir são opcionais, mas podem ser úteis: • Cloud Provisioning and Governance • Padrões de descoberta e mapeamento de serviços
☐	Estime o número de resultados de testes que você espera importar. Verifique se sua instância pode aceitar o número de resultados de testes que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow Suporte técnico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem um administrador para gerenciar as integrações e corrigir os resultados de testes: O administrador instala a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções.

Você está pronto para Instalar e configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud.

Instalar e configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud

Instale a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud para usar os dados importados do Prisma Cloud. Use esses dados para priorizar e corrigir erros de configuração em seus ativos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Plug-ins**.
2. Na barra de pesquisa, pesquise `Integração de resposta a vulnerabilidades com Palo Alto Prisma Cloud`.
3. Clique em **Instalar**.

   Todas as dependências que serão instaladas são exibidas.
4. Navegar até **Todos** > **Integração na nuvem do Prisma** > **Administração** > **Configuração** > **Configuração do Prisma Cloud**.
5. No formulário, preencha os campos.

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL da API	URL para integração com o Prisma Cloud.
ID da chave de acesso	Chave exclusiva para autenticar a solicitação de acesso ao Prisma Cloud. **Nota:** Você deve gerar a chave após fazer login no portal do Prisma Cloud.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Chave secreta	Chave privada para autenticar a solicitação de acesso ao Prisma Cloud. **Nota:** Você deve gerar a chave secreta após fazer login no portal do Prisma Cloud.

6. Clique **em Salvar e testar**.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Integração na nuvem do Prisma** > **Configuração** para continuar com a configuração.

Configurar a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud

Configure a aplicação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud. Use os dados importados do Prisma Cloud para priorizar e corrigir erros de configuração em seus ativos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Integração na nuvem do Prisma** > **Configuração**.
2. No formulário, preencha os campos.

Configuração do Prisma Cloud

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL da API	URL para integração com o Prisma Cloud.
ID da chave de acesso	Uma chave exclusiva para autenticar a solicitação de acesso ao Prisma Cloud. Você deve gerar a chave após fazer login no portal do Prisma Cloud.
Chave secreta	Uma chave privada para autenticar a solicitação de acesso ao Prisma Cloud. Você deve gerar a chave secreta após fazer login no portal do Prisma Cloud.

3. Clique **em Salvar e testar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de concluir a configuração, navegue até **Integração na nuvem do Prisma** > **Integrações** para verificar se a execução da integração foi bem-sucedida.

Verifique o status de execução de importação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud

Use o status de execução de importação Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud para verificar o sucesso das execuções de integração e identificar quaisquer problemas.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 14.8.5 do Conformidade de configurações, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Integração na nuvem do Prisma** > **Integrações**.
2. Clique **em Integração de políticas do Prisma**.
3. Clique em **Executar Agora**.
   Quando esta integração é executada, as seguintes tabelas são preenchidas nesta ordem:
   a. sn_vulc_test.list (Testes de configuração)
   b. sn_vulc_auth_src (origem autorizada
   c. sn_vulc_citation (citações)
4. Na guia **Itens**, exiba o número de novos testes criados, atualizados e ignorados clicando na execução da integração de vulnerabilidade.

Nota: As políticas são definidas no Prisma Cloud para a instância de nuvem selecionada. A instância é verificada com base nas políticas definidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique **em Prisma Alerts Integration**.
6. Clique em **Executar Agora**.
   As seguintes tabelas são preenchidas com base na integração:
   - Resultados de testes
   - Itens descobertos: se os itens de configuração não estiverem disponíveis no sistema, eles serão criados. A classe é sempre Recurso de nuvem. Na página Item descoberto, três novos campos são criados: **Tipo de recursoem nuvem , Provedor de serviço em nuvem**e **Categoria de ativo**.

     Na guia **Itens**, clique na execução de integração de vulnerabilidade para exibir o número de novos resultados de testes importados, atualizados e ignorados. A guia **Itens de configuração** também é preenchida com base no número de resultados de testes criados.

Mapeamento de dados

Os dados do Prisma Cloud são importados no módulo Conformidade de configuraçõesServiceNow da instância [].

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Os dados do Prisma Cloud são importados com um nome diferente em Conformidade de configurações, conforme mencionado na tabela.

Mapeamento de dados do Prisma Cloud no Configuration Compliance

Prisma Cloud	Conformidade de configurações
Política	Teste
Alerta	Resultado do teste
Padrão de conformidade	Fonte autorizada
Seções	Citação
Ativo	Item da Descoberta/Item de configuração (IC)

Testes

Uma política no Prisma Cloud é importada como um teste em Conformidade de configurações. As políticas estão relacionadas a documentos oficiais e registros de teste e podem ser modificadas para atender às necessidades da sua organização. Você pode exibir os testes navegando até **Conformidade de configurações** > **Testes**.

Se **a integração da Resposta a vulnerabilidades com o Palo Alto Prisma Cloud** estiver instalada, o trabalho de integração *`Prisma Policy Integration`* recuperará os testes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir este trabalho de integração navegando até **Todos** > **Integrações do Prisma Cloud** > **Prisma Policy Integration**.

Resultados de testes

Um alerta no Prisma Cloud é importado como um resultado de teste em Conformidade de configurações. Os alertas são corrigidos usando **Tarefas**de correção . Você pode exibir os resultados de testes navegando até **Conformidade de configurações** > **Resultados de testes**.

O Conformidade de configurações importa resultados de testes como parte de uma integração de terceiros. Depois que estiverem visíveis na aplicação Conformidade de configurações, eles serão corrigidos usando as Tarefas de correção.

Se **a Integração de resposta a vulnerabilidades com o Palo Alto Prisma Cloud** estiver instalada, o trabalho de integração **Integração de alertas do Prisma** recuperará os resultados de testes. Você pode exibir este trabalho de integração navegando até **Todos** > **Integração na nuvem do Prisma** > **Integrações** > **Prisma Alert Integration**.

A **Integração de alertas do Prisma** é um trabalho de integração que é executado diariamente e extrai os resultados de testes com mudança de status após a hora definida no campo **Hora** de início na guia **Integração**.

Nota: Se você executar o trabalho de integração, **Prisma Alert Integration** manualmente, execute-o depois de executar o trabalho de integração, **Prisma Policy Integration**.

Quando a **Integração do alerta do Prisma** conclui a importação dos dados, um evento é iniciado para acionar os cálculos de fim da importação. Se o alerta falhar continuamente nos últimos dias, a integração não buscará os alertas, pois não há mudança de status para o alerta. Portanto, para manter os dados de resultados de testes atualizados com os alertas do Prisma, um novo trabalho de integração, **Integração de alerta abrangente do Prisma**, foi adicionado, o que extrai os alertas atualizados nos últimos sete dias. Ele é executado semanalmente e extrai todos os resultados de testes, que não foram aprovados.

Fontes Autorizadas

Conformidade de configurações usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente mapeiam para seções de padrões publicados do setor, como ISO 27001 e PCI DSS 3.2.1.

Esses registros de origem contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas na área de segurança de computadores. As referências definem requisitos para políticas e procedimentos de segurança. Navegar até **Conformidade de configurações** > **Fontes Autorizadas** para exibir as fontes autorizadas.

Ativos

Se o Integração de Resposta a vulnerabilidades com Palo Alto Prisma Cloud estiver instalado, o trabalho agendado *`Prisma Alerts Integration`* capturará as informações relacionadas ao alerta no módulo ou na tabela Itens descobertos. Você pode exibir este trabalho agendado navegando até **Integração na nuvem do Prisma** > **Integrações**.

A integração do Prisma Alerts importa tipos adicionais de informações, como marcadores de recursos e atributos de nuvem que são armazenados em tabelas. Essas informações são exibidas no formulário Itens descobertos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marcadores de host: um recurso pode ter vários marcadores. Os marcadores de host estão disponíveis no formato de par de chave-valor. Por exemplo, o sistema operacional é o Windows 10 e a versão do Java é 1.8.
- Atributos de nuvem para ativos: os seguintes atributos de nuvem estão disponíveis:
  - Conta em nuvem: fornece o ID da conta da integração. As informações são preenchidas a partir da tabela Contas de nuvem [sn_sec_cmn_cloud_account.LIST].
  - Região da nuvem: fornece o local onde o recurso foi hospedado. As informações são preenchidas a partir da tabela Regiões de nuvem [sn_sec_cmn_region.LIST].
  - Tipo de recurso de nuvem: fornece informações sobre o tipo de recurso, por exemplo, se é uma máquina virtual ou uma instância de banco de dados e assim por diante. As informações são preenchidas a partir da tabela Tipo de recurso de nuvem [sn_sec_cmn_cloud_resource_type.LIST].
  - Provedor de serviços em nuvem: fornece informações sobre o provedor de serviços em nuvem, seja Amazon Web Services (AWS), Oracle Cloud e assim por diante. As informações são preenchidas a partir da tabela Provedor de serviços em nuvem [sn_sec_cmn_cloud_service_provider.LIST].
  - Grupos de contas em nuvem: fornece informações sobre os grupos de contas. As informações são preenchidas a partir da tabela Grupos de contas de nuvem [sn_vul_prismacloud_account_group.list].

    Nota: O atributo Grupos de contas em nuvem está disponível somente para o Prisma.

Regras de pesquisa de IC

As regras de pesquisa de IC do sistema de base estão disponíveis para ID de recurso, Nome e Bucket S3. Para obter mais informações sobre as regras de pesquisa de IC, consulte Regras de pesquisa de IC para Microsoft Defender for Cloud Integration para Operações de segurança e Palo Alto Prisma Cloud.

Mensagens de REST do Prisma Cloud

As mensagens REST do Prisma são usadas para fazer chamadas para a Interface de programação de aplicações (API) do Prisma para buscar os dados de conformidade.

As seguintes mensagens de REST são enviadas com o sistema de base.

Integrações do Prisma Cloud

Todas as integrações do Prisma Cloud usam o JSON Web Token (JWT) para autenticação e autorização.

Mensagem REST de login do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/login	Obtém o token JWT para uso em todas as integrações subsequentes.	*POST*	`{ "username": <<access key id >>, "password": <<secret`	https://pan.dev/prisma-cloud/api/cspm/app-login/

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem REST de login do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
			access key>>}	

Mensagem REST do token de atualização do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/auth_token/extend	Renova automaticamente o token JWT na expiração. A duração padrão da expiração do token é de 60 minutos.	*GET*	N/D	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Mensagem REST da política do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/v2/política	Recupera todos os dados de política do Prisma.	*GET*	N/D	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Mensagem de REST de alerta do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/v2/alerta	Recupera todos os alertas do Prisma.	*POST*	{ "detailed": "false", "filters": [{ "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED" }], "sortBy": ["resource.id"], "pageToken": "", "offset": 0, "limit": 2000, "timeRange": { "type": "absolute", "value": {	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem de REST de alerta do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
			"startTime": <<Import since at integration level>>, "endTime": << Current integration run time>> } } }	

Para a integração do Alerta de compreensão do Prisma, os filtros no corpo POST acima devem ser substituídos da seguinte forma:

```
"filters": [
 {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "open"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "dismissed"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "snoozed"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "pending_resolution"
                },
                {
                    "name": "timeRange.type",
                    "operator": "=",
                    "value": "ALERT_UPDATED"
                }

    ],
```

Qualys integração com Conformidade de configurações

A Qualys Política de Conformidade coleta os dados e os envia automaticamente para a aplicação Qualys, que analisa e correlaciona continuamente as informações. Ele se integra facilmente como a Integração da Qualys para Operações de segurança para mapear descobertas de configuração para ICs e serviços de negócio para determinar o impacto e a prioridade de possíveis erros de configuração.

Se você tiver várias implantações da aplicação Qualys Cloud Platform, poderá adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de terceiros e suas vulnerabilidades, são consolidados e reconciliados com o seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados obtidos de cada implantação são identificados e estão disponíveis em uma única instância de Resposta a vulnerabilidades.

Nota: Você não pode excluir a integração de vulnerabilidade original, mas pode desativá-la. As integrações criadas a partir de modelos inativos são desabilitadas por padrão.

Marcadores de host

Todos os marcadores de host são importados como parte da integração Qualys de lista de hosts. Os marcadores de host são usados principalmente para filtragem em Resposta a vulnerabilidades Regras de grupo de atribuição e vulnerabilidade. Eles são exibidos no formulário Item descoberto.

Nota: A integração Qualys da lista de hosts deve ser executada antes de criar as regras de atribuição ou de tarefa de correção em Resposta a vulnerabilidades para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Se um marcador **San Diego** for criado, um marcador **SAN DIEGO** não poderá ser armazenado na tabela de marcadores do host. “San Diego” e “SAN DIEGO” são considerados o mesmo marcador de host. O marcador que foi importado primeiro vence.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condições.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags**. Esta propriedade é definida como verdadeira por padrão. A desativação dos marcadores os desativa em todas as instâncias.

As etiquetas de host (também chamadas de etiquetas do ativo) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos ativos do host. Em seguida, ao iniciar verificações, você pode selecionar marcadores associados aos hosts que deseja verificar. O módulo Marcadores de host permite que você baixe dados de marcador de host de Qualys para sua instância de forma programada.

Integrando Qualys com a aplicação ServiceNow® Conformidade de configurações

Se o Qualys Vulnerability Integration já estiver instalado no seu sistema e suas credenciais de API forem diferentes daquelas que você deseja usar para Conformidade de configurações, vá para o Assistente de configuração (em Resposta a vulnerabilidades) e atribua-as a cada integração de **PC da Qualys**.

Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** e edite o campo **Credenciais de API** da **Qualys na guia Detalhes de REST** da Qualys.

Configurar os parâmetros de PCRS

A partir da v12.6.3 de Integração Qualys para Operações de segurança, você pode usar a integração de host de política da Qualys PCRS e a integração de resultados de testes de PCRS da Qualys para importar resultados de testes com novos conjuntos de Qualys APIs. Essas integrações precisam de um URL de gateway para buscar informações de Qualys.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Ao instalar o Integração Qualys para Operações de segurança para Resposta a vulnerabilidades, você pode configurar o **gateway_url** para as novas integrações de PCRS em Conformidade de configurações. Para obter mais informações sobre como encontrar a URL do gateway para a URL da API, consulte Identificar sua plataforma Qualys .

O URL do gateway deve ser adicionado à sua instância ServiceNow.

Procedimento
1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.

   Nota: Certifique-se de que o escopo em que você está seja Qualys for Security Operations.

2. Abra a instância que é usada pelas integrações de PCRS.
3. Na guia Parâmetros de instância de integração, adicione a URL do gateway para a configuração **gateway_url**.

   Nota: A integração de resultados de testes de PCRS da Qualys depende da integração de host da política de PCRS da Qualys. Portanto, se você retroceder os Resultados de testes de integração Qualys PCRS, talvez precise executá-los na mesma ordem novamente.

Componentes instalados com o Qualys Integration for Security Operations
As seguintes funções, trabalhos agendados e tabelas são instalados com a Integração da Qualys para Operações de segurança.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Exibir listas filtradas de componentes instalados com uma aplicação
Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos agendados e as tabelas instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Resposta a vulnerabilidades**.
3. No Construtor de condições, para adicionar um segundo filtro, selecione **AND e**, em seguida, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, Trabalho **agendado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_vul_qualys.read	Tem acesso de leitura aos registros Qualys Vulnerability Integration.	
sn_vul_qualys.usuário	Usuário para Qualys Vulnerability Integration. Pode ler e gravar registros	sn_vul_qualys.read
sn_vul_qualys.admin	Administrador paraQualys Vulnerability Integration. Por exemplo, você pode modificar as datas de início da integração e executar algumas definições de configuração avançadas.	• sn_vul_qualys.usuário • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Pode configurar o Qualys Vulnerability Integration	sn_vul_qualys.admin

Trabalhos agendados instalados

Trabalho agendado	Descrição
Qualys Políticas de PC	Recupera políticas de Qualys. A saída é armazenada na tabela sn_vulc_policy. A API usada nesta integração não é compatível com paginação, portanto, todas as políticas são baixadas em uma única página.
Qualys Detalhe das políticas de PC	Recupera os detalhes completos da política, como tecnologias e seções, por exemplo.
Qualys Controles do PC	Recupera informações de controles de conformidade para diferentes IDs de controle de Qualys.
Qualys Resultados de PC	Recupera registros de postura de conformidade de Qualys. A saída desta integração são os Resultados de testes. Por padrão, os detalhes do parâmetro são passados para importar informações do host, datas/horas da última verificação, ID de controle e informações de evidências.
Qualys Resultados abrangentes de PC	Recupera registros de postura de conformidade de Qualys com base na data da última avaliação dos resultados de testes que não foram aprovados. Este trabalho é executado uma vez por semana. A saída desta integração são os resultados de testes. Por padrão, os detalhes do

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Descrição
	parâmetro são passados para importar as informações do host, datas/horas das últimas verificações, ID de controle e informações de evidência.
Qualys Integração de host de política de PCRS	Recupera dados do host de Qualys e os processa em sua instância. A saída desta integração são IDs de host de política. Os dados Qualys do host são importados nesta integração. **Nota:** • Este trabalho agendado aparece somente quando Conformidade de configurações está instalado. • Configure os parâmetros de instância de integração gateway_url e pcrs_page_size antes de executar esta integração. Essas duas integrações ficarão OOB inativas. Se você ativar qualquer uma dessas integrações, as integrações de resultados do PC serão desativadas. Essas duas integrações são adicionadas com base nas novas APIs de streaming da Qualys.
Qualys Integração de resultados de testes de PCRS	Recupera os resultados de testes para cada ID de host. Esta integração usa o parâmetro Hora de início na guia Detalhes da integração. **Nota:** • Este trabalho agendado aparece somente quando Conformidade de configurações está instalado. • Configure os parâmetros de instância de integração gateway_url e pcrs_page_size antes de executar esta integração. • Se você optar por executar a integração manualmente, execute Qualys Integração de resultados de testes de PCRS após Qualys Políticas de PC, Qualys Detalhe de políticas de PC e Qualys Integração de host de política de PCRS.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As integrações Qualys de host de política de PCRS e Qualys de resultados de testes de PCRS estão inativas por padrão. Essas duas integrações são baseadas nas novas APIs de streaming de Qualys. Se você ativar qualquer uma dessas integrações, a integração de resultados do PC será desativada e vice-versa.

Tabelas instaladas

Tabela	Descrição
Qualys Importação de resultado de PC sn_vul_qualys_pc_result_import	Tabela que estende a linha do conjunto de importação. A transformação de mapas de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Id de host de política sn_vul_qualys_policy_host_id	Tabela que armazena o mapeamento entre a política e o host para o qual esta política foi verificada. Esta tabela é usada na nova integração Qualys de PCRS. **Nota:** Esta tabela é exibida somente quando Conformidade de configurações está instalado.
Qualys Importação de host de política de PCRS sn_vul_qualys_pcrs_policy_host_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete. **Nota:** Esta tabela aparece somente quando Conformidade de configurações está instalado.
Qualys Importação de política do PC sn_vul_qualys_pc_policy_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.

Atualizar itens de configuração com o identificador de partição de rede para a integração da Qualys

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão na aplicação Resposta a vulnerabilidades, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas são armazenados como um IC no seu CMDB.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC `(IC 1)` durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_ID	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	REPOSITORY_ID	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. A partir de uma nova importação de dados, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para as integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

A partir da v14.0 de Resposta a vulnerabilidades e v12.1 da Integração de vulnerabilidade Qualys Vulnerability Integration, os Modelos de classe de IC do CMDB (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

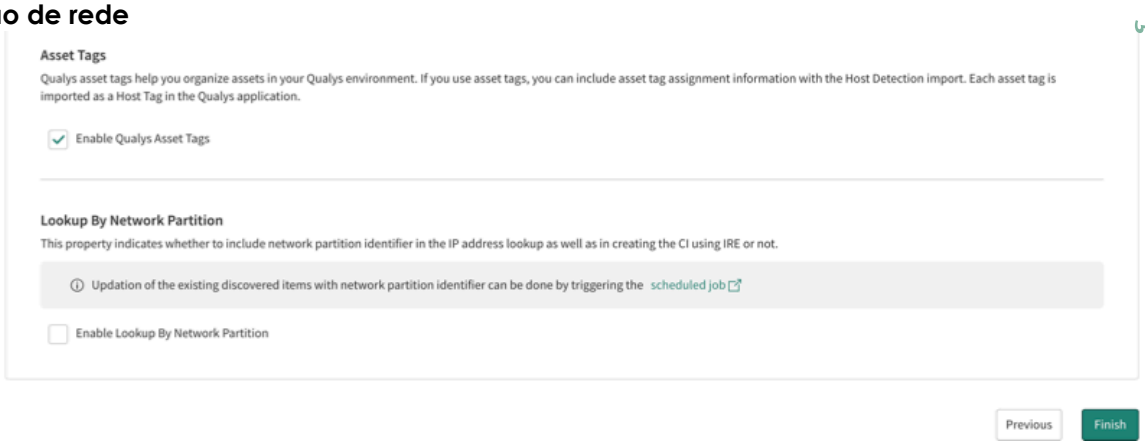
Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. Os ICs dos dados Qualys Vulnerability Integration existentes são criados ou atualizados para incluir a granularidade do identificador de partição de rede. Itens descobertos, itens

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	vulneráveis e registros de detecção são todos atualizados com os novos ICs.
Aguarde as importações de novos dados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo trabalho agendado. IC, item vulnerável e registros de detecção são todos atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Escolha Qualys Vulnerability Integration.
3. **Edite** a integração necessária.
4. Escolher **Configuração de Detecção de Host**.
5. Escolher **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede**



seção.

6. Clique em **Concluir**.

Identificadores de partição de rede NETWORK_ID e REPOSITORY _ID incluídos na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

As regras de pesquisa de identificação de IC de endereço IP e endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration.

Depois de ativar o trabalho agendado e salvar os registros, você pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando trabalhos agendados sob demanda. Os ICs em seu item descoberto existente, item vulnerável e registros de detecção são atualizados automaticamente.

Definir parâmetros de filtro adicionais para Qualys importações

Personalize os parâmetros de filtragem das suas consultas programadas com Qualys Vulnerability Integration para ajudá-lo a refinar ainda mais os dados de vulnerabilidade importados com as integrações Qualys compatíveis.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para que você possa revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por IPs ou intervalos de IP específicos. Ou você deseja importar somente máquinas que estão no seu escopo, por exemplo, somente máquinas em sua rede corporativa que não sejam dispositivos externos.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros Qualys para ajudá-lo a importar os detalhes específicos da vulnerabilidade necessários.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com Qualys parâmetros em seu Now Platform. Você modifica ou adiciona esses valores ao registro do método HTTP no método REST para as integrações Qualys compatíveis do Qualys Vulnerability Integration.

Função necessária: sn_vul.vulnerability_admin

Procedimento

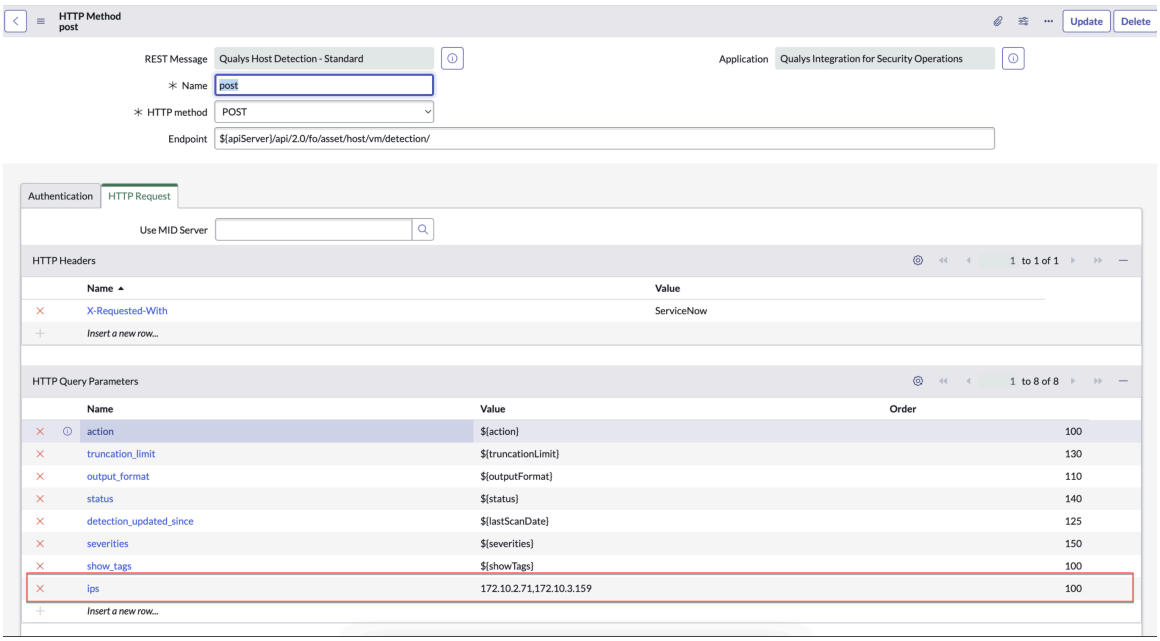
1. Localize os parâmetros compatíveis com o produto Qualys no site do desenvolvedor que você deseja usar para a filtragem.
   Os parâmetros e valores inseridos no produto Qualys são compatíveis somente no nível da instância de integração em seu Now Platform. Todas as Qualys integrações oferecem suporte à filtragem usando parâmetros de consulta.
2. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na página da lista de integrações Qualys, clique no registro da integração que você deseja abrir.
4. Com a guia Qualys Detalhes de REST selecionada, localize e clique no ícone de informações (I) do método REST, seguido por **Abrir registro** para abrir o registro do método HTTP.
5. Selecione a guia **Solicitação HTTP**.
6. Em Parâmetros de consulta HTTP do corpo da solicitação, adicione os valores obtidos do site do desenvolvedor Qualys.

   Na imagem a seguir, como exemplo, o parâmetro que ingere somente determinados endereços/intervalos IP, *ips={value}* foi adicionado. Nesse caso, o **valor** é um ou mais IPs/intervalos especificados por você. Várias entradas são separadas por vírgulas, `172.10.2.71, 172.10.3.159`, e um intervalo é especificado com um hífen, `10.10.10.1-10.10.10.100`. Consulte o site do desenvolvedor Qualys para obter mais informações.



   Se você quiser inserir mais de um parâmetro, consulte a documentação Qualys para obter mais informações sobre como separar cada valor.

   Nota: Você deve estar ciente de seus requisitos de API. Pode ser necessário adicionar essas propriedades de API aos Parâmetros de consulta ou ao conteúdo do corpo.

   Alguns outros parâmetros que podem ser úteis no site do desenvolvedor Qualys :

   - *ag_ids* - IDs da lista do grupo de ativos a serem recuperados. Este parâmetro garante que somente máquinas no seu escopo sejam trazidas.
   - *qids* - Este parâmetro limita os resultados a somente determinadas vulnerabilidades (QID na tabela Entrada de terceiros). Esta configuração evita que o sistema seja inundado com registros informativos.
7. Clique em **Atualizar**.

Resolvendo Qualys problemas de integração de vulnerabilidade

Alguns problemas comumente encontrados, junto com as soluções alternativas, são discutidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anexos não aparecem após a importação

Se os anexos não estiverem aparecendo conforme o esperado para as fontes de dados ou em um incidente de segurança após as importações de integração de terceiros, verifique as restrições de IP.

As restrições de acesso por IP podem impedir que os anexos sejam vistos, a menos que você esteja conectado a partir de um IP seguro. Como um novo anexo é adicionado a cada importação, isso pode resultar em duplicatas que você precisa remover.

Por exemplo, ao executar uma integração de importação de host de terceiros, se você não vir nenhum anexo em suas fontes de dados, verifique as restrições de IP e adicione usuários à lista segura antes da importação.

Modificar mapas de transformação

Mapas de transformação são fornecidos com configurações de base e geralmente são suficientes. Você pode modificar mapeamentos de transformação dependendo das necessidades da sua organização.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin + import_admin

Procedimento

1. Navegar até **Todos** > **Conjuntos para importação do sistema** > **Administração** > **Mapas de transformação** para exibir as mensagens de REST.
2. Filtre a lista resultante por aplicação e limite a lista à aplicação **Qualys Vulnerability Integration**.
3. Modifique os mapas de transformação de acordo com os requisitos do cliente.

   Para obter detalhes sobre os dados fornecidos pela API da Qualys, consulte a documentação da API da Qualys .

Verificar o tamanho da propriedade de anexo XML

Verifica se a propriedade de anexo XML é suficiente para arquivos grandes.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Propriedades do sistema** > **Importação/Exportação**.
2. Role para baixo até **Propriedades de importação** > **Formato XML** na parte inferior da página.

3. Se necessário, altere o valor para 250 e clique em **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Propriedades do sistema disponíveis

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados da Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa gravidade que um cliente não está disposto a corrigir usando o processo de resposta a vulnerabilidades. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection – Standard/post**. Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método post com os seguintes valores:

- Nome: gravidades
- Valor: 3-5 (ou qualquer gravidade apropriada desejada)

A integração da base de conhecimento da Qualys está falhando

Resolva Qualys falha de integração da base de conhecimento reduzindo o tamanho do anexo de carga recebido de Qualys para o limite especificado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Certifique-se de que o tamanho do anexo de carga esteja dentro do limite especificado.
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   b. Selecione a guia **Parâmetros de instância de integração**.
   c. Selecione **max_delta_days** e modifique o valor padrão para 3.
2. Se a integração ainda falhar, execute as seguintes etapas:
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias**.
   b. Selecione **Base de conhecimento da Qualys**.
   c. Selecione a guia **Detalhes da integração**.
   d. No campo **Hora** de início, selecione a data atual para ignorar a execução da execução desse dia.
   e. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   f. Selecione a guia **Parâmetros de instância de integração**.
   g. Selecione **kb_backfill_full_import** e modifique o valor padrão para verdadeiro.

Resultados

A execução da integração de preenchimento da base de conhecimento da Qualys atualiza todas as entradas de terceiros (TPEs) no sistema. Enquanto a integração de detecção de host da Qualys cria uma entrada de espaço reservado, a integração de preenchimento da base de conhecimento da Qualys a atualiza.

Qualys gráfico de status de execução de integração

O módulo Qualys Status de execução de integração é uma exibição gráfica do status de Qualys execuções de integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir o status das execuções de integração, navegue até **Integração de Vulnerabilidade da Qualys** > **Status da Execução da Integração**.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

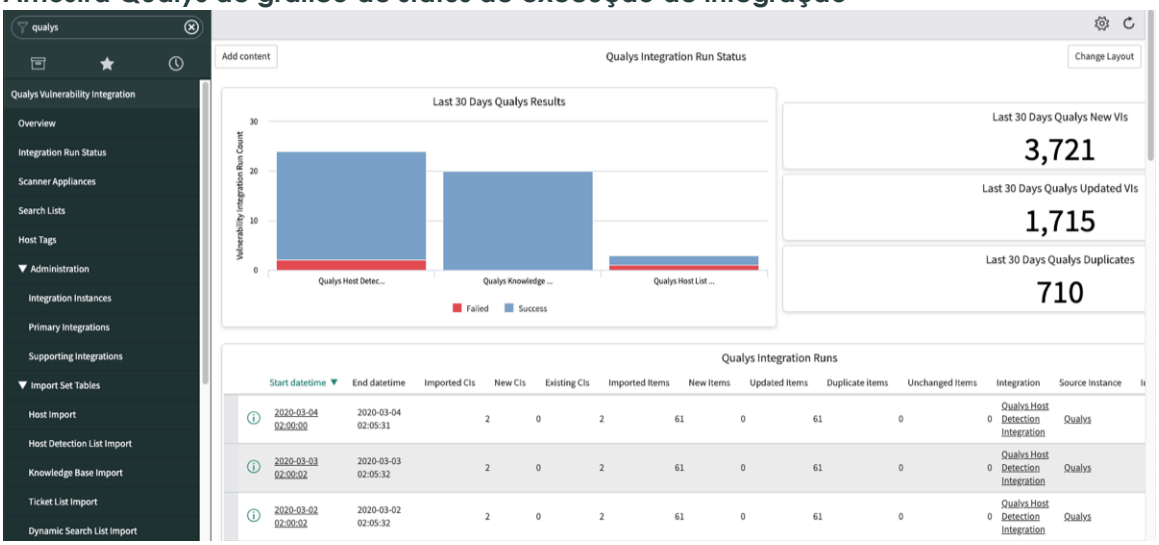
Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

O Qualys Status de execução de integração exibe o status de execução da integração de vulnerabilidades nos últimos 30 dias. A contagem de IVs atualizados da Qualys[qualys] indica a contagem de detecções exclusivas no mesmo ativo. O VI é atualizado com a nova detecção.

Nota: A contagem de execuções de integração de vulnerabilidade é exibida somente para as integrações, que estão definidas para o estado ativo. Navegar até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias** e defina o estado como ativo.

Amostra Qualys de gráfico de status de execução de integração



- Os valores na coluna Itens importados representam o número total de registros que são criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de registros que são criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que os registros são atualizados durante uma execução de integração. Este valor não é o número de registros exclusivos que são atualizados. Se, por exemplo, um registro for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como 2 itens atualizados.
- A coluna Itens inalterados exibe registros encontrados durante a execução de integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campos relevantes foi alterado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A integração é executada sem resultados para todos os quatro dos seguintes valores: **Novos ICs**, **ICs existentes**, **Novos itens**e **Itens atualizados** são filtrados da lista de execuções de **integração da Qualys**.

Qualys relatórios de gráfico de status de execução de integração

Nome	Descrição
Resultados dos últimos 30 dias Qualys	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Qualys Novos IVs	O número de novos registros importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys VIs atualizados	O número de registros atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys duplicados	O número de registros duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Qualys Execuções de integração	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções desta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na contagem de detecção ou descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem de data até" na instância, após a conclusão da execução da integração.
Últimos 30 dias Qualys Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparados nos últimos 30 dias.
Últimos 30 dias Qualys Taxa de transferência de desempenho de ingestão de item vulnerável	Taxa de transferência de ingestão de item vulnerável diária medida para a integração de detecção de host Qualys nos últimos 30 dias.

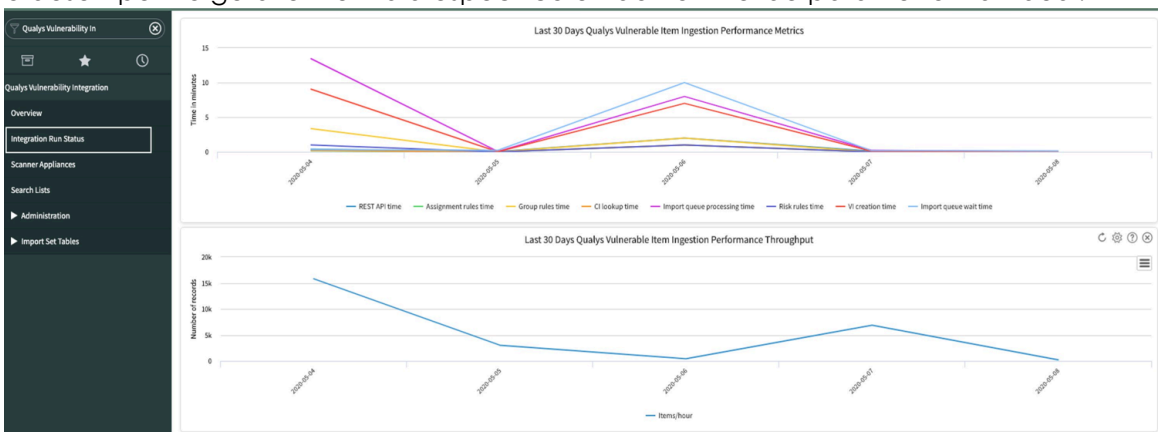
Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois gráficos comparam as métricas de desempenho:

- Qualys Métricas de desempenho de ingestão de itens vulneráveis: compare as métricas diárias de desempenho para regras de atribuição, regras de grupo, regras de risco, tempo de espera na fila, tempo de processamento da fila e outras estatísticas de itens vulneráveis nos últimos 30 dias para identificar a causa de quaisquer desvios no desempenho. O desempenho é calculado com base no tempo necessário para cada atividade. Esses parâmetros são calculados e associados no nível de execução da integração. Cada parâmetro é codificado por cores para facilitar a identificação.
- Qualys Rendimento de desempenho de ingestão de itens vulneráveis: compare o rendimento de ingestão de itens vulneráveis diários para a integração Qualys de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

detecção de host. O rendimento é medido em itens por hora. Este relatório mostra o desempenho geral em um dia específico e não no nível de parâmetro individual.



Mensagens REST da Qualys

As mensagens REST da Qualys são usadas para fazer chamadas para a APIda Qualys para buscar os dados de conformidade.

As seguintes mensagens REST são enviadas com o sistema de base.

Mensagem REST de políticas de PC da Qualys

A mensagem REST de políticas de PC da Qualys recupera dados de política da Qualys. As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações de política.

Parâmetros de mensagem REST de políticas de PC da Qualys

Nome do Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório.
detalhes	Todos	Indica o nível de detalhe mostrado para as políticas recuperadas. É seguro modificar de acordo com seus requisitos.

Mensagem REST de controles de PC da Qualys

A mensagem REST de Controles de PC da Qualys recupera informações de controles de conformidade para diferentes IDs de controle da Qualys.

Parâmetros de mensagem REST de controles de PC da Qualys

Nome do Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de controles de PC da Qualys

Nome do Parâmetro	Valor	Descrição
detalhes	Todos	Indica o nível de detalhe mostrado para os controles recuperados. É seguro modificar de acordo com seus requisitos.

Mensagem REST de detalhe das políticas de PC da Qualys

A mensagem REST de detalhes das políticas de PC da Qualys recupera os detalhes completos da política, como tecnologias e seções.

Parâmetros de mensagem REST de detalhe de políticas de PC da Qualys

Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação que está sendo solicitada. Parâmetro obrigatório.
mostrar_usuário_controles	Booliano	• Defina como 1 para incluir controles definidos pelo usuário (UDCs) na saída XML. • Quando não especificado, os UDCs não são incluídos. Este é um parâmetro opcional. É seguro modificar de acordo com seus requisitos.
mostrar_apêndice	Booliano	(Opcional) Defina como 1 para mostrar a seção do apêndice na saída XML. Quando não especificado.

Mensagem REST de resultados de PC da Qualys

A mensagem de descanso Resultados de PC da Qualys recupera registros de postura de conformidade da Qualys.

Parâmetros de mensagem REST de resultados de PC da Qualys

Campo de origem	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de resultados de PC da Qualys

Campo de origem	Valor	Descrição
mostrar_extended_evidence	Booliano	• Defina como 1 para mostrar as informações de evidência estendida na saída. • Definido como 0 ou quando não especificado, as informações de evidência estendida não são mostradas na saída. **Nota:** • Você não pode especificar `show_extended_evidence=1` na mesma solicitação que `hide_evidence=1`. Isso resulta em um erro. A evidência estendida faz parte dos dados de evidência e é mostrada somente quando os dados de evidência são mostrados. • Este parâmetro não é enviado com o sistema de base.
causa_de_falha	Booliano	Se você aprovar "1", a Qualys retornará a causa da falha. Se você passar '0', a Qualys não retornará esses atributos. **Nota:** Este parâmetro não é enviado com o sistema de base.
policy_id		Mostra registros de informações de postura de conformidade para uma política especificada. É necessário um ID de política válido.
detalhes	Todos	Indica o nível de detalhe mostrado para posturas recuperadas. É seguro modificar de acordo com seus requisitos.
mostrar_remediação_info		(Opcional) Defina como 1 para mostrar informações de correção na saída XML ou CSV. Por padrão, a saída não inclui as informações de correção. Quando não especificado, as informações de correção não são incluídas na saída.

Mensagem de REST de integração de host de política de PCRS da Qualys

A integração de host da política PCRS da Qualys recupera dados de host da Qualys e os processa em sua instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de integração de host de política de PCRS da Qualys

Nome do Parâmetro	Valor	Descrição
policyId	${lastRunDatetime}	IDs de política para avaliação de conformidade.

Integração de resultados de testes de PCRS da Qualys

A tabela mostra os parâmetros de solicitação que são enviados.

Parâmetros de mensagem REST de integração de resultados de testes de PCRS da Qualys

Nome do Parâmetro	Valor	Descrição
evidência necessária	${lastRunDatetime}	• O valor padrão é 0, o que indica que os dados de evidência não serão recuperados para a postura do host. • Defina o valor como 1 para recuperar os dados de evidência. **Nota:** Alterar o valor para 1 aumenta o tempo necessário para buscar dados de postura.
compactaçãonecessária		• O valor padrão é 1, o que indica que a saída será compactada. • Defina o valor como 0 se você não quiser que os dados sejam compactados. **Nota:** Não compactar os dados aumenta o tempo necessário para buscar dados de postura.

Noções básicas sobre a integração de vulnerabilidade da Tenable

A aplicação Integração de Resposta a vulnerabilidades com Tenable desenvolvida pela engenharia ServiceNow para a integração de vulnerabilidade da Tenable usa dados importados dos produtos Tenable.io e Tenable.sc para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. A aplicação está disponível com uma assinatura separada do ServiceNow® Store.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

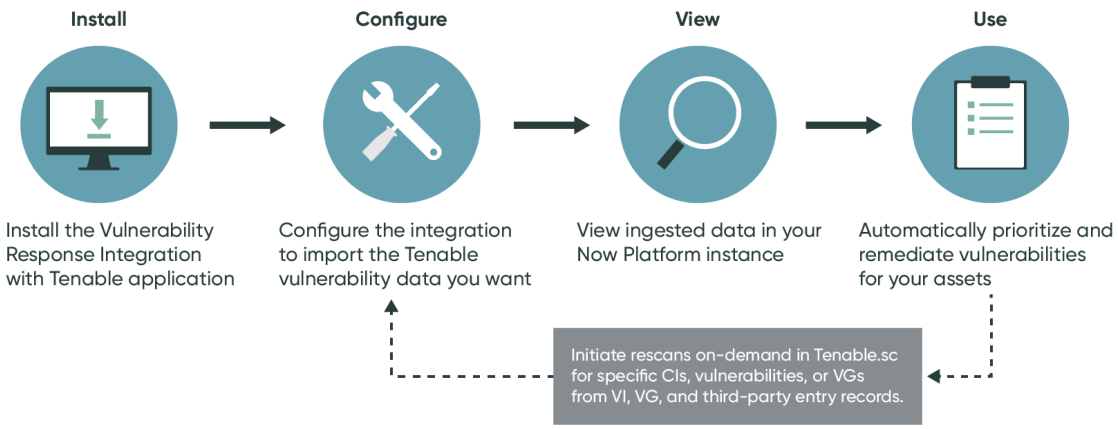
A integração de vulnerabilidade da Tenable emprega duas integrações da Tenable, Tenable.io e Tenable.sc, para importar dados de scanners de terceiros sobre seus ativos e vulnerabilidades. A aplicação Integração de Resposta a vulnerabilidades com Tenable é compatível com o produto Tenable.sc a partir da versão 5.13.

- Tenable.io é uma integração empresarial baseada na nuvem.
- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

A aplicação Integração de Resposta a vulnerabilidades com Tenable está disponível no ServiceNow Store com uma assinatura separada.

Para obter listas e descrições das integrações no Integrações de vulnerabilidade da Tenable, consulte Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações e Tenable.sc integrações com a aplicação Resposta a vulnerabilidades.

Integração de vulnerabilidade Tenable



Versões disponíveis para Xanadu

Versão de lançamento	Notas de versão
Integração de Resposta a vulnerabilidades com Tenable v3.5, v3.6	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado em sua instância Now Platform quando:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Uma vulnerabilidade importada de um scanner de terceiros é correspondida com um ativo existente (um item de configuração em seu CMDB). O produto da Tenable se refere a essas correspondências como **vulnerabilidades**.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente em seu CMDB. Nesse caso, um IC incompatível também é criado junto com um item vulnerável.

  Para ICs não correspondentes, você também pode usar o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido com um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatível. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação.

Entradas de vulnerabilidade e plug-ins de terceiros

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros e listadas na tabela Entradas de vulnerabilidade de terceiros na instância Now Platform. As entradas de vulnerabilidade de terceiros da Tenable são ingeridas em Resposta a vulnerabilidades e correspondidas aos ativos existentes listados em CMDB. A Tenable se refere às entradas de vulnerabilidade de terceiros como Plug- **ins**.

IC (Configuration Item, item de configuração)

Itens de configuração são os ativos existentes listados em seu CMDB.

Item descoberto

Os ativos ingeridos da importação de ativos da Tenable são correspondidos com os itens de configuração existentes em seu CMDB. Ativos importados são atualizados.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Se o plug-in Modelos de classe de IC do CMDB estiver habilitado, o Mecanismo de Identificação e Reconciliação (IRE) criará novos ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Resposta a vulnerabilidades usando o mecanismo de identificação e reconciliação. Se o IC original incompatível for reclassificado, os registros de itens descobertos serão atualizados para refletir o estado. Os itens descobertos dão visibilidade sobre como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados de uma integração de terceiros, a Resposta a vulnerabilidades usa automaticamente os dados do host (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). Regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de VI quando os IVs são criados para ajudá-lo na correção.

Nova verificação e verificação de correção

Você pode iniciar um comando de nova verificação direcionada em um item de configuração específico, tarefa de correção ou entrada de terceiro diretamente do item vulnerável, tarefa de correção e registros de entrada de vulnerabilidade de terceiros em sua instância Now Platform. A Tenable se refere a esta nova verificação como uma **verificação de correção**.

Fechar automaticamente IVs mais antigos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com o módulo de fechamento automático de itens vulneráveis obsoletos em seu Now Platform, você pode limpar itens vulneráveis (VI) obsoletos mais antigos que não foram encontrados recentemente por suas integrações de terceiros. Mover esses IVs para **Encerrado** ajuda a reduzir o número de itens vulneráveis ativos e tarefas de correção e reconciliar ativos em seu CMDB. Você pode usar todas as integrações com Integração de Resposta a vulnerabilidades com Tenable para fechar automaticamente IVs obsoletos.

Instância

Este termo se refere a uma ocorrência distinta da sua aplicação Now Platform®.

Integração

Uma integração é uma referência específica de produto a uma integração, como a Tenable.io Assets Integration, ou a Tenable.sc Plugin Integration. Essas são as integrações separadas que pertencem a produtos específicos da Tenable na integração de vulnerabilidade da Tenable em sua instância.

Instância de integração

Este termo se refere às integrações separadas da Tenable listadas por seus produtos Tenable.io e Tenable.sc.

Implantação

Quando uma integração oferece suporte a várias origens, uma existência de integração única e distinta é chamada de implantação da sua integração. O termo é usado para se referir à(s) integração(ões) e produto(s) em seu ambiente. Por exemplo, você pode ter várias implantações de várias integrações dos produtos Tenable.io e Tenable.sc em seu ambiente.

As integrações Tenable.io e Tenable.sc também incluem os seguintes recursos principais:

- As descobertas da avaliação de configuração, ou seja, resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas podem ser importadas para a aplicação Conformidade de configurações com o produto Tenable.io. Consulte Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações e Explorando Conformidade de configurações para obter mais informações sobre como essa integração funciona com a aplicação Conformidade de configurações.
- A partir da v2.1 do Integrações de vulnerabilidade da Tenable, crie itens de configuração (ICs) exclusivos que incluem diferentes identificadores de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. Identifique os ativos distintos em seu ambiente e atualize os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações Tenable.io e Tenable.sc. Você também pode executar trabalhos agendados manualmente sob demanda.
- Para importações de ativos com Tenable.io, você pode habilitar etiquetas do ativo para organizar e rastrear os ativos listados em seu ambiente CMDB no Tenable.io.
- As integrações Tenable.io e Tenable.sc permitem configurar regras de pesquisa de IC para definir como os dados de ativos de fontes de terceiros são usados para identificar itens de configuração (ICs) em seu Now Platform CMDB.
- As integrações Tenable.io e Tenable.sc permitem que você defina filtros de importação na importação de vulnerabilidades para importar somente as vulnerabilidades desejadas da Tenable. Para Tenable.io, você tem a opção de importar vulnerabilidades **fixas** da Tenable com a importação de vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para Tenable.sc, você tem a opção de iniciar novas verificações sob demanda diretamente do item vulnerável, da tarefa de correção e dos registros de entrada de terceiros em sua instância Now Platform. Se os IVs tiverem sido transicionados para **Encerrado/Corrigido**, mas ainda não estiverem atualizados em sua instância, você poderá verificar se as vulnerabilidades em itens de configuração específicos foram corrigidas. Consulte Iniciar nova verificação para a integração Tenable.sc.

As seções a seguir listam mais detalhes sobre as integrações da Tenable.

Funções necessárias de Now Platform

As tarefas de integração exigem as funções a seguir em sua instância Now Platform.

administrador

O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das integrações da Tenable no Assistente de configuração. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. O administrador de vulnerabilidades configura todas as aplicações e regras de VR para integrações de terceiros instaladas.

sn_vul_tenable.configure_integration

Essa função contém a função granular sn_vul_tenable.read_integration e os usuários com essa função podem configurar a aplicação Integração de Resposta a vulnerabilidades com Tenable.

sn_vul_tenable.read_integration

Usuários com essas funções podem exibir (ler), mas não editar registros da aplicação Integração de Resposta a vulnerabilidades com Tenable.

Grupo de Resposta a vulnerabilidades

Por padrão, o grupo de Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Itens vulneráveis

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de tarefa de correção e atribuídos para correção com base nas regras de atribuição. Para obter mais informações, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral e Resposta a vulnerabilidades visão geral das regras de atribuição.

Regras de pesquisa de item de configuração (IC)

As Regras de pesquisa de IC identificam ICs e determinam quando adicioná-los a um item vulnerável. Para obter mais informações sobre como as regras de pesquisa de IC funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Resposta a vulnerabilidades integrações de vulnerabilidade de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desabilite-as ao criar novas.

As regras de pesquisa Tenable.io a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nome do host
- DNS
- IP

As regras de pesquisa Tenable.sc a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Nota: Vários valores para ip_address, mac_address, fqdns e network_interfaces são usados para um ativo. Todos os valores são considerados nas regras de pesquisa de IC para correspondência. Todos os valores são usados para criar vários adaptadores de rede usando o IRE.

Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos em nuvem incompatíveis.

Novas propriedades para ignorar endereços IP

Em Tenable.io, há duas propriedades disponíveis se você quiser ignorar vários endereços IP ou vários endereços Mac como parte de suas regras de pesquisa de IC:

ignorarEndereçoIP

Uma lista de endereços IP a serem ignorados para pesquisa de IC e criação de IC.

ignoreMacAddress

Uma lista de endereços MAC a serem ignorados para pesquisa de IC ou criação de IC.

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação das integrações de itens vulneráveis da Tenable e das integrações de ativos da Tenable.

Nota: O filtro padrão para esta lista está definido como `Incompatível`. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter mais informações sobre o módulo Itens descobertos, consulte Itens Descobertos.

Etiquetas do ativo

As etiquetas do ativo (também chamadas de etiquetas de host) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Em seguida, ao iniciar verificações, você pode selecionar marcadores associados aos ativos que deseja verificar. O módulo Etiquetas do ativo permite que você baixe dados de etiqueta do ativo de Tenable.io para sua instância de forma programada. Os dados de ativos que incluem etiquetas de ativos são extraídos de Tenable.io e transformados usando os mapas de transformação de integração de transformação de ativo da Tenable.io.

Todas as etiquetas do ativo são importadas como parte da integração do ativo Tenable.io. As etiquetas do ativo geralmente são usadas para filtrar em Resposta a vulnerabilidades regras de atribuição e Regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Nota: Execute a integração de ativo Tenable.io antes de criar regras de atribuição Resposta a vulnerabilidades ou regras de tarefa de correção na aplicação Resposta a vulnerabilidades para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcadores não faz distinção entre maiúsculas e minúsculas. Por exemplo, se você criar um marcador para descrever ativos em seu local de San Diego e criar o marcador `San Diego`, também não poderá criar um marcador `SAN DIEGO` e armazená-lo na tabela de etiquetas do ativo. `San Diego` e `SAN DIEGO` são consideradas a mesma etiqueta do ativo pelo sistema. O marcador que for importado primeiro será o marcador armazenado e reconhecido daqui em diante.
- O uso de etiquetas do ativo como chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As etiquetas do ativo devem ser usadas somente no Construtor de condições.
- As etiquetas do ativo são controladas pela propriedade do sistema global sn_vul.import_asset_tags. Esta propriedade é definida como `verdadeira` por padrão. Desabilitar os marcadores os desabilita em todas as Now Platform® instâncias.

Filtros de recuperação de dados

As configurações de recuperação de dados ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da aplicação Tenable para sua instância Now Platform®. Para obter uma lista das configurações mais usadas, consulte Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable.

Classificação de prioridade de vulnerabilidade (VPR)

A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com uma nova calculadora de risco padrão em Resposta a vulnerabilidades. A Regra de risco da Tenable é instalada com a aplicação Integração de Resposta a vulnerabilidades com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade de Resposta a vulnerabilidades.

Esta regra de risco está desabilitada por padrão.

Ao habilitar a regra da calculadora de risco da Tenable, os valores de VPR importados são usados para calcular a pontuação de risco dos itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR = 70%, Ativo = 15% e Criticalidade dos negócios = 15%. Habilitar esta regra da Calculadora de risco da Tenable pode afetar o desempenho de ingestão de dados. Para obter mais informações sobre Resposta a vulnerabilidades calculadoras e a regra da calculadora de risco da Tenable, consulte Resposta a vulnerabilidades calculadoras e regras da calculadora de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalação e configuração

Depois de baixar o Integração de Resposta a vulnerabilidades com Tenable do ServiceNow® Store, a instalação e a configuração são compatíveis com o Assistente de configuração em Resposta a vulnerabilidades. Para obter mais informações, consulte Configuração de Resposta a vulnerabilidades usando o Assistente de configuração.

Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações

As integrações Integração de Resposta a vulnerabilidades com TenableTenable.io na aplicação [] estão disponíveis nas aplicações Resposta a vulnerabilidades e Conformidade de configurações.

Lista de Tenable.io integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente a partir do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura a aplicação Integração de Resposta a vulnerabilidades com Tenable no Assistente de configuração.

Tenable.io é uma integração empresarial baseada na nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com o produto Tenable.io.

A Tenable.io Integração de resultados de conformidade e a Tenable.io Integração de aterramento de resultados de conformidade estão inativas por padrão.

Para ativá-los:

1. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações da Tenable, clique no nome de uma integração para abrir o registro e marque a caixa de seleção **Ativo** para habilitá-lo. Você pode preferir deixar as configurações de programação em seus valores padrão para que essas integrações sejam iniciadas.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de ativos	• Recupera todos os dados de ativos, incluindo etiquetas de ativos, do produto Tenable.io e os processa em sua instância. • A partir da v3.0, se a integração de resultados de conformidade Tenable.io estiver ativada, você poderá importar dados de avaliação de configuração segura junto com os dados de ativos importados. Esses dados podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Coordena as chamadas de mensagem REST para a API de ativos. • A saída desta integração são itens descobertos. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. • A partir da v2.2, *Last Scan Time* é importado e atualizado somente para ativos que têm vulnerabilidades.
Tenable.io Integração de resultados de conformidade	• A partir da versão 3.0, os dados importados de avaliação de configuração segura da Integração de resultados de conformidade junto com os dados importados da Integração de ativos podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Se habilitado, recupera dados de avaliação de configuração segura de alto nível e os processa em sua instância Now Platform. Os dados importados incluem resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas. • Dados de avaliação para ativos ausentes ou ativos sem IDs de ativo não são importados. • Se um resultado de testes for importado e o ativo correspondente não puder ser correspondido em sua instância, o resultado do teste será ignorado e o ID do ativo ausente será armazenado em um registro temporário na tabela [sn_vul_tenable_missing_asset]. • O valor total de ativos ignorados (ausentes) é listado no campo **ICs ignorados** na guia **Configuração** no registro de execução de integração para esta integração.
Tenable.io Integração de preenchimento de resultados de conformidade	• Quando ativada, essa integração é executada automaticamente depois que a integração de ativos é concluída com sucesso como parte de uma execução de integração encadeada. Esta integração corresponde aos dados de avaliação de configuração com ativos ausentes listados na tabela [sn_vul_tenable_missing_asset]. • Importa até 200 IDs de ativo para todos os ativos ausentes descobertos ou presentes na instância após a conclusão bem-sucedida da importação de integração de ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Remove os registros temporários da tabela [sn_vul_tenable_missing_asset] quando os ativos podem ser correspondidos com os dados de avaliação de configuração correspondentes.
Tenable.io Verificar integração de credenciais	• Esta integração recupera as credenciais de verificação configuradas em Tenable.io. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential],. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.io Integração de modelo	Um registro de modelo é enviado para Tenable.io durante uma nova verificação. Esta integração recupera Tenable.io credenciais disponíveis para usar em novas verificações. As credenciais são específicas da instância e um único registro de modelo é importado e armazenado com segurança temporariamente na tabela [sn_vul_tenable_io_template].
Tenable.io Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.io. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma execução de integração Tenable.io. • Esta importação garante que os Tenable.io Identificadores (Dez IDs) sejam atuais. • Coordena as chamadas de mensagem REST para a API do plug-in. • A saída desta integração são vulnerabilidades de terceiros.
Tenable.io Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de gravidade do produto Tenable.io e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **fixas**, mas os itens vulneráveis não serão criados para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	detecções **fixas** por padrão, porque a Tenable considera as vulnerabilidades **fixas** como **mitigadas**. • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidade fixa** estiver ativado no Assistente de configuração, novos IVs serão criados no estado **Fixo** para que você tenha visibilidade sobre as detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem na sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. Esta execução de integração está programada. É uma integração em cadeia, o que significa que depois que uma execução é concluída com sucesso, a integração de vulnerabilidades aberta descrita abaixo é acionada. A partir do Tenable v3.3, você pode exibir as seguintes informações para as execuções de integração de vulnerabilidade: • **Total de blocos:** número total de blocos gerados pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow
Tenable.io Integração de vulnerabilidades abertas	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.io Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de gravidade do produto Tenable.io e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são Itens vulneráveis (IVs) **novos/reabertos**. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. A Tenable considera as vulnerabilidades ativas **cumulativas** (atuais). • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. A partir do Tenable v3.3, você pode exibir as seguintes informações para as execuções de integração de vulnerabilidade: • **Total de blocos:** número total de blocos gerados pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow

Tenable.sc integrações com a aplicação Resposta a vulnerabilidades

As Tenable.sc integrações na aplicação Integração de Resposta a vulnerabilidades com Tenable.

A partir de Resposta a vulnerabilidades v20.0, se um ativo for verificado por um agente, a coluna Agente existe exibirá o valor verdadeiro na lista Itens descobertos, o que indica que se trata de uma verificação autentica.

Lista de Tenable.sc integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente a partir do Assistente de configuração em Resposta a vulnerabilidades. Você também instala e configura a aplicação Integração de Resposta a vulnerabilidades com Tenable no Assistente de configuração.

- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de ativos	Para evitar a criação de itens descobertos duplicados com dados de ativos importados, a integração de ativos do produto Tenable.sc é composta por duas integrações. A Tenable.sc Integração de Ativos Abertos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Cumulativos** (atuais) ou **Abertos**. Os itens vulneráveis (IVs) criados em sua instância com esses dados de ativo importados são considerados abertos, ou seja, no estado **Aberto**. Esses itens vulneráveis requerem investigação e podem precisar de correção. A Tenable.sc integração de ativos fixos Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Mitigados** (não mais vulneráveis) ou **Corrigidos**. Os itens vulneráveis desses ativos fazem a transição do estado **Aberto** para o estado **Fechado/Corrigido** em sua instância, pois os resultados das verificações mostram que eles não estão mais vulneráveis. • Recupera todos os dados de ativos do produto Tenable.sc e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativos. • A saída desta integração são itens descobertos. • O filtro de consulta da Tenable selecionado no Assistente de configuração também se aplica à integração de ativos Tenable.sc. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.
Tenable.sc Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.sc. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma execução de integração Tenable.sc. • Esta importação garante que os Tenable.sc Identificadores (Dez IDs) sejam atuais e que somente as vulnerabilidades ativas sejam importadas. • Coordena as chamadas de mensagem REST para a API de plug-ins. • A saída desta integração são vulnerabilidades de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de gravidade do produto Tenable.sc e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pela Resposta a vulnerabilidades se as detecções forem **fixas**, mas os itens vulneráveis não serão criados para detecções **fixas** por padrão, porque a Tenable considera as vulnerabilidades **fixas** como **mitigadas**. • Quando o sinalizador **Criar tempos vulneráveis para detecções de vulnerabilidade fixa** é ativado no Assistente de configuração, ele cria novos IVs no estado **Fixo** para que você tenha visibilidade sobre as detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem na sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. Esta execução de integração é uma execução programada. É uma integração em cadeia, o que significa que, depois que uma execução é concluída com sucesso, a Tenable.sc Integração de vulnerabilidades abertas descrita abaixo é acionada. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de vulnerabilidades abertas	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.sc Integração de vulnerabilidades corrigidas. • Recupera dados de vulnerabilidade com base nos filtros de consulta selecionados no produto Tenable.sc e os processa em sua instância. • Cria itens vulneráveis correspondentes para vulnerabilidades ativas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	• Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é **Atualizar/Criar novos** itens vulneráveis (IVs), caso eles ainda não existam. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Verificar integração de credenciais	• Esta integração recupera as credenciais de verificação configuradas em Tenable.sc. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.sc Integração de vulnerabilidades de preenchimento	• Esta integração de aterramento importa todas as vulnerabilidades abertas e corrigidas que possam ter sido perdidas durante uma importação. • Esta integração importa vulnerabilidades abertas e corrigidas dos últimos sete dias para atualizar suas detecções e itens vulneráveis. • Esta integração pode afetar seu desempenho. • Esta integração está desabilitada por padrão. • Para atualizar seus dados de vulnerabilidade e evitar possíveis problemas de desempenho, talvez você prefira programar as Integrações de vulnerabilidades corrigidas e abertas do Tenable.sc para serem executadas quando nenhuma outra verificação estiver em execução. • A saída desta integração é:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	◦ Itens vulneráveis (IVs)**encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. ◦ para **atualizar/criar novos** itens vulneráveis (IVs) se eles ainda não existirem. Ele também cria itens de configuração e entradas de terceiros se eles não existirem.

Autenticação de usuário e Tenable.sc

A autenticação de usuário é compatível com sua instância Now Platform® e a versão 5.13 do produto Tenable.sc. A autenticação de usuário será necessária se você estiver usando a versão 5.12 e anterior do produto Tenable.sc.

Quando você seleciona a autenticação de usuário para as integrações Tenable.sc, os tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de Execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, `Erro: falha na validação de token`. Nenhuma ação será necessária se esta mensagem for exibida. Os tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro no processo de integração.

Preparação para a integração de vulnerabilidade da Tenable

Prepare-se para a integração de vulnerabilidade ServiceNow® da Tenable executando as seguintes tarefas de configuração.

Antes de começar

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Para uma instalação e configuração tranquilas da aplicação Integração de Resposta a vulnerabilidades com Tenable, talvez você prefira imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para sua instância Now Platform®.

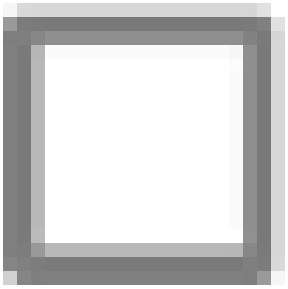
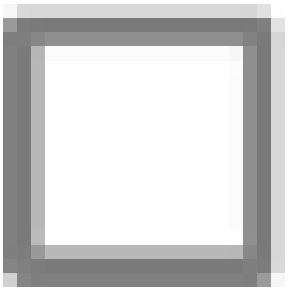
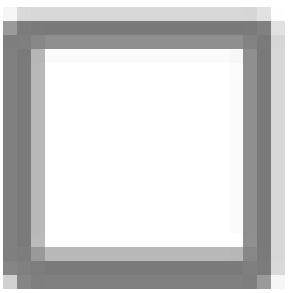
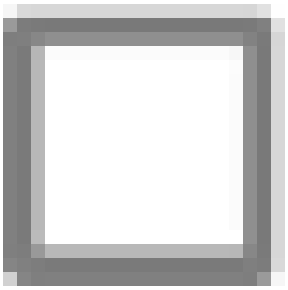
Nota: Se você estiver importando dados com a integração criada pela Tenable e quiser começar a usar a Integração de resposta a vulnerabilidades ServiceNow® com a Tenable, consulte

Para obter informações atuais de limpeza e migração de dados da integração criada pela Tenable para a integração criada por ServiceNow, consulte o artigo Diretrizes para migrar da Integração de resposta a vulnerabilidades da Tenable para a Integração de resposta a vulnerabilidades da ServiceNow com a Tenable [KB0960667] .

Função necessária: administrador para baixar e instalar a aplicação.

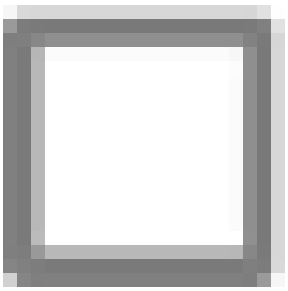
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Resposta a vulnerabilidades antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Resposta a vulnerabilidades, consulte, Como instalar Resposta a vulnerabilidades. Esta integração requer a versão 12.1 de Resposta a vulnerabilidades ou posterior.
	Se você ainda não o tiver em sua instância, obtenha direitos e baixe a aplicação Integração de Resposta a vulnerabilidades com Tenable para sua instância Now Platform®. A aplicação Integração de Resposta a vulnerabilidades com Tenable é compatível com o produto Tenable.sc a partir da versão 5.13. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a tempos de carregamento longos. Se você não souber o tamanho da sua instância ou precisar de assistência, entre em contato com o ServiceNow® Suporte técnico.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. administrador O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. sn_vul.vulnerability_admin Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das integrações da Tenable. Esta função tem acesso completo à aplicação Resposta a vulnerabilidades (VR) e seus registros. Configura todas as aplicações e regras de VR e configura integrações de terceiros. sn_vul_tenable.configure_integration

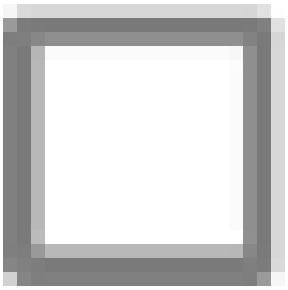
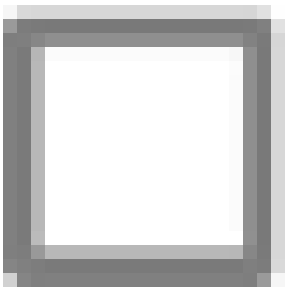
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Pode configurar a integração de vulnerabilidade da Tenable. Esta função contém a função granular sn_vul_tenable.read_integration. sn_vul_tenable.read_integration Pode exibir (ler) registros da integração de vulnerabilidade da Tenable. Grupo de Resposta a vulnerabilidades Por padrão, o grupo de Resposta a vulnerabilidades está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Resposta a vulnerabilidades herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos no Assistente de configuração para a integração. Por padrão, o grupo de Resposta a vulnerabilidades está disponível. Se ainda não tiver sido criado, você pode preferir criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Consulte Criação de um grupo de usuários . Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.
	Para promover um desempenho aprimorado para sua primeira importação, talvez você prefira desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não as usar. Essas calculadoras, além de qualquer outra que você tenha definido, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Consulte Desabilitar calculadoras de vulnerabilidade. • Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, talvez você prefira Desabilitar regras de negócio relacionadas a notificações, conforme descrito em Importar modificações para a integração de vulnerabilidade da Tenable.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. • Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Integração de Resposta a vulnerabilidades com Tenable e sua instância Now Platform estiverem no mesmo ambiente. Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . • Verifique se o plug-in IntegrationHub está instalado e ativado. Este plug-in permite que os componentes do sistema de base chamem sistemas externos usando APIs de integração e ative etapas de protocolo como REST. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.
	Obter credenciais da Tenable. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seus produtos Tenable para que você tenha acesso a eles. Tenable.io requer acesso de administrador com um atributo de permissão maior ou igual a 64. Tenable.sc requer acesso de analista de segurança ou gerente. **Nota:** A partir da v3.8 de Integração de Resposta a vulnerabilidades com Tenable, o acesso a Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

Você está pronto para Instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable usando o Assistente de configuração.

Instalar a aplicação Integração de Resposta a vulnerabilidades com Tenable usando o Assistente de configuração

Antes de executar a ServiceNow® Tenable Vulnerability Integration, você precisa baixar a aplicação Integração de Resposta a vulnerabilidades com Tenable da ServiceNow Store, instalar e configurar usando o Assistente de configuração na aplicação Resposta a vulnerabilidades.

Antes de Iniciar

Antes de instalar a aplicação Tenable, verifique se você concluiu todos os itens na check-list em Preparação para a integração de vulnerabilidade da Tenable.

Nota: Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Prossiga para .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Tenable no Assistente de configuração. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) para configurar a aplicação no Assistente de configuração após sua instalação.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Depois de alguns momentos, as aplicações que estão disponíveis para instalação em sua instância são exibidas.

2. Localize o bloco **Tenable (Plataforma Tenable)** e clique em **Instalar**.

   Esta ação instala a aplicação Integração de Resposta a vulnerabilidades com Tenable que você baixou de ServiceNow Store.

3. Siga os avisos fornecidos no Assistente de configuração para continuar com a instalação.
4. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Resposta a vulnerabilidades aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de integração>Integrações do scanner** no Assistente de configuração para continuar com a configuração. Se você quiser obter mais informações para complementar os avisos fornecidos no Assistente de configuração, consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração.

Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable

As configurações de recuperação de dados a seguir ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da ServiceNow® Integração de vulnerabilidade da Tenable para sua instância Now Platform®.

As configurações descritas nas seções a seguir ajudam a controlar os dados que você deseja importar. Além disso, você pode definir os valores desses filtros em Instâncias de integração. Para exibir instâncias de integração, navegue até **Integração de vulnerabilidade Tenable** > **Instâncias de Integração** e clique na sua integração, Tenable.io ou Tenable.sc.

Na página Instância de integração exibida, clique em Parâmetros de instância de integração para exibir uma lista de parâmetros ou nas guias Integrações de vulnerabilidade para uma programação, Detalhes de REST, Detalhes de integração, Fontes de dados e informações de execução de integração.

Configurações e filtros comuns de gravidade e recuperação para Tenable.io e Tenable.sc em sua instância Now Platform

As configurações a seguir estão disponíveis para as integrações Tenable.io e Tenable.sc em sua instância Now Platform. Essas e outras definições de configuração são exibidas na página Instância de integração da sua instância Now Platform. Você pode preferir deixar essas configurações em seus padrões para as primeiras execuções de integração.

Tenable.io

inserir_fixo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

severidade_crítica

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade crítica das Tenable.io Integrações de Vulnerabilidades Abertas e Tenable.io Vulnerabilidades Corrigidas.

gravidade_alta

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de gravidade de alto nível das Tenable.io Integrações de Vulnerabilidades Abertas e Tenable.io Vulnerabilidades Corrigidas.

gravidade_média

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade média das integrações de Tenable.io vulnerabilidades abertas e Tenable.io vulnerabilidades fixas.

sever_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade no nível de informação das integrações de Tenable.io vulnerabilidades abertas e Tenable.io vulnerabilidades fixas.

severidade_baixa

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de gravidade baixa das integrações de Tenable.io vulnerabilidades abertas e Tenable.io vulnerabilidades fixas.

tamanho

Esta configuração define o número de registros de plug-in a serem incluídos no conjunto de resultados da Tenable.io Integração de plug-ins. Deve estar no formato int32. O valor padrão é 1.000. O tamanho máximo é 10.000.

num_assets

O número máximo de vulnerabilidades por bloco exportado das Tenable.io Integrações de Vulnerabilidades Corrigidas e Tenable.io de Vulnerabilidades Abertas. O valor padrão é 50.

chunk_size

Especifica o número de ativos por bloco exportado pela Tenable.io Integração de ativos. O padrão é 1.000.

Tenable.sc

assíncrono_request

Este parâmetro está inativo por padrão (falso). Habilite ou desabilite este parâmetro para fazer chamadas de API assíncronas ou síncronas com Tenable.sc, respectivamente. Para chamadas síncronas, se houver um tempo limite de 30 segundos, entre em contato com o suporte do produto Tenable para ajustar a caixa. Este parâmetro, uma vez habilitado, é aplicável a todas as integrações de Tenable.sc. Para clientes existentes que usam chamadas assíncronas, um script de correção está disponível, o que adiciona um novo parâmetro async_request às instâncias de integração Tenable.sc existentes. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Scripts de correção**.

inserir_fixo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

deslocamento

Especifica o número de ativos, plug-ins e vulnerabilidades importados em uma execução de integração.

Filtros de consulta

Os filtros de consulta são configurados no console da Tenable. Esses filtros de consulta têm IDs que podem ser selecionados no Assistente de configuração ou na página Instâncias de integração em sua instância Now Platform. Esses filtros são aplicados ao recuperar os dados das integrações Tenable.sc.

Mensagens de REST para a integração de vulnerabilidade da Tenable

As ServiceNow® mensagens REST de integração de vulnerabilidade da Tenable são usadas para fazer chamadas para a API da Tenable.

Tenable.io Mensagem REST de ativos

A mensagem Tenable.io Assets REST recupera informações de ativos para a integração de ativos Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de ativos. O trabalho de exportação de ativos é enviado com os seguintes filtros:

- "is_deleted": falso
- "is_licensed": verdadeiro

Tenable.io Mensagem REST de plug-ins

A mensagem REST Tenable.io de plug-ins recupera informações de plug-in para a integração de plug-in Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de plug-ins.

Tenable.io Mensagem REST de vulnerabilidades

A mensagem Tenable.io de REST de vulnerabilidades recupera informações de vulnerabilidade para vulnerabilidades abertas e fechadas da integração de vulnerabilidade Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de vulnerabilidades.

Mensagem REST de consultas da Tenable.sc

A mensagem de REST de consultas do Tenable.sc recupera as informações do filtro de consulta para a integração de ativos do Tenable.sc e a integração de vulnerabilidades do Tenable.sc em que o filtro de consulta está configurado.

Tenable.sc Mensagem REST de plug-ins

A mensagem REST de plug-in Tenable.sc recupera informações de plug-in para a integração de plug-ins Tenable.sc. As mudanças no registro do método Obter plug-ins da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar informações de plug-ins.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do parâmetro	Valor	Descrição
tipo	ativo	Indica a origem da qual a Tenable extrai dados. Usado pelo código. Mudanças não são recomendadas.
campos	id, descrição, cvssVector,cvssV3Vector, cvssV3TemporalVector, sinopse, cvssVector, baseScore, temporalScore, cvssV3Vector, cvssV3BaseScore, cvssV3TemporalVector, name, vprScore, vprContext, plug-inPubDate, plug-inModDate, xrefs, família, riscoFator, cpe, vprContext, plug-inPubDate, plug-inModDate, xrefs, família, riscoFator, cpeArame, soluções para trabalho, explorar tipo, direitos autorais, versão, sourceFile, dependências, necessáriosPorts, necessáriosUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stígSeverity, patchPubDate, patchModDate, vulnPubDate, modificadoTempo, md5	Indica a lista de campos importados da Tenable.

Tenable.sc Mensagem REST de vulnerabilidades

A mensagem REST Tenable.sc de vulnerabilidades recupera informações de vulnerabilidade da integração Tenable.sc. As mudanças na mensagem REST do método Buscar vulnerabilidades ou Buscar vulnerabilidades corrigidas ou, a partir da versão v14.0 Resposta a vulnerabilidades e v2.2 da Integração de vulnerabilidades da Tenable, Buscar registro de vulnerabilidades de preenchimento afetam as solicitações feitas a Tenable.sc para recuperar informações de vulnerabilidades.

Tenable.sc Verificar mensagem REST de credenciais

Tenable.sc Mensagem de REST da política

A mensagem POST REST da política Tenable.sc adiciona uma política para os plug-ins solicitados. A política gerada será usada em Tenable.sc solicitações de verificação.

Tenable.sc Verificar mensagem REST

A mensagem POST REST de verificação do Tenable.sc adiciona uma verificação que depende do acesso e da permissão definidos no corpo da solicitação da mensagem REST. Ele usa política, ID de plug-in e IP(s) no corpo da solicitação para a solicitação de verificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.sc Mensagem REST do resultado da verificação

A mensagem Tenable.sc Resultado da verificação GET REST fornece detalhes da verificação gerada usando a mensagem Scan REST. Ele usa o scanResultId na resposta das mensagens REST de verificação e recupera detalhes da verificação acionada.

Tenable.sc Verificar credenciais

A mensagem REST Tenable.sc de verificação de credenciais recupera as informações de credenciais de Tenable.sc. As mudanças no registro do método "Importar" da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar as informações de credenciais.

Nome do parâmetro	Valor	Descrição
campos	ID, nome, descrição, tipo	Indica a lista de campos importados de Tenable.sc
filtros	utilizável	Indica que a integração extrai somente credenciais utilizáveis de Tenable.sc Mudanças em qualquer um dos parâmetros não são recomendadas.

Transformação de dados para a integração de vulnerabilidade da Tenable

Depois de identificar os dados a serem importados, eles são recuperados do produto Tenable e processados por meio de um conjunto de fontes de dados e transformações em sua instância.

Durante a instalação, os mapas de severidade normalizada são instalados no módulo Mapeamento de severidade normalizada. Esses mapas transformam os níveis de severidade importados da Tenable em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de severidade, consulte Criar um mapa de severidade da Resposta a vulnerabilidades na documentação Resposta a vulnerabilidades.

Importação de ativo da Tenable.io

Os dados de ativos importados são carregados primeiro na tabela Importação de ativos do Tenable.io [sn_vul_tenable_io_asset_import].

O mapa de transformação de integração de ativos da Tenable.io é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de ativos da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise `Tenable.io Asset Transform`.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
u_id	source_id	A Tenable fornece um ID exclusivo para ativos e

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
		mapas para o registro do item descoberto e é usado para pesquisa de IC.
u_ipv4s	ip_address	Mapeia o primeiro valor de IP para o campo ip_address no registro de item descoberto.
u_mac_address	mac_address	Mapeia o primeiro valor de mac_address para o campo de endereço mac no registro de item descoberto.
u_fqdns	fqdn	Mapeia o primeiro valor de fqdn para o campo fqdn no registro de item descoberto.
u_netbios_names	netbios	Mapeia o primeiro valor netBIOS para o campo netBIOS no registro do item descoberto.
u_operating_systems	os	Mapeia o primeiro valor de SO para o campo de SO no registro de item descoberto.
(Antes da v 14.0 Resposta a vulnerabilidades e v2.2 da Integração de vulnerabilidade da Tenable)u_last_scan_time	última_scan_date	Mapeia para o campo last_scan_date no registro do item descoberto.
u_last_authenticated_scan_date	last_auth_scan_date	Mapeia para o campo last_auth_scan_date no registro do item descoberto.
[script]	nome	Mapeia o nome do host usando a lógica do script.
u_tags		Os marcadores são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo e finalidade do script do mapa de transformação de ativo da Tenable.io

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Uma função usada para atualizar valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Integração de plug-ins Tenable.io

O mapa de transformação de plug-ins do Tenable.io é usado para transformar plug-ins importados do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados recebidos dos plug-ins da Tenable são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise a transformação do plug-in Tenable.io.

A carga dos plug-ins da Tenable.io contém todos os campos na coluna u_attributes da tabela sn_vul_tenable_io_plugin_import. O campo de atributos é analisado e mapeado para os registros da tabela de entrada de terceiros, conforme listado na tabela a seguir.

Campo de origem	Campo de destino	Descrição
ID	ID	Mapeia o ID da origem e adiciona o prefixo TEN- a ele. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
Descrição	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	A origem do TPE importado é Tenable.io.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família	categoria	Mapeia a família do plug-in para a coluna de categoria

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
plug-in_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
plug-in_publication_date	date_published	Mapeia o plugin_publication_date para a data de publicação.
tem_patch	correção_tipo	Mapeia o tipo de correção do valor has_patch.
synopsis	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
cvss_base__pontuação	pontuação	Mapeia a pontuação base de cvss para a coluna de pontuação na tabela de entrada de terceiros.
solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
exploit_available	exploração	Mapeia o exploit_available fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros
pontuação.vpr	pontuação_risco_origem	Mapeia a pontuação de vpr fornecida pelo scanner para o source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para a coluna age_of_vuln na tabela de entrada de terceiros.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		na tabela de entrada de terceiros.
vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
vpr.drivers.threat_sources_last28	ameaças_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para o Threat_sources na tabela de terceiros.
vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.
vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_reCency na tabela de entrada de terceiros.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto cvss3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
pontuação_temporais_cvss	pontuação_temporais_cvss	Mapeia a pontuação temporal do CVSS v2.
cvss_v3_pontuação_temporais	v3_tempo_pontuação	Mapeia a pontuação temporal do CVSS v3.
risk_factor	gravidade_origem	Mapas para a severidade de origem na tabela de entrada de terceiros.
nome	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
sting_severity	sting_severity	Mapeia a pontuação de vpr fornecida pelo scanner para o source_risk_score na tabela de entrada de terceiros.
plug-in_type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor para a coluna unsupported_by_vendor.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base nas colunas exploit_available e v3_attack_vector.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados ao CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como uma referência.
[script]	A lista de explorações para esse plug-in e insere o mapeamento da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Uma função usada para atualizar os valores na entrada de terceiros e verificar se a entrada de terceiros já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A inclusão de script TenableIOPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.io e a transforma em Now Platform entradas de vulnerabilidade de terceiros. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados dos plug-ins Tenable.io na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.io

O mapa de transformação de item vulnerável do Tenable.io é usado para transformar informações de vulnerabilidades abertas e fixas importadas do Tenable.io.

Nota: As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades da Tenable são processados.

O mesmo mapa de transformação é usado para a integração de vulnerabilidades fixas do Tenable.io e a integração de vulnerabilidades abertas do Tenable.io. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise o `mapa de transformação de item vulnerável da Tenable.io`.

Campo de origem	Campo de destino	Descrição
u_asset.uuid	ID	Uuid é mapeado para o campo de ID do registro cmdb_ci.
u_asset.ipv4	ip_address	O campo IPv4 é mapeado para o campo de endereço IP do registro cmdb_ci.
u_asset .last_authenticated_results	last_auth_scan_date	A data da última verificação autenticada é mapeada para a data da última verificação autenticada do registro cmdb_ci.
u_ativo.mac_addess	mac_address	O endereço MAC é mapeado para o campo de endereço MAC do host do registro cmdb_ci.
u_asset.netbios_name	netbios	O NetBIOS é mapeado para o campo netBIOS do registro cmdb_ci.
u._plugin.cvss3_base_score	v3_base_score	A pontuação base do CVSS v3 é mapeada para a pontuação base v3 do registro de entrada de terceiros.
u._plugin.cvss3_tempo_score	v3_tempo_pontuação	A pontuação temporal do CVSS v3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u._plugin.cvss_base_score	pontuação	A pontuação base do CVSS é mapeada para o campo de pontuação do registro de entrada de terceiros.
u._plugin.cvss_tempo_score	pontuação_ temporal	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_plugin.description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada de terceiros.
u_plugin.family	categoria	Mapeia a família do plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plugin.modification_date	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_plugin.publication_date	date_published	A data de publicação é mapeada para o campo de data de publicação do registro de entrada de terceiros.
plug-in.risco_fator	gravidade_origem	O fator de risco é mapeado para o campo source_severity do registro de entrada de terceiros.
u_plugin.solução	solução	A solução é mapeada para o campo de solução do registro de entrada de terceiros.
u_plugin.sinopsis	ameaça	A sinopse é mapeada para o campo de ameaça do registro de entrada de terceiros.
u_severity_id	prioridade	A prioridade é mapeada para o ID de severidade da carga. O valor padrão é 5.
u_plugin.exploit_available	exploração	Mapeia o exploit_available

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
pontuação.vpr	pontuação_risco_origem	Mapeia a pontuação de vpr fornecida pelo scanner para o source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_plugin.vpr.drivers.age_of_vuln	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_sources_last_28	ameaças_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para Threat_sources na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_intensity_last_28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plugin.vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_reCency na tabela de entrada de terceiros.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS3 v3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
u_plugin.type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor no plug-in para a coluna unsupported_by_vendor.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base nas colunas exploit_available e v3_attack_vector.
u_plugin.family_id	ID da família	Mapeia o ID de família do plug-in para a colunafamily_id na tabela de entrada de terceiros.
porta	porta	A porta é mapeada para o campo de porta do registro de item vulnerável.
protocolo	protocolo	O protocolo é mapeado para o campo de protocolo do registro de item vulnerável.
u_first_found	first_found	Primeiro encontrado é mapeado para o primeiro campo encontrado do registro de item vulnerável.
u_last_found	último_encontrado	O último encontrado é mapeado para o último campo encontrado do registro do item vulnerável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_state	estado	O estado é mapeado para o campo Estado no registro do item vulnerável
[script]	origem	A origem da integração está preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.io como origem.
[script]	integração_instance	O integration_instance é o nome da instância da qual o item vulnerável é importado.
u_plugin.name	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
u_plugin.sting_severity	sting_severity	Mapeia a severidade de sting do plug-in para a coluna de severidade de sting na tabela de entrada de terceiros

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados ao CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como uma referência.
[script]	A lista de explorações desse plug-in e o mapeamento de inserções da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação aciona o TenableIOVulnerabilitiesProcessor, que importa dados do Tenable.io usando o conjunto para importação e carrega cada registro na tabela de IC do CMDB, na tabela de itens vulneráveis e na tabela de vulnerabilidade de terceiros. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Uma função para verificar se a entrada e as detecções de terceiros já existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para atualizar a contagem de ICs, IVs e Detecções conforme importados do Tenable.io. Para uso interno. Não é recomendável modificar ou excluir.

Importação de ativo da Tenable.sc

Os dados de ativos importados do Tenable.sc são carregados primeiro na tabela Importação de ativos do Tenable.sc (sn_vul_tenable_sc_asset_import). O mapa de transformação de integração de ativos da Tenable.sc é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de ativos da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise a `transformação de ativo Tenable.sc`.

Campo de origem	Campo de destino	Descrição
u_uuid	ID	O UUID não é preenchido pela API da Tenable, portanto, o atributo "u_uniqueness" é usado para criar um campo UUID exclusivo para ativos e mapeá-lo para o registro cmdb_ci.
u_ip	ip_address	Mapeia o campo IP da API para o campo ip_address em um registro cmdb_ci.
u_macaddress	mac_address	Mapeia o campo de endereço eletrônico da API para o campo de endereço no registro cmdb_ci.
u_dnsname	fqdn	Mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_netbiosname	netbios	Mapeia o campo netBIOS da API para o campo netBIOS no registro cmdb_ci.
u_oscpe	os	As informações do sistema operacional são extraídas do atributo oscpe na carga e mapeadas para o campo do sistema operacional no registro cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mapeia o campo lastauthrun da API para o campo last_auth_scan_date no registro do item descoberto.
u_lastauthrun e u_lastauthrun	última_scan_date	O lastauthrun é extraído da API da Tenable ou lastauthrun. Com base no valor que aparece na carga útil, o campo last_scan_date no registro do item descoberto é preenchido.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Função usada para atualizar os valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Importação de plug-ins Tenable.sc

Os dados de plug-ins importados do Tenable.sc são carregados primeiro na tabela de importação de plug-ins do Tenable.sc (sn_vul_tenable_sc_plugin_import). O mapa de transformação do plug-in Tenable.sc é usado para transformar as informações de plug-in que foram importadas. As mudanças nesta transformação alteram como os dados de importação do plug-in Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos para importação do sistema** > **Mapas de transformação**. Pesquise o mapa de transformação do `plug-in Tenable.sc`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_id	ID	Mapeia o ID da origem e adiciona o prefixo TEN-. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
u_description	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	origem	O TPE importado desta integração tem o Tenable.sc como origem.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família_u	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria.
u_plugin_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
u_plugin_publication_date	date_published	Mapeia o plugin_publication_date para a data de publicação.
u_has_patch	Tipo_de_correção	Mapeia o tipo de correção do valor has_patch.
sinopse_u	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
u_cvss_pontuação_base	pontuação	Mapeia a pontuação base do CVSS para a coluna de pontuação na tabela de entrada de terceiros.
u_solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
u_cvss_pontuação_temporais	pontuação_temporais_cvss	Mapeia a pontuação temporal do CVSS v2.
u_cvss_v3_tempo_score	v3_tempo_pontuação	Mapeia a pontuação temporal do CVSS v3.
u_risk_factor	severidade de origem	Mapas para a severidade de origem na tabela de entrada de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_cvss_v3_base_score	v3_base_score	Mapeia a pontuação base do CVSS na tabela de entrada de terceiros.
u_exploit_available	exploração	Mapeia o exploitAvailable fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
pontuação_u_vpr	pontuação_risco_origem	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id="threat_sources_last_28"]	ameaça_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.
u_vpr_context[id="threat_intensity_last_28"]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id="threat_recency"]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		Threat_reCency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impact_score]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_name	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_sting_severity	sting_severity	Mapeia o campo stíg_severity no plug-in para stíg_severity na tabela de entrada de terceiros.
u_check_type	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in "family_id" para "family_id" na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela de entrada de terceiros é preenchida com base nas colunas exploit_available e v3_attack_vector.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas a entradas de terceiros.

Campo de origem	Descrição
u_cpe	A lista de CPEs é adicionada como uma referência.
u_ver_também	A lista de URLs é adicionada como uma referência.
u_exploit_frameworks	A lista de explorações para esse plug-in e insere o mapeamento da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Função usada para atualizar os valores na entrada de terceiros e verificar se a entrada de terceiros já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de plug-ins criados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

A inclusão de script TenableSCPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.sc e a transforma em entradas de vulnerabilidade de terceiros da ServiceNow. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados de plug-ins Tenable.sc na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.sc

O mapa de transformação de vulnerabilidades abertas do Tenable.sc é usado para transformar dados importados da integração de vulnerabilidades abertas do Tenable.sc, e o mapa de transformação de vulnerabilidades fixas e Tenable.sc é usado para transformar dados importados da integração de vulnerabilidades fixas do Tenable.sc.

Nota: As mudanças nesses mapas de transformação alteram como os dados da importação de vulnerabilidades fixas/abertas da Tenable são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e corrigidas do Tenable.sc, navegue até **Integração de vulnerabilidade Tenable** > **Administração** > **Instâncias de Integração** > **Tenable.sc Integração de vulnerabilidades fixas/abertas** > **Fontes de dados** > **Vulnerabilidades abertas/corrigidas do Tenable.sc** > **Transformações**.

Campo de origem	Campo de destino	Descrição
u_pluginID	Id	Usado como o identificador do plug-in. Este campo é mapeado para o ID do plug-in no registro de entrada de terceiros.
u_riskfactor	gravidade_origem	Este campo é mapeado para source_severity no registro de entrada de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
gravidade_u	prioridade	O campo de prioridade é mapeado com a gravidade. O valor padrão é 5.
u_hasbeenmitigado	estado	Hasbeenmitigado é mapeado para o campo de estado do registro de vulnerabilidade. Para a integração de vulnerabilidades corrigidas, todos os IVs estão no estado "Encerrado".
u_ip	ip_address	O endereço IP é mapeado para o campo de IP do host da tabela cmdb_ci.
u_port	porta	A porta é mapeada para o campo de porta do registro de item vulnerável.
u_protocol	protocolo	O protocolo está mapeado para o campo de porta do registro de item vulnerável.
u_firstVisto	first_found	O primeiro valor visto é mapeado para o primeiro campo encontrado do registro VI.
u_lastVisto	último_encontrado	O último valor visto é mapeado para o último campo encontrado do registro VI.
u_exploitDisponível	exploração	ExploitAvailable é mapeado para o campo de exploração no registro de entrada de terceiros.
sinopse_u	ameaça	A sinopse é mapeada para o campo de ameaça no registro de entrada de terceiros.
u_description	resumo	A descrição é mapeada para o campo de resumo no

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		registro de entrada de terceiros.
u_solução	solução	A solução é mapeada para o campo de solução no registro de entrada de terceiros.
u_basescore	pontuação	BaseScore é mapeado para o campo de pontuação no registro de entrada de terceiros.
Pontuação_temporal	pontuação_ temporal	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada de terceiros.
u_cvssv3basescore	v3_base_score	Cvssv3basescore é mapeado para a pontuação base v3 no registro de entrada de terceiros.
u_cvsspontuação temporal	v3_tempo_pontuação	A pontuação temporal Cvssv3 é mapeada para a pontuação temporal v3 no registro de entrada de terceiros.
u_pluginpublicar	date_published	A data de publicação do plug-in é mapeada para a data de publicação do plug-in no registro de entrada de terceiros.
u_pluginmoddate	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada de terceiros.
u_dnsname	fqdn	DnsName é mapeado para o campo FQDN do registro cmdb_ci.
u_macaddress	mac_address	MacAddress é mapeado para o campo mac_address do registro cmdb_ci.
u_netbiosNome	netbios	O NetBIOSName é mapeado para o

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		campo NETBIOS do registro cmdb_ci.
u_ip	ip	O IP está mapeado para o campo IP do registro cmdb_ci.
hostUniqueness	uuid	A exclusividade do host não é mapeada para nenhum campo, mas é usada para determinar o UUID do host.
família_u	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria do registro de entrada de terceiros.
u_plugintext	prova	O texto do plug-in é mapeado para a prova no registro de TPE.
[script]	origem	A origem da integração está preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.sc como origem.
[script}	integração_instance	O integration_instance é o nome da instância da qual o item vulnerável é importado.
pontuação_u_vpr	pontuação_risco_origem	Mapeia a pontuação de VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação de vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 – Crítico • 7 – 9 – Alto

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		• 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	idade_de_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mapeia a maturidade do código de exploração do scanner para exploit_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id="threat_sources_last_28]	ameaças_fontes	Mapeia origens de ameaças nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.
u_vpr_context[id="threat_intensity_last_28]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id="threat_recency"]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_reCency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_pluginname	nome	Mapeia o nome do plug-in para a coluna

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		de nome na tabela de entrada de terceiros.
gravidade_ust	sting_severity	Mapeia o campo stíg_severity no plug-in para stíg_severity na tabela de entrada de terceiros.
u_checktype	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in "family.id" para "family_id" na tabela de entrada de terceiros.
[script]	exploit_attack_vector	A coluna exploit_attack_vector na tabela third_party_entry é preenchida com base nas colunas exploit_available e v3_attack_vector.

Campo de origem	Descrição
u_cve	Insere dados relacionados ao CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento é encontrado em sn_vul_m2m_entry_cve.
u_bid	A lista de traqs de erros é adicionada como uma referência.
u_cpe	A lista de CPEs é adicionada como uma referência.
u_seetambém	A lista de URLs é adicionada como uma referência.
u_xrefs	A lista de X-REFs é adicionada como uma referência.
u_exploitframeworks	A lista de explorações desse plug-in e o mapeamento de inserções da estrutura de exploração aplicável e do plug-in para sn_vul_m2m_framework_vul.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Não é recomendável modificar ou excluir.
onBefore (antes de um conjunto para importação concluir a transformação).	Função usada para atualizar os valores na vulnerabilidade e verificar se a vulnerabilidade já existe. Com base nos resultados, modifica os valores em uma tabela de itens vulneráveis. Para uso interno. Não é recomendável modificar ou excluir.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos IVs criados e VIs que foram atualizados e ignorados. Para uso interno. Não é recomendável modificar ou excluir.

Definir parâmetros de filtro adicionais para Tenable.io importações

Personalize os parâmetros de filtragem das suas consultas programadas com Integrações de vulnerabilidade da Tenable para ajudá-lo a refinar ainda mais os dados de vulnerabilidade importados com o produto Tenable.io.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidades, convém filtrar os dados de suas consultas para que você possa revisar somente detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por *cidr_range*, *num_assets*, *indexed_at*e *plugin_family*. Ou digamos que você queira executar uma integração Tenable.io, de modo que uma execução importe somente vulnerabilidades críticas a cada quatro horas e outra seja executada a cada 24 horas para buscar todas as outras vulnerabilidades não críticas.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros compatíveis com a Tenable para ajudá-lo a importar os detalhes específicos da vulnerabilidade necessários.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com parâmetros Tenable em seu Now Platform. As seguintes integrações Tenable.io oferecem suporte à filtragem fornecendo conteúdo JSON no corpo da solicitação:

- Integração de ativos
- Integração de vulnerabilidade fixa
- Integração de vulnerabilidades abertas

Você deve saber como usar cadeias de caracteres JSON para este recurso.

Função necessária: sn_vul.vulnerability_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

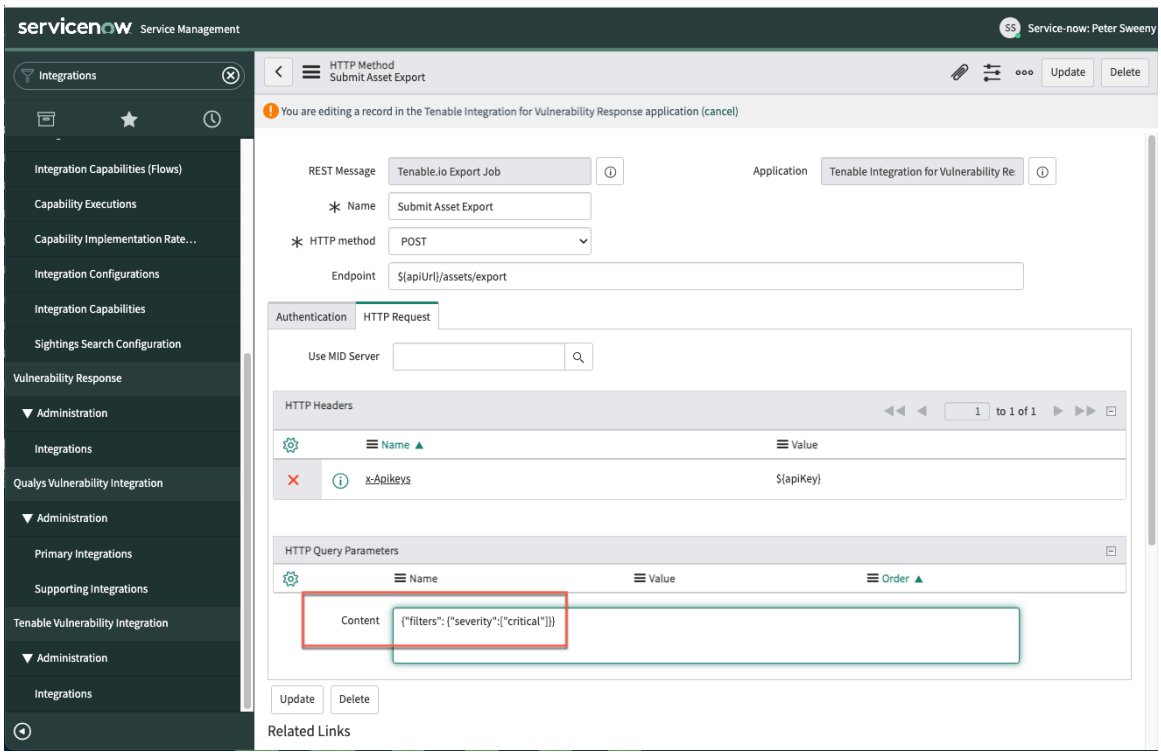
Procedimento

1. Localize os parâmetros compatíveis com o produto Tenable.io no site do desenvolvedor que você deseja usar para a filtragem.

   Os parâmetros e valores inseridos no produto Tenable.io são compatíveis somente no nível da instância de integração.

2. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
3. Na página da lista Integrações da Tenable, clique no registro da integração Tenable.io que você deseja abrir.
4. Com a guia Métodos REST da Tenable selecionada, clique no ícone de informações (I) para o método REST, seguido por **Abrir registro**.
5. Selecione a guia **Solicitação HTTP**.
6. Para editar o registro, na parte superior da página, clique no link em. Para editar o registro, clique **aqui**.
7. No registro Método REST no campo Conteúdo, insira o conteúdo JSON que você deseja como parte do corpo da solicitação.

   Na imagem a seguir, como exemplo, o parâmetro de severidade para vulnerabilidades importadas, `{"filters": {"severity": ["critical"]}}` foi personalizado para a integração de Tenable.io ativos. Este valor importa somente vulnerabilidades críticas (pontuação de CVSS de 10,0).



   Se você quiser inserir mais de um parâmetro, consulte a documentação Tenable.io para obter mais informações sobre como separar cada valor.

8. Clique em **Atualizar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Emissão de relatórios de integração de vulnerabilidade da Tenable

Exiba relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Resposta a vulnerabilidades.

Visualizações de dados nos espaços Resposta a vulnerabilidades

Os espaços Resposta a vulnerabilidades incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a gravidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Resposta a vulnerabilidades Espaços, Explorar o Vulnerability Manager Workspace e Explorar o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Versões anteriores de Resposta a vulnerabilidades

O painel de visão geral da Resposta a vulnerabilidades (Gestão de vulnerabilidades) fornece uma exibição executiva das vulnerabilidades e itens vulneráveis, ajudando o Administrador de vulnerabilidades a identificar rapidamente as áreas de preocupação. O painel de correção da Resposta a vulnerabilidades (Correção de vulnerabilidades) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Para obter mais informações, consulte Usando os painéis padrão Resposta a vulnerabilidades.

Função necessária: responsável pela correção.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

para exibir o painel, navegue até **Resposta a vulnerabilidades** > **Visão Geral da Correção**.

Gráfico de status de execução de integração para a integração de vulnerabilidade da Tenable

O módulo Status da execução de integração da Tenable fornece uma exibição gráfica do status das execuções de integração da Tenable.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer parte do gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: administrador de vulnerabilidade.

Personas e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Resposta a vulnerabilidades. Para a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Resposta a vulnerabilidades.

Tradução automática

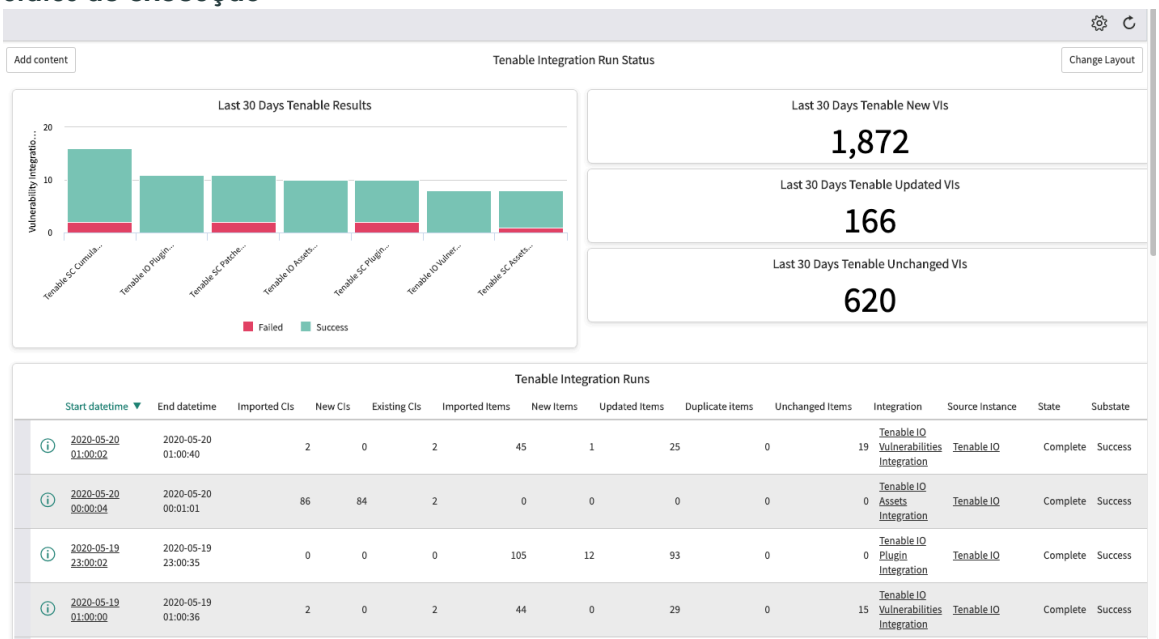
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir os dados, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Status da Execução da Integração**.

A partir da versão 19.0 do Resposta a vulnerabilidades, este painel está disponível na IU da nova experiência.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Status de execução



Relatórios do gráfico de status de execução da integração da Tenable

Nome	Descrição
Resultados do Tenable nos últimos 30 dias	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Cada execução é exibida como uma barra no gráfico.
VIs novos do Tenable nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs atualizados do Tenable nos últimos 30 dias	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs inalterados do Tenable nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Execuções de integrações do Tenable	Os registros de execução de integração em uma lista.

Tradução automática

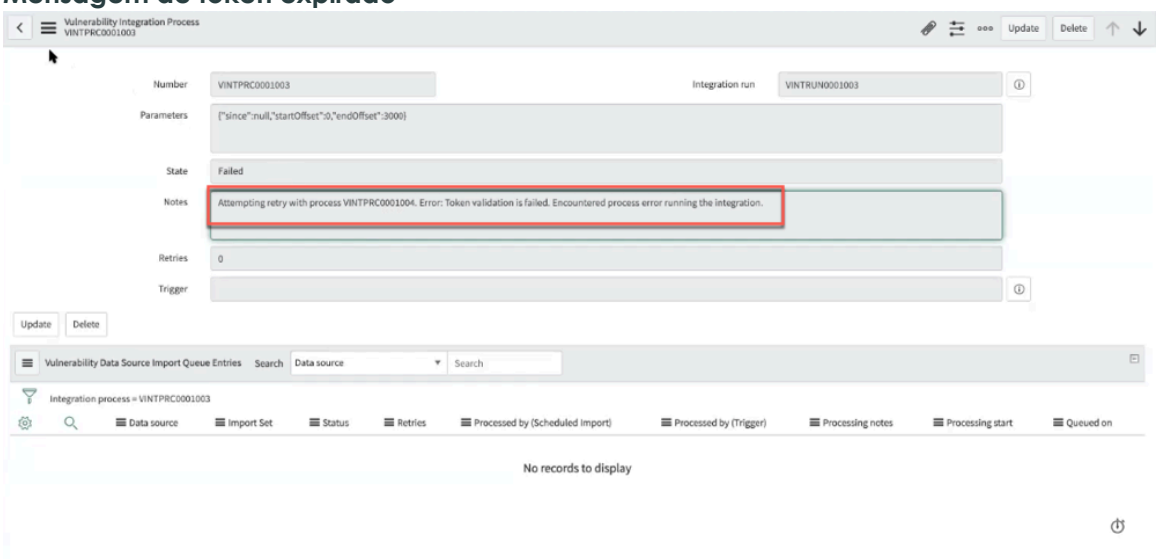
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: **V16.1:** para verificar as detecções desta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow[*sn_vul_detection*] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na contagem de detecção ou descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem de data até" na instância, após a conclusão da execução da integração.

Expiração da validação do token

Se uma execução de integração do Tenable.sc falhar por qualquer motivo, o token de autenticação do Tenable.sc expirará automaticamente e uma mensagem será exibida no registro do processo de integração de vulnerabilidade.

Mensagem de token expirado



Um novo token é gerado automaticamente para o próximo processo de integração. Todos os processos de integração, com falha e bem-sucedidos, são exibidos na guia Processo de integração de vulnerabilidade no registro Processo de integração de vulnerabilidade.

Iniciar nova verificação para a integração Tenable.sc

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.sc da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Nota: Tenable.sc não é compatível com o início de uma nova verificação em máquinas baseadas em agente.

Verifique se o scanner está ativado antes de começar. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
Para iniciar uma nova verificação a partir dos espaços, consulte Verificar novamente itens vulneráveis Tenable.io e Tenable.sc dos espaços Resposta a vulnerabilidades.

Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, responsáveis pela correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de itens vulneráveis (VI), tarefas de correção (RT), entradas de terceiros (TPE) ou registros de itens descobertos da sua instância Now Platform.

As novas verificações permitem que os proprietários de correção e os analistas de vulnerabilidade verifiquem se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada a partir de seus Now Platform para Tenable.sc itens vulneráveis.

Nota: Ao solicitar uma nova verificação da instância Now Platform®, a seleção das credenciais Integração de Resposta a vulnerabilidades com Tenable é opcional. A ServiceNow® Tenable.sc Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.sc em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais de conta da Tenable. A ServiceNow® Tenable.sc Integração de credencial de verificação é habilitada (`Ativo`) automaticamente no Assistente de configuração em sua instância quando você configura as Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades abertas e corrigidas).

Observe as seguintes informações sobre as credenciais importadas para que os usuários possam vê-las conforme necessário na instância Now Platform :

- As credenciais criadas com a função de usuário de administrador Tenable.sc estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.sc estão disponíveis somente para usuários dentro dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

Consulte o site de documentação Tenable.sc para obter mais informações.

Consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração para obter mais informações sobre como configurar a aplicação Tenable.sc. Para exibir mais informações sobre a Integração de credencial de verificação, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.sc**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável a partir do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Você só pode iniciar novas verificações de IVs com Tenable.sc como origem. Verifique se Tenable.sc é exibido na coluna **Origem** nas exibições de lista de VI ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condições para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição de lista de VI, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **Origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de VI, o VI deve ser do produto Tenable.sc e estar em qualquer estado diferente de **Closed**. Para vários registros de VI, todos os IVs devem ser do produto Tenable.sc e estar em qualquer estado diferente de **Closed**.
   - Em um registro de RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Tenable.sc.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do produto Tenable.sc em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro, clique em **Verificar novamente**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você será solicitado a escolher as credenciais do scanner para acessar o scanner. Estas são as credenciais importadas pela Tenable.sc Scan Credential Integration.

5. Na caixa de diálogo, selecione os filtros e tipos de credenciais desejados.
6. Clique **em Solicitar verificação**.

   Uma mensagem é exibida indicando que a verificação está sendo processada. O status de todas as novas verificações pode ser encontrado a qualquer momento nas listas relacionadas a Verificação nos registros VI, RT e TPE usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e outras verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. O registro de verificação primário é um contêiner para as verificações secundárias.

   Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram ou farão a transição para **Encerrado/Corrigido** são importados com a próxima importação programada da Integração de vulnerabilidades fixas da Tenable.sc.

Iniciar nova verificação para a integração Tenable.io

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.io da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Verifique se o scanner está ativado antes de começar. Navegar até **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

- Consulte e Verificar novamente registros e tarefas de correção no Espaço do gerenciador de vulnerabilidades e Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI para iniciar uma nova verificação nos espaços da Resposta a vulnerabilidades.
- Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Nota: Tenable.io não é compatível com o início de uma nova verificação em máquinas baseadas em agente.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, como responsável pela correção, especialista em TI, analista de vulnerabilidade ou gerente de vulnerabilidades, você pode iniciar novas verificações direcionadas sob demanda. você pode verificar vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de itens vulneráveis (VI), tarefas de correção (VUL), entrada de terceiros (TPE) ou registros de itens descobertos (SDI) da instância Now Platform. As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Ao solicitar uma nova verificação da instância Now Platform®, a seleção das credenciais Integração de Resposta a vulnerabilidades com Tenable é opcional. A ServiceNow® Tenable.io Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.io em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais de conta da Tenable.

As informações a seguir descrevem as credenciais que você importa para que os usuários possam vê-las conforme necessário na sua instância Now Platform :

- As credenciais criadas com a função de usuário de administrador Tenable.io estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.io estão disponíveis somente para usuários dentro dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

  Consulte o site de documentação Tenable.io para obter mais informações.

- A integração de modelo Tenable.io e a integração de credencial de verificação Tenable.io precisam ser ativadas antes de iniciar novas verificações. Para exibir mais informações sobre a Integração de credencial de verificação, navegue até **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.io**.

  Por padrão, as integrações de credencial de modelo e verificação estão desativadas. Quando você insere suas credenciais para Tenable.io, todas as integrações Tenable.io são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

  1. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
  2. Na lista exibida, localize os registros de integração Tenable.io desejados.
  3. Abra cada registro e marque a caixa de seleção **Ativo** para ativar a integração.
  4. Clique em **Atualizar** para salvar suas mudanças.
  5. Retorne ao Assistente de configuração para continuar com a configuração para Integrações de vulnerabilidade da Tenable com Resposta a vulnerabilidades.

Consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração para obter mais informações sobre como configurar os produtos Tenable.io e Tenable.sc.

Digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada a partir de seus Now Platform para Tenable.io itens vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação agendada da Integração de vulnerabilidades corrigidas.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas de fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 de Resposta a vulnerabilidades, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Se estiver, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota: O campo **Último registro processado** é atualizado com base no que está definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**.
2. Localize o registro de item vulnerável a partir do qual você deseja acionar uma nova verificação e abra-o.

   Nota: Se você estiver usando o Tenable.io Scanner, só poderá iniciar novas verificações de IVs com Tenable.io como origem. Verifique se Tenable.io é exibido na coluna **Origem** nas exibições de lista de VI ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condições para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição de lista de VI, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **Origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção** ou **Resposta a vulnerabilidades** > **Bibliotecas** > **Terceiros** para os registros que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de VI, o VI deve estar em qualquer estado diferente de **Closed**. Para vários registros de VI, todos os IVs devem ser do produto Tenable.io e estar em qualquer estado diferente de **Closed**.
   - Para registros de tarefa de correção, somente tarefas de correção em qualquer estado diferente de **Encerrado** são compatíveis. Todos os IVs associados devem estar em qualquer estado diferente de **Encerrado** e usar Tenable.io como origem.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro VI associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.

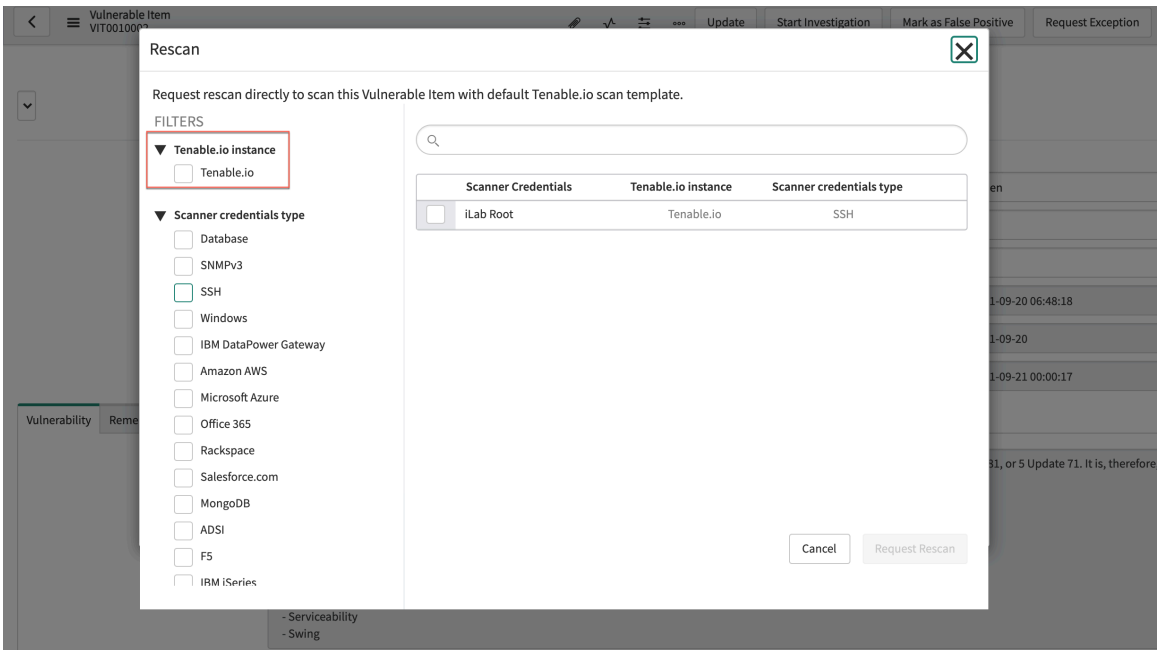
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em registros de Itens descobertos, o registro deve ter pelo menos um registro VI associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.
- Na lista Itens vulneráveis, você pode selecionar itens vulneráveis individuais que deseja verificar novamente. Use o menu Ações nas linhas selecionadas no canto inferior esquerdo da tela para iniciar a nova verificação. Você será solicitado a inserir suas credenciais.

4. No canto superior direito de um registro, clique em **Verificar novamente**.
   Você será solicitado a escolher a instância ou as instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pela Tenable.io Scan Credential Integration.
5. Na caixa de diálogo, selecione a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Na imagem a seguir, uma instância de integração, `Tenable.io`, é exibida. Se você tiver mais de uma instância Tenable.io, todas elas serão exibidas na seção `Tenable.io` no formulário.



Campo	Descrição
Instância da Tenable.io	Escolha uma instância de integração Tenable.io a partir da qual você deseja iniciar a nova verificação. Todas as suas instâncias de integração para Tenable.io são exibidas. Se houver um VI em mais de uma instância de integração, você poderá usar este filtro para limitar ou expandir as instâncias que deseja verificar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se você optar por verificar novamente os IVs de um registro de tarefa de correção para uma única instância de integração, somente os VIs ativos que estão associados a essa tarefa de correção, para essa instância, usando as credenciais selecionadas serão verificados.
Filtro de tipo de credenciais do scanner	Use este filtro para exibir credenciais por tipo.
Painel com credenciais do scanner, instância Tenable.io, tipo de credenciais do scanner	Estas são as credenciais de scanner disponíveis importadas dos produtos Tenable.io. Escolha uma ou mais credenciais a serem usadas na verificação.

6. Clique **em Solicitar nova verificação**.

Uma mensagem é exibida indicando que a verificação está sendo processada e que um registro de verificação primário foi criado. O status de todas as verificações secundárias pode ser encontrado a qualquer momento nas listas relacionadas a Verificação nos registros de VI, tarefa de correção, TPE e SDI usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e outras verificações iniciadas a partir de um determinado registro.

O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. Cada verificação oferece suporte a uma combinação exclusiva de instância de integração, TPE, IP e ID de rede. Você pode ver várias verificações secundárias em um registro de verificação primário. Por exemplo, o número máximo de endereços IP que uma verificação secundária pode suportar é 1000. Se houver 1002 IPs para um item vulnerável, duas verificações secundárias serão criadas e listadas na lista relacionada Verificações para oferecer suporte à solicitação. O registro de verificação primário é um contêiner para as verificações secundárias e seu estado de reflete o status das verificações secundárias.

Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** são importados com a próxima importação agendada da Tenable.io Integração de vulnerabilidades corrigidas.

Para verificações com erro, você pode verificar as verificações secundárias no registro de verificação primário. Exiba o erro na carga de resposta da verificação secundária.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação agendada da Integração de vulnerabilidades corrigidas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizar itens de configuração com o identificador de partição de rede para o Integrações de vulnerabilidade da Tenable

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão na aplicação Resposta a vulnerabilidades, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC `(IC 1)` durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	Network_id	Item de configuração
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	Repository_id	Item de configuração
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. A partir de uma nova importação de dados, você pode atualizar seus ICs existentes com mais granularidade que inclui o identificador de partição de rede [network_partition_identifier] executando o trabalho agendado, *`Update existing discovered items with network partition identifier`*.

Este trabalho agendado está desativado por padrão. Ative este recurso para as integrações de ativos e vulnerabilidades fixas e abertas dos produtos Tenable.io e Tenable.sc no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho agendado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho agendado também cria ICs que incluem o identificador de partição de rede começando com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

Tradução automática

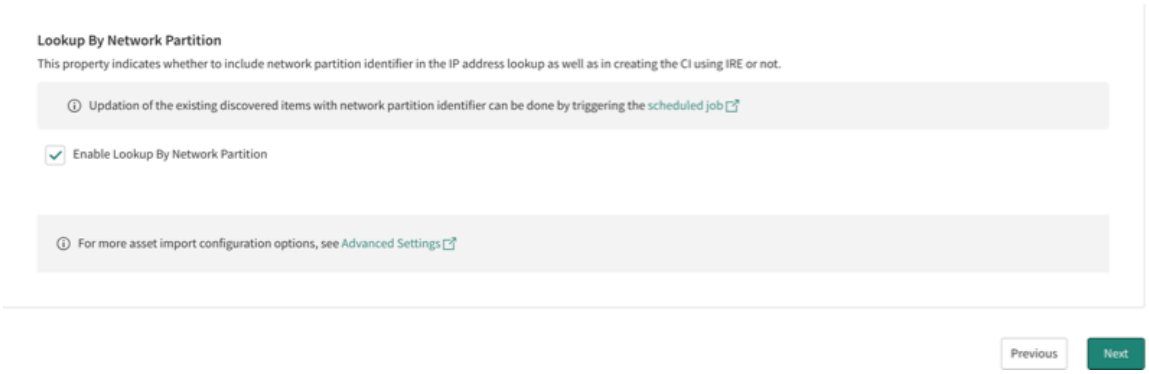
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando você faz upgrade a partir da v14.0 de Resposta a vulnerabilidades e v2.2 da Integração de vulnerabilidade da Tenable, os modelos de classe de IC do CMDB (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

Opção	Descrição
Execute os trabalhos agendados sob demanda.	Atualize seus itens descobertos existentes. Os ICs dos dados existentes da Tenable são criados ou atualizados para incluir a granularidade do identificador de partição de rede. Itens descobertos, itens vulneráveis e registros de detecção são todos atualizados com os novos ICs.
Aguarde as importações de novos dados das integrações com os próximos trabalhos agendados.	Crie ICs para cada novo ativo usando o identificador de partição de rede, começando com o próximo trabalho agendado. IC, item vulnerável e registros de detecção são todos atualizados para incluir a nova granularidade. Novos ICs são criados quando uma correspondência exata não é encontrada.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Selecione Tenable.io integrações ou Tenable.sc integrações.
3. **Edite** a integração necessária.
4. Selecionar **Configuração de importação de ativo**.
5. Selecionar **Habilitar pesquisa por partição de rede** caixa de seleção do **Habilitar pesquisa por partição de rede** seção.



6. Clique em **Avançar**.

   Os identificadores de partição de rede NETWORK_ID e REPOSITORY _ID estão incluídos e atualizam os ICs existentes ou criam ICs com o próximo trabalho agendado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo do identificador de partição de rede incluído na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITORY_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

Com o próximo trabalho agendado, as regras de pesquisa de identificação de endereço IP e IC de endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para os produtos Tenable.io e Tenable.sc.

Depois de habilitar a propriedade do sistema e salvar os registros, você também pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando os trabalhos agendados sob demanda.

Importar modificações para a integração de vulnerabilidade da Tenable

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração de importação de vulnerabilidades da Tenable na ServiceNow® Integração de vulnerabilidade da Tenable.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação e conhecimento avançado sobre o Now Platform.

Siga estas etapas para criar importações separadas por domínio para as integrações de vulnerabilidades da Tenable. O exemplo a seguir é para a integração Tenable.io Open Vulnerabilities, mas este conteúdo é aplicável a outras integrações da Tenable.

Procedimento

1. Crie um domínio.
2. Para cada domínio criado, crie um usuário e atribua o usuário a esse domínio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

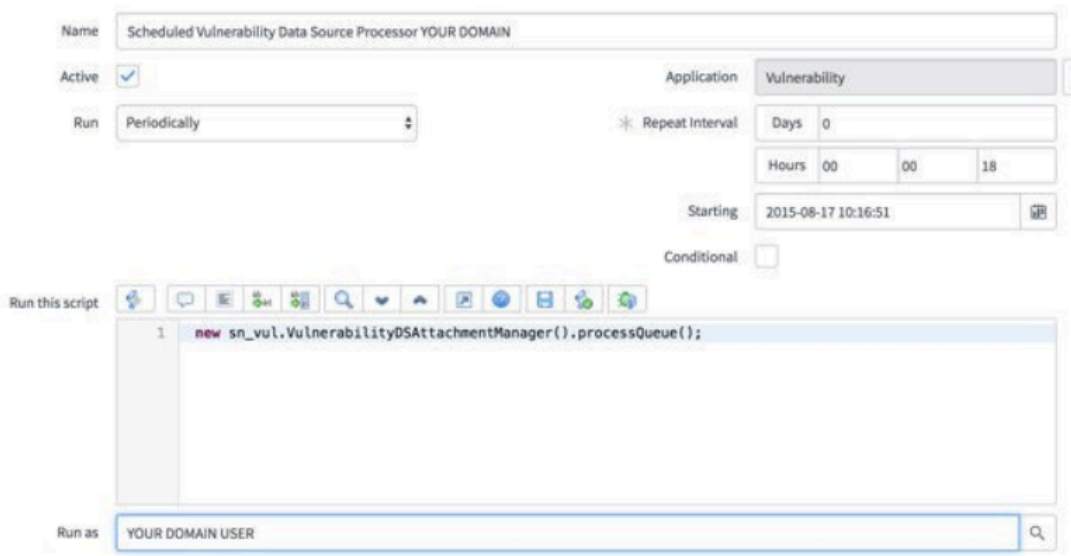
Pense neste usuário como um espaço reservado run_as para o domínio no Tenable.io.

3. Integração de vulnerabilidades abertas.
   O usuário é o equivalente ao usuário VR.System no domínio global e deve ter as seguintes funções: sn_vul.tenable_configure_integration, import_admin e sn_vul.vulnerability_write. Este usuário requer acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota: Considere este usuário como específico para esta função. O usuário não deve ter outra finalidade

4. Em cada domínio, crie um trabalho agendado copiando o Processador da Fonte de Dados de Vulnerabilidade Programada encontrado em **Definição do Sistema** > **Trabalhos agendados**.
5. Anexe o domínio ao nome para identificar o trabalho agendado.
6. Altere o usuário run_as para o usuário que você criou na etapa anterior.

   Nota: Edite a ação de IU a seguir para que a integração seja executada no domínio do usuário run_as.



7. Edite a ação de IU Executar agora na integração de vulnerabilidades abertas do Tenable.io para adicionar este bloco de código à parte superior do arquivo.
   ```
   //sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
   ```

   Nota: Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário run_as.

8. Edite o método de inclusão de script VulnerabilityIntegrationUtils addIntegrationRun para adicionar o código realçado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edite o método de inclusão de script VulnerabilityIntegrationUtils addProcessRun para adicionar o código realçado.

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edite o método de inclusão de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups para alterar este código original: código _processFromDataSourcesGroups original para código _processFromDataSourcesGroups editado.
11. Edite o método de inclusão de script VulnerabilityDSAttachmentManager, queueItem para adicionar os seguintes blocos de código realçados queueItem, _getNext, _processQueueEntry.

    Você está pronto para importações de detecção de host separadas por domínio.

    Desabilitar calculadoras antes da importação

    Siga estas etapas para desabilitar a calculadora padrão se não for usada. Se você não usar calculadoras de vulnerabilidade, é melhor desabilitar as calculadoras padrão, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é acessado e pode afetar o desempenho da instância.

    Função necessária: sn_vul.vulnerability_admin.

12. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Calculadoras de vulnerabilidade**.
13. Abra o grupo Impacto de vulnerabilidade.
14. Abra a calculadora de impacto baseado em pontuação e serviço.
15. Desmarque o campo Ativo para desativar a calculadora.
16. Clique em Atualizar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você desativou a calculadora padrão.

Desabilitar regras de negócio baseadas em notificação antes da importação inicial

Siga estas etapas para desabilitar Regras de negócio relacionadas a notificações antes da importação do registro inicial. Durante a importação inicial de registros, determinadas regras de negócio relacionadas à notificação podem gerar muitas notificações, afetando o desempenho. Essas regras de negócio devem ser modificadas para desativá-las durante a importação.

A função necessária é sn_vul.vulnerability_admin.

17. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócio**.
18. Pesquise notificações de ICs afetados.
19. Abra a regra de negócio e insira a seguinte condição: *`current.sys_class_name != "sn_vul_vulnerable_item"`*.
20. Clique em **Atualizar**.
21. Repita este procedimento para as seguintes regras de negócio:
    - Notificações do centro de custos afetado
    - Notificações do grupo afetado
    - Notificações de locais afetados

Nota: Após a conclusão da importação do registro inicial, você tem a opção de habilitar novamente essas regras de negócio. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Modificar uma data de início inicial

Siga estas etapas para modificar uma data de início inicial. Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações da Tenable. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado nas etapas a seguir.

22. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
23. Clique em qualquer integração.
24. Clique em Detalhes da integração.
25. Defina o campo Hora de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde essa hora sejam detectadas.

    Se você configurou a Tenable usando o Assistente de configuração, o campo Hora de início será preenchido previamente, inicialmente até três meses antes da data de hoje e, posteriormente, até a data de hoje. Observação: considere definir o valor para no máximo um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Tenable, bem como o acionamento de tempos limites de execução.

26. Clique em **Enviar** ou **Atualizar**.
27. Opcional: Clique **em Executar agora** para executar imediatamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações correção

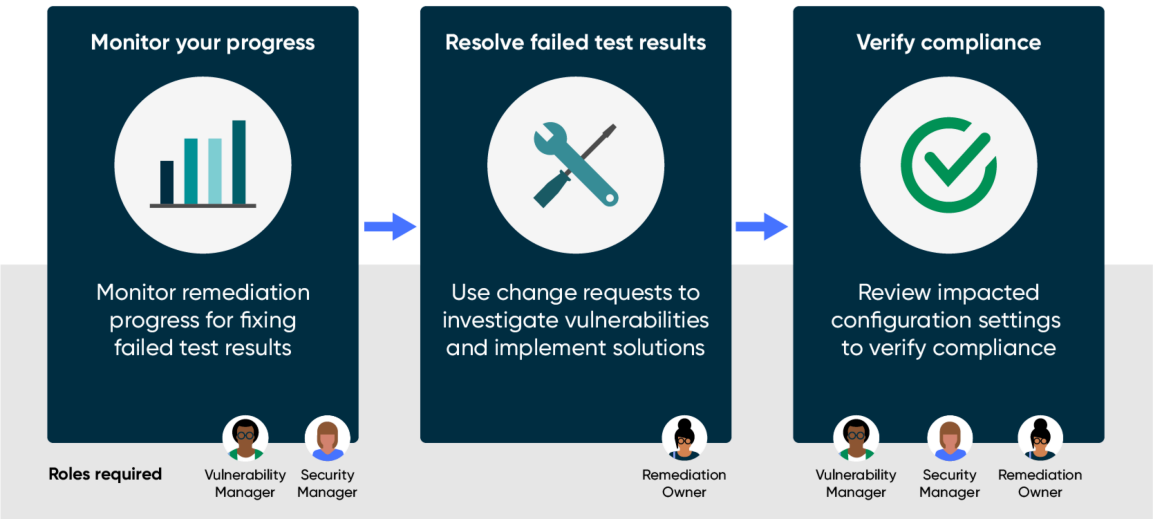
Conformidade de configurações A correção é principalmente um processo manual aprimorado por trabalhos agendados (integrações), tarefas de correção, fluxos de trabalho e solicitações de mudança.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Remediation of test result groups



Plug-ins SCA de terceiros separados adquirem e transformam dados em Conformidade de configurações. Antes de poder usar Conformidade de configurações para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede.

Use as solicitações de mudança para corrigir falhas de teste individuais das tarefas de correção.

Os estados das tarefas de correção fazem a transição automaticamente conforme as solicitações de mudança associadas se movem por seus ciclos de vida com Sincronização de estado entre solicitações de mudança e tarefas de correção. Usuários com a função itil podem criar e gerenciar solicitações de mudança diretamente das tarefas de correção.

Criar manualmente uma Conformidade de configurações tarefa de correção

Você pode criar manualmente uma tarefa de correção no módulo **Tarefas** de correção e executar a correção.

Antes de Iniciar
Função necessária: sn_vulc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O uso de regras de tarefa de correção preenche automaticamente a guia **Resultados de testes**. A criação manual é útil para um grupo que não precisa de uma regra ou de repetição.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

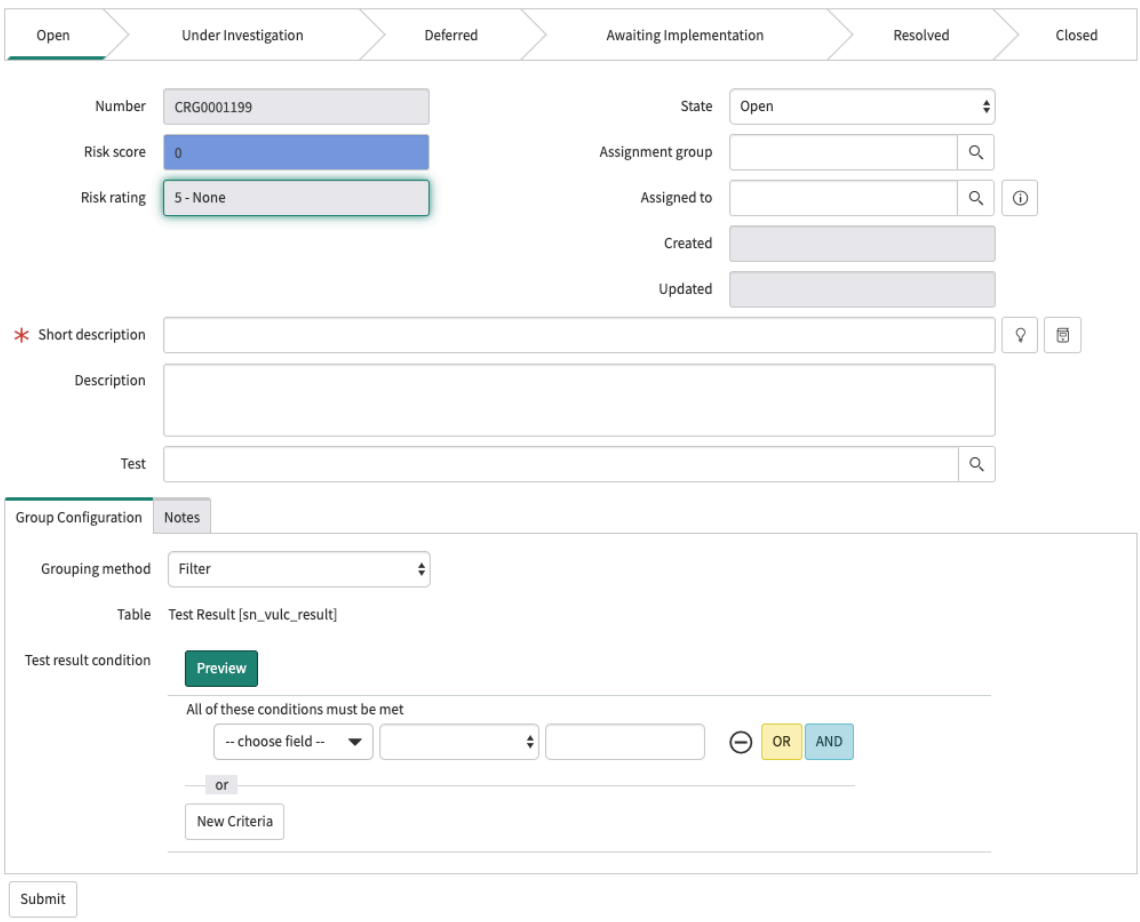
Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Tarefas de correção**.
2. No painel de navegação, clique em **Minhas tarefas em aberto** ou **Todas as tarefas** em aberto para exibir a lista.
3. Clique em **Nova**.

Formulário de tarefa de correção



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Preencha os campos no formulário Tarefa de correção, conforme apropriado.

Formulário Tarefa de correção

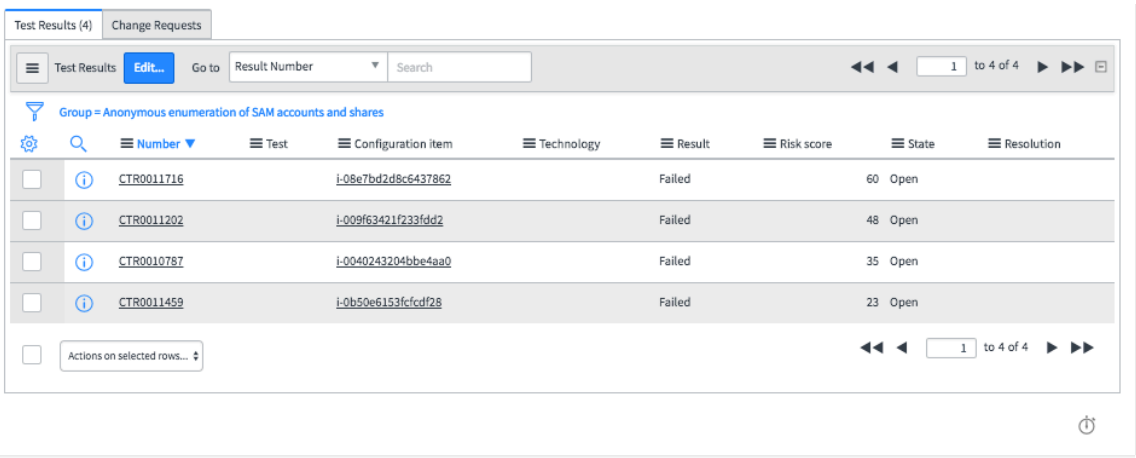
Campo	Descrição
Número	ID atribuído automaticamente no sistema.
Pontuação de risco	Preenchido automaticamente pela calculadora de pontuação de risco. Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máximo em todos os Resultados de testes não "Encerrada" (Aberto, Sob investigação, Aguardando implementação, Adiado, Resolvido) e 15% da pontuação do número de testes resultados que não estão "Encerrados".
Pontuação de risco	Preenchido automaticamente pela calculadora de pontuação de risco. Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Estado	Inicialmente **Aberto**, é o estado de correção do grupo. Para obter mais informações, consulte Conformidade de configurações estados.
Grupo de atribuição	Atribua a tarefa de correção a um grupo de correção.
Atribuído a	Atribua uma equipe para corrigir a tarefa de correção.
Criação	Data em que você criou este grupo.
Atualizado em	Data em que você atualizou este grupo.
Descrição resumida	Nome da tarefa de correção.
Descrição	Descrição desta tarefa de correção.
Teste	Selecione um Teste de configuração para esta Tarefa de correção.
Guias relacionadas	
Configuração de Grupo	Métodos de agrupamento a serem usados: ◦ Manual (padrão): ◦ Regra de filtro ou grupo: Tabela: pré-selecionada como resultado de testes [sn_vulc_result] Condição de resultado de testes: escolha os filtros a serem usados. **Nota:** O link de condição de correspondência de registros acima das condições de filtro exibe os registros de resultado de testes que você escolheu em uma nova janela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Clique em **Visualizar** para ver quantos resultados seus critérios de filtro retornam antes de salvar o novo grupo. A lista relacionada Resultados de testes deve ser criada manualmente clicando no botão **Editar** na guia relacionada **Resultados de testes**.
Anotações	Anotações de trabalho relacionadas a esta tarefa de correção.

5. Clique com o botão direito do mouse no cabeçalho para **Salvar** ou clique em **Enviar** para salvar e retornar à lista de tarefas de correção.
   Exibe as listas relacionadas a **Resultados de testes** e **Solicitação de mudança**.



Criar manualmente uma tarefa de correção Conformidade de configurações na lista Resultados de testes

Você pode criar manualmente uma tarefa de correção na lista **Resultado de testes** e executar a correção a partir da tarefa de correção resultante.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Este método requer a seleção de resultados de testes a serem incluídos e a criação do grupo no menu **Ações em linhas selecionadas....** Este método é bom para resultados que não são facilmente filtrados ou situações em que você deseja especificar resultados de testes para correção.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

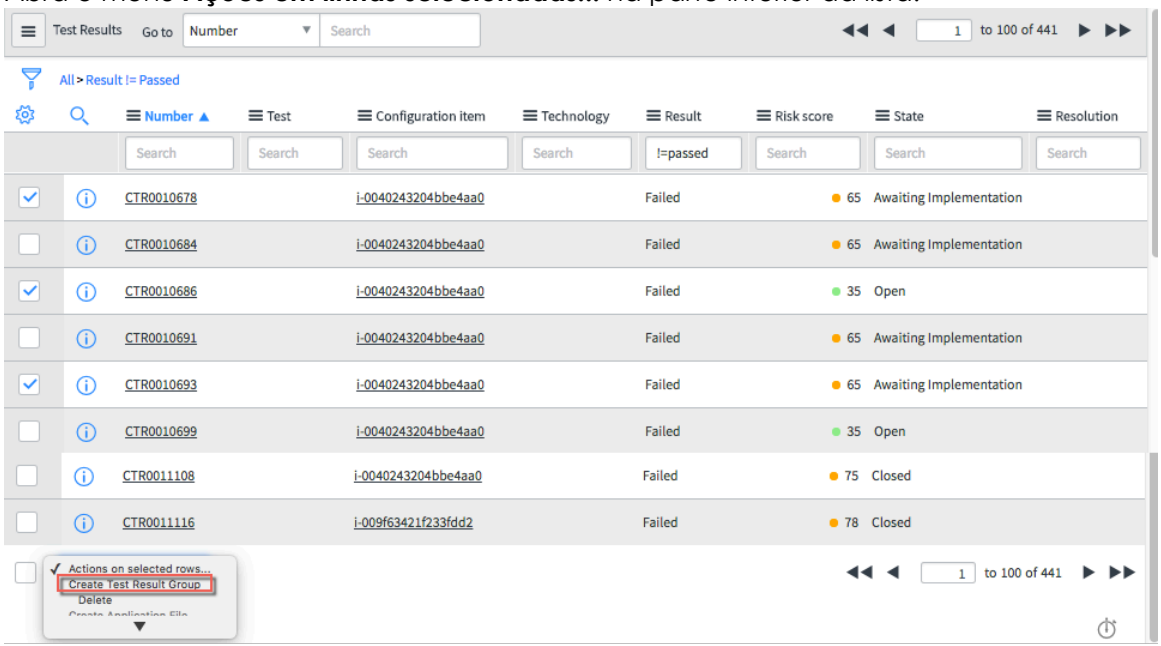
Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Resultados de testes**.
2. No painel de navegação, selecione um módulo de Resultado de testes para abrir uma lista.
3. Selecione os resultados de testes a serem incluídos no grupo marcando a caixa ao lado de cada um.
4. Abra o menu **Ações em linhas selecionadas...** na parte inferior da lista.

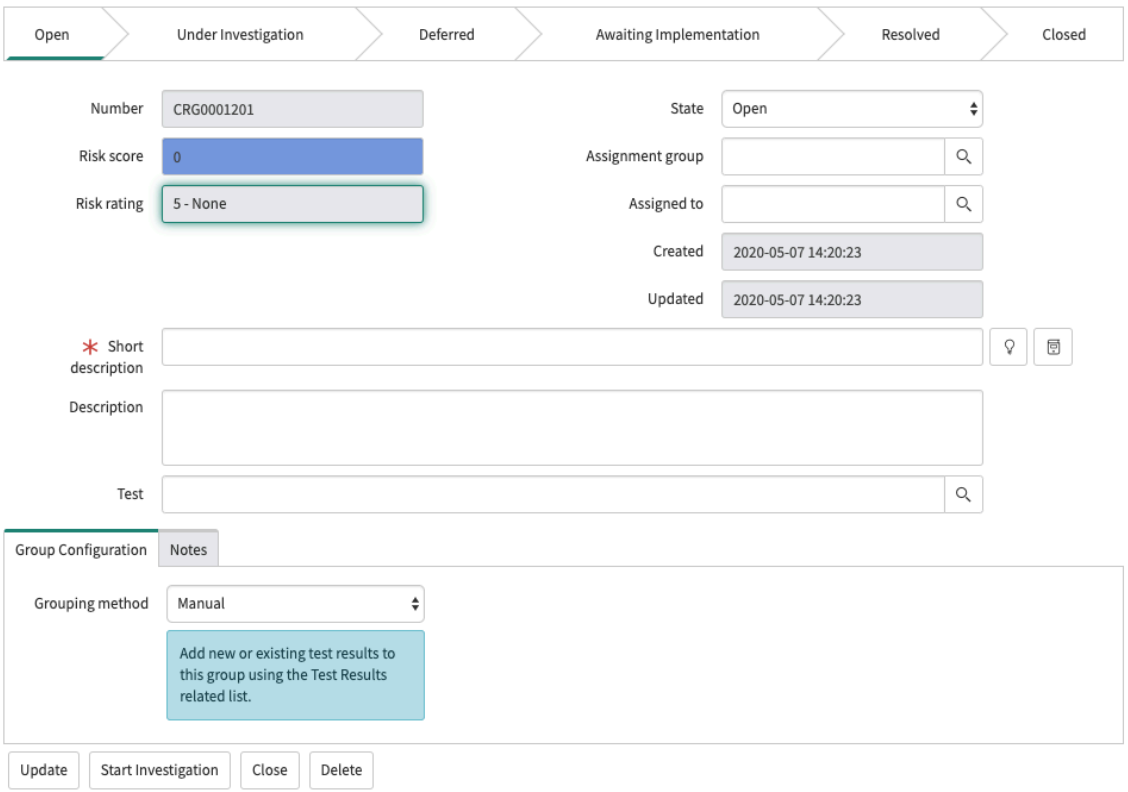


5. Escolha **Criar tarefa**de correção .
   A tarefa de correção é criada e aberta.

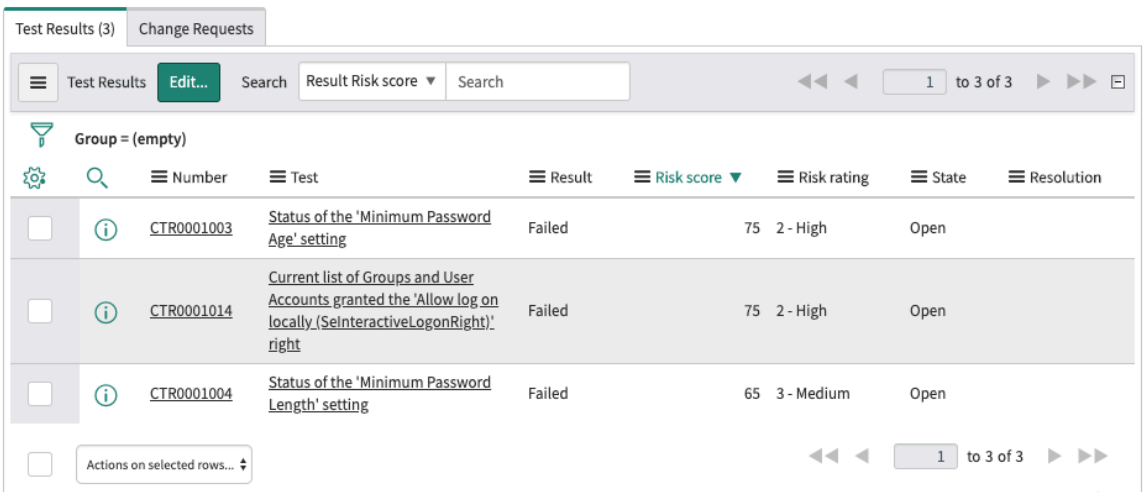
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Grupo de resultados de testes



Os resultados de testes selecionados para o grupo são exibidos na lista relacionada Resultados de testes junto com todas as solicitações de mudança associadas.



6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Número	ID atribuído automaticamente no sistema.
Pontuação	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máximo em todos os Resultados de testes não "Encerrada" (Aberto, Sob investigação, Aguardando implementação, Adiado, Resolvido) e 15% da pontuação do número de testes resultados que não estão "Encerrados".
Classificação	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Pontuação de risco histórico	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. A pontuação de risco inerente em todos os resultados de testes aprovados em uma tarefa de correção. Este campo exibe a quantidade de risco que foi corrigida por um grupo de teste e só é exibido depois que um grupo de teste está no estado "Encerrado" e a pontuação de risco é zero.
Estado	Inicialmente **Aberto**, é o estado de correção do grupo. Para obter mais informações, consulte Conformidade de configurações estados.
Grupo de atribuição	Atribua a tarefa de correção a um grupo de correção.
Atribuído a	Atribua uma equipe para corrigir o grupo.
Criação	Data em que você criou este grupo.
Atualizado em	Data em que você atualizou este grupo.
Descrição resumida	Nome da tarefa de correção.
Descrição	Descrição de texto desta tarefa de correção.
	Selecione um Teste de configuração para esta Tarefa de correção.
Guias relacionadas	
Configuração de Grupo	Métodos de agrupamento a serem usados: ◦ Manual (padrão) ◦ Filtrar Tabela: pré-selecionada como Resultado de testes Condição de resultado de testes: escolha os filtros a serem usados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O link de condição de correspondência de registros acima das condições de filtro exibe os registros de resultado de testes que você escolheu em uma nova janela. Clique em **Visualizar** para ver quantos resultados seus critérios de filtro retornam antes de salvar o novo grupo.
Anotações	Anotações de trabalho relacionadas a esta tarefa de correção.
Listas relacionadas	
Resultados de testes	Resultados de testes incluídos neste grupo.
Solicitações de mudança	Solicitações de mudança associadas a este grupo.

7. Clique com o botão direito do mouse no cabeçalho para **Salvar** ou clique em **Enviar** para salvar e retornar à lista de tarefas de correção.

Como criar uma solicitação de mudança no Conformidade de configurações

Você pode criar uma solicitação de mudança a partir de uma tarefa de correção na aplicação Conformidade de configurações.

Antes de Iniciar
Função necessária: usuário com a função itil

Por Que e Quando Desempenhar Esta Tarefa
Como especialista em TI ou em correção, crie uma solicitação de mudança (CHG) diretamente de uma tarefa de correção para todos os resultados de testes do grupo. Crie uma solicitação de mudança com informações preenchidas previamente para agilizar sua investigação de vulnerabilidades que requerem intervenção manual.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente das tarefas de correção atribuídas a você. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente de uma tarefa de correção:

Padrão

Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento ou instrução de trabalho especificada.

Normal

As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.

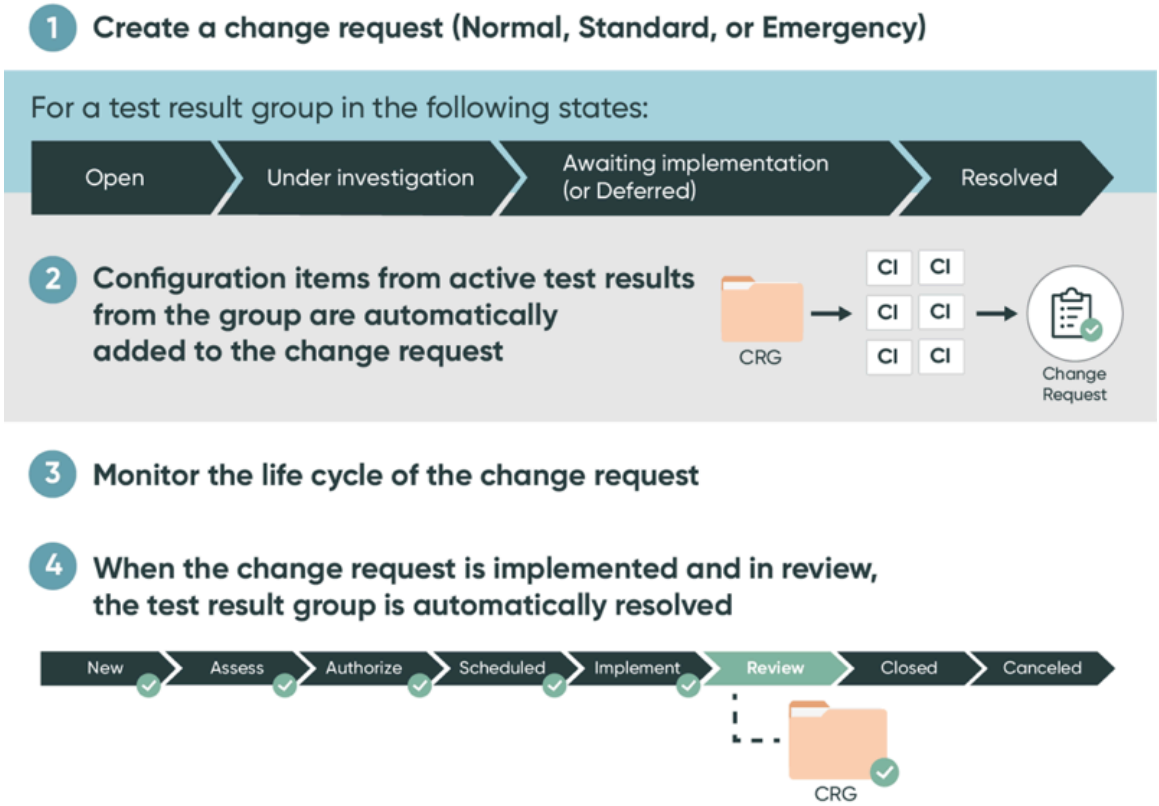
Emergência

Uma mudança para resolver um incidente grave.

A imagem a seguir ilustra o fluxo básico para criar uma solicitação de mudança a partir de uma tarefa de correção. As etapas detalhadas para este fluxo seguem a imagem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A partir da versão 19.0 do Resposta a vulnerabilidades, você pode criar solicitações de mudança para Tarefas de correção no Espaço de correção de TI. Para obter mais informações, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Tarefas de correção** > **Meus grupos abertos**.
   A lista de tarefas de correção atribuídas aos seus grupos é exibida.
2. Na coluna Número, clique na tarefa de correção para a qual você deseja criar uma solicitação de mudança.
   Você pode criar solicitações de mudança a partir de tarefas de correção em qualquer estado diferente de **Encerrado** ou **Em revisão**.

   O registro da tarefa de correção é exibido.
3. No canto superior direito do registro, clique em **Criar mudança**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O formulário de solicitação de mudança é exibido.

4. Preencha os campos.

   a. Na lista do campo **Aplica-se a**, escolha uma para continuar.

Opção	Descrição
Todos os resultados de testes ativos neste grupo	Se selecionado, todos os resultados de testes ativos desta tarefa de correção com um estado diferente de **Encerrado** serão adicionados automaticamente à solicitação de mudança depois que você clicar em **Criar mudança**.
Todos os resultados de testes ativos neste grupo que atendem a um conjunto de condições	Se selecionado, o construtor de condições será exibido. Insira critérios de filtro para identificar os resultados de testes que você deseja para a nova solicitação de mudança. Um exemplo de um filtro que você pode criar localizaria somente os resultados de testes do grupo que correspondem a um estado e pontuação de risco específicos: O estado é **Em aberto** e a Pontuação de risco é maior que **50**.

5. Para a caixa de seleção **Adicionar ICs ao CR**, escolha um para continuar.

Opção	Descrição
Caixa de seleção selecionada	O padrão é selecionado. Se a caixa de seleção estiver marcada, todos os itens de configuração (ICs) que pertencem aos resultados de testes ativos desta tarefa de correção serão adicionados a esta solicitação de mudança. O resultado de testes muda para **Aguardando implementação**.
Caixa de seleção desmarcada	Desmarque a caixa de seleção se você não quiser que os ICs dos resultados de testes ativos desta tarefa de correção sejam adicionados à nova solicitação de mudança. A tarefa de correção permanece no estado atual.

6. Na lista do campo **Tipo de mudança**, escolha uma para continuar.

Opção	Descrição
Emergência	Uma mudança para resolver um incidente grave.
Normal	Um tipo de mudança que é usado para implementar qualquer mudança em um serviço que não seja uma mudança padrão ou de emergência.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Padrão	Uma solicitação de mudança pré-autorizada de baixo risco que é implementada com frequência. As solicitações de mudança padrão aprovadas podem ser predefinidas em um catálogo de modelos para tornar mais eficiente o acesso e a solicitação de uma mudança padrão. Se selecionado, dois campos serão exibidos. Selecione um de cada lista para preencher estes campos: ◦ Categoria de**mudança**: selecione uma categoria para a mudança no catálogo existente, por exemplo, `Hardware`, `Mudanças padrão do servidor`, `Software`. ◦ Modelo de**mudança**: selecione um modelo disponível para solicitações de mudança com tarefas de suporte predefinidas do seu catálogo. Para obter mais informações sobre categorias, modelos e tipos de mudança de solicitação de mudança do ITSM, consulte Tipos de mudança .

O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Gestão de mudanças. Por exemplo, se você alterar o nome das solicitações de mudança padrão no ITSM de `Padrão` para `Pré-aprovado`, o novo nome será exibido automaticamente na lista Tipo de mudança no formulário Criar solicitação de mudança.

7. Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações da tarefa de correção.
   Se necessário, edite esses campos.
8. Clique **em Criar mudança**.
   A solicitação de mudança é exibida. Na lista relacionada de ICs afetados, os ICs dos resultados de testes que correspondem aos seus critérios são exibidos. Se a solicitação de mudança exigir aprovação, o botão **Solicitar aprovação** será exibido.

   Depois que a solicitação de mudança é criada, o grupo do resultado de testes passa para o estado **Aguardando implementação**. Depois que a solicitação de mudança para esta tarefa de correção for resolvida, se não houver outras solicitações de mudança em aberto associadas a esta tarefa de correção, a tarefa de correção também será movida para o estado **Resolvido**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados das solicitações de mudança não movem automaticamente a tarefa de correção dos estados `Encerrado` ou `Adiado`.

Associar uma tarefa de correção a uma solicitação de mudança existente

Associe uma tarefa de correção na aplicação Conformidade de configurações a uma solicitação de mudança existente.

Antes de Iniciar
Função necessária: um usuário com a função itil

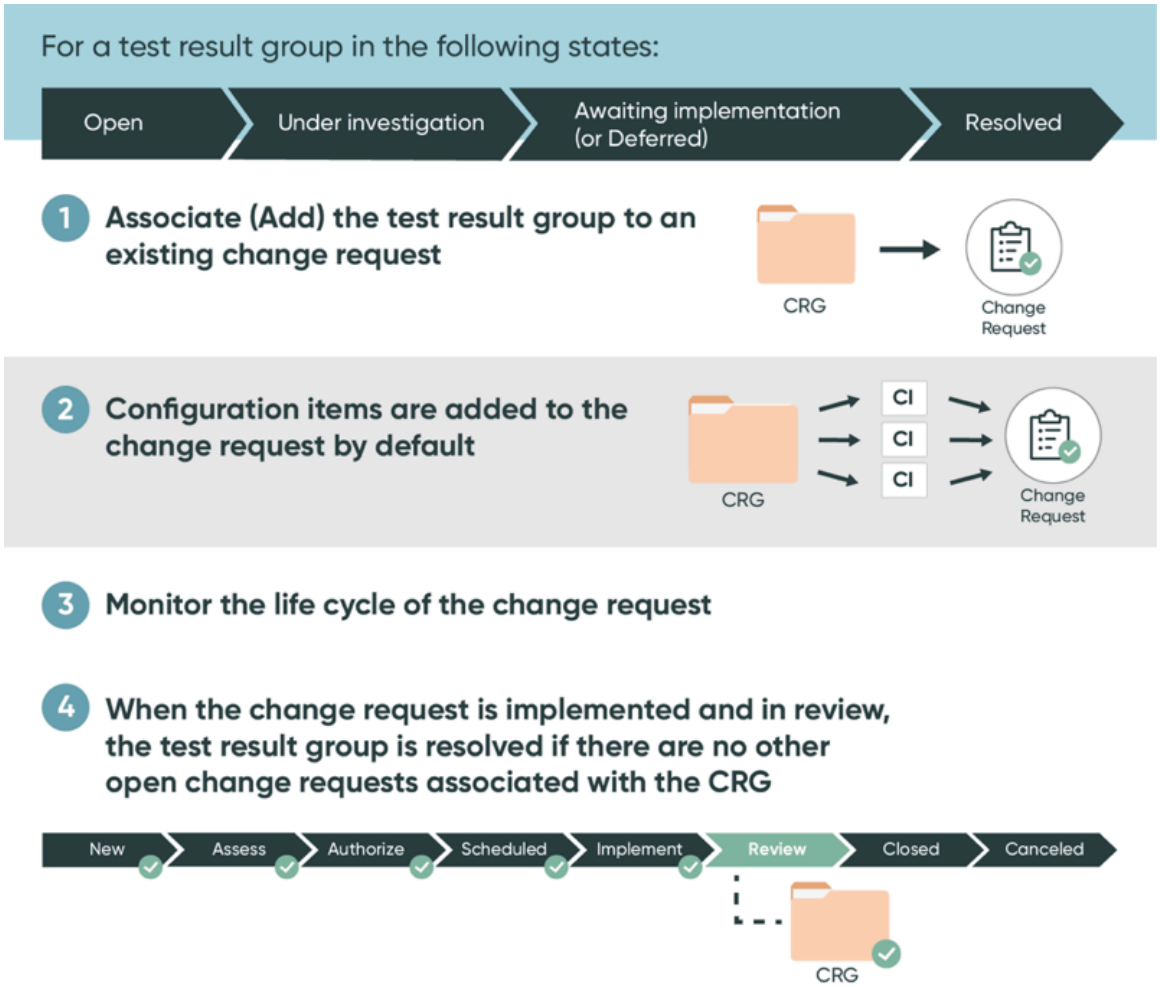
Por Que e Quando Desempenhar Esta Tarefa
Como especialista em TI ou em correção, evite criar solicitações de mudança duplicadas (CHG) enquanto trabalha para resolver suas tarefas de correção associando uma tarefa de correção (RT) a uma solicitação de mudança que já está disponível em sua instância.

Você pode associar tarefas de correção atribuídas a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros da tarefa de correção. A imagem a seguir ilustra o fluxo básico para associar uma solicitação de mudança existente a uma tarefa de correção. As etapas detalhadas para este fluxo seguem a imagem.

Nota: Você pode associar uma solicitação de mudança existente a uma tarefa de correção em qualquer estado diferente de **Cancelado** (**Aberto**, **Sob investigação**, **Aguardando implementação**, **Encerrado**e **Adiado**). As solicitações de mudança, incluindo as encerradas nos últimos 90 dias, estão disponíveis para associação no formulário. Quando você associa uma solicitação de mudança a uma tarefa de correção existente, somente os resultados de testes ativos e seus itens de configuração são adicionados à solicitação de mudança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Tarefas de correção** > **Minhas Tarefas em Aberto**.
   A lista de tarefas de correção atribuídas aos seus grupos é exibida.
2. Na coluna Número, clique na tarefa de correção para a qual você deseja criar uma solicitação de mudança.

   O registro da tarefa de correção é exibido.
3. No canto superior direito do registro, clique em **Criar mudança**.
   O formulário de solicitação de mudança é exibido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas à tarefa de correção são exibidas junto com o botão **Adicionar**.
5. Clique em **Adicionar**.
   A caixa de diálogo Adicionar solicitação de mudança existente ao grupo de resultados de teste é exibida.
6. Clique no ícone de pesquisa e selecione um item na lista.
   Você pode filtrar a lista exibida para restringir a pesquisa.
7. Clique em **Enviar**.
   O TRG é exibido junto com uma mensagem que indica que a solicitação de mudança foi associada com sucesso à tarefa de correção. Na lista relacionada às solicitações de mudança, a nova solicitação de mudança é exibida. Os ICs da tarefa de correção são adicionados por padrão à solicitação de mudança e são exibidos na lista relacionada de ICs afetados. Você também pode adicionar ICs à solicitação de mudança a partir desta lista relacionada. Uma mensagem indica o número de resultados de testes que foram movidos para o novo grupo e o novo TRG é exibido.

   Nota: Para menos de 200 resultados de testes, a operação de divisão é feita de forma síncrona e os resultados de testes são exibidos no novo grupo.

   Para mais de 200 resultados de testes, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os resultados de testes apareçam no novo grupo. A mensagem a seguir também é exibida: `n resultados de testes serão movidos de TRGxxxxxxx para o novo grupo de resultados de testes GRCxxxxxx em breve.`

   Você pode associar qualquer solicitação de mudança à tarefa de correção, com as seguintes exceções:

   - Solicitações de mudança no estado **Cancelado**.
   - Solicitações de mudança no estado **Encerrado** com mais de 90 dias.
   - Solicitações de mudança já associadas ao TRG. O sistema não permitirá que você associe uma solicitação de mudança que já está associada ao TRG.

   Depois que a solicitação de mudança para esta tarefa de correção for resolvida, se não houver outras solicitações de mudança em aberto associadas a esta tarefa de correção, a tarefa de correção também será movida para o estado**Resolvido**.

   Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados das solicitações de mudança não movem automaticamente a tarefa de correção dos estados `Encerrado` ou `Adiado`.

   Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Dividir uma tarefa de correção

Em uma tarefa de correção existente na aplicação Conformidade de configurações, identifique um subconjunto de resultados de testes que você deseja mover para uma nova Tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

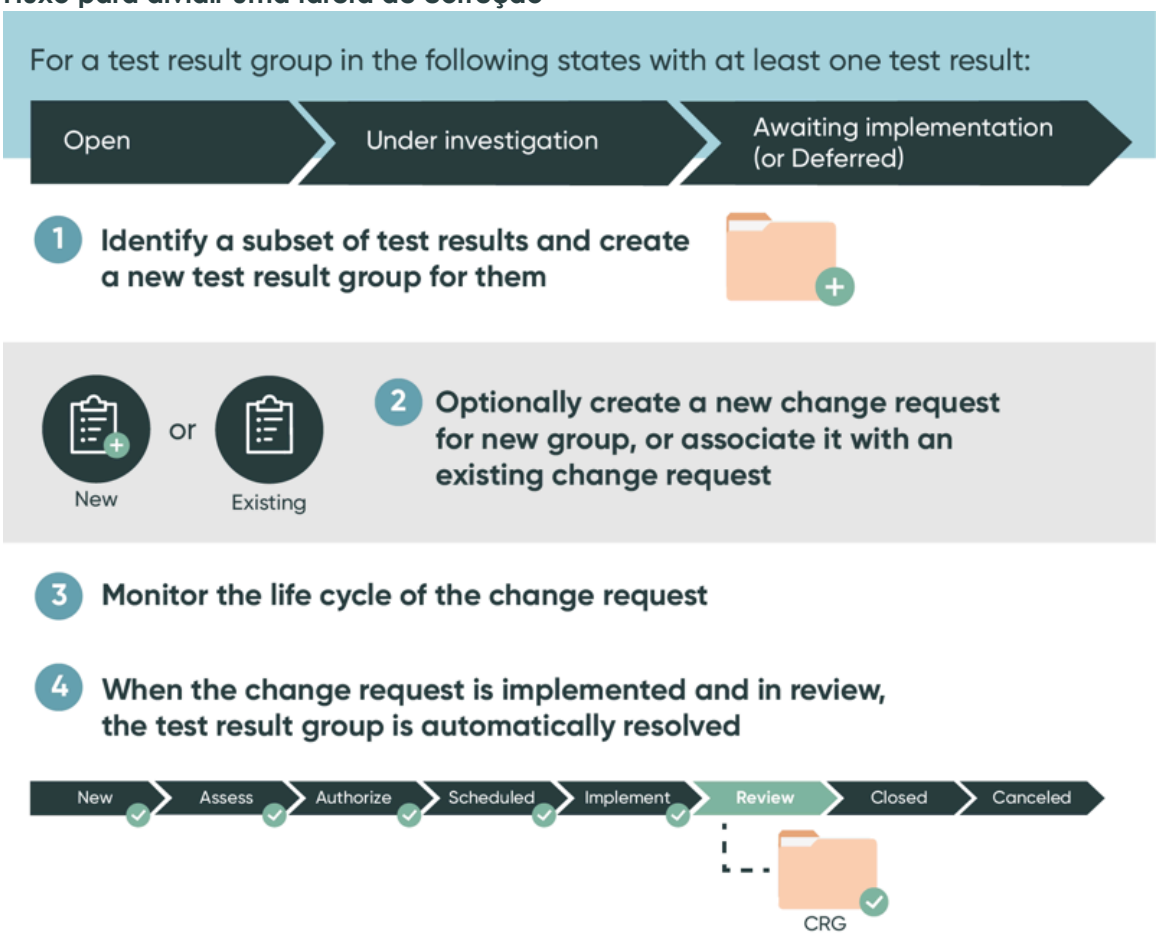
Antes de Iniciar
Função necessária: um usuário com a função itil

Por Que e Quando Desempenhar Esta Tarefa
Como especialista em TI ou em correção, você pode dividir as tarefas de correção existentes nos estados **Aberto**, **Sob investigação**ou **Aguardando implementação** com mais de um resultado de testes. Ao criar uma nova Tarefa de correção com resultados de testes que correspondem a critérios específicos, você pode trabalhar com um grupo específico de resultados de testes sem afetar a tarefa de correção original.

Quando você especifica as condições dos resultados de testes que deseja mover para uma nova tarefa de correção com o Construtor de condições, somente os resultados de testes ativos que correspondem aos seus critérios são movidos para a nova tarefa. Você não é obrigado a criar solicitações de mudança (CHGs) ao dividir uma tarefa de correção. Você tem a opção de dividir uma tarefa de correção ao mesmo tempo em que cria uma solicitação de mudança ou pode dividir uma tarefa de correção sem criar uma solicitação de mudança.

A imagem a seguir ilustra o fluxo básico para dividir uma tarefa de correção. As etapas detalhadas para este fluxo seguem a imagem.

Fluxo para dividir uma tarefa de correção



Os casos de uso para dividir resultados de testes de Tarefas de correção existentes em novas tarefas podem incluir os seguintes exemplos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando você deseja criar uma solicitação de mudança ou solicitações de mudança para um grupo dividido.
- Quando você reatribui uma tarefa de divisão a outro usuário em seu grupo de atribuição.
- Quando você solicita um adiamento ou uma exceção para uma tarefa dividida porque sabe que alguns resultados de testes em itens de configuração (IC) específicos não podem ser corrigidos em um determinado intervalo de tempo.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Testes** > **Tarefas de correção** > **Minhas Tarefas em Aberto**.
   A lista de Tarefas de correção atribuídas aos seus grupos é exibida.
2. Na coluna Número, clique na tarefa de correção que você deseja dividir.

   O registro da Tarefa de correção é exibido.
3. Para criar um subconjunto de resultados de testes para uma nova tarefa que corresponda a critérios específicos, siga estas etapas.

   No canto superior direito do registro, clique em **Dividir grupo**.

   Você pode preferir este método de criação de um novo grupo se estiver trabalhando em um grupo grande com vários resultados de testes.

   O formulário Dividir tarefa de correção é exibido.
4. Com o construtor de condições exibido, especifique as condições dos resultados de testes que você deseja mover para uma nova tarefa de correção.

   Por exemplo, você pode preferir filtrar somente os resultados de testes que correspondam às seguintes condições:

   - No estado **Aberto**.
   - Pontuações de risco superiores a 75.
   - O resultado é **Falha**.

   Se os resultados de testes corresponderem ao seu filtro depois de inserir as condições, será exibida uma mensagem com o número de resultados de testes correspondentes.

   Se for exibida uma mensagem informando que nenhum resultado de testes corresponde ao seu filtro ou que todos os resultados de testes correspondem aos seus critérios, ajuste as condições para que pelo menos um resultado de testes corresponda aos critérios do filtro.
5. Clique em **Visualizar itens** para exibir os resultados de testes correspondentes.
   Uma nova janela, Tarefas de correção, exibe os itens.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Para visualizar detalhes sobre os resultados de testes que correspondem aos seus critérios de filtro, siga estas etapas antes de clicar em **Dividir grupo** para criar o novo grupo. Esses detalhes incluem o grupo de atribuição e a quem o resultado do teste foi atribuído. Exibir essas informações na visualização pode ajudar a garantir que a nova tarefa seja atribuída corretamente.

   a. Com a lista de Correções exibida na visualização, clique em um item na coluna Resultado.
   O registro Resultado de testes é exibido.

   b. Verifique se os campos **Grupo de atribuição** e **Atribuído a** estão corretos.

   c. Clique em **Atualizar**.

7. Quando estiver pronto para criar o novo grupo, clique em **Dividir grupo**.
   Uma mensagem indica o número de resultados de testes movidos para o novo grupo e a nova tarefa de correção é exibida. Para ajudá-lo a identificar a nova tarefa, talvez você prefira editar o texto no campo **Descrição resumida** e editar novamente os campos Grupo de atribuição ou Atribuído a, se necessário.

   Nota: Para menos de 200 resultados de testes, a operação de divisão é feita de forma síncrona e os resultados de testes são exibidos na nova tarefa.

   Para mais de 200 resultados de testes, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os resultados de testes apareçam na nova tarefa. A mensagem a seguir também é exibida: `n resultados de testes serão movidos de TRGxxxxxxx para o novo grupo de resultados de testes GRCxxxxxx em breve.`

8. Como alternativa, você pode criar uma nova tarefa de correção selecionando resultados de testes diretamente na lista relacionada Resultados de testes em uma tarefa de correção.

   Você pode preferir este método se tiver apenas alguns resultados de testes em um grupo ou se souber exatamente quais testes deseja mover para uma nova tarefa.

   a. Com o registro da tarefa de correção exibido, role até a lista relacionada Resultados de testes.

   b. Na coluna mais à esquerda, marque as caixas de seleção dos resultados de testes para os quais você deseja criar uma nova tarefa de correção.

   c. Na lista Ações em linhas selecionadas no canto inferior esquerdo do registro, clique em **Dividir grupo**.

   d. No formulário Dividir tarefa de correção que é exibido, para ajudá-lo a identificar o novo grupo, talvez você prefira editar o texto no campo **Descrição resumida**.

   e. Clique **em Dividir grupo**.
   Uma mensagem indica o número de resultados de testes que foram movidos para a nova tarefa e a nova tarefa de correção é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que a solicitação de mudança para esta tarefa de correção for resolvida, se não houver outras solicitações de mudança em aberto associadas a esta tarefa de correção, a tarefa de correção também será movida para o estado **Resolvido**.

Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados das solicitações de mudança não movem automaticamente a tarefa de correção dos estados `Encerrado` ou `Adiado`.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

O que Fazer Depois

Você pode criar ou associar solicitações de mudança para suas novas tarefas de correção. Para obter mais informações, consulte Associar uma tarefa de correção a uma solicitação de mudança existente e Como criar uma solicitação de mudança no Conformidade de configurações.

Remover atribuições de tarefas de correção para você ou seus grupos

Reatribua os registros de resultado de testes na aplicação Conformidade de configurações se os registros tiverem sido atribuídos incorretamente a você ou ao seu grupo.

Antes de Iniciar

Função necessária: sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

A partir da v14.3 da aplicação Conformidade de configurações, se você determinar que as tarefas de correção (RTs) e os resultados de testes associados não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou a seus grupos, convém remover a si mesmo ou seus grupos de os campos Atribuído a e Grupo de atribuição nos registros do TRG.

O botão **Cancelar atribuição** é exibido em registros de tarefa de correção em qualquer estado que não seja Encerrado ou Resolvido.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até um registro de tarefa de correção atribuído a você que esteja em qualquer estado diferente de Encerrado ou Resolvido.
2. Para limpar os campos **Atribuído a** e **Grupo de atribuição**, na parte superior do registro, selecione **Cancelar atribuição**.
3. Na caixa de diálogo **Cancelar atribuição**, forneça anotações de trabalho e selecione **Enviar**.
   - As anotações de trabalho fornecidas são exibidas na seção Anotações.
   - Na guia **Aprovação** de mudança de estado, o registro de aprovação de mudança de estado (CA#) exibe o estado Em revisão, o que ajuda a rastrear o fluxo de trabalho de aprovação.
   - Na guia **Aprovações solicitadas**, sua solicitação para a remoção de você ou seu grupo de atribuição é exibida como o estado Solicitado.

Resultados

A solicitação é aprovada usando um fluxo de trabalho de aprovação padrão de um nível. Para obter mais informações, consulte Aprovação de uma solicitação de não atribuição em Conformidade de configurações.

- Se sua solicitação for aprovada, o registro de aprovação de mudança de estado e o registro de aprovação solicitada passarão para **Aprovado**. Você e seus grupos são removidos dos campos **Atribuído a** e **Grupo de atribuição**. `Não atribuído` é exibido no campo **Tipo de atribuição** e a tarefa de correção é exibida na lista do módulo Não atribuído para a aplicação Conformidade de configurações.

  As notificações de que os registros não estão atribuídos são enviadas automaticamente para gerentes de vulnerabilidade ou analistas no grupo Notificação de não atribuição. Para obter mais informações sobre as notificações e as propriedades desse recurso, consulte Remoção de atribuições de grupos de resultados de testes de Conformidade de configurações.

- Se sua solicitação for rejeitada, o registro de aprovação de mudança de estado e o registro de aprovação solicitada passarão para Rejeitado.

Nota: Como administrador de vulnerabilidades, você pode definir a propriedade do sistema *`sn_vulc.unassign_test_result_group.approval_required`* como **falsa** para desabilitar o processo de aprovação.

O que Fazer Depois

Navegue até o módulo Não atribuído da aplicação Conformidade de configurações para monitorar todos os registros não atribuídos de itens que possam se enquadrar no seu escopo e reatribua-os a você mesmo.

Aprovar uma solicitação de não atribuição no Conformidade de configurações

Aprove solicitações para a remoção de tarefas de correção de um grupo de atribuição ou de um usuário individual na aplicação Conformidade de configurações.

Antes de Iniciar

Função necessária: sn_vulc.unassign_approver

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, uma configuração de aprovação é fornecida. Para aprovações não atribuídas, é necessário um aprovador no grupo de aprovação Aprovador – Nível 1. Por padrão, o grupo de aprovação não atribuído (`Cenular atribuição do aprovador CC - nível`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1) é criado e os usuários que fazem parte desse grupo podem aprovar a solicitação. Por padrão, este grupo contém a função de aprovador unassign, sn_vulc.unassign_approver. Você pode modificar ou criar um grupo e atualizar a configuração de aprovação navegando até **Todos** > **Conformidade de configurações** > **Minhas aprovações** > **Regras de aprovação** > **Solicitação de mudança do campo do grupo de resultados de testes** > **Cancelar atribuição de grupo de resultados de testes**.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Minhas aprovações**.
2. Selecione uma solicitação da fila.
3. Aprove ou rejeite a solicitação adicionando os comentários apropriados.

Fechamento automático de resultados de testes

Você pode fechar automaticamente os resultados de testes (TRs) associados a itens de configuração (ICs) desativados.

Para configurar a opção de fechamento automático, navegue até a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** e defina-a como verdadeira. Para fechar automaticamente TRs relacionados a ICs desativados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

Para obter informações sobre como trabalhar com itens de configuração desativados, consulte Como trabalhar com itens de configuração desativados na Conformidade de configuração.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Como trabalhar com itens de configuração desativados na Conformidade de configuração

Itens de configuração (ICs) desativados são movidos para o estado desativado, arquivado ou excluído no Configuration Management Database (CMDB). Conformidade de configurações contém resultados de testes (TRs) que são compostos por ICs. Quando o estado de um IC é atualizado para desativado, os TRs associados são encerrados com o subestado "IC desativado".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Se o CMDB mudar o status da fase do ciclo de vida de um IC para descontinuado, você poderá optar por fechar automaticamente os TRs associados. Para obter mais informações sobre como fechar automaticamente os TRs associados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

O IC desativado será eventualmente arquivado ou excluído permanentemente do CMDB.

Impacto da descontinuação dos ICs:

- **Impacto nos itens descobertos:** quando o IC é descontinuado, o DI relacionado é marcado como "IC desativado".
- **Impacto nos resultados de testes:** quando o estado de uma DI é atualizado para "IC desativado", o TR associado é encerrado e a seção Anotações é atualizada automaticamente.

Nota: O estado de um DI é atualizado automaticamente para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um TR é atualizado para Encerrado somente quando a propriedade **sn_vulc.auto_close_test_results_linked_to_retired_CIs** está definida como verdadeira. Para obter mais informações sobre como fechar automaticamente os TRs associados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

O trabalho agendado *Close Test Results for decommissioned CIs* é executado diariamente para as DIs atualizadas. Se a opção de configuração de fechamento automático estiver habilitada para ICs desativados, ela identificará a DI que contém um IC desativado e fechará o TR relacionado com o subestado "IC desativado". Se todos os TRs em uma tarefa de correção estiverem encerrados e seu subestado for IC desativado, a tarefa de correção também será encerrada com o subestado "Cancelado".

Nota: Se um IC voltar ao estado original do estado "Descontinuado", a entrada "Itens descobertos" também será atualizada. Os TRs são abertos automaticamente quando os dados são ingeridos novamente do scanner.

Fechar automaticamente os resultados de testes relacionados a ICs desativados

Se o Configuration Management Database (CMDB) mudar o status da fase do ciclo de vida de um item de configuração (IC) para desativado, você poderá optar por fechar automaticamente os resultados de testes associados (TRs).

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Para fechar automaticamente os TRs associados, você deve habilitar a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** para fechar automaticamente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

os TRs associados a ICs desativados. Se esta opção estiver habilitada, TRs novos e existentes relatados para o mesmo IC serão criados ou atualizados automaticamente no estado "Encerrado". Eles são baseados no ID do ativo na carga do scanner e no status de entrada dos itens descobertos. Para obter mais informações sobre o impacto dos ICs desativados, consulte Como trabalhar com itens de configuração desativados na Conformidade de configuração.

Nota: O estado de uma DI é atualizado para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um TR é atualizado para Encerrado somente quando a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** está habilitada.

Procedimento

1. Navegar até **Propriedades do sistema** > **Todas as propriedades** e filtrar por *sn_vulc.auto_close_test_results_linked_to_retired_CIs* na coluna Nome.
2. Selecione a propriedade.
3. Para fechar automaticamente os resultados de testes associados aos ICs desativados, defina o valor da propriedade como verdadeiro.

Fechando automaticamente os resultados de testes obsoletos no Conformidade de configurações

Você pode ativar o recurso de fechamento automático de resultados de testes obsoletos para fechar automaticamente os resultados de testes mais antigos que não foram encontrados recentemente por suas integrações de terceiros. Mover esses resultados de testes para **Encerrado-Obsoleto** reduz o número de resultados de testes ativos e tarefas de correção em sua instância e ajuda a reconciliar ativos em seu Configuration Management Database (CMDB).

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Visão geral

O módulo Fechar automaticamente resultados de testes obsoletos ajuda a fechar automaticamente resultados de testes mais antigos e obsoletos que não foram encontrados recentemente por suas integrações de terceiros. Os resultados de testes são movidos para **Closed-Obsoleto** com base nas condições definidas no Construtor de condições.

Termos principais

Resultado do teste

Os resultados de testes são resultados importados de bibliotecas de testes de configuração que são mapeados para estruturas, políticas e fontes autorizadas que definem como uma classe de ativos de tecnologia deve ser regida. A

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aplicação Conformidade de configurações não calcula os resultados de testes, mas os importa com integrações de terceiros.

Data da última verificação do ativo

Refere-se ao valor da coluna Data da última verificação de conformidade da tabela Item descoberto que está relacionada ao resultado do teste. Esta data se refere à data e hora mais atuais em que um ativo foi verificado pela última vez por um scanner de terceiros.

Data da última falha

Refere-se à data da coluna Visto pela última vez da tabela Resultados de testes quando o valor do campo **Resultado** é [falha].

Resultados de testes obsoletos

Refere-se aos resultados de testes em sua instância que são antigos e não foram encontrados, atualizados ou detectados por verificações de integração de terceiros por um período significativo.

Últimos resultados de testes encontrados

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data mais atual ou mais recente (dias atrás) em que os resultados de testes foram encontrados novamente pelo scanner. Este parâmetro pode ser configurado.

Caso de uso

Às vezes, os ativos (itens de configuração) podem ser desativados em seu ambiente ou limpos por scanners de terceiros. Quando isso acontece, os resultados de testes de configuração associados aos ativos não são atualizados na aplicação Conformidade de configurações por detecções importadas e se tornam inativos (obsoleto).

Para reduzir o número de resultados de testes ativos (TRs) e tarefas de correção (RTs) em sua instância, ative o recurso de fechamento automático de resultados de testes obsoletos. Este recurso fecha automaticamente os resultados de testes antigos que têm estados inalterados ou que não foram importados recentemente por suas integrações.

Por exemplo, suponha que um item de configuração (IC) específico tenha vários IDs de ativo e um desses IDs não tenha sido importado em detecções de um scanner de terceiros nos últimos 90 dias. Se você definir o construtor de condições no módulo Fechar automaticamente resultados de testes obsoletos para fechar resultados de testes que não foram encontrados ou atualizados nos últimos 90 dias ou mais, este recurso fechará automaticamente todos os resultados de testes que correspondam a esta filtragem.

Nota: Este recurso só encerra detecções de resultado de testes com base nas condições de filtro que você define no Construtor de condições e são detectadas por suas integrações de scanner de terceiros.

O campo Resolução

Para diferenciar entre as detecções que são encerradas por scanners de terceiros, como os produtos Qualys e Tenable.io e o recurso de fechamento automático de resultados de testes obsoletos em sua instância, um novo valor para o campo **Resolução**, [Closed-Stale], foi foi adicionado. **Encerrado-obsoleto** indica que um TR foi encerrado pelo recurso de fechamento automático. **Encerrado** ou **Fixo-Encerrado** indica que um TR foi encerrado por um scanner.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acúmulo de estados de TR para TRGs com o recurso de fechamento automático

A progressão do estado e a precedência dos resultados de testes são: **Aberto** > **Encerrado** > **Fixo-Fechado** > **Encerrado-Obsoleto**.

1. Se algum TRs em um TRG estiver **Aberto**, o estado do TRG não será alterado.
2. Se pelo menos um TR for **Encerrado - Fixo** e o restante for **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Fixo**.
3. Se todos os TRs em um TRG forem **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Cancelado**.

Integrações compatíveis

Para obter mais informações sobre as integrações de terceiros que oferecem suporte a este recurso, consulte Noções básicas sobre Qualys Vulnerability Integration e Tenable.io integrações com as aplicações Resposta a vulnerabilidades e Conformidade de configurações.

Usar fechamento automático de resultados de testes obsoletos no Conformidade de configurações

Ative o fechamento automático de resultados de testes obsoletos (TRs) para fechar automaticamente os resultados de testes mais antigos com base nas condições de filtro definidas.

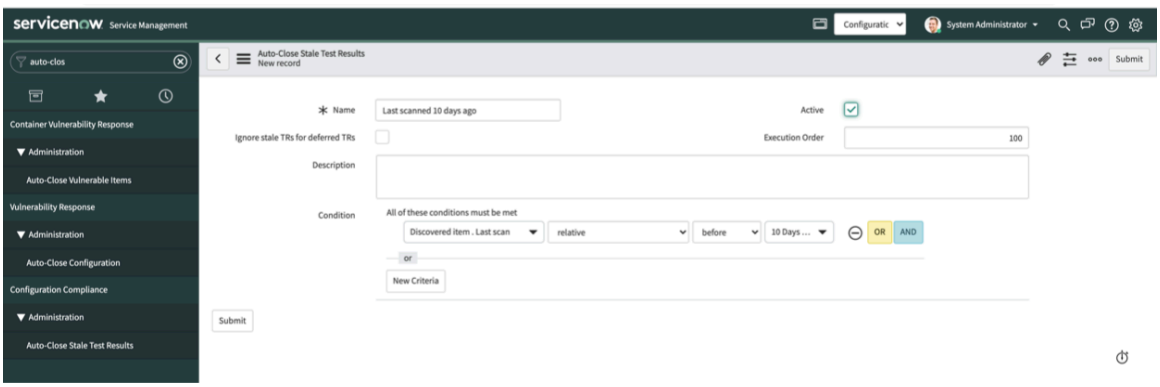
Antes de Iniciar

Para obter mais informações sobre esse recurso, termos-chave e qualquer configuração que possa ser necessária para suas integrações de terceiros que importam dados de resultados de testes, consulte Fechando automaticamente os resultados de testes obsoletos no Conformidade de configurações.

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Administração** > **Fechar automaticamente os Resultados de testes obsoletos**.
2. No formulário, preencha os campos.



Campo	Valor
Nome	Nome para este registro de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
Ativo	Se selecionado, este registro estará ativo e fechará automaticamente todos os resultados de testes que correspondam aos critérios de filtro.
Ignorar TRs obsoletos para TRs adiados	Se selecionado, todos os TRs mapeados para os estados **Em revisão** ou **Adiado** serão ignorados e não encerrados. Se você desmarcar esta opção, todos os TRs que corresponderem aos seus critérios serão encerrados.
Ordem de execução	100 é o valor padrão. Este valor determina a ordem de execução em ordem crescente para cada registro de configuração usado para localizar e marcar resultados de testes que estão obsoletos.
Descrição	Uma descrição para este registro. Este texto pode ajudá-lo a encontrá-lo facilmente se você criar um número maior de registros.
Condição	As condições de filtragem usadas para encontrar TRs que você deseja fechar. O filtro padrão é **Item descoberto** > **Últimas varreduras** > .

3. Clique em **Enviar**.

   O trabalho agendado, *Auto-Close Stale Test Results*, é executado diariamente. Este trabalho identifica os TRs com base nas condições que você forneceu e faz a transição daqueles que correspondem a **Closed-Stale**.

   Depois que os TRs forem marcados como **Closed-Obsoleto**, se o scanner encontrar esses TRs novamente, os resultados de testes serão reabertos e os estados passarão para**Aberto**.

   Se um TR estiver marcado como **Closed-Obsoleto**e o scanner descobrir que ele foi corrigido, o TR passará para**Closed-Fixed**. Os estados também são acumulados para tarefas de correção conforme descrito na lista a seguir:

   a. Se algum TRs em uma tarefa de correção estiver **Aberto**, o estado da tarefa de correção não será alterado.

   b. Se pelo menos um TR for **Encerrado - Fixo** e os demais forem **Encerrado - Obsoleto**, o estado da tarefa de correção mudará para **Encerrado - Fixo**.

   c. Se todos os TRs em uma tarefa de correção forem **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Cancelado**.

Fechar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção pode ser encerrado imediatamente sem análise adicional, poderá usar o recurso **Fechar**.

Antes de Iniciar

Função necessária:

- sn_vulc.admin
- sn_vulc.remediation_owner

Nota: Com a função sn_vulc.remediation_owner, você pode reatribuir ou fechar tarefas de correção atribuídas a você ou aos seus grupos de atribuição.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A partir da v15.0 de Conformidade de configurações, o botão **Fechar** foi removido para uma tarefa de correção.

Quando você resolve uma tarefa de correção, as anotações de resolução são refletidas nas anotações de trabalho de todos os resultados de testes.

Procedimento

1. Abra o registro da tarefa de correção.
2. Selecione o botão **Fechar**.
3. Descreva por que o problema está sendo encerrado na janela pop-up.
4. Selecione **Fechar**.

Informações relacionadas

Conformidade de configurações estados

Como solicitar e aprovar uma exceção para uma tarefa de correção

Você pode solicitar o adiamento da correção de uma tarefa de correção por um período especificado. Os usuários que fazem parte do grupo de aprovadores podem aprovar solicitações de exceção.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Para solicitar ou aprovar solicitações de exceção, consulte:

- Solicitar uma exceção para uma tarefa de correção no Conformidade de configurações
- Aprovar uma solicitação de exceção no Conformidade de configurações

Nota:

As notificações por e-mail são enviadas em todas as fases da gestão de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v14.11 de Conformidade de configurações, você pode configurar os intervalos de tempo para aprovar exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o resultado do teste muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o resultado do teste será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar uma exceção para uma tarefa de correção no Conformidade de configurações

Solicite uma exceção para adiar a correção de uma tarefa de correção por um período especificado se ela não puder ser corrigida imediatamente.

Antes de Iniciar

Função necessária: sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Importante: Você pode solicitar uma exceção para:

- tarefas de correção em Vulnerability Manager Workspace e Espaço de correção de problemas de TI. Para obter mais informações, consulte Solicitar uma exceção no Espaço de correção de problemas de TI.
- vários resultados de testes simultaneamente do Vulnerability Manager Workspace. Para obter mais informações, consulte Solicitar exceção em massa no Espaço do gerenciador de vulnerabilidades.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Tarefas de correção** > **Todas as tarefas**.
2. Selecione a tarefa de correção para a qual você deseja solicitar uma exceção. A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No formulário Tarefa de correção, clique em **Solicitar exceção**.

   Nota: Dependendo se Resposta a vulnerabilidades ou GRC: Gestão de políticas e conformidade está selecionado no **Conformidade de configurações** > **Gestão de exceção** Na tela, o formulário Solicitar exceção muda. Veja Configurar Gestão de exceções para Conformidade de configurações

4. Se Resposta a vulnerabilidades for selecionado na tela Gestão de exceções, faça o seguinte:

   a. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	da duração selecionada em **Todos** > **Conformidade de configurações** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado Aberto. **Nota:** A partir da versão 14.7 do Conformidade de configurações (CC), se uma tarefa de correção adiada for reaberta por um scanner antes que a janela de exceção expire, o estado da tarefa de correção mudará de Aberto para Adiado. Esta funcionalidade está desabilitada por padrão. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema *sn_vulc.auto_defer_test_result_in_active_exc* como verdadeiro. Além disso, a data adiada até persiste mesmo depois que a tarefa de correção é reaberta após a data de expiração.
Motivo	Motivo da exceção. Estas são as opções: ▪ Risco aceito ▪ Aguardando janela de manutenção ▪ Correção indisponível ▪ Redução do controle no local ▪ Outro Para ver como adicionar novas opções de motivo, consulte Definir mapeamentos de motivo da política.
Informação adicional	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Solicitar aprovação**.

Resultados
O estado da tarefa de correção muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma extensão para uma regra de exceção no Conformidade de configurações

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer esta solicitação.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão nos espaços Resposta a vulnerabilidades. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ◦ Risco aceito ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção associadas. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar uma exceção para tarefas de correção usando GRC: Gestão de políticas e conformidade

Solicite exceções de política usando a capacidade de gestão de exceções de política GRCGestão de políticas e conformidade na aplicação [] de dentro de Conformidade de configurações.

Antes de Iniciar

Antes de poder usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Gestão de políticas e conformidade do ServiceNow Store.

Função necessária: sn_vulc.remediation_owner

Você também pode solicitar exceções na IU clássica.

Por Que e Quando Desempenhar Esta Tarefa

A partir da versão 19.0 do Resposta a vulnerabilidades, você pode solicitar exceções às políticas para Tarefas de correção (RTs) no Espaço de correção de TI. Para obter mais informações, consulte Solicitar uma exceção usando GRC: Gestão de políticas e conformidade no Espaço de correção de problemas de TI.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades de aplicações** > **Itens vulneráveis da aplicação** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.
3. Se GRC: Gestão de políticas e conformidade for selecionado na tela Gestão de exceções, faça o seguinte.

   a. No formulário, preencha os campos.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	estiver selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e quando o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Solicitar aprovação**.
O estado da tarefa de correção muda para Em revisão e uma exceção à política é criada. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

c. Exiba a exceção à política clicando na lista relacionada Exceções às políticas.

d. Clique no número da exceção à política.

e. No campo **Aprovador**, selecione o nome do aprovador.

f. Clique na guia Origem e selecione um objetivo de **controle no campo Objetivo** de controle.

g. Clique na guia Avaliação de risco e selecione a classificação de **risco** no campo Classificação de risco.

h. Salve o formulário.

i. Clique na guia **Controles afetados**.

j. Adicione os controles clicando em **Adicionar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

k. Salve o formulário.

> **Nota:** Você pode gerar uma revisão de conformidade clicando em **Solicitar revisão de conformidade**.

O formulário de aprovação é enviado ao aprovador.

O aprovador pode aprovar a solicitação clicando em **Aprovar** ou solicitar aprovação adicional clicando em **Solicitar aprovação adicional**.

O estado do registro muda para Adiado. O motivo declarado é aquele que você selecionou ao gerar a solicitação de exceção. A guia **Adiamento** fornece anotações adicionais sobre o registro.

> **Nota:** Se a solicitação for rejeitada, o registro será movido para o estado anterior.

4. Clique em **Enviar**.
Para obter mais informações sobre a integração de exceção à política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Aprovar uma solicitação de exceção no Conformidade de configurações

Aprove solicitações de exceção para tarefas de correção que não podem ser corrigidas imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar
Função necessária: sn_vulc.exception_approver

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Minhas aprovações**.

2. Selecione uma solicitação da fila.

3. Aprove ou rejeite a solicitação com os comentários apropriados.

> **Nota:** No caso de um fluxo de trabalho de aprovação de dois níveis, após a aprovação de primeiro nível, a solicitação é enviada para o segundo nível para aprovação posterior. Se não houver usuários no segundo nível, a solicitação será aprovada automaticamente após a aprovação de primeiro nível.
>
> Depois que a solicitação é aprovada, a tarefa de correção é movida para um estado Adiado. Em caso de rejeição, a tarefa de correção será revertida para o estado anterior.

Definir mapeamentos de motivo da política

Você pode definir as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar
Função necessária: sn_vul.compliance.manager e sn_vulc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Políticas e conformidade** > **Exceções às políticas** > **Registro de Integração**.

   Nota: Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Escolhas de motivo ou adicionar um novo motivo.

2. Clique no registro de integração do Container Vulnerability Response - CVIT.
3. Para adicionar uma opção de motivo existente, execute as seguintes etapas:
   a. Na lista Escolhas de motivo, clique em **Novo**.
   b. Clique no ícone de lupa para selecionar um motivo.
4. Para adicionar novas opções de motivo à tabela Escolhas de motivo, execute as seguintes etapas:
   a. Na lista Escolhas de motivo, clique em **Novo**.
   b. Clique no ícone de lupa.
   c. Clique em **Nova**.
   d. No formulário, preencha os campos.

Formulário Lista de seleção de motivo

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamentos de motivo de exceção à política para as respectivas aplicações. Para navegar até esta tabela, insira sn_sec_cmn_policy_reason_mapping.LIST no navegador de filtros.
Ordem	Ordem para esta opção. Os motivos são ordenados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção à política sob demanda for solicitada. Se o registro de integração não contiver nenhuma opção específica da aplicação, todas as opções de motivo com o campo **Padrão** selecionado estarão disponíveis.
Ativo	Opção para exibir a opção na lista de opções de motivo.

5. Clique em **Enviar**.

Análise e emissão de relatórios para Conformidade de configurações

Os relatórios a seguir são fornecidos para monitoramento.

Exiba políticas, ICs, testes e resultados de testes nos relatórios de visão geral Conformidade de configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Conformidade de configurações emissão de relatórios

A página inicial Conformidade de configurações fornece uma exibição executiva de políticas, ICs, testes e resultados de testes, ajudando a equipe de segurança a identificar rapidamente as áreas de preocupação. Conformidade de configurações gráficos de significância podem ser adicionados, conforme necessário. Você também pode retornar informações relacionadas a Conformidade de configurações usando o recurso de pesquisa global.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

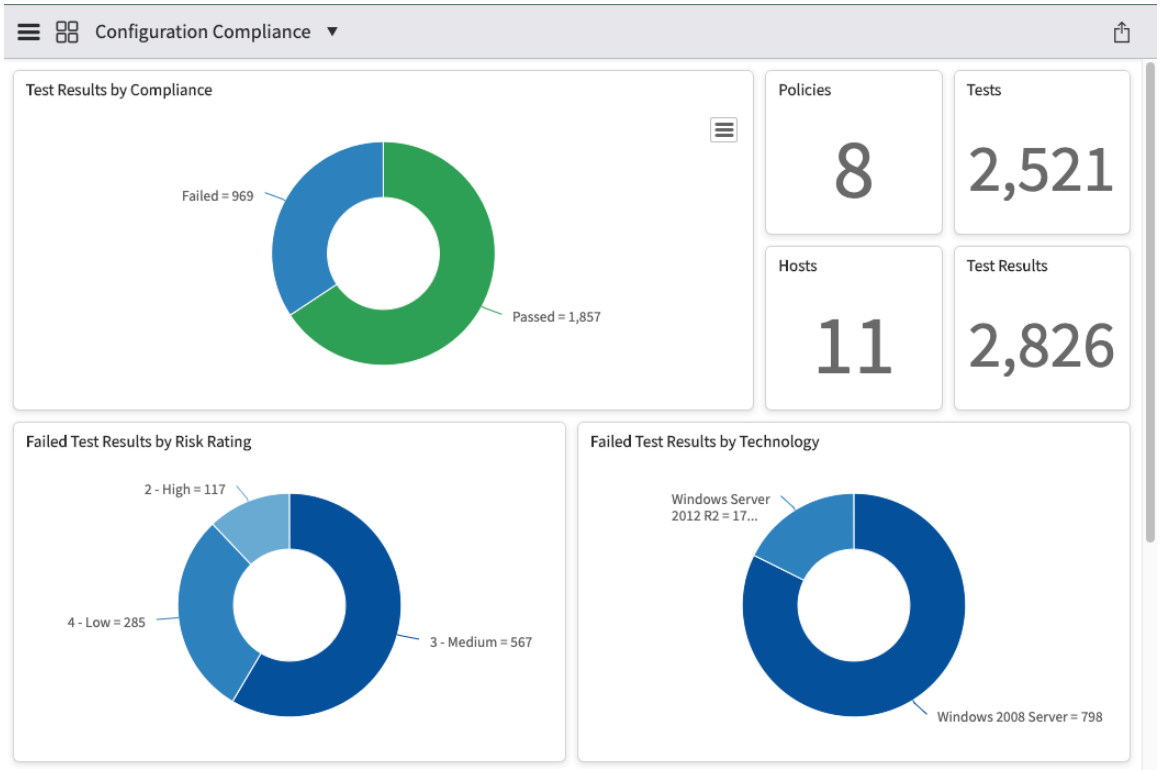
Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados) para exibir dados gerais específicos dessa parte do gráfico. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Nota: Qualquer pessoa com a função sn_vulc.read pode exibir o painel. Qualquer pessoa na função sn_vulc.write ou sn_vulc.admin pode criar e editar um painel. Somente sn_vulc.admin pode excluir um painel.

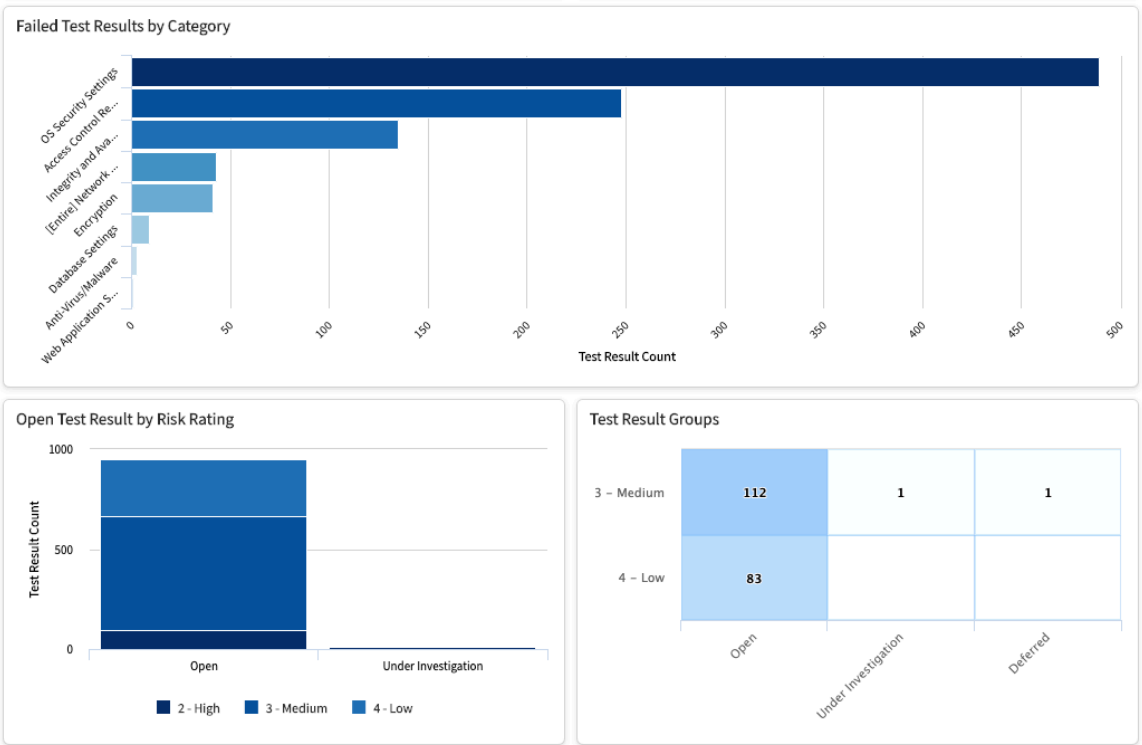
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral de vulnerabilidade



Relatório de Conformidade de configuração



Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Resultados de testes por conformidade	Donut	Exibe o número de testes abertos que foram aprovados ou reprovados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Políticas	Número	Número de políticas com resultados de testes com falha.
Testes	Número	Número de testes com resultados de testes com falha.
Hosts	Número	Número de hosts com resultados de testes com falha.
Resultados de testes	Número	Exibe o número de resultados de testes.
Resultados de testes com falha por classificação de risco	Donut	Exibe o número de testes com falha por classificação de risco.
Resultados de testes com falha por tecnologia	Donut	Exibe modelos com testes com falha.
Resultados de testes com falha por categoria	Barra	Exibe as categorias com os resultados de testes com mais falhas.
Resultado de testes em aberto por classificação de risco	Barra	Exibe o número de resultados de testes em aberto por classificação de risco.
Tarefas de correção	Gráfico	Exibe tarefas de correção por estado e classificação de risco.

Conformidade de configurações painel

Este Solução Performance Analytics e relatórios contém conteúdo Performance Analytics e Emissão de relatórios pré-empacotado para uso com outros produtos Now Platform. Este Solução Performance Analytics e relatórios fornece visibilidade sobre o nível de host fora de conformidade e as configurações do plano de controle de nuvem.

Esta solução de análise da plataforma contém conteúdo pré-empacotado de análise de desempenho e emissão de relatórios para uso com outros produtos da Now Platform. Esta solução de análise da plataforma fornece visibilidade sobre configurações no nível do host e do plano de controle de nuvem fora de conformidade.

O painel Performance Analytics para Conformidade de configurações contém vários widgets que apresentam dados para diferentes dimensões. Ele fornece uma exibição abrangente das tendências de conformidade, problemas de configuração, tendências de correção e gestão de exceções.

Nota: O plug-in Performance Analytics para Conformidade de configurações deve ser instalado para exibir o painel Conformidade de configurações [PA] na estrutura Next Experience. Se não estiver instalado, você poderá exibir o painel existente, que foi criado usando a estrutura de emissão de relatórios.

Ativar Performance Analytics para Conformidade de configurações

Ative a aplicação do pacote de conteúdo ServiceNow Store para o Solução Performance Analytics e relatórios.

Antes de Iniciar

Ative a versão completa de assinatura de Performance Analytics na instância em que você está ativando este Solução Performance Analytics e relatórios. Você pode ativar Performance Analytics em uma instância de não produção sem comprar uma assinatura. Para obter mais informações, consulte Ativar assinatura da Análise de desempenho .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você precisa de uma conta Now Support e permissão para solicitar aplicações para as instâncias em consideração. A conta Now Support e a instância devem fazer parte da mesma empresa. Para obter mais informações, consulte Instalação de um produto da ServiceNow no ServiceNow Store.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Use Performance Analytics para o painel Conformidade de configurações para gerar relatórios sobre as tarefas de correção, o status de conformidade, as ações de correção e as solicitações de exceção.

Procedimento

1. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações** > **ServiceNow Store**.
2. Pesquise Performance Analytics para Conformidade de configurações e verifique se você tem direitos válidos.
3. Pesquise `Performance Analytics para Conformidade de configurações`.
4. Instale a aplicação.

   Ao instalar esta aplicação, você também ativa a aplicação Conformidade de configurações.

Exibição do painel Performance Analytics para Conformidade de configurações

Você pode gerenciar seus problemas de configuração mais importantes e corrigi-los rapidamente exibindo os relatórios no painel Conformidade de configurações Performance Analytics (PA).

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Funções necessárias de Now Platform

As funções a seguir são necessárias para o painel Conformidade de configurações Performance Analytics :

- admin: um administrador pode instalar e ativar o Performance Analytics para Conformidade de configurações e fazer mudanças nas propriedades do sistema.
- pa_admin: um administrador de análise de desempenho pode criar e revisar trabalhos em segundo plano, indicadores, detalhamentos, widgets e painéis. Este administrador também pode configurar e iniciar a coleta de dados.
- sn_vulc.read: um usuário com a função de leitura pode revisar os dados do painel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acessar o painel Conformidade de configurações

Para abrir o painel, navegue até **Todos** > **Conformidade de configurações** > **Visão geral**.

A partir da versão 14.9 do Conformidade de configurações, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Espaço do gerenciador de vulnerabilidades e Painéis no Espaço de correção de TI.

Nota: Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Conformidade de configurações [PA] guias do painel

Guia Visão Geral

A guia **Visão geral** fornece cinco filtros. Esses filtros são Categoria de ativo, Tipo de recurso de nuvem, Provedor de serviço em nuvem, Conta de nuvem e Região de nuvem, que você pode aplicar para visualizar os relatórios dos filtros aplicados. Se você selecionar uma categoria e aplicar as mudanças, todos os widgets compatíveis com a categoria serão atualizados. Cada widget exibe o filtro aplicado na parte inferior e o número de filtros aplicados no ícone de filtro do widget. Clique no relatório em um widget para exibir as informações adicionais na guia **Detalhes de KPI**. Na guia **Detalhes de KPI**, você pode:

- Mostrar os registros.
- Compare os registros.
- Mude o tipo de gráfico.
- Selecione o intervalo de datas.
- Exiba as tendências baseadas na duração.
- Aplique os filtros adicionais, incluindo os filtros que não estão disponíveis na guia **Visão geral**. Um exemplo é o marcador de host.

O exemplo a seguir mostra como você pode aplicar os filtros na guia **Visão geral** e executar as ações na guia **Detalhes de KPI**.

Guia Visão geral no painel Conformidade de configuração

Guia Conformidade

A guia **Conformidade** exibe a porcentagem de conformidade das várias fontes autorizadas, como a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) e a DISA (Data Interchange Standards Association). Você pode refinar esta lista usando os filtros de cabeçalho de coluna e selecionando uma categoria.

O exemplo a seguir mostra como você pode filtrar os dados na guia **Conformidade**.

Guia Conformidade no painel Conformidade de configuração

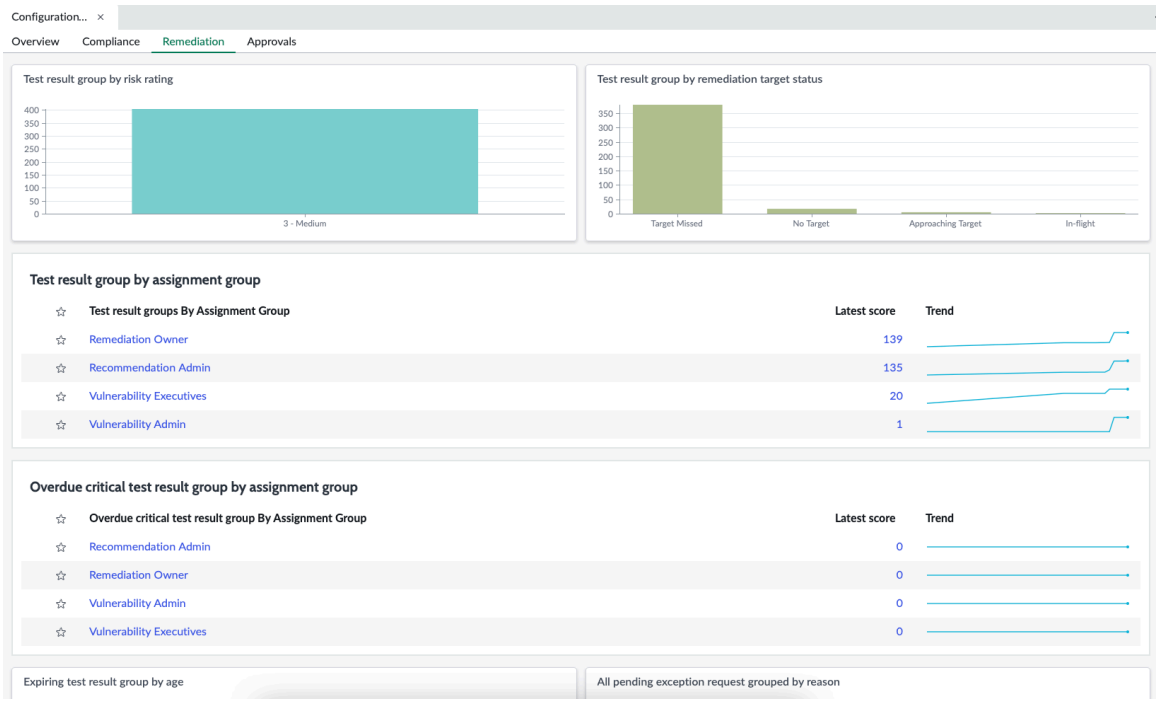
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Correção

A guia **Correção** exibe as informações sobre o andamento da correção. Você pode usar esta guia para ver a higiene de correção de erros de configuração.

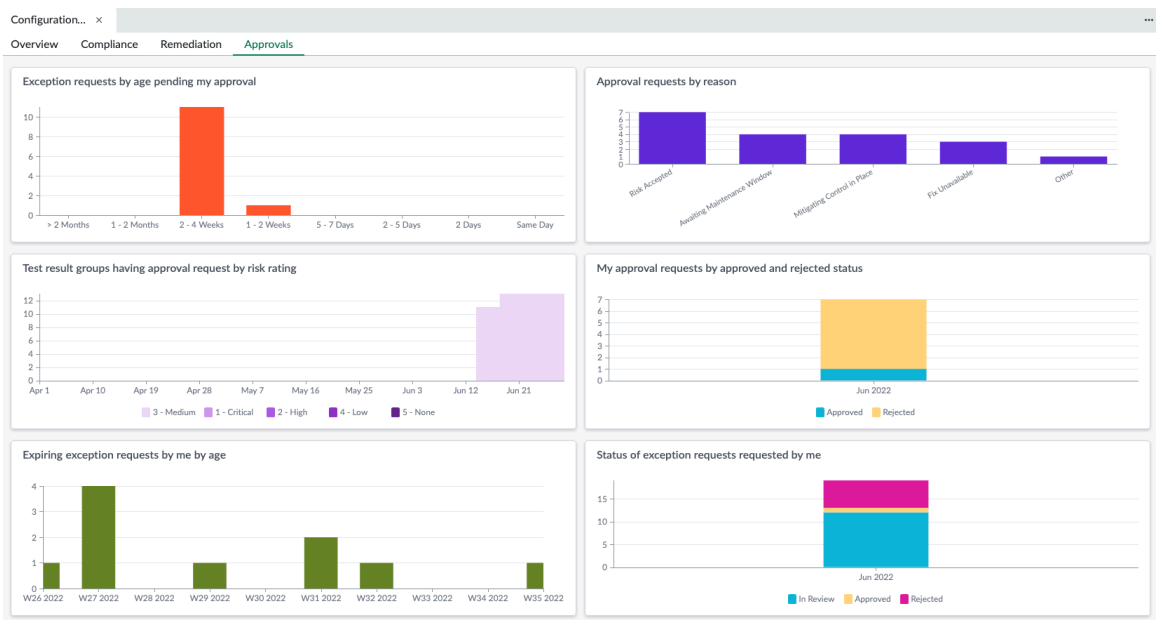
O exemplo a seguir mostra a guia **Correção**.



Guia Aprovações

Os relatórios na guia **Aprovações** exibem as informações sobre as solicitações de exceção e seu status de aprovação.

O exemplo a seguir mostra a guia **Aprovações**.



Detalhamentos

Os detalhamentos usados pelos indicadores são os seguintes:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Motivo adiado
- Idade
- Grupo de atribuição
- Status da Correção
- Resultado
- Pontuação de risco
- Categoria do ativo
- Marcador de host
- Teste de configuração
- Provedor de serviços em nuvem
- Região da nuvem
- Conta de nuvem
- Tipo de recurso de nuvem

Filtros

Na guia **Visão geral**, você pode aplicar os seguintes filtros aos widgets para visualizar os dados filtrados.

Nome	Tipo	Descrição
Categoria do ativo	Escolha	Tipo de ativo. As quatro opções são: • Nuvem • Contêiner • Infraestrutura • OT
Tipo de recurso de nuvem	Escolha	Tipo de recurso. Um exemplo é uma máquina virtual. Os dados no filtro são preenchidos quando você executa a integração.
Provedor de serviços em nuvem	Escolha	Provedor de serviço para a nuvem. As três opções são: • Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)

Tradução automática

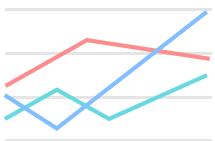
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Conta de nuvem	Escolha	ID da conta criada quando uma conta é criada em um serviço em nuvem. Por exemplo, AWS. Os dados de ID da conta são preenchidos no filtro quando você executa a integração.
Região da nuvem	Escolha	Local onde o recurso está hospedado.

Nota: Você pode selecionar várias opções nos filtros e selecionar **Aplicar**. Cada widget mostra os filtros aplicados e os filtros que não foram aplicados. Dependendo dos dados disponíveis, o relatório é gerado. O widget também mostra a contagem do filtro compatível.

Visualizações de dados

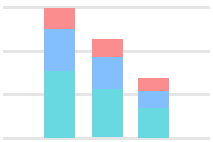
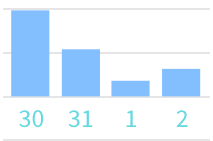
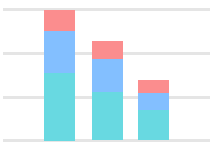
Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
Tendência de conformidade	Gráfico de linhas 	Resultados de testes	Informações sobre a tendência de conformidade: • Recursos: número total de recursos que estão disponíveis no sistema. • Falha: número de recursos com pelo menos um resultado de testes com falha. • Aprovado: número de recursos com todos os resultados de testes no estado aprovado.
Tarefa de Correção	Pontuação única	Resultados de testes	Número de tarefas de correção que estão presentes no sistema e em um estado ativo.
Tarefas de correção críticas próximas ao vencimento	Pontuação única	Resultados de testes	Número de tarefas de correção em que a classificação de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
			risco é "crítica" e o status de correção é "aproximando-se da meta".
Resultados de testes por classificação de risco	Barra 	Resultados de testes	Resultados de testes no estado de falha, que são agrupados de acordo com a classificação de risco.
Resultados de testes por idade	Barra 	Resultados de testes	Resultados de testes no estado de falha, que são agrupados de acordo com quando os resultados de testes foram criados.
Resultados de testes encerrados por adesão à meta de correção	Barra 	Resultados de testes	Resultados de testes no estado aprovado, o que indica que este teste está encerrado.
Resultados de testes críticos atrasado por grupo de atribuição	Listar e Pontuar	Resultados de testes	Número de resultados de testes em que a classificação de risco é "crítica" e o status de correção é "meta atingida". O relatório indica que os resultados de testes estão em um estado Aberto. Se os resultados de testes ultrapassarem a data da meta de correção, eles serão considerados atrasados.

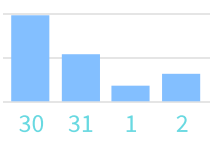
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
Resultados de testes atrasados - serviços	Lista, Pontuação e Tendência	Exibição do banco de dados de painéis do PA para serviços	Número de resultados de testes para serviços em que o status de correção é "meta não atingida". Este relatório também exibe o nome dos serviços ou departamentos com os resultados de testes mais altos.
Resultados de testes atrasados - responsáveis pelo serviço	Lista, Pontuação e Tendência	Exibição do banco de dados de painéis do PA para serviços	Número de resultados de testes para proprietários de serviço cujo status de correção é "meta não atingida". Este relatório também exibe o nome dos serviços ou departamentos com os resultados de testes mais altos.

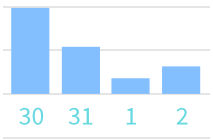
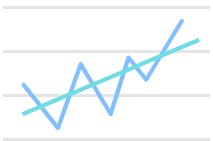
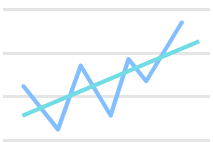
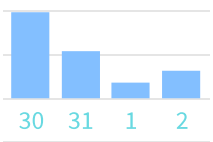
Visualizações da guia de correção

Título	Tipo	Tabela de origem	Descrição
Tarefa de correção por classificação de risco	Barra 	Tarefa de correção	Detalhamento das classificações de risco de todos os grupos de resultados de testes que estão no estado ativo.
Tarefa de correção por status da meta de correção	Barra	Tarefa de correção	Detalhamento das metas de correção de todos os grupos de resultados de testes que

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

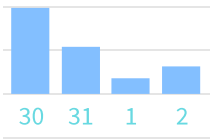
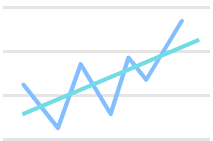
Visualizações da guia de correção

Título	Tipo	Tabela de origem	Descrição
			não atingiram a meta, não têm meta e estão se aproximando da meta.
Tarefa de correção por grupo de atribuição	Lista, Pontuação e Tendência 	Tarefa de correção	Detalhamento das tarefas de correção baseadas em um grupo de atribuição.
Tarefa de correção crítica em atraso por grupo de atribuição	Lista, Pontuação e Tendência 	Tarefa de correção	Detalhamento das tarefas de correção baseadas em um grupo de atribuição. Essas tarefas de correção têm uma classificação de risco "crítica" e sua meta de correção não foi atendida.
Tarefa de correção expirando por idade	Barra 	Tarefa de Correção	Tarefas de correção que vão expirar dentro de uma determinada duração. É possível criar no máximo 10 buckets de duração.
Todas as solicitações de exceção pendentes	Barra	Aprovação de mudança de estado	Solicitações de aprovação de mudança de estado

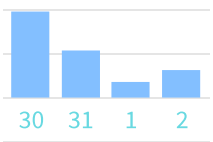
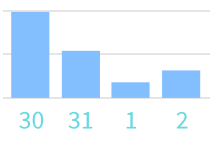
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia de correção

Título	Tipo	Tabela de origem	Descrição
agrupadas por motivo			que são agrupadas pelo motivo da exceção.
Exceções críticas nos resultados de testes por grupo de atribuição	Lista, Pontuação e Tendência 	Resultados de testes	Resultados de testes que estão em um estado adiado e crítico e são agrupados com base no grupo de atribuição.

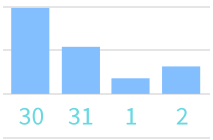
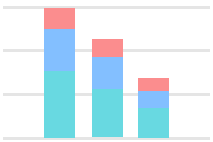
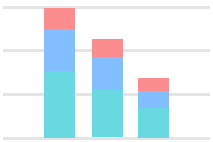
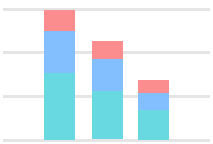
Visualizações da guia Aprovações

Relatórios	Tipo	Tabela de origem	Descrição
Solicitações de exceção por idade com minha aprovação pendente	Barra 	Aprovação	Solicitações de exceção criadas por você e que estão com aprovação pendente. As solicitações são agrupadas de acordo com a duração da solicitação.
Solicitações de aprovação por motivo	Barra 	Aprovação de mudança de estado	Indique as solicitações de aprovação de mudança para criar uma exceção e inclua o motivo da exceção.
Tarefas de correção com solicitação de aprovação por avaliação de risco	Barra	Tarefa de correção	Tarefas de correção que têm uma solicitação de aprovação baseada na criticidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Aprovações

Relatórios	Tipo	Tabela de origem	Descrição
			
Minhas solicitações de aprovação por status aprovado e rejeitado	Barra 	Aprovação de mudança de estado	Solicitações de exceção agrupadas pelos status aprovado e rejeitado.
Expiração das solicitações de exceção por mim por idade	Barra 	Aprovação de mudança de estado	Solicitações de exceção que vão expirar nas próximas semanas. As solicitações de exceção são agrupadas com base em semanas. Sempre que uma solicitação de exceção é criada, uma data é selecionada para a validade da solicitação de exceção. O cálculo da idade da solicitação se baseia nesta data.
Status das solicitações de exceção solicitadas por mim	Barra 	Aprovação de mudança de estado	Solicitações de exceção criadas por você e agrupadas de acordo com os seguintes status: • Em revisão • Aprovado • Rejeitado

Conformidade de configurações informações de referência

Vários tipos de componentes são instalados com a ativação da aplicação Conformidade de configurações, incluindo tabelas, trabalhos agendados e funções de usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os tópicos a seguir fornecem informações de referência, solução de problemas, além de dados de campo nos formulários e registros encontrados em Conformidade de configurações.

- Componentes instalados com Conformidade de configurações
- Campos de Resultados de testes
- Resolvendo Conformidade de configurações problemas de importação
- Modificar data de início dos resultados de PC da Qualys

Exibir Conformidade de configurações grupos de teste

Depois de importar os resultados de uma verificação de terceiros para sua instância, você poderá ver sua conformidade de teste no nível do grupo de teste. Use esta exibição antes de uma auditoria desse grupo de teste e de todos os registros de teste associados.

Antes de Iniciar

Função necessária: sn_vulc.read e sn_vulc.remediation_owner para exibir

Por Que e Quando Desempenhar Esta Tarefa

As políticas são registros importados e não podem ser editados dentro de Conformidade de configurações.

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Grupos de teste**.
   A lista de resultados de testes é exibida. A partir da v15.0 de Conformidade de configurações, a coluna **% de conformidade do resultado de testes** exibe a porcentagem de resultados de testes que estão em conformidade com os testes em um grupo de teste.

   Percentual de conformidade do resultado de testes = (nº de resultados de testes encerrados em um grupo de testes/nº total de resultados de testes associados a um grupo de testes) * 100

2. Clique na **descrição resumida** do grupo de teste que você deseja exibir.

Conformidade de configurações Campos do formulário Grupo de teste

Campo	Descrição
Origem	Nome do sistema do scanner de terceiros ou o nome inserido no plug-in ServiceNow da API usada para se comunicar com Conformidade de configurações.
Tecnologias	Lista de tecnologias associadas ao grupo de teste na aplicação de scanner de terceiros.
ID da origem	Identificador atribuído a este grupo de teste pelo scanner de terceiros.
Origem criada	Data e hora em que o grupo de teste foi definido na aplicação de scanner de terceiros.
Origem atualizada	Data e hora em que o grupo de teste foi modificado pela última vez na aplicação de scanner de terceira política.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Descrição resumida ou título atribuído ao grupo de teste na aplicação de scanner de terceiros.
Descrição	Descrição detalhada do grupo de teste conforme definido na aplicação de scanner de terceiros.
Testes	Lista de testes que fazem referência a este grupo de testes. Importado do scanner de terceiros. Você pode navegar na lista para obter informações detalhadas sobre um teste específico, se necessário.
Status de correção (versão 12.0)	
Exclui os adiados	Esses valores não incluem ICs de resultados de testes adiados. ◦ **ICs restantes**: o número (contagem) de itens de configuração (ICs) com resultados de testes ativos (qualquer estado diferente de **Encerrado**) para esta política. ◦ Percentual de**ICs corrigidos**: percentual de ICs compatíveis para este grupo de teste. Este número exclui ICs com resultados de testes adiados. ◦ **Total de ICs**: o número total de ICs afetados por este grupo de teste. Esta contagem exclui resultados de testes adiados.
Inclui os adiados	Os valores representam ICs de todos os resultados de testes ativos (qualquer estado diferente de **Closed**). ◦ **ICs restantes**: o número de ICs exclusivos associados a um ou mais resultados de testes não encerrados aos quais este grupo de testes foi aplicado. ◦ Percentual de**ICs corrigidos**: o percentual de ICs compatíveis para este grupo de teste. ◦ **Total de ICs**: número total de ICs afetados por este grupo de teste.

A partir da versão 12.0, para atualizar esses valores sob demanda, abaixo da guia Status da correção, clique no link relacionado **Atualizar status**. Uma mensagem é exibida indicando que os dados estão sendo atualizados. Clique no link **Exibir status** para exibir o andamento da atualização. Depois de alguns momentos, todos os dados que foram alterados ou atualizados desde o último trabalho agendado são atualizados no registro. Os valores de campos atualizados são atualizados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Opcional: Desabilite a importação de resultados de testes para um grupo de testes selecionando o botão **Desabilitar importação**.

   (Optional) O valor na coluna **Importação desabilitada** muda para *verdadeiro*. Os resultados de testes do grupo de teste não são importados da próxima ingestão.

   Nota: O botão **Desabilitar importação** está disponível somente para os resultados de testes obtidos do scanner Qualys.

   A partir da v23.0 de Resposta a vulnerabilidades:

   - Você pode habilitar ou desabilitar a importação de resultados de testes para um grupo de testes Qualys no Vulnerability Manager Workspace. Para obter mais informações, consulte Habilitar ou desabilitar a importação de resultados de testes para um grupo de testes Qualys.
   - O botão **Marcar como obsoleto** foi renomeado para **Desabilitar importação**.
   - A coluna **Está obsoleta** foi renomeada para **A importação está desabilitada**.

Exibir Conformidade de configurações fontes autorizadas

Use este módulo para exibir informações de resumo sobre cada fonte autorizada e para pesquisar as publicações de origem que foram usadas para criar o registro.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar
- sn_vulc.remediation_owner para exibir

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Dados de suporte** > **Fontes Autorizadas**.
2. Clique na **descrição resumida** da fonte autorizada que você deseja exibir.

Conformidade de configurações campos de formulário de fontes autorizadas

Campo	Descrição
Número	Número de ID atribuído à origem autorizada por sua instância durante o processo de importação.
Origem	Nome do sistema da aplicação de scanner de terceiros ou o nome inserido no plug-in do scanner para a API que se comunica com Conformidade de configurações.
ID da origem	Identificador atribuído à fonte autorizada pelo scanner de terceiros.
Descrição resumida	Nome dado a esta fonte autorizada no scanner de terceiros.
Fornecedor	Nome da organização ou publicação que foi a fonte original de informações para esta fonte autorizada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Citações	Lista de informações citadas sobre os resultados de testes. Importado do scanner de terceiros. Você pode navegar nesta lista para obter informações detalhadas sobre um teste específico, se necessário.

3. Opcional: Adicionar um **fornecedor**.
4. Clique em **Atualizar**.
5. Você pode excluir este registro clicando em **Excluir**.
   Remove o registro da sua instância. Se ainda estiver em uso na integração de terceiros, ele retornará na próxima importação

Exibir Conformidade de configurações tecnologias

Use este módulo para exibir informações de resumo sobre cada fonte autorizada e citação (também conhecida, na Qualys, como uma estrutura). Você pode pesquisar as publicações de origem que foram usadas para criar o registro.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar
- sn_vulc.remediation_owner para exibir

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Dados de suporte** > **Tecnologias**.
2. Clique na **descrição resumida** da fonte autorizada que você deseja exibir.

Conformidade de configurações campos de formulário de fontes autorizadas

Campo	Descrição
Número	Número de ID atribuído à origem autorizada por sua instância durante o processo de importação.
Origem	Nome do sistema do scanner de terceiros ou o nome inserido no plug-in do scanner de terceiros para a API que se comunica com Conformidade de configurações.
ID da origem	Identificador atribuído à fonte autorizada pelo scanner de terceiros.

3. Você pode excluir este registro clicando em **Excluir**.
   Remove o registro da sua instância. Se ainda estiver em uso na integração de terceiros, ele retornará na próxima importação

Exibir Conformidade de configurações testes

Use este módulo para pesquisar informações detalhadas sobre esses testes. Estão incluídas as citações de fontes de especialistas que foram usadas ao criá-las, as políticas de configuração de terceiros nas quais elas são usadas e os resultados obtidos da verificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar
- sn_vulc.remediation_owner para exibir

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Controles**.
2. Navegar até **Todos** > **Conformidade de configurações** > **Testes**
3. Na lista, abra o controle (teste de conformidade) que você deseja exibir.

A partir da versão 12.0, para atualizar esses valores sob demanda, abaixo da guia Status da correção, clique no link relacionado **Atualizar status**. Uma mensagem é exibida indicando que os dados estão sendo atualizados. Clique no link **Exibir status** para exibir o andamento da atualização. Depois de alguns momentos, todos os dados que foram alterados ou atualizados desde o último trabalho agendado são atualizados no registro. Valores de campos como**Pontuação**de **risco , Classificação**de risco , **Data da meta**de correção , **Estado**e os campos na guia **Status** da correção são atualizados.

Conformidade de configurações campos de formulário de teste

Campo	Descrição
Número	Número atribuído ao controle durante o processo de importação.
Resultado	Status da verificação. Aprovado ou reprovado. Se este teste pertencer a várias tarefas de correção, seu estado será determinado seguindo uma ordem de precedência.
Origem	Nome do sistema da aplicação de integração de terceiros ou o nome inserido no plug-in da API usada para se comunicar com Conformidade de configurações.
Criticidade	Gravidade do problema ou problemas de configuração associados ao controle, conforme definido na integração de terceiros. O nível de criticidade é ajustado para corresponder à granularidade de indicadores de vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	semelhantes disponíveis em Resposta a vulnerabilidades. Os níveis possíveis são: Crítico O problema de configuração associado ao controle está causando uma interrupção em um ou mais ICs críticos para os negócios. Alto(a) O problema de configuração associado ao controle é uma ameaça, mas não está causando o desligamento de recursos de rede críticos. Moderado(a) O problema de configuração associado ao controle é um risco, mas não é uma ameaça imediata. Baixo O problema de configuração associado ao controle é uma ameaça de baixo nível e pode ser ignorado em favor dos ICs que estão em maior risco. Secundário(a) O problema de configuração associado ao controle é um risco menor e pode ser ignorado se necessário.
ID da origem	Identificador atribuído ao controle pela integração de terceiros.
Categoria	Categoria de classificação principal fornecida a este tipo de controle pelo fornecedor terceirizado.
Pontuação de risco	Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máximo em todos os Resultados de testes não "Encerrada" (Aberto, Sob investigação, Aguardando implementação, Adiado, Resolvido) e 15% da pontuação do número de testes resultados que não estão "Encerrados".Valor calculado por calculadoras de pontuação de risco que se baseia nos valores de criticalidade dos negócios e de criticalidade de teste dos resultados de testes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Subcategoria	Subcategoria atribuída a esta classe de teste pelo fornecedor terceirizado.
Pontuação de risco	Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Tecnologias	Lista de tecnologias cobertas por este teste.
Origem criada	Data em que o teste foi definido pela primeira vez na integração de terceiros.
Origem atualizada	Data em que o teste foi atualizado pela última vez na integração de terceiros.
Descrição resumida	Descrição resumida ou título inserido ou atribuído ao teste na integração de terceiros.
Status de correção (v 12.0)	
Exclui os adiados	Esses valores não incluem resultados de testes adiados. ◦ **Resultados de testes abertos**: o número (contagem) de resultados de testes ativos (qualquer estado diferente de **Fechado**) para este teste de configuração. ◦ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos para esta tarefa de correção. ◦ **Total de resultados de testes**: o número total de resultados de testes para esta tarefa de correção.
Inclui os adiados	Esses valores incluem resultados de testes adiados. ◦ **Resultados de testes abertos**: o número (contagem) de todos os resultados de testes ativos (qualquer estado diferente de **Fechado**) para esta tarefa de correção. ◦ **Percentual de resultados de testes corrigidos**: o percentual de resultados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de testes corrigidos para esta tarefa de correção. ◦ **Total de resultados de testes**: o número total de resultados de testes para esta tarefa de correção.
Descrição	Descrição longa do teste. Para a integração de vulnerabilidade da Qualys, este campo assume como padrão o conteúdo da página de capa Qualys Cloud Platform.
Correção	Instruções de etapas que descrevem como corrigir a não conformidade.
Guias relacionadas	
Citações	Lista de citações inseridas para cada fonte autorizada associada ao teste.
Grupos de teste	Lista de Conformidade de configurações grupos de teste que usam este teste.
Resultados de testes	Lista de ICs afetados pelo problema ou problemas de configuração associados a este teste. Você pode acessar testes individuais, ServiceNow itens de configuração ou a lista de tecnologias afetadas, se necessário.
Declarações de políticas de GRC	Se o plug-in GRC Gestão de políticas e conformidade estiver instalado, esta guia conterá a política GRC relacionada. Você pode editar esta lista para adicionar ou remover declarações de política.

Exibir Conformidade de configurações resultados de testes

Exibir resultados de testes Conformidade de configurações para auditoria e correção. Os resultados de testes são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Importante: Você pode exibir os resultados de testes criados durante as importações de integração de vulnerabilidade de terceiros no Espaço do gerenciador de vulnerabilidades. Para obter mais informações, consulte Visão geral de listas.

Antes de Iniciar

Função necessária:

- sn_vulc.read para exibir
- sn_vulc.remediation_owner para exibir e atualizar
- sn_vulc.delete para excluir

Por Que e Quando Desempenhar Esta Tarefa

Conformidade de configurações O não cria nem atualiza os resultados de testes, mas os importa como parte de uma integração de terceiros. Depois que podem ser exibidos em Conformidade de configurações, eles são corrigidos usando **Grupos de resultados de testes**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Resultados de testes**.
   A partir da v15.0 de Conformidade de configurações, as seguintes colunas aparecem na lista de Resultados de testes.

Lista de resultados de testes

Coluna	Descrição
Ativo	Indica se um resultado de teste está ativo. Um resultado de testes é marcado como: ◦ Verdadeiro: se o estado não for Fechado. ◦ Falso: se o estado for Encerrado.
Momento do fechamento	Período de tempo durante o qual um resultado de testes está no estado Fechado. Este campo está vazio para um resultado de teste ativo. Formato: Dias HH:MM: SS
Idade	Período de tempo durante o qual um resultado de testes está ativo desde que foi aberto pela última vez. Este campo está vazio para os resultados de testes encerrados. Formato: Dias HH:MM: SS
Encerrado	Carimbo de data/hora do encerramento de um resultado de testes. Formato: AAAA-MM-DD HH:MM: SS
Aberto pela última vez	Carimbo de data/hora da abertura de um resultado de testes, ou seja, quando o valor do campo **Ativo** muda para *verdadeiro*.

2. Abra o controle que você deseja exibir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conformidade de configurações campos de formulário de resultado de testes

Campo	Descrição
Número	O número atribuído ao teste durante o processo de importação.
Origem	O nome do sistema da aplicação SCA de terceiros ou o nome inserido no plug-in da aplicação para a API usada para se comunicar com Conformidade de configurações.
ID da origem	O identificador atribuído ao controle pela aplicação SCA.
Resultado	Aprovado, Com falha, Erro ou Desconhecido. Importado da Qualys.
Pontuação de risco	Resultado da calculadora para este teste. Antes da v15.0 de Conformidade de configurações, a pontuação de risco de um resultado de teste aprovado era definida como '0'. A partir da v15.0 de Conformidade de configurações, a pontuação de risco do resultado de testes aprovado não é alterada para '0' para que você possa estimar o risco reduzido. A pontuação de risco do resultado de testes aprovado não é incluída no cálculo da pontuação de risco de uma tarefa de correção.
Pontuação de risco	Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Estado	Calculado a partir das tarefas de correção às quais o resultado de testes pertence. Se o resultado do teste pertencer a vários grupos, uma ordem de precedência será aplicada para determinar o estado.
Resolução	Calculado a partir das tarefas de correção às quais o resultado de testes pertence. Se o resultado do teste pertencer a vários grupos, uma ordem de precedência será aplicada para determinar a resolução.
Visto pela primeira vez	Data importada pela primeira vez para Conformidade de configurações. A partir da v13.1.1, o campo **Visto pela primeira vez** exibe a data fornecida pelo scanner. Caso contrário, ele exibirá a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	data importada pela primeira vez em Conformidade de configurações.
Visto pela última vez	Data da última importação para Conformidade de configurações. A partir da v13.1.1, o campo **Visto pela última vez** exibe a data fornecida pelo scanner. Caso contrário, ele exibirá a data da última importação para Conformidade de configurações.
Última aprovação	Data mais recente em que o resultado do teste foi aprovado.
Teste	Nome do teste.
Item de configuração	Nome do IC anexado ao teste.
Tecnologia	Versão do software em execução no IC.
Descrição	Descrição do teste
Valores Esperados	Valores esperados configurados na Qualys e importados por Conformidade de configurações. Este valor é uma expressão booliana que, quando avaliada como verdadeira, torna o resultado do teste **Aprovado**. A expressão pode ser uma combinação de operadores lógicos, de conjunto ou de expressão regular.
Valores reais	Valores retornados pelo teste. Esses valores são conectados à expressão booliana de valores esperados para determinar se o resultado deve ser aprovado ou reprovado. Eles são importados da Qualys. A partir da versão 14.9 de Conformidade de configurações, os valores de Evidência Estendida e Causa de Falha são adicionados à coluna Valores Reais.
Correção	Instruções de correção.
Guias relacionadas	
Tarefas de correção	Tarefas de correção associadas a este resultado de testes.
Histórico de Resultado de testes	Lista relacionada de resultados de testes que mostra o histórico de resultados de aprovação/falha para o mesmo IC/tecnologia/teste.

Exibir uma tarefa de correção

Você pode exibir ou, como alternativa, criar uma tarefa de correção e executar a correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Você pode exibir as tarefas de correção no Espaço do gerenciador de vulnerabilidades. Para obter mais informações, consulte Visão geral de listas.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar ou criar
- sn_vulc.remediation_owner para exibir

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Conformidade de configurações** > **Tarefas de correção**.
2. Na lista, clique no registro que deseja exibir.
3. Como alternativa, clique em **Novo** para criar uma nova tarefa de correção e preencha os campos.

Campos de formulário da Tarefa de correção da Conformidade de configuração

Campo	Descrição
Número	O número gerado automaticamente para este registro.
Estado	Status de andamento do grupo. ◦ Aberto ◦ Sob investigação ◦ Aguardando Implementação ◦ Adiado ◦ Resolvido ◦ Encerrado
Pontuação de risco	Essa pontuação é o valor acumulado das pontuações de risco para todos os resultados de testes ativos em uma tarefa de correção. Essa pontuação muda conforme os resultados de testes são corrigidos no grupo de resultados de testes.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.
Pontuação de risco	A quantidade de risco que um resultado de teste com falha representa para o seu

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	sistema. Ele se baseia em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica os riscos como Críticos (1) a Nenhum (5).
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha neste conjunto de tarefas.
Meta de correção	Data em que os resultados de testes devem ser corrigidos, desde a primeira identificação.
Criação	A data e hora em que esta tarefa de correção foi criada.
Status da Correção	Status da correção do grupo. É determinado pelo resultado de testes com a data de vencimento mais próxima. Para grupos abertos, os estados incluem Em andamento, Aproximando-se do destino e Destino não atingido. Para grupos fechados, os estados incluem Sem meta, Meta atingida e Meta não atingida. Para datas de meta de correção calculadas, se a tarefa de correção estiver fechada, o status geral de correção de todos os resultados de testes encerrados será mostrado na tarefa de correção. Eles determinam se o grupo atendeu à data ou não. Um status de correção de tarefa de correção encerrada será **Sem meta** se nenhum de seus resultados encerrados tiver uma data de meta de correção. É **meta** não atingida se algum de seus resultados encerrados perdeu a data de destino. Será **meta** atingida se pelo menos um resultado encerrado atender à meta e nenhum dos outros a perder.
Atualizado em	A data e a hora em que este registro foi modificado pela última vez.
Descrição resumida	Breve descrição deste grupo de resultados de testes.
Descrição	Descrição longa do grupo de resultados de testes que inclui a lista de softwares associados a este grupo de resultados de testes.
Teste	O teste de configuração associado a este grupo de resultados de testes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status de correção (versão 12.0)	
Exclui os adiados	Esses valores não incluem resultados de testes adiados. ◦ **Resultados de testes abertos**: o número (contagem) de resultados de testes ativos (qualquer estado diferente de **Fechado**) para esta tarefa de correção. ◦ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos (encerrados) para este grupo de resultados de testes. ◦ **Total de resultados de testes**: o número total de resultados de testes para esta tarefa de correção.
Inclui os adiados	Os valores representam todos os resultados de testes ativos (qualquer estado diferente de **Encerrado**). ◦ **Resultados de testes abertos**: o número (contagem) de resultados de testes ativos (qualquer estado diferente de **Fechado**) para este grupo de resultados de testes. ◦ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos (encerrados) para esta tarefa de correção. ◦ **Total de resultados de testes**: o número total de resultados de testes para esta tarefa de correção.
Configuração de Grupo	O tipo de filtragem usado para selecionar os resultados de testes da tarefa de correção.
Método de agrupamento	Nome do método usado.
Regra de grupo	Nome da regra de grupo usada.
Anotações	Anotações do sistema associadas ao registro.
Links relacionados	**Versão 12.0: atualizar link de status**. Atualize os valores no registro de resultados de testes sob demanda. Exibir todos os dados que foram alterados ou atualizados desde o último trabalho agendado.
Resultados de testes	Os resultados de testes nesta tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Solicitações de mudança (v 12.0)	A lista de solicitações de mudança associadas a este grupo de resultados de testes.
Aprovações de mudança de estado (v 12.0)	Status e estados das aprovações de solicitação de mudança associadas a esta tarefa de correção.

Resultados de testes e transições de estado da tarefa de correção na aplicação Conformidade de configurações

Os estados dos registros de teste de configuração e suas tarefas de correção (RTs) associadas serão afetados se os registros de resultados de testes forem adiados, resolvidos, reabertos e transferidos para outros esforços de correção (REs).

Cenários de transição de estado entre resultados de testes e tarefas de correção

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

A tabela a seguir detalha como os estados e subestados fazem a transição entre os resultados de testes de configuração e as tarefas de correção.

Se um estado de tarefa de correção fizer a transição de...	...para estados/ subestados	A transição de estados dos resultados de testes associados de...	...para estados/ subestados	Descrição
Aberto	Sob Investigação	Aberto	Sob Investigação	Os estados fazem a transição bidirecionalmente.
Aberto	Em Revisão	Aberto	Em Revisão	Os estados fazem a transição bidirecionalmente.
Aberto	Adiado/com qualquer motivo selecionado para resolução	Aberto	Adiado	Os resultados de testes mantêm o mesmo motivo de resolução da tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se um estado de tarefa de correção fizer a transição de...	...para estados/ subestados	A transição de estados dos resultados de testes associados de...	...para estados/ subestados	Descrição
Adiado/com qualquer motivo para resolução	Aberto	Os resultados de testes permanecem adiados		Os resultados de testes mantêm a mesma resolução da tarefa de correção.
Aberto	Resolvido/ Corrigido	Aberto	Resolvido	Os estados/ subestados fazem a transição bidirecionalmente.
Aberto	Resolvido e Resolvido para Encerrado/ Corrigido	Aberto	Resolvido	Se uma tarefa de correção fizer a transição para Encerrado/ Fixo, ela poderá fazer a transição de volta para Aberto. Se a tarefa fizer a transição para Aberto, os resultados de testes associados passarão de Resolvido de volta para Aberto.
Aberto	Resolvido	Abertos	Resolvido	Os estados/ subestados fazem a transição bidirecionalmente.
Aberto	Resolvido/ Cancelado	Aberto	Resolvido	Os estados/ subestados fazem a transição bidirecionalmente.
Aberto	Resolvido e Resolvido para Encerrado	Aberto	Resolvido	Se uma tarefa de correção for transicionada para Encerrada automaticamente, os resultados de testes associados poderão fazer

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se um estado de tarefa de correção fizer a transição de...	...para estados/ subestados	A transição de estados dos resultados de testes associados de...	...para estados/ subestados	Descrição
				a transição de volta para Aberto.
Aberto	Resolvido e Resolvido para encerrado/ Resultado inválido	Aberto	Resolvido e Resolvido para encerrado/ Resultado inválido	Se uma tarefa de correção for transicionada para Resolvida, ela poderá fazer a transição de volta para Aberta. Se uma tarefa de correção fizer a transição para Encerrado/ Resultado inválido, ela e os resultados de testes associados não poderão ser reabertos.
Aberto	Encerrado/ Corrigido	Os resultados de testes permanecem abertos		

Nota:

- A partir da v14.12 de Conformidade de configurações, a opção **Resultado inválido** é removida na **resolução** arquivada no modal Fechar.
- A partir da v14.12 de Conformidade de configurações, o fluxo de trabalho **de Aprovação do estado da tarefa** de correção foi descontinuado e substituído pelo fluxo de Aprovação do estado da tarefa de correção no Flow Designer.

Sincronização de estado entre solicitações de mudança e tarefas de correção

Há um relacionamento sincronizado entre os campos de estado das tarefas de correção e os campos de estado das solicitações de mudança (CHGs) na aplicação Conformidade de configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também move o estado de todas as tarefas de correção relacionadas automaticamente. A sincronização de estado é habilitada por uma propriedade do sistema por padrão em sua instância quando você baixa a aplicação Conformidade de configurações do ServiceNow Store, começando com v12.0.

Quando a sincronização de estado está habilitada, o campo Estado CHG muda o campo Estado da tarefa de correção automaticamente nos seguintes casos:

- Quando uma nova solicitação de mudança é criada para uma tarefa de correção, se não estiver em **Aguardando implementação**, o estado da tarefa de correção avançará para **Aguardando implementação**.
- Quando uma solicitação de mudança existente estiver associada a uma tarefa de correção, se não estiver em **Aguardando implementação**, o estado da tarefa de correção avançará para **Aguardando implementação**.
- Depois que as tarefas em uma solicitação de mudança são concluídas (`Implementado`) e o CHG é movido para o estado **Revisão**, a tarefa de correção avança para **Resolvido**.

Para obter mais informações e exemplos de sincronização de estado, consulte as seções a seguir.

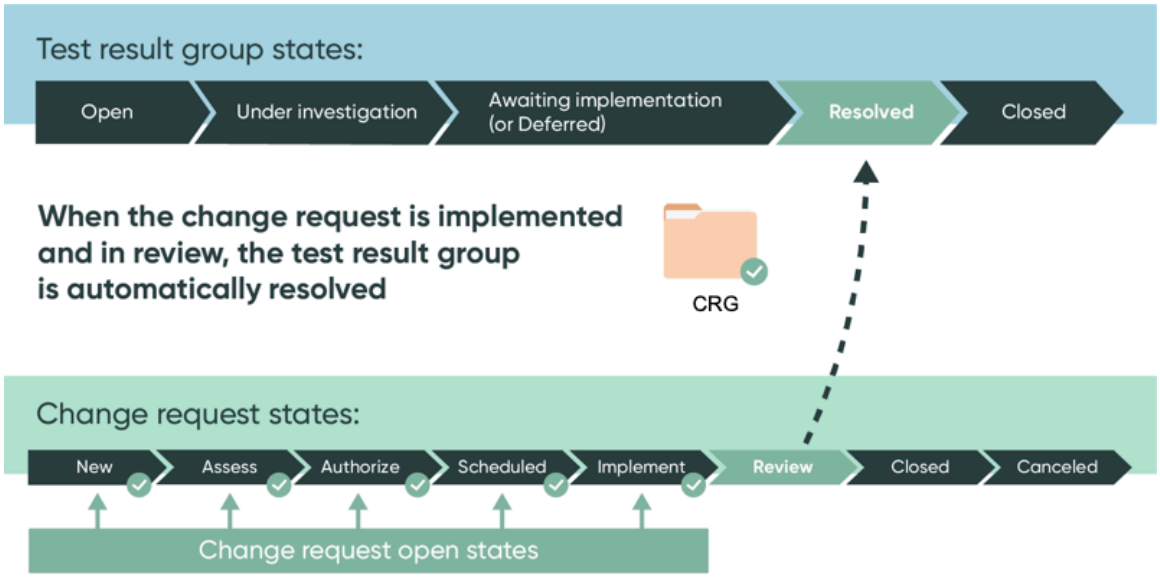
Nota: Você ainda pode mover manualmente solicitações de mudança e tarefas de correção por meio dos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, você adiciona uma solicitação de mudança ou a remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados da solicitação de mudança não movem automaticamente a tarefa de correção de **Encerrado**.

Sincronização de estado de encaminhamento

A imagem a seguir ilustra como os estados de CHG movem automaticamente os estados da tarefa de correção em um ciclo de vida avançado, ou seja, de **Aberto** para **Resolvido**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode criar novas solicitações de mudança para qualquer tarefa de correção em um estado diferente de **Resolvido** ou **Encerrado**. A sincronização de estado move automaticamente o TRG bidirecionalmente pelos estados **Aberto**, **Sob investigação**, **Aguardando implementação**e **Resolvido**. Este movimento é baseado em determinados valores do campo de estado na solicitação de mudança. A sincronização de estado entre a solicitação de mudança e a tarefa de correção é invocada automaticamente, a menos que a caixa de seleção (**Adicionar ICs ao CR**) seja exibida em um formulário e você opte por desmarcar a caixa de seleção.

A tarefa de correção não avança para **Resolvido** quando um CHG está em seus estados abertos. Qualquer CHG em estados anteriores a **Revisão** em seu ciclo de vida, como **Novo**, **Avaliar**, **Autorizar**, **Programado** ou **Implementar**, conforme mostrado na figura anterior, são considerados estados abertos para o CHG. Estados em aberto não movem o campo de estado na tarefa de correção porque as investigações ou tarefas no CHG não foram concluídas. A sincronização de estado é invocada quando um CHG é criado para a tarefa de correção ou associado a ela ou quando o estado de um relacionamento existente muda no CHG. Os estados de CHG concluídos são **Revisão** e **Encerrado**com sucesso . Quando um CHG é encerrado com sucesso, seus códigos encerrados são: Bem-**sucedido**ou **Bem-sucedido com problemas**. Nesse caso, a tarefa de correção avança para **Resolvido**.

Sincronização de estado reverso

Como um CHG é processado durante seu ciclo de vida, ele pode ser cancelado em algum momento. Nesse caso, se o CHG for **Cancelado**ou **Encerrado** (com um código de encerramento **Malsucedido**), a tarefa de correção voltará automaticamente para **Sob investigação**. A tarefa de correção volta para **Sob investigação**porque não há nenhum plano ativo para corrigir a vulnerabilidade.

Se uma tarefa de correção estiver em um estado **Resolvido** e você criar um novo CHG ou associá-lo a um CHG existente em um dos estados abertos iniciais, a tarefa de correção voltará automaticamente para **Aguardando implementação**. A tarefa de correção volta para este estado, porque mais trabalho agora está atribuído ao CHG.

Tarefas de correção com mais de um CHG

Se uma tarefa de correção em **Aguardando implementação** tiver mais de um CHG associado a ela, a sincronização de estado será baseada no status do CHG no estado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mais antigo de seu ciclo de vida. Por exemplo, digamos que uma tarefa de correção tenha quatro CHGs associados a ela, CHG1, CHG2, CHG3 e CHG4, conforme mostrado na tabela a seguir.

Número CHG	Estado CHG
1	**Implementar**
2	**Cancelado**
3	Encerrado (código de encerramento **malsucedido**)
4	Encerrado (código de fechamento **malsucedido**)

A sincronização de estado entre o CHG e a tarefa de correção, neste caso, é baseada no CHG1, que está no estado mais antigo dos quatro CHGs, (**Implementar**). Nesse caso, a tarefa de correção permanece em **Aguardando implementação**.

Em outro exemplo, se uma tarefa de correção estiver no estado **Resolvido** e tiver um CHG existente que foi implementado e está no estado **Revisão**, e um novo CHG for criado, a tarefa de correção voltará de **Resolvido** para **Aguardando implementação**. A sincronização de estado é baseada no CHG no estado **Novo**, que é o CHG no estado mais antigo.

Número CHG	Estado CHG
1	Revisão
2	Novo

Além disso, quando as tarefas de correção têm mais de um CHG, o estado da tarefa de correção muda automaticamente nos seguintes casos:

- Quando um CHG avança para **Revisão**, se todos os outros CHGs associados à tarefa de correção estiverem nos estados **Revisão** ou **Encerrado** (com um código de encerramento bem-sucedido), a tarefa de correção faz a transição automaticamente para **Resolvido**. Todos os outros CHGs relacionados que são cancelados ou encerrados sem sucesso são ignorados.
- Quando um CHG passa para **Cancelado** ou**Encerrado** (código de fechamento de **Malsucedido**), se todos os outros CHGs associados à tarefa de correção estiverem no mesmo estado, a tarefa de correção voltará automaticamente para **Sob investigação .**

Para obter mais informações sobre os estados da tarefa de correção e o que você pode fazer em cada estado, consulte Conformidade de configurações estados.

Separação de domínios e Conformidade de configurações

Separação de domínios é compatível com Conformidade de configurações. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Conformidade de configurações

Com o Domain Separation, você pode padronizar (Conformidade de configurações) procedimentos em toda a base de clientes que atende, com custos operacionais reduzidos e uma qualidade de serviço superior.

Separar espaços de trabalho do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínio em Conformidade de configurações por versões

Versão	Nível de suporte	Anotações
Orlando	Padrão	
Paris	Padrão	
Quebec	Padrão	
Rome	Padrão	
San Diego	Padrão	
Tokyo	Padrão	
Utah	Padrão	
Vancouver	Padrão	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Domain Separation para a aplicação Conformidade de configurações cobre a seguinte funcionalidade do produto:

- Ingere os resultados de testes de scanners de terceiros (Qualys) no domínio correto.

  Os dados são ingeridos no mesmo domínio do usuário de integração, cujas credenciais são usadas para integração.

- Verifica novamente hosts específicos de Conformidade de configurações no domínio do qual foi solicitado.
- Usa o processo de pesquisa de IC do CMDB para garantir que as informações de IC dos scanners correspondam aos ICs no CMDB do domínio do usuário de integração.
- Calcula pontuações de risco no nível do resultado de testes de acordo com a calculadora de pontuação de risco definida no mesmo domínio do usuário de integração.
- Regra(s) de tarefa de correção pode(m) ser definida(s), atribuída(s) e permanecer(em) no mesmo domínio que o domínio do usuário de integração.
- As tarefas de correção criadas usando as regras de tarefa de correção de documento permanecem no mesmo domínio em que as regras de tarefa de correção são criadas.
- O fluxo de trabalho de adiamento passa pelo processo de aprovação no mesmo domínio para o qual o adiamento é solicitado.
- Relatórios e painéis exibem os estados do resultado de testes, como idade dos resultados de testes, resultados de testes abertos por IC, resultados de testes por impacto no domínio ao qual pertencem.
- O conhecimento de scanners de terceiros (Qualys) pode ser ingerido no domínio global e os dados podem ser compartilhados entre vários clientes.

Nota: Em todos os casos acima, aplicam-se os princípios abrangentes de visibilidade na separação de domínios separados na NOW Platform.

Casos de uso

A aplicação Conformidade de configurações gerencia o ciclo de vida de um resultado de testes de ponta a ponta. Os seguintes casos de uso reconhecem a separação de domínios:

- **Ingerir** resultados de testes de Qualys
  - Ingerir dados de várias instâncias
  - Desduplicar os resultados de testes
  - Corresponder ao IC do CMDB
- **Aprimoramento** de resultados de testes com pontuações de risco
  - Aprimoramento de ativos (CMDB)
  - Pontuação de risco
- **Agrupar** resultados de testes e atribuir a tarefa de correção
  - Agrupar automaticamente os resultados de testes
  - Atribuir automaticamente a tarefa de correção
- **Corrigir**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tarefa de correção atribuída como uma tarefa de correção
- Ciclo de vida de correção abrangente
- Fluxo de trabalho de adiamento

- **Medir** a postura de segurança da organização e do programa de gestão de conformidade
  - Tendência de resultados por conformidade, categoria, criticalidade e tecnologia
  - Status e distribuição de políticas, testes, hosts, resultados de testes e pontuação de risco

Configuração

A configuração do Domain Separation para Conformidade de configurações não requer etapas adicionais. Todas as tabelas Conformidade de configurações adquirem a coluna Domínio depois que a instância é separada por domínio. Você pode direcionar os dados de importação da integração de resultados de testes para domínios específicos. Para obter mais informações, consulte Criar importações separadas por domínio para uma integração. Para obter mais informações sobre precauções e configurações adicionais, consulte Configurações adicionais para Separação de domínios.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os resultados de testes ingeridos de scanners de terceiros permanecem no mesmo domínio que o domínio do usuário de integração e não podem ser acessados de nenhum outro domínio.
- Os resultados de testes ou hosts em um domínio não podem ser exibidos de outros domínios.
- O algoritmo de pontuação de risco e as regras da tarefa de correção não podem ser exibidos por ninguém fora do domínio.
- Os fluxos de trabalho de adiamento criados em um domínio não são visíveis em outro domínio.
- Todas as notificações por e-mail estão contidas no domínio ao qual pertencem.

Como os analistas de conformidade gerenciam seus próprios dados de aplicações

- Os analistas criam suas próprias regras de instalação de aplicações, gerenciamento de aplicações de várias origens e pesquisa de IC.
- Os analistas podem configurar integrações específicas exclusivamente para uso no domínio.
- Os analistas podem criar seus próprios fluxos de trabalho de adiamento e gestão de mudanças.
- Os analistas podem criar suas próprias regras de tarefa de correção, lógica de pontuação de risco para priorizar resultados com precisão, atribuir automaticamente tarefas de correção e atribuir ao grupo de atribuição correto.
- Os usuários do domínio criam uma tarefa de correção manual e a fecham.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Conformidade de configurações usuários e grupos
- Conformidade de configurações integrações (a partir da versão Madrid)
- Conclua a configuração de configuração (gestão de usuários e grupos, instalação de aplicações, gestão de aplicações de várias origens, regras de pesquisa de IC, regras de tarefa de correção, calculadoras de risco etc.)
- Concluir o ciclo de vida de correção, incluindo o adiamento

Informações relacionadas

Domain Separation para provedores de serviço

Campos de Resultados de testes

Os resultados de testes são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Conformidade de configurações O não cria nem atualiza os resultados de testes, mas os importa como parte de uma integração de terceiros. Depois que podem ser exibidos em Conformidade de configurações, eles são corrigidos usando **Grupos de resultados de testes**.

Campos de resultados de testes

Campo	Descrição
Número	Número atribuído ao resultado de testes durante o processo de importação.
Origem	Nome do sistema da aplicação de integração de terceiros ou o nome inserido na aplicação para a API que é usada para se comunicar com Conformidade de configurações.
ID da origem	Identificador atribuído ao resultado de testes pela integração de terceiros.
Pontuação de risco	Pontuação com base no valor *Criticality* do teste. Se você não tiver instalado e configurado, um valor médio de 50 será usado.
Resolução	Resolução do resultado de testes, calculado a partir de grupos associados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Resultado	Status da verificação. Aprovado ou reprovado. Se este teste pertencer a várias tarefas de correção, seu estado será determinado seguindo uma ordem de precedência.
Estado	Estado do resultado do teste, calculado a partir de grupos associados.
Grupo de atribuição	Grupo selecionado para trabalhar neste resultado de testes.
Atribuído a	Indivíduo do grupo de atribuição selecionado para trabalhar neste resultado de teste.
Tipo de atribuição	Tipo de atribuição. As opções são: • Regra • Manual • Nenhum(a)
Regra de atribuição	Qual regra de atribuição foi usada com este resultado de testes, quando aplicável.
Visto pela primeira vez	Hora e data em que o resultado do teste foi visto pela primeira vez.
Visto pela última vez	Hora e data em que o resultado do teste foi visto pela última vez.
Teste	O controle ao qual este resultado pertence.
Item de configuração	Item de configuração associado a este resultado de testes.
Tecnologia	Tecnologia associada a este resultado de testes.
Descrição	
Descrição	Descrição detalhada do resultado do teste conforme definido na aplicação de scanner de terceiros.
Valores Esperados	
Valores esperados	Descrição e valores esperados conforme definidos na aplicação de scanner de terceiros.
Valores reais	
Valores reais	Descrição e valores reais conforme definidos na aplicação de scanner de terceiros.
Correção	
Correção	Ação de correção conforme definido na aplicação de scanner de terceiros.

A seguir estão os itens vulneráveis listas relacionadas.

Lista relacionada	Descrição
Tarefas de correção	Tarefas de correção associadas a este resultado de testes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Histórico de Resultado de testes	Lista de registros anteriores que contêm resultados diferentes.

Conformidade de configurações mapas de criticalidade

Conformidade de configurações mapeamento de criticalidade transforma campos de criticalidade da origem em campos em Conformidade de configurações.

O sistema base Conformidade de configurações é fornecido com um mapeamento padrão Qualys Cloud Platform para padrão ServiceNow. A criação ou a edição de um mapa de criticalidade se destina somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente.

Conformidade de configurações estados

Com Conformidade de configurações, você pode ver um modelo de estado para saber qual é o status da tarefa de correção a qualquer momento. Os estados da tarefa de correção controlam os estados do resultado de testes por precedência.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

Estados da tarefa de correção

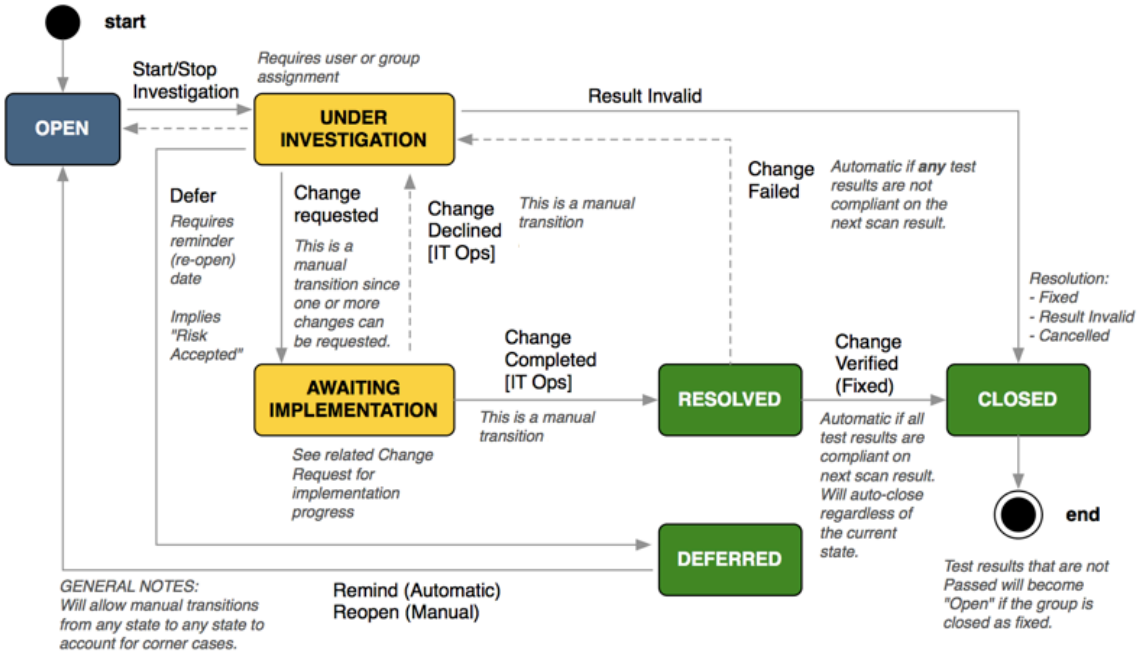
As tarefas de correção têm muitos estados possíveis. A transição automática está disponível a partir do estado Resolvido com base nos resultados da próxima verificação. Se todos os resultados de testes forem aprovados na próxima verificação, a tarefa de correção será encerrada. Caso contrário, ele fará a transição para o estado Sob investigação. O sistema verifica esse estado fechado, mas reavalia o estado da tarefa de correção se um resultado de testes for adicionado ou excluído da tarefa de correção. As anotações de trabalho são atualizadas para refletir a transição.

A figura a seguir mostra como o estado de uma tarefa de correção faz a transição do estado Aberto para o estado Fechado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de estado da Conformidade de configurações (anterior à v15.0)



Nota:

- Cada formulário de tarefa de correção contém os botões **Seguir** e **Atualizar**, que são padrão para tarefas ServiceNow.
- A partir da v15.0 de Conformidade de configurações, o seguinte foi removido:
  - Botão**Fechar**
  - o campo **Resolução** no modal Resolver.

A tabela a seguir lista os estados Conformidade de configurações.

Estados da Conformidade de configuração

Estado	Descrição
Aberto	Estado após a criação.
Sob Investigação	Acionado pelo botão **Iniciar investigação**. A partir deste estado, você pode: Criar uma solicitação de mudança Para obter mais informações, consulte Como criar uma solicitação de mudança no Conformidade de configurações. Exceção de Solicitação Forneça um motivo e selecione uma data de reabertura. Excluir Confirmar a exclusão. Remove a tarefa de correção. Marcar como falso positivo Forneça um motivo e anotações. Marca a tarefa de correção como falso-positivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da Conformidade de configuração

Estado	Descrição
Adiado	Acionado pelo botão **Adiar**. A partir deste estado, você pode: Reabrir Faça a transição de volta para um estado Aberto. Excluir Confirmar a exclusão. Remove a tarefa de correção. As informações de adiamento aparecem na guia relacionada **Adiar/ Fechar**. Na data de adiamento, a tarefa de correção é reaberta para correção.
Aguardando Implementação	Acionado pelo botão **Aguardando implementação**. A partir deste estado, você pode: Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Criar uma solicitação de mudança Para obter mais informações, consulte Como criar uma solicitação de mudança no Conformidade de configurações. Resolver Nas **Anotações de resolução**, adicione o motivo pelo qual você está resolvendo a Tarefa de correção. O estado se torna Resolvido. As anotações aparecem na guia relacionada **Resolução**. Excluir Confirmar a exclusão. Remove a tarefa de correção.
Resolvido	Acionado a partir do botão **Resolver**. A partir deste estado, você pode: Criar um incidente de segurança Para obter mais informações, consulte Criar um incidente de segurança. Reabrir Faça a transição de volta para um estado Aberto. Excluir Confirmar a exclusão. Remove a tarefa de correção. As anotações aparecem na guia relacionada **Anotações**. As informações de resolução aparecem na guia relacionada **Resolução**. As anotações são refletidas nas **Anotações de trabalho** de todos os resultados de testes associados à Tarefa de correção.
Encerrado	Acionado a partir do botão **Fechar** ou **Marcar como falso-positivo**. A partir da v14.12 de Conformidade de configurações, você pode fechar uma tarefa de correção marcando-a como falso-positivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da Conformidade de configuração

Estado	Descrição
	A partir deste estado, você pode: Reabrir Faça a transição de volta para um estado Aberto. Excluir Confirmar a exclusão. Remove a tarefa de correção. As informações de fechamento aparecem na guia relacionada **Adiar/Fechar**. As anotações são refletidas nas **Anotações de trabalho** de todos os resultados de testes associados à Tarefa de correção.

- Se a Tarefa de correção estiver marcada como Encerrada ou Fixa e o resultado de testes adicionado não for Fechado ou Fixo, o estado do resultado de testes não mudará e o estado da tarefa de correção será alterado para Aberto.
- Quando você cria uma nova tarefa de correção ou divide uma tarefa de correção, os campos **Motivo**e **Até** são reavaliados para tarefas de correção novas e antigas. Quando o estado de todos os resultados de testes é Adiado, o valor nos campos **Motivo** e **Até** é acumulado para a tarefa de correção.
  - Se todos os resultados de testes em uma tarefa de correção forem adiados e tiverem o mesmo **Motivo**, a tarefa de correção será atribuída ao mesmo **Motivo**. Caso contrário, o campo **Motivo** será alterado para **Nenhum**.
  - A data no campo **Até** é atualizada com a data mais próxima até de todas as tarefas de correção às quais os resultados de testes pertencem.

  Nota: Esta avaliação é feita pelo trabalho agendado *`Rollup test result values to test result group and configuration test`*, que é executado a cada hora.

- Se **Visto pela última** vez for maior que a **Data de resolução** de um resultado de teste resolvido, o resultado de teste será reaberto. Em uma Tarefa de correção resolvida, se pelo menos um resultado de testes for reaberto durante a ingestão, a tarefa de correção passará para o estado Sob investigação.

Estados do resultado de testes

O estado de uma tarefa de correção também muda o estado dos resultados de testes associados. Este mecanismo tem dois casos:

Resultados de testes que pertencem a apenas uma tarefa de correção

Os resultados correspondem ao estado da tarefa de correção, com três exceções:

- Se a tarefa de correção mudar seu estado para Encerrado e sua resolução (subestado) para Fixo, o item ignorará essa mudança e retornará ao estado Aberto.
- Se a tarefa de correção mudar seu estado para Encerrado e sua resolução (subestado) para Cancelado, o item ignorará essa mudança e retornará ao estado Aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o status da origem do resultado de testes for Fixo (atualizado por uma verificação ou importação), quando a tarefa de correção mudar de estado, o resultado de testes mudará seu estado para Fechado (Fixo), independentemente do estado em que a tarefa de correção esteja .

Resultados de testes que pertencem a várias tarefas de correção

Os resultados de testes não correspondem ao estado da tarefa de correção automaticamente. Em vez disso, ele pesquisa entre todos os grupos associados para encontrar o estado com a precedência mais alta a ser aplicada. Este é o estado de precedência:

Encerrado (subestado: resultado inválido) Encerrado (subestado: falso-positivo)> **Adiado** > **Resolvido** > **Aguardando implementação** > **Sob investigação** > **Aberto**

Nota: **Encerrado (subestado: Fixo)** e **Encerrado (subestado: Cancelado)** são dois casos especiais.

Nota: A partir da v15.0 de Conformidade de configurações, o subestado **Resultado inválido** foi descontinuado.

Exemplos de estado da Tarefa de correção

Por exemplo:

Estado das tarefas de correção	Estado do resultado de testes
Grupo A: **Aberto** > **Sob Investigação** Grupo B: **Aberto**	**Sob Investigação** Quando o Grupo A está Sob investigação e o Grupo B está Aberto, o resultado do teste muda para Sob investigação, pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.
Grupo A: **sob investigação** Grupo B: **Aberto** > **Sob Investigação**	**Sob Investigação** Quando o Grupo B está Sob Investigação e o Grupo A está Sob Investigação, o resultado do teste permanece como Sob Investigação, pois após a pesquisa, entre o Grupo A e o Grupo B, eles têm o estado com a mesma precedência.
Grupo A: **sob investigação** Grupo B: **Sob Investigação** > **Aguardando Implementação**	**Aguardando Implementação** Quando o Grupo B está Aguardando Implementação e o Grupo A está Sob Investigação, o resultado do teste muda para Aguardando Implementação, pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com a precedência mais alta.
Grupo A: **Sob Investigação** > **Adiado** Grupo B: **Aguardando Implementação**	**Adiado** Quando o Grupo A está Adiado e o Grupo B está Aguardando Implementação, o resultado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado das tarefas de correção	Estado do resultado de testes
	do teste muda para Adiado, pois após a pesquisa, o item 1 descobriu que entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta
Grupo A: **Adiado** Grupo B: **Aguardando Implementação** > **Encerrado (resultado inválido)**	**Encerrado (resultado inválido)** > **Adiado** Quando o Grupo B é Encerrado e a resolução (subestado) é Resultado inválido e o Grupo A é Adiado, o resultado do teste muda para Encerrado (resultado inválido), pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com a precedência mais alta.
Grupo A: **Adiado** Grupo B: **Encerrado (resultado inválido)** > **Aberto (via Reabrir)**	**Adiado** Quando o Grupo B é reaberto e seu estado muda para Aberto e o Grupo A é Adiado, o resultado do teste muda para Adiado, pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.
Grupo A: **adiado** Grupo B: **Aguardando Implementação** > **Encerrado (falso-positivo)**	**Encerrado (falso-positivo)** Quando o Grupo B for Encerrado e a resolução (subestado) for Falso-positivo e o Grupo A for Adiado, o resultado do teste mudará para Encerrado (Falso-positivo), pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com o precedência mais alta.

Casos especiais do estado do resultado de testes

Estado da tarefa de correção	Estado do resultado de testes
Grupo A: **Sob Investigação** Grupo B: **Aguardando Implementação** > **Encerrado (fixo ou cancelado)**	**Sob Investigação** Quando o Grupo B é Fechado (subestado Fixo ou subestado Cancelado) e o Grupo A está Sob Investigação, o resultado do teste muda de Aguardando Implementação (anteriormente, a precedência mais alta) para Sob Investigação (atualmente, a precedência mais alta).
Grupo A: qualquer estado Grupo B: qualquer estado	Se o status da origem do resultado de testes for Fixo (atualizado por uma verificação ou importação), quando a tarefa de correção mudar de estado, o estado do resultado de testes mudará para Fechado (Fixo), independentemente do estado das outras tarefas de correção associadas estão em. A pesquisa de resultado de testes para o estado da tarefa de correção não ocorre.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resolvendo Conformidade de configurações problemas de importação

Resolva problemas com a importação de integração de terceiros.

Importar resolução do problema

Problema	Resolução
Os resultados de testes estão ausentes	Verifique o *Start Time* na integração de **resultados de PC da Qualys**. Pode não estar atrasado o suficiente. Consulte Modificar data de início dos resultados de PC da Qualys.
A integração está falhando	Verifique o status **de execução da integração de vulnerabilidade**. As entradas do processo de integração individual contêm o XML importado, que pode ser examinado em busca de informações inesperadas. Navegar até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Resultados da QualysPC** > **Execuções de integração de vulnerabilidade** guia relacionada. Escolha a execução mais recente. Examine o status e as anotações das entradas na lista relacionada **Processo de integração de vulnerabilidades** em busca de anomalias. .

Modificar data de início dos resultados de PC da Qualys

Se houver dados ausentes para a data de início na importação de resultados de PC da Qualys, eles poderão ser modificados.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
2. Clique em Integração de **resultados de PC da Qualys**.
3. Clique **em Detalhes da integração**.
4. Defina o campo **Hora** de início com um valor no passado, para que todos os resultados de testes verificados e detectados, desde essa hora, sejam detectados.

   Nota: Se a data for deixada em branco, nenhum dado será retornado na primeira execução. Defina o valor como no máximo um mês no passado. Essa configuração evita que uma grande quantidade de dados exceda as limitações de taxa da API da Qualys, bem como o acionamento de tempos limites de execução.

5. Clique em **Enviar** ou **Atualizar**.
6. Opcional: Clique **em Executar agora** para executar imediatamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de pesquisa de IC para Microsoft Defender for Cloud Integration para Operações de segurança e Palo Alto Prisma Cloud

Você pode usar as regras de pesquisa de item de configuração (IC) para as integrações Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud para encontrar uma correspondência correta para os tipos de recursos usados com frequência no Configuration Management Database (CMDB).

Visão geral

O módulo Regras de pesquisa de IC contém as regras que ajudam a definir os campos que têm os dados correspondentes no Configuration Management Database (CMDB). Você pode usar essas regras para identificar as aplicações e as versões da aplicação. Todos os ativos Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud são identificados exclusivamente pela combinação de ID de objeto, conta em nuvem e datacenter lógico na plataforma [ServiceNow. A descoberta ServiceNow preenche o ID do recurso na coluna `Object_id` do CMDB em diferentes formatos para os diferentes tipos de recurso. A tabela a seguir mostra os formatos de ID de objeto dos tipos de recursos usados com frequência que o serviço de descoberta usa para preencher a coluna `Object_id` do IC. Qualquer scanner que queira pesquisar um ativo de um tipo de recurso específico deve pesquisar usando o formato de ID de objeto correto. Você pode obter o formato de ID de objeto correto consultando a coluna de ID de objeto da classe de IC CMDB correspondente e, em seguida, tentar construir o ID de objeto usando os valores recebidos do scanner.

Formato de ID de objeto para vários tipos de recurso

Tipo de recurso	Formato
AWS::EC2::Instance	ID do objeto
AWS::ElasticLoadBalancing::LoadBalancer	Nome do balanceador de carga
AWS::S3::Bucket	arn:aws:s3:::<Bucket Name>

A correspondência de IC para um resultado de testes pode não ser encontrada com precisão no Configuration Management Database (CMDB), a menos que o mesmo formato do `object_id` seja usado na regra de pesquisa. Na maioria das vezes, as regras de pesquisa de IC OOB encontram uma correspondência para os tipos de recursos usados com mais frequência para Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud. Se as seguintes regras de pesquisa de IC não encontrarem os ICs em CMDB para os resultados de testes, você poderá criar uma regra de pesquisa de IC para um tipo de recurso. Para obter mais informações sobre como criar uma regra de pesquisa de IC, consulte Criação de uma regra de pesquisa de IC.

Regras de pesquisa de IC

As regras de pesquisa de IC a seguir são específicas para Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud.

Bucket S3

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo valor que foi obtido pela concatenação de `arn:aws:s3:::` e o nome do recurso. O valor obtido é pesquisado na coluna `object_id` da tabela `cmdb_ci_cloud_object_storage`. Esta regra de pesquisa se aplica somente quando o tipo de recurso é `AWS::S3::Bucket`.

Nome

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo nome. O nome, que é pesquisado na coluna `Object_id` da classe de IC, corresponde a um tipo de recurso na tabela `sn_capi_resource_type`.

Nota: Para a aplicação Palo Alto Prisma Cloud, esta regra de pesquisa de IC é executada somente para os tipos de recurso `AWS::RDS::DBInstance`, `AWS::ElasticLoadBalancing::LoadBalancer`e `AWS::CloudTrail::Trail` . Você pode adicionar os tipos de recursos para os quais deseja executar esta regra de pesquisa de IC.

ID de recurso

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo ID do recurso. O ID do recurso, que é pesquisado na coluna `Object_id` da classe de IC, corresponde a um tipo de recurso na tabela `sn_capi_resource_type`.

Nota: Você pode definir a prioridade de uma regra de pesquisa de IC no campo **Ordem**. A regra de pesquisa de IC com o menor valor de ordem é executada primeiro.

Base para resposta a vulnerabilidades

O plug-in Vulnerability Response Common é instalado quando você instala a aplicação Vulnerability Response.

A partir da v20.0 da Resposta a vulnerabilidades, você pode usar a estrutura de relatórios agregados no Vulnerability Response Common para criar relatórios de vulnerabilidades de host, vulnerabilidades de aplicação, vulnerabilidades de contêiner e erros de configuração.

Estrutura de relatórios agregados

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas em tempo real complexas e de longa execução para melhor desempenho.

A estrutura de relatórios agregados melhora o desempenho:

- usando menos recursos e renderizando relatórios com mais rapidez,
- agregar os dados e reutilizar agregações e detalhamentos (Agrupar por) e
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de itens vulneráveis, use a estrutura fornecida em Vulnerability Response Common ao lado dos relatórios padrão.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- Now Platform administrador (admin): instale e ative este Solução Performance Analytics e relatórios e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics administrador (pa_admin): revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Administrador (sn_vul_cmn.admin): criar agregações.
- Gravação de VR (sn_vul_cmn.write): edite os dados em Agregações e Resultados agregados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Leitura de VR (sn_vul_cmn.read): revise os dados em Agregações e Resultados agregados.
- Analista de vulnerabilidade (sn_vul.vulnerability_analyst): revisa os resultados agregados.

Informações relacionadas

Configurar uma agregação para dados de origem

Executar várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Criar um relatório usando uma agregação

Configurar uma agregação para dados de origem

Para analisar o desempenho de um aspecto específico em um processo de negócios registrado em uma tabela ServiceNow, crie uma agregação específica para o aspecto e crie um relatório para essa agregação.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Procedimento

1. Navegar até **Todos** > **Relatórios de agregados** > **Definições de agregação** > **Todos** e clique em **Novo**.
2. No campo **Nome**, dê à agregação um nome descritivo.
3. No campo **Descrição**, forneça uma breve descrição sobre a agregação.
4. Na guia **Origem**, preencha os campos.

Campos da guia Origem

Campo	Descrição
Tabela	Tabela da qual você deseja buscar os dados do relatório. Esta lista suspensa contém somente as tabelas app-sec common, app-vul, app-vulc, app-vul-container e de vulnerabilidade da aplicação.
Agregar função	Função a ser aplicada à coluna selecionada em **Campo**. ◦ **Contagem**: número de registros. ◦ **Soma**: soma total dos valores na coluna selecionada em **Campo**. ◦ **Média**: média de todos os valores em uma coluna selecionada em **Campo**. ◦ **Máximo**: valor máximo na coluna selecionada em **Campo**. ◦ **Mínimo**: valor mínimo da coluna selecionada em **Campo**. ◦ **Contagem separada**: valores exclusivos na coluna selecionada em **Campo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Campo	Coluna na qual você deseja aplicar a função. **Nota:** Este campo não aparece quando você seleciona **Contagem** no campo **Função agregada**.

5. Na guia **Condições adicionais**, forneça a condição no campo **Condições** para selecionar um conjunto específico de registros para o qual você deseja obter os resultados agregados.
6. Na guia **Agrupar por**, selecione as colunas da tabela pelas quais você deseja agrupar ou empilhar os dados.
   Você pode selecionar até dois detalhamentos.

   Se você selecionar a coluna de **data** em qualquer campo agrupar por, o campo **Tendência por** será exibido. Você pode obter os resultados de agregação categorizados por semana, dia, minutos etc. selecionando as opções no campo **Tendência por**.
7. Na guia **Programação**, selecione ou crie uma programação de agregação, que define a frequência na qual você pode executar a agregação para buscar os dados.
   Para criar uma programação de agregação, consulte Executar várias agregações simultaneamente.

   Nota: Você não pode programar a execução de agregação para uma definição de agregação inativa.
8. Clique em **Enviar** para criar a agregação.
   A agregação aparece na lista Agregação. Na frequência predefinida, a agregação é executada e um registro é criado junto com uma data e hora de execução na lista relacionada Execuções programadas para cada execução.
9. Navegar até **Todos** > **Resultados agregados** e abra sua agregação para ver os resultados agregados e as execuções programadas.
   Os resultados agregados são listados na lista relacionada **Resultados agregados**. Se a execução de agregação falhar, consulte a coluna **Anotações** na lista relacionada **Execuções programadas** para obter mais informações.
10. Opcional: Selecione **Executar agora** para coletar os resultados da agregação, independentemente da programação de agregação.
    Se você encerrar a execução programada quando ela estiver em andamento, nenhuma mudança será feita nos resultados agregados. Você também pode excluir ou desativar uma agregação.

O que Fazer Depois

Crie um relatório usando sua agregação. Para obter mais informações sobre como criar um relatório usando uma agregação, consulte Criar um relatório usando uma agregação.

Informações relacionadas

- Estrutura de relatórios agregados
- Executar várias agregações simultaneamente
- Configure o número de agregações que podem ser executadas simultaneamente
- Criar um relatório usando uma agregação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar várias agregações simultaneamente

Você pode programar a execução de várias agregações usando uma única programação de agregação.

Antes de Iniciar
Função necessária: sn_vul_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa
Suponha que você queira executar seis agregações ao mesmo tempo. Crie uma programação de agregação e adicione todas as agregações a ela. Essas agregações são executadas na frequência e no tempo definidos.

Procedimento
1. Navegar até **Todos** > **Relatórios de agregados** > **Programação**.
2. Selecione **Novo**.
3. No formulário Programação de agregação, preencha os campos.

Campo	Descrição
Nome da programação	Nome da programação de agregação.
Programar trabalho	Execução de script agendada que define a frequência na qual as agregações devem ser executadas. Você pode criar um trabalho agendado selecionando o botão **Novo**.

4. Selecione **Enviar**.
   A programação de agregação aparece na lista Programação de agregações.
5. Abra sua programação de agregação.
6. Selecione **Editar**, adicione as agregações à **Lista**de agregação e selecione **Salvar**.
   As agregações selecionadas aparecem na lista relacionada Agregações.

   Nota: Se você adicionar uma agregação inativa a uma programação, a execução programada não será iniciada.

7. Selecione **Atualizar**.
   Essas agregações são executadas na frequência definida na programação de agregação.

Informações relacionadas

Estrutura de relatórios agregados

Configurar uma agregação para dados de origem

Configure o número de agregações que podem ser executadas simultaneamente

Criar um relatório usando uma agregação

Configure o número de agregações que podem ser executadas simultaneamente

Um novo processador ou um trabalho em segundo plano, o Processador do Aggregated Reporting Framework, é enviado com o sistema base, que executa os trabalhos agendados relacionados à tabela do Aggregated Reports Framework. Isso permite que o subsistema

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

inteiro seja executado em segundo plano e permite uma melhor utilização dos recursos do sistema quando eles estão disponíveis.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Configuração de trabalho em segundo plano – Calculadora de resultado de agregação comum da Resposta a vulnerabilidades**.
2. Defina o número de agregações que você deseja executar simultaneamente no campo **Máximo de threads simultâneos** e selecione **Salvar**.
   Por padrão, quatro agregações são executadas simultaneamente.
3. Navegue até a lista Pools de processadores de trabalho em segundo plano, **sn_sec_cmn_background_job_processor_pool.list**e selecione **Novo** para criar um processador de trabalho em segundo plano para a Estrutura de relatórios agregados.
   Para obter mais informações sobre como criar um pool de processadores de trabalho em segundo plano, consulte Processamento paralelo avançado para trabalhos em segundo plano na Resposta a vulnerabilidades .

   Nota: O número de processadores de trabalho em segundo plano deve ser igual ao número máximo de threads simultâneos fornecido no formulário **Configuração de trabalho em segundo plano – Calculadora de resultado de agregação comum de Resposta a vulnerabilidades**. Consulte a Etapa 2.

Informações relacionadas

- Estrutura de relatórios agregados
- Configurar uma agregação para dados de origem
- Executar várias agregações simultaneamente
- Criar um relatório usando uma agregação

Criar um relatório usando uma agregação

Para visualizar e analisar os dados específicos de uma agregação que você criou, gere um relatório fornecendo uma condição para a agregação no Construtor de condições.

Antes de Iniciar
Função necessária: pa_admin

Procedimento

1. Navegar até **Todos** > **Relatórios** > **Criar novo(a)**.
2. Na guia **Dados**, preencha os campos.

Campos da guia Dados

Campo	Descrição
Nome do relatório	Nome do relatório.
Tipo de origem	Tipo de origem da qual os dados são obtidos. Selecione **Tabela**.
Tabela	Nome da tabela para a qual a agregação é criada. Selecione a tabela de resultados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	agregados, Resultado agregado [sn_vul_cmn_aggregate_result].

3. No Construtor de condições, defina a condição para a agregação para a qual você deseja gerar um relatório.

Condição no Construtor de condições

Parte	Descrição
Campo	Selecione **Agregação**.
Operador	Selecione **é**.
Valor	Nome da agregação.

4. Na guia **Dados**, clique em **Avançar**.
5. Na guia **Tipos**, selecione como você deseja visualizar os dados e clique em **Avançar**. Para saber mais sobre os tipos de relatório, consulte Criação de relatórios .

   As visualizações compatíveis são gráfico de barras, gráfico de pizza e mapa térmico. Você pode modificar os gráficos de linhas e outras visualizações de tendências para usar as visualizações compatíveis com o resultado agregado para representar os mesmos dados. A exibição de lista não é compatível.
6. Na guia **Configurar**, preencha os campos.

Campo	Descrição
Agrupar por	Selecione **Agrupado por 1** que você selecionou na guia **Agrupar por** da agregação.
Empilhar por	Selecione **Agrupado por 2** que você selecionou na guia **Agrupar por** da agregação.
Agregação	Aplique a função **Mínimo** ou **Máximo** em **Valor**.

7. Na guia **Estilo**, preencha os campos conforme apropriado e clique em **Executar**. Para obter mais informações sobre os campos nas guias **Configurar** e **Estilo**, consulte o vídeo Criação de um relatório .
8. No Construtor de condições, defina a condição da agregação para a qual você deseja gerar um relatório e clique em **Executar**.

   O relatório é exibido.
9. Para classificar os valores no eixo x, selecione **Adicionar classificação**.

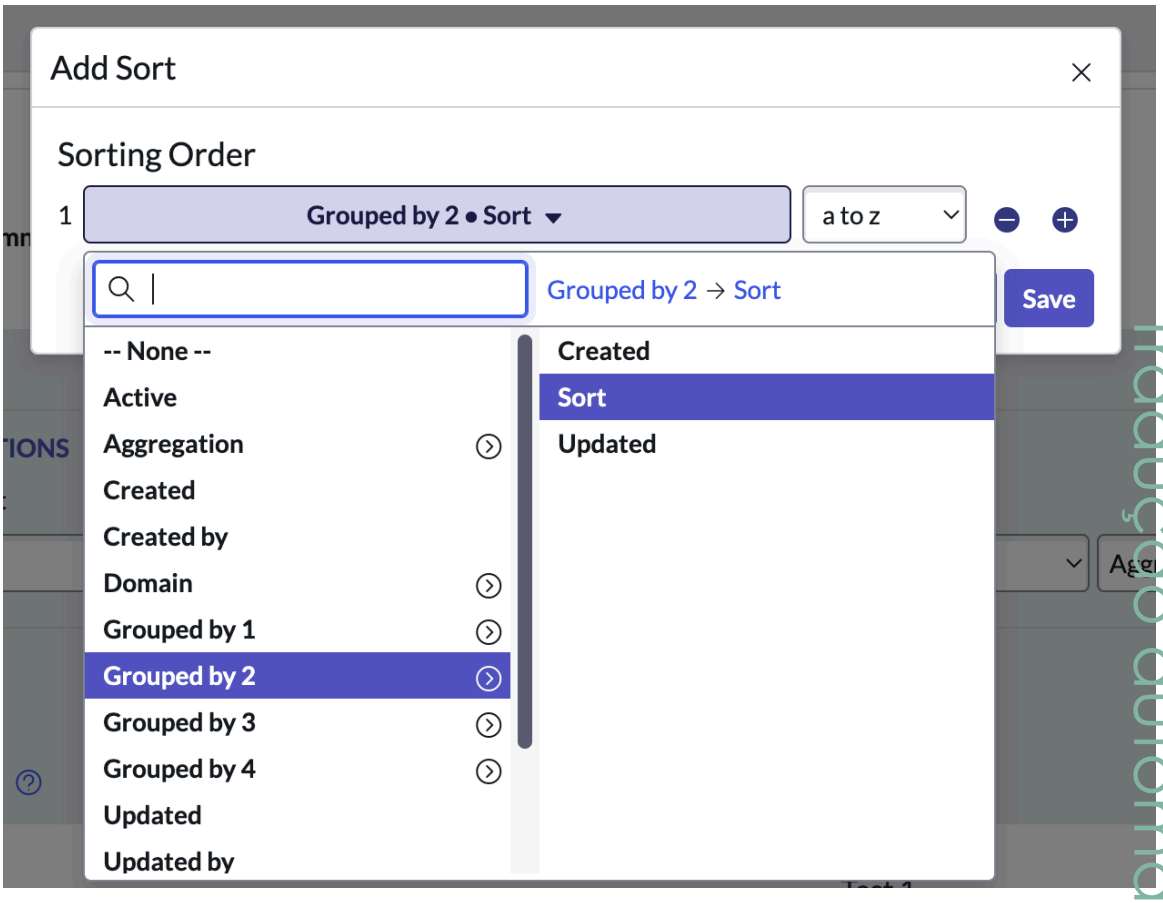
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para cadeias de caracteres, forneça a condição como **Agrupado por > az ou za** para classificar as cadeias de caracteres em ordem alfabética.

b. Para valores de tipo de dados inteiros e de data, forneça a condição como **Agrupado por.classificar > az ou za** para classificar os valores em ordem crescente e decrescente, respectivamente.

Classificando números inteiros no eixo X

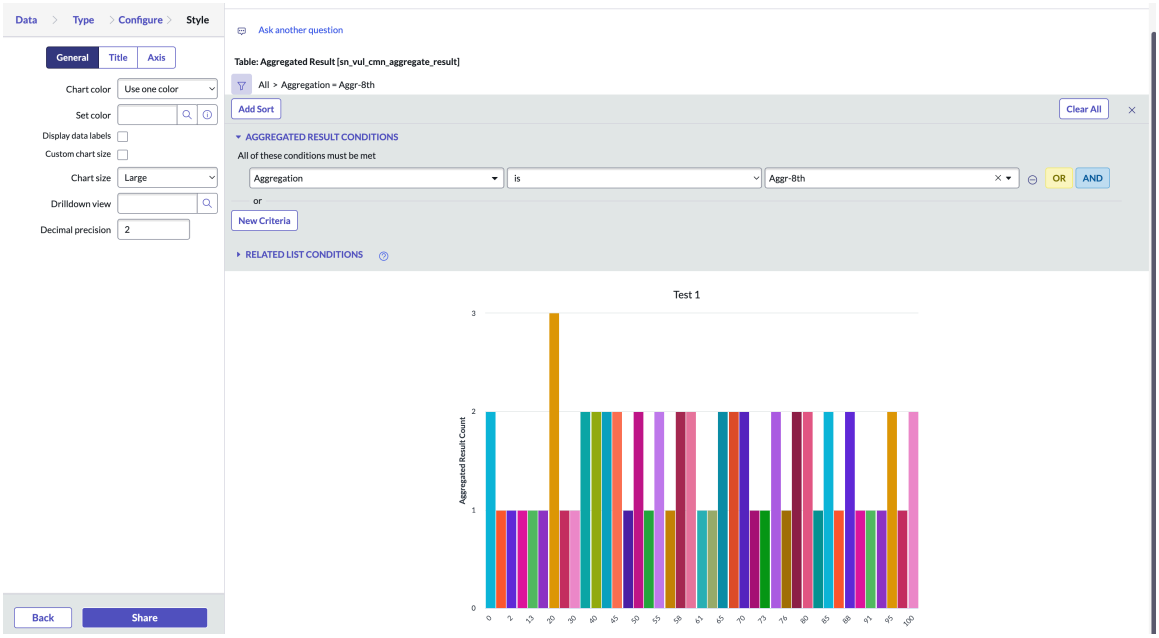


c. Selecione **Executar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os valores inteiros e de data são classificados no eixo X.



10. Clique em **Salvar** para salvar seu relatório.
    O relatório gerado para uma agregação é exibido na guia **Resultados** do respectivo formulário de **Agregação**.
11. Opcional: Adicione seu relatório a um painel.
    Para obter mais informações sobre como adicionar um relatório a um painel, consulte Como adicionar um relatório a um painel dinâmico .

    O painel **Gestão de vulnerabilidades [Agregado]** que consiste em relatórios criados usando a estrutura de relatórios em cache é enviado com o sistema de base. Para exibir este painel, navegue até **Todos** > **Análise de desempenho** > **Painéis** > **Todos** > **Gestão de vulnerabilidades [Agregado]**. As agregações ativas correspondentes aos relatórios neste painel são enviadas com o sistema de base.
12. Compartilhe seu relatório com outros usuários.
    Para obter mais informações sobre como compartilhar relatórios, consulte Distribuir relatórios .

Informações relacionadas

Configurar uma agregação para dados de origem

Estrutura de relatórios agregados

Executar várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

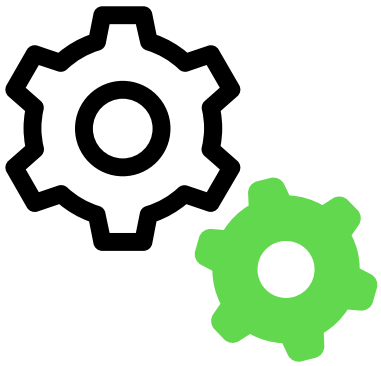
Resposta a vulnerabilidades Espaços

Os Espaços de resposta a vulnerabilidades oferecem uma exibição consolidada dos recursos que permite realizar várias tarefas no mesmo painel, aumentando a produtividade e economizando tempo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades Espaços

Espaço para gerentes de vulnerabilidades	Espaço de correção de TI	Espaço de avaliação de vulnerabilidade
		
Saiba mais sobre o Espaço do gerenciador de vulnerabilidades	Saiba mais sobre o Espaço de correção de TI	Saiba mais sobre o Espaço de avaliação de vulnerabilidade

Tradução automática

Antes de começar

Antes de usar os espaços:

- Você precisa executar algumas tarefas de configuração. Para obter mais informações, consulte Configurar os Resposta a vulnerabilidades Espaços.
- Revise informações importantes sobre atualizações de tarefas de correção, regras de tarefa de correção e termos e conceitos-chave sobre os espaços, em Resposta a vulnerabilidades Espaços e atualizações para tarefas de correção e regras de tarefa de correção.

Solucionar problemas e obter ajuda

- Operações de segurança na comunidade da ServiceNow
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Orquestração de patches com os espaços Resposta a vulnerabilidades

Você pode gerenciar patches e implantações de patches para vulnerabilidades críticas de grandes grupos de ativos com a Orquestração de patches com Resposta a vulnerabilidades.

Orquestração de patches nos espaços

A orquestração de patches com a aplicação Resposta a vulnerabilidades usa importações agendadas de integrações de soluções de terceiros, fornecedores de patch e scanners de vulnerabilidade.

A orquestração de patches com a aplicação Resposta a vulnerabilidades é compatível com o ambiente clássico e os espaços Resposta a vulnerabilidades. Os dados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

correlacionados são acumulados e exibidos nos espaços e no ambiente clássico. Para obter uma visão geral sobre os recursos, requisitos e informações sobre a orquestração de patches no ambiente clássico, consulte Orquestração de patches com Resposta a vulnerabilidades.

- Para obter mais informações sobre as integrações compatíveis com fornecedores de patch, consulte Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades e Noções básicas sobre a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM.
- Para obter informações sobre como programar patches de registros de formulário nos espaços, consulte Programar patches com a integração Microsoft do SCCM com Resposta a vulnerabilidades e Programar patches com o HCL BigFix de integração de orquestração de patches Resposta a vulnerabilidades.

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

Para exibir dados de Orquestração de patches e atualizações disponíveis (patches) nos espaços em Resposta a vulnerabilidades, as aplicações a seguir são necessárias. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas. Consulte Orquestração de patches com Resposta a vulnerabilidades.

Funções necessárias

Além das funções sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin necessárias para os espaços Resposta a vulnerabilidades, os usuários precisam de funções que sejam específicas para as integrações de orquestração de patches que você está usando para exibir dados e programar patches. Consulte as seguintes integrações compatíveis para obter mais informações sobre essas funções.

Consulte Noções básicas sobre a integração de orquestração de patches do BigFix de HCL com Resposta a vulnerabilidades e Noções básicas sobre a integração de orquestração de patches [Resposta a vulnerabilidades com Microsoft SCCM.

Dados de patch nos espaços Resposta a vulnerabilidades

No IT Remediation Workspace, você pode exibir dados de patch nos espaços:

- Na exibição inicial, clique em cartões de pontuação para exibir registros de soluções preferenciais em IVs, ICs vulneráveis e patches preferenciais em IVs.
- Na exibição de lista, exiba todos os registros de atualização de patch (VPUs) e os itens vulneráveis atribuídos a você que têm patches dos links disponíveis.

Você pode programar patches dos seguintes registros:

- Atualização de patch (VPU)
- Tarefa de correção (RT)
- Item descoberto (SDI)

No Espaço para gerentes de vulnerabilidades, você pode exibir patches:

- Na exibição inicial em tópicos de observação na guia Itens vulneráveis, você pode exibir patches preferenciais e potenciais, datas programadas de patch e outras informações.
- Na exibição de lista em registros de esforço de correção, você pode exibir dados de patch em registros de VIT na guia Itens vulneráveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a vulnerabilidades Espaços e atualizações para tarefas de correção e regras de tarefa de correção

As tarefas de correção agrupam itens vulneráveis nos espaços Resposta a vulnerabilidades.

Termos-chave para os Resposta a vulnerabilidades Espaços

Espaços de resposta a vulnerabilidades, ou espaços

Resposta a vulnerabilidades é compatível com os espaços Resposta a vulnerabilidades. Você pode usar a experiência clássica IU principal ou os espaços.

IU clássica (legada)

Refere-se à experiência IU principal. Você ainda executa algumas ações e exibe algumas listas no ambiente clássico.

Espaço para gerentes de vulnerabilidades

Neste espaço, os gerentes monitoram as vulnerabilidades direcionadas e selecionam os IVs e resultados de testes com os quais mais se importam para atribuir à TI.

Espaço de correção de TI

Neste espaço, as equipes de TI podem se concentrar nas vulnerabilidades mais importantes atribuídas a elas pela segurança. As informações centradas em TI que incluem itens de configuração (ICs) distintos afetados, soluções e o andamento da correção estão facilmente disponíveis para os responsáveis pela correção neste espaço.

Espaço de avaliação de vulnerabilidade

Neste espaço, os analistas de vulnerabilidade podem executar a avaliação de vulnerabilidade durante a análise de vulnerabilidade de dia zero. Depois que uma vulnerabilidade de dia zero é identificada, eles podem avaliar o possível impacto e o risco associados à vulnerabilidade. Os analistas podem analisar o sistema, as aplicações ou os componentes de rede afetados para entender a gravidade e os possíveis vetores de ataque na organização.

Tópico de observação

Os tópicos de observação definem um segmento dos itens vulneráveis que os gerentes e analistas de vulnerabilidades desejam monitorar no Espaço do gerenciador de vulnerabilidades. Os tópicos de observação mostram um conjunto de visão geral focado de relatórios que pertencem a um segmento de IVs e resultados de testes com tendências, IC e estatísticas relacionadas a vulnerabilidades. Os painéis desses tópicos podem ser usados para monitorar tendências. Os painéis também podem ajudar os gerentes a:

- Exibir o andamento da correção em itens críticos
- Determinar a existência de vulnerabilidades em sistemas críticos
- Ver quando uma nova exploração é lançada
- Gerar resposta rápida para resolver um conjunto específico de vulnerabilidades

Esforço de correção (RE)

Os esforços de correção são criados por gerentes de vulnerabilidade quando eles determinam que é hora de a TI corrigir as vulnerabilidades listadas em um tópico de observação. Os gerentes e analistas de vulnerabilidade podem escolher como desejam criar tarefas de correção, por grupo de atribuição e

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidade, por exemplo. As tarefas de correção estão contidas no esforço de correção.

Tarefa de correção (VUL)

As equipes de TI usam tarefas de correção para corrigir as vulnerabilidades atribuídas a elas pela segurança. Tarefas de correção são listas das ações necessárias para corrigir vulnerabilidades. Tarefas de correção são criadas automaticamente quando os gerentes de segurança criam esforços de correção.

Desenvolvimento dos espaços

Nas versões anteriores do Resposta a vulnerabilidades, você tinha duas opções para monitorar um conjunto de itens vulneráveis (IVs) como analista de segurança e vulnerabilidade:

- O painel Visão geral, que resume todos os IVs
- Tarefas de correção

Itens vulneráveis foram classificados em tarefas de correção automaticamente de acordo com suas regras de tarefa de correção predefinidas. As tarefas de correção foram projetadas para oferecer suporte às equipes de TI na correção de blocos gerenciáveis de itens vulneráveis.

Essa automação tornou possível agrupar um número muito grande de IVs automaticamente para atribuição e correção em massa. No entanto, os analistas e gerentes de vulnerabilidade consideraram o monitoramento de todo o conjunto de itens vulneráveis das tarefas de correção um desafio. Além de problemas de desempenho com grupos grandes, pode ser difícil criar regras funcionais de tarefa de correção que filtram somente as vulnerabilidades que você considerou mais críticas.

Os Resposta a vulnerabilidades Espaços:

- Ajude os gerentes de segurança a filtrar, monitorar IVs ativos e resultados de testes ao longo do tempo e orientar a correção das vulnerabilidades que eles determinam como as mais importantes.
- Forneça às equipes de TI informações centradas na TI em um local que elas possam usar para corrigir as vulnerabilidades atribuídas a elas pela segurança.

Atualizações para tarefas de correção nos espaços

No espaço do Gerenciador de vulnerabilidades, os analistas e gerentes de vulnerabilidade usam os tópicos de observação e os esforços de correção como dois novos métodos para monitorar e atribuir IVs para correção.

Os grupos de vulnerabilidade foram renomeados para Tarefas de correção. Esta mudança se aplica a rótulos em listas, registros e regras na IU legada e nos espaços. As tarefas de correção são configuradas para que as equipes de TI possam trabalhar com elas no espaço de correção de TI. A lista a seguir ilustra como, como gerente de vulnerabilidades ou analista de vulnerabilidades, você pode monitorar vulnerabilidades e resultados de testes, filtrá-los e atribuí-los:

1. No Espaço do gerenciador de vulnerabilidades, os gerentes monitoram as vulnerabilidades importadas nos tópicos de observação. Gerentes e analistas usam tópicos de observação para monitorar um conjunto dinâmico de IVs filtrados ao longo do tempo que eles consideram os mais críticos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Com os tópicos de observação, os gerentes de segurança podem determinar quando e que tipo de IVs devem ser entregues às equipes de TI em Esforços de correção (REs). Esses REs são listas estáticas dos IVs que a segurança deseja que as equipes de TI corrijam.

   Nos esforços de correção, os gerentes têm quatro opções para agrupar IVs em Tarefas de correção (VULs). As tarefas de correção são atribuídas automaticamente às equipes de TI com base nos grupos de atribuição que estão originalmente associados aos IVs.

3. As equipes de TI trabalham em tarefas de correção no Espaço de correção de TI sem precisar classificar todos os IVs.

   Uma tarefa de correção faz a transição pelos mesmos estados que a tarefa de correção faz nas versões anteriores do Resposta a vulnerabilidades. Quando todos os IVs em uma tarefa de correção são encerrados, a tarefa de correção é encerrada e definida como **Inativa**.

   O andamento da correção é atualizado nas visualizações de dados nos tópicos de observação e na página inicial de correção de TI.

Atualizações nas regras de tarefa de correção nos espaços

As Regras de grupo de vulnerabilidade são chamadas de Regras de tarefa de correção. Esta mudança se aplica aos rótulos em listas, registros e regras na IU legada e nos espaços.

Nomes de tabela, por exemplo, [sn_vul_m2m_vul_group_item], não são alterados.

Se você criou regras de grupos de vulnerabilidades em versões anteriores do Resposta a vulnerabilidades, elas ainda estarão disponíveis para você, rotuladas como regras de tarefa de correção.

No entanto, nos espaços, as regras do grupo de vulnerabilidades não são mais usadas como o método primário de organizar um grande volume de itens vulneráveis em grupos de vulnerabilidades. Você pode preferir deixar suas regras de tarefa de correção inativas conforme você se acostuma com os espaços.

Você pode preferir começar a usar os espaços Resposta a vulnerabilidades de forma incremental.

1. Se você estiver atualizando de uma versão anterior do Resposta a vulnerabilidades, suas regras de VG existentes serão preservadas. Eles ainda estão disponíveis para você nos espaços. A regra de grupo padrão, Vulnerabilidade, está inativa por padrão.
2. Configure regras de atribuição e, talvez se quiser, regras de risco e execute uma importação.
3. Como gerente ou analista de vulnerabilidades, você pode escolher segmentos para monitorar nos tópicos de observação no Espaço do gerenciador de vulnerabilidades. Você pode usar tópicos de observação como recursos autônomos. Escolha qualquer subconjunto de IVs e use o painel neles para monitorar tendências. Com eles, você pode decidir onde e quando concentrar os esforços de correção.
4. Como gerentes ou analistas de vulnerabilidade, você cria esforços de correção a partir de tópicos de observação quando decide que é hora de corrigir um subconjunto de itens vulneráveis. Uma tarefa de correção também é criada automaticamente para ser entregue à TI quando você cria um esforço de correção.
5. Com o tempo, como gerente ou analista de vulnerabilidades, você pode descobrir alguns padrões de rotina que pode processar automaticamente com regras de tarefas de correção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir suas regras de tarefa de correção, navegue até **Resposta a vulnerabilidades** > **Administração** > **Regras de tarefa de correção**.

Mais informações sobre regras de atribuição, regras de tarefa de correção, esforços de correção e itens vulneráveis nos espaços Resposta a vulnerabilidades

- Os registros da Tarefa de correção (VUL) são exibidos em listas e registros no ambiente clássico e nos espaços.
- Uma tarefa de correção faz a transição pelos mesmos estados que um grupo de vulnerabilidades. Quando todos os IVs em uma tarefa de correção são encerrados, a tarefa de correção faz a transição para o estado Inativo.
- Para ajudar suas equipes na correção, um item vulnerável só pode estar em um esforço de correção. Quando estiver em um esforço de correção, um item vulnerável não será adicionado a nenhum outro esforço de correção criado.
- Se você excluir um esforço de correção, o esforço de correção se tornará inativo e todos os IVs ativos estarão disponíveis para novos esforços de correção.
- Um item vulnerável pode estar em várias tarefas de correção.
- As tarefas de correção são atribuídas automaticamente às equipes de TI com base no grupo de atribuição que está associado a um item vulnerável em um esforço de correção. Se você criar uma tarefa de correção sob demanda, selecione o grupo de atribuição.
- Se você estiver atualizando de uma versão anterior do Resposta a vulnerabilidades, suas regras de atribuição foram preservadas na IU legada.
- Se você estiver atualizando de uma versão anterior do Resposta a vulnerabilidades, seus usuários e grupos atuais serão herdados e estarão acessíveis para você nos espaços.

Para obter mais informações sobre os ciclos de vida dos esforços de correção, consulte Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades.

Configuração e configuração dos espaços Resposta a vulnerabilidades

Para obter mais informações sobre regras de atribuição e regras de tarefa de correção, consulte Configurar os Resposta a vulnerabilidades Espaços e Resposta a vulnerabilidades visão geral das regras de atribuição.

Se você é um novo cliente e ainda não os adicionou, deverá configurar usuários e grupos para que itens vulneráveis e tarefas de correção sejam atribuídos aos grupos de correção desejados. As regras de atribuição da Resposta a vulnerabilidades são usadas para atribuir trabalho a grupos.

Configurar os Resposta a vulnerabilidades Espaços

Antes de usar os espaços, confirme se concluiu as tarefas de configuração a seguir.

Antes de Iniciar

Função necessária: administrador para atribuir funções a usuários e grupos e usuários a grupos.

sn_vul.vulnerability_admin para editar, criar regras e configurar a aplicação Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

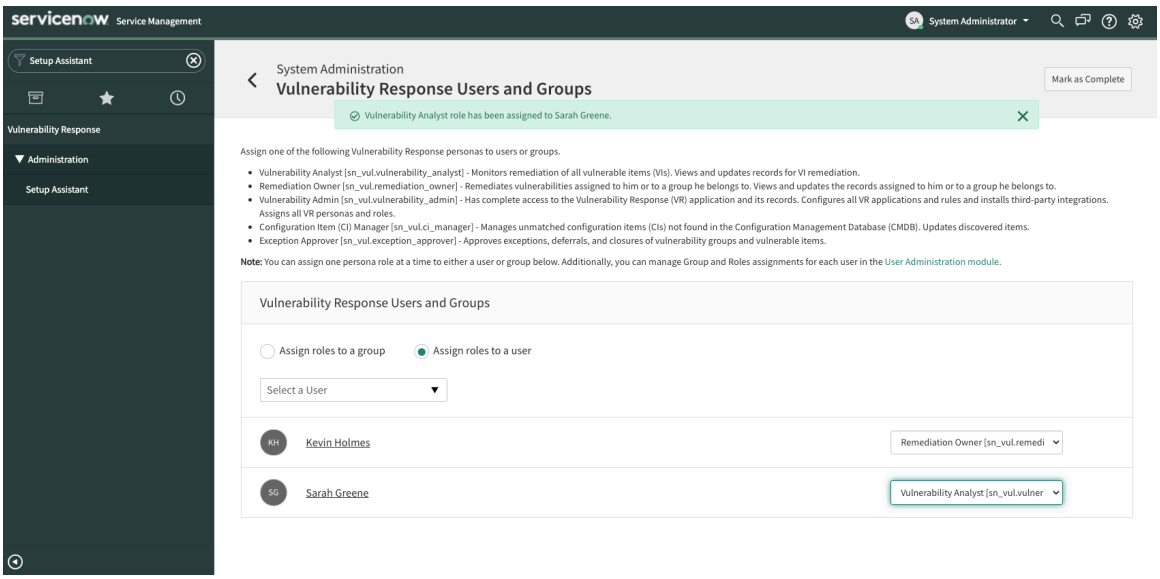
Confirme que você concluiu as tarefas de configuração a seguir. Consulte as etapas após a lista para obter mais informações sobre como executar essas tarefas.

Tarefa	Descrição
☐	Se ainda não estiver atribuído, atribua usuários e grupos com as funções apropriadas para que eles tenham acesso aos espaços. Função necessária: administrador Consulte as etapas abaixo para obter mais informações.
☐	Configure regras de atribuição para que os itens vulneráveis sejam atribuídos aos grupos apropriados para correção. Função necessária: sn_vul.vulnerability_admin. Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Você cria e edita regras de atribuição no ambiente clássico.
☐	(Opcional): edite ou crie suas regras de tarefa de correção. Função necessária: sn_vul.vulnerability_admin. **Nota:** Funcionalmente, as regras de tarefa de correção funcionam da mesma forma que as regras de tarefa de correção nas versões anteriores do Resposta a vulnerabilidades. No entanto, ao contrário dos grupos de vulnerabilidades que foram criados automaticamente a partir das regras de tarefa de correção, as tarefas de correção são criadas quando você cria esforços de correção. Você tem as seguintes opções para agrupar os itens vulneráveis em um esforço de correção em tarefas de correção: • Por grupo de atribuição • Por grupo de atribuição e item de configuração • Por grupo de atribuição e vulnerabilidade • Nenhum - Use esta opção se quiser adicionar IVs manualmente a uma tarefa de correção. Para obter mais informações, consulte Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades. Para obter mais informações sobre como os IVs são agrupados automaticamente e como as regras de grupo são reaplicadas no ambiente clássico, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral.
☐	Editar regras de destino de correção. Função necessária: sn_vul.vulnerability_admin. Adicione regras de destino de correção no ambiente clássico. Para obter mais informações sobre regras de destino de correção, consulte Criar ou editar Resposta a vulnerabilidades regras de destino de correção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Depois de instalar e ativar a aplicação Resposta a vulnerabilidades, no ambiente clássico como um usuário com a função de administrador, navegue até **Todos** > **Resposta a vulnerabilidades** > **Administração** > **Assistente de configuração**.



2. No Assistente de configuração, atribua usuários aos seguintes grupos.

   Nota: 1000 é o limite para o número de grupos de usuários aos quais um usuário pode ser atribuído nos Espaços de resposta a vulnerabilidades.

   Os grupos a seguir são fornecidos com a aplicação Resposta a vulnerabilidades e são usados nos espaços. Você pode atribuir usuários a eles no Assistente de configuração:

   - Responsável pela correção - este grupo é para responsáveis pela correção de TI no espaço de correção de TI. Usuários com esta função corrigem vulnerabilidades atribuídas a eles em tarefas de correção.

     Nota:

     Se você quiser que os proprietários de correção criem e exibam solicitações de mudança e exibam dados de item de configuração (IC) vulnerável no espaço de correção de TI e no ambiente clássico, atribua a eles a função itil. Você pode preferir atribuir a função itil a usuários individuais em vez de a todos os membros de um grupo. A função cmdb_read também é uma opção para os usuários exibirem dados de IC nos espaços.

   - A partir da v16.1, você pode configurar lembretes por e-mail para os responsáveis pela correção de TI. Para configurar notificações por e-mail para os espaços, consulte Configurar notificações por e-mail nos espaços Resposta a vulnerabilidades.
   - Administrador de vulnerabilidade - este grupo é para gerentes de vulnerabilidade. Esta função configura a aplicação Resposta a vulnerabilidades no Assistente de configuração. Esta função também tem permissão para processar solicitações de exceção e falso-positivo.
   - Analista de vulnerabilidade - este grupo é para gerentes de segurança, gerentes de vulnerabilidade e analistas no Espaço do gerente de vulnerabilidade. Esta função monitora vulnerabilidades, cria tópicos de observação e esforços de correção e monitora o andamento da correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Aprovador de falso-positivo - Os usuários neste grupo processam solicitações de falso-positivo para itens vulneráveis ou tarefas de correção. Uma solicitação de falso-positivo requer um processo de aprovação de nível único. Você pode gerenciar a atribuição de usuários a este grupo fora do Assistente de configuração em **Administração de usuários**.
- Aprovador de exceção - uma solicitação de exceção para um item vulnerável ou tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. A solicitação de exceção requer dois níveis de aprovadores. Adicione usuários a ambos os grupos de aprovação: Aprovador de exceção - nível 1 e Aprovador de exceção nível - 2. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de segundo nível. Você gerencia a atribuição de usuários a este grupo fora do Assistente de configuração em **Administração de usuários**.

> **Nota:** Adicione usuários aos grupos de aprovação antes de enviar solicitações de falso-positivo e de exceção. Se você criar solicitações antes de atribuir usuários com permissão de aprovação, as solicitações podem não estar visíveis para eles.

Como alternativa, clique no link **Administração de usuário** para gerenciar e atribuir as funções granulares a seguir aos usuários e grupos existentes. Essas funções permitem que os usuários executem ações específicas na aplicação Resposta a vulnerabilidades e nos espaços.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Para criar e exibir solicitações de mudança no Espaço de correção de TI e no ambiente clássico, atribua a eles a função itil.

Consulte Resposta a vulnerabilidades personas e funções granulares e Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração para obter mais informações sobre como atribuir funções de persona a usuários e usuários a grupos.

3. As tarefas de correção são transferidas automaticamente para grupos de atribuição de correção de TI para processamento quando são criadas.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum - Use esta opção se quiser adicionar IVs manualmente a uma tarefa de correção.

   > **Nota:** Para a versão 18.0 de Resposta a vulnerabilidades, a opção **Nenhum** não está disponível.

   Se você estiver atualizando de uma versão anterior do Resposta a vulnerabilidades, seus grupos de atribuição serão preservados. No entanto, você pode preferir editar esses grupos para que os itens vulneráveis sejam associados a grupos de atribuição específicos até que você se acostume com o funcionamento dos tópicos de observação e dos esforços de correção. Por exemplo, você pode criar grupos de atribuição por produto ou região, mas pode usar qualquer critério que melhor se adeque à sua organização.

   Você também pode usar regras de atribuição para atribuir tarefas de correção a grupos. Você pode preferir executar somente regras de alta prioridade para os seguintes itens:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Itens que precisam de tratamento especial
- Itens em que o risco é crítico ou um VI requer tratamento pela conformidade regulatória

As seguintes regras de atribuição fornecidas com a aplicação estão ativas por padrão:

- Regra de atribuição de IC descontinuada
- Atribuir ao grupo de suporte de IC
- Regra de atribuição de estação de trabalho
- Regra de atribuição de banco de dados
- Regra de atribuição da aplicação web
- Regra de atribuição do Windows Server
- Regra de atribuição de servidor não Windows
- Regra de atribuição de contato alternativo

Para obter mais informações sobre regras de atribuição, consulte Resposta a vulnerabilidades visão geral das regras de atribuição. Você cria e edita regras de atribuição no ambiente clássico.

4. Opcional: Edite ou crie suas regras de tarefa de correção.

(Optional) Nos espaços, as tarefas de correção são criadas quando você cria esforços de correção. Você tem as seguintes opções para agrupar os itens vulneráveis em um esforço de correção em tarefas de correção:

- Por grupo de atribuição
- Por grupo de atribuição e item de configuração
- Por grupo de atribuição e vulnerabilidade
- Nenhum - Use esta opção se quiser adicionar IVs manualmente a uma tarefa de correção. Para obter mais informações, consulte Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades.

> **Nota:** Na versão 18.0 de Resposta a vulnerabilidades, a opção **Nenhum** não está disponível.

Para obter mais informações sobre como os IVs são agrupados automaticamente e como as regras de grupo são reaplicadas no ambiente clássico, consulte Resposta a vulnerabilidades tarefas de correção e regras de tarefa de correção visão geral.

Vulnerability Manager Workspace

O Vulnerability Manager Workspace permite que gerentes e analistas de vulnerabilidade monitorem as vulnerabilidades com as quais mais se importam e decidam estrategicamente quais vulnerabilidades eles enviam para as equipes de TI corrigirem.

Visão geral

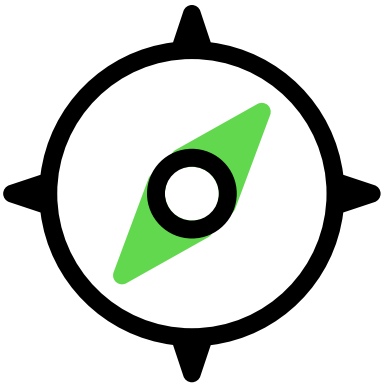
Demonstração do espaço do gerenciador de vulnerabilidades V18.0

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

Explorar

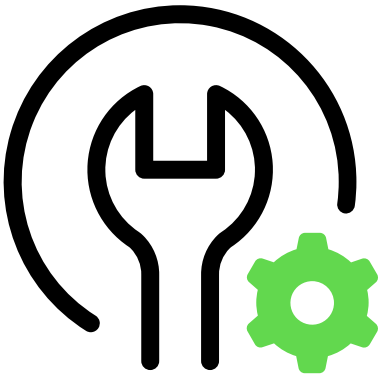


Saiba mais sobre os recursos do Espaço do gerenciador de vulnerabilidades

Monitorar e gerenciar

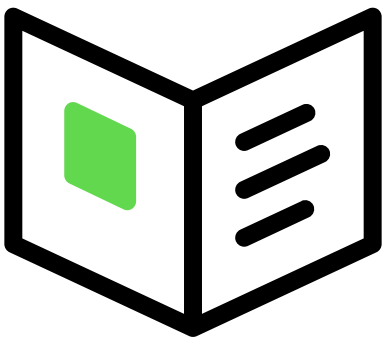
Aprenda a monitorar e gerenciar itens vulneráveis (VITs, AVITs e CVITs) e testar resultados no Espaço do gerenciador de vulnerabilidades

Corrigir



Aprenda a corrigir itens vulneráveis (VITs, AVITs e CVITs) e testar resultados no Espaço do gerenciador de vulnerabilidades

Referência



Saiba mais sobre as informações adicionais necessárias para usar o Espaço do gerenciador de vulnerabilidades

Solucionar problemas e obter ajuda

- Operações de segurança na comunidade da ServiceNow
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar o Vulnerability Manager Workspace

Como gerente e analista de vulnerabilidades, obtenha uma exibição unificada de todos os tipos de vulnerabilidade no Vulnerability Manager Workspace. Você pode ver vulnerabilidades e problemas de configuração de host, aplicação e contêiner, criar tópicos de observação nessas vulnerabilidades e configurações incorretas e criar tarefas de correção.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Você pode exibir o Vulnerability Manager Workspace navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades**.

O Espaço do gerenciador de vulnerabilidades consiste nas seguintes páginas:

Página inicial

Consiste em filtros predefinidos que são usados para visualizar o resumo dos registros.

Para obter mais informações sobre a Página inicial, consulte Visão geral da página inicial.

Nota: A partir da v21.0 de Resposta a vulnerabilidades, os tópicos de observação aparecem na página Tópicos de observação.

Página Tópicos de observação

Consiste em uma lista de tópicos de observação, que são categorizados em quatro módulos: vulnerabilidades do host, vulnerabilidades da aplicação, vulnerabilidades do contêiner e resultados de testes de configuração.

Para obter mais informações sobre tópicos de observação, consulte Visão geral dos tópicos de observação.

Página Painéis

Consiste nos painéis Gestão de vulnerabilidades, Gestão de vulnerabilidades (PA), Aprovações de vulnerabilidades, CISO, Visão geral da Gestão de vulnerabilidades de contêineres, Gestão de vulnerabilidades de aplicações, Resposta unificada a vulnerabilidades e Integridade.

Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace.

Nota: A página Painéis aparece a partir da versão 19.0 de Resposta a vulnerabilidades.

Página da lista

Consiste nas páginas de lista padrão e personalizadas para esforços de correção, tarefas de correção, itens vulneráveis de host, itens vulneráveis de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aplicação, itens vulneráveis de contêiner, resultados de testes de configuração, exceções, aprovações e bibliotecas.

Para obter mais informações, consulte Visão geral de listas.

Visão geral da página inicial

A partir do Resposta a vulnerabilidades v21.0, a página inicial no Vulnerability Manager Workspace fornece um resumo dos registros ativos, mostrando visualizações de classificação de risco, andamento da correção, atribuições a grupos de atribuição, registros em tarefas de correção e vulnerabilidades de recursos em nuvem.

A partir da v21.0 da Resposta a vulnerabilidades, os tópicos de observação aparecem na página Tópicos de observação. Para obter mais informações, consulte Visão geral dos tópicos de observação.

Na página inicial, você pode exibir as visualizações dos itens vulneráveis de host pré-filtrados, itens vulneráveis de contêiner, itens vulneráveis de aplicação e resultados de testes de configuração. Você também pode exibir visualizações de um conjunto de registros desejados criando e aplicando filtros. Para obter mais informações sobre como criar, atualizar, aplicar e excluir filtros, consulte Criar e aplicar filtros para visualizar o resumo dos registros ativos.

Dica:

Se você definir a propriedade do sistema *sn_vul_cmn_ws.navigate_to_workspace* como verdadeira, ao selecionar os links de filtro predefinidos no painel de navegação, esses links serão abertos no Vulnerability Manager Workspace com a seleção automática do filtro salvo correspondente.

Por exemplo, se você selecionar **Alto risco** navegando até **Todos** > **Resposta a vulnerabilidades** > **Itens vulneráveis**, este link é redirecionado para a página inicial no Vulnerability Manager Workspace com seleção automática do filtro de **alto risco**.

Na página inicial, você pode executar o seguinte:

- navegue até a lista de registros ativos na IU clássica selecionando o link **Exibir lista clássica** a partir da v22.0 de Resposta a vulnerabilidades.
- exiba a lista de registros ativos no Vulnerability Manager Workspace selecionando a contagem de registros ativos ao lado do menu suspenso **Exibir por** a partir da v22.0 de Resposta a vulnerabilidades.
- exiba as informações mais recentes selecionando a opção **Atualizar** no menu de três pontos em um widget.

Vulnerabilidades do host

A guia **Vulnerabilidades do host** contém visualizações que fornecem um resumo geral das vulnerabilidades do host ativo.

Funções necessárias:

- sn_vul.vulnerability_analyst e sn_vul.vulnerability_admin para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vul.read_all para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades do host na página inicial

Visualização	Tipo	Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2 - Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Na tarefa de correção	Rosca de semicírculo	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com explorações existentes	Rosca de semicírculo	Registros ativos com e sem explorações conhecidas.
Por face externa	Rosca de semicírculo	Registros rativos categorizados pela exposição do ativo à internet.
Por classe de IC	Barra	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Gráfico de donut	Registros rativos categorizados por vários recursos de nuvem.
Itens adiados por motivo	Gráfico de donut	Registros adiados ativos agrupados por motivo.

Tradução automática

Vulnerabilidades do contêiner

A guia **Vulnerabilidades do contêiner** contém visualizações que fornecem um resumo geral dos itens vulneráveis de contêiner ativos.

Funções necessárias:

- sn_vul_container.vulnerability_analyst e sn_vul_container.vulnerability_admin para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vul_container.read_all para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades do contêiner na página inicial

Visualização	Tipo	Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2 - Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Na tarefa de correção	Rosca de semicírculo	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com explorações existentes	Rosca de semicírculo	Registros ativos com e sem explorações conhecidas.
Por face externa	Rosca de semicírculo	Registros rativos categorizados pela exposição do ativo na internet.
Imagens do Docker	Contagem	Número de imagens exclusivas do Docker.
Por imagem base	Gráfico de donut	Registros ativos categorizados pelo tipo de imagem.
Itens adiados por motivo	Gráfico de donut	Registros adiados ativos agrupados por motivo.

Tradução automática

Vulnerabilidades de aplicação

A guia **Vulnerabilidades da aplicação** contém visualizações que fornecem um resumo geral das vulnerabilidades da aplicação.

Funções necessárias:

- sn_vul.app_sec_manager para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vul.app_read_all para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades da aplicação na página inicial

Visualização	Tipo	Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2 - Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Na tarefa de correção	Rosca de semicírculo	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com explorações existentes	Rosca de semicírculo	Registros ativos com e sem explorações conhecidas.
Por face externa	Rosca de semicírculo	Registros rativos categorizados pela exposição do ativo à internet.
Por classe de IC	Barra	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Gráfico de donut	Registros rativos categorizados por vários recursos de nuvem.
Itens adiados por motivo	Gráfico de donut	Registros adiados ativos agrupados por motivo.

Tradução automática

Resultados de testes de configuração

A guia **Resultados de testes de configuração** contém visualizações que fornecem um resumo geral dos erros de configuração ativos dos ativos em sua organização.

Funções necessárias:

- sn_vulc.admin para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vulc.read para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Resultados de testes de configuração na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Resultados de testes de configuração na página inicial

Visualização		Descrição
Por grupo de atribuição e status de correção	Barra de distribuição	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Barra	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Gráfico de pizza	Registros ativos categorizados por classificação de risco (1 - Crítico, 2 - Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Por tecnologia	Barra	Registros ativos categorizados por tecnologia.
Por teste	Barra	Registros ativos categorizados por testes.
Por face externa	Rosca de semicírculo	Registros rativos categorizados pela exposição do ativo à internet.
Por classe de IC	Barra	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Gráfico de donut	Registros rativos categorizados por vários recursos de nuvem.
Itens adiados por motivo	Gráfico de donut	Registros adiados ativos agrupados por motivo.

Tradução automática

Visão geral dos tópicos de observação

Um tópico de observação é um conjunto de visualizações de dados que permite monitorar um conjunto filtrado de registros ao longo do tempo em um painel que pode ser de um interesse ou prioridade específico para sua organização.

A partir da v21.0 de Resposta a vulnerabilidades, os tópicos de observação aparecem na página Tópicos de observação.

Os dados exibidos nas visualizações de dados nos tópicos de observação são atualizados dinamicamente conforme os dados de vulnerabilidade mudam após a importação. Use os painéis para monitorar as tendências, o escopo e os tipos de vulnerabilidades e seus itens de configuração para o tópico de observação selecionado. Essas informações ajudam a determinar como as vulnerabilidades em cada tópico de observação afetam seu ambiente. Para obter mais informações sobre as guias de itens relacionados e

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

suas visualizações em um tópico de observação, consulte Lista de itens relacionados e visualizações em um tópico de observação.

Os seguintes tópicos de observação são fornecidos com o sistema de base no módulo de vulnerabilidades do host:

- Vulnerabilidades em ativos voltados externamente
- Vulnerabilidades com explorações disponíveis
- Vulnerabilidades em servidores Windows
- Vulnerabilidades em servidores LINUX
- Vulnerabilidades atrasadas críticas
- Vulnerabilidades críticas fora das Tarefas de correção

Nota: Se uma visualização de dados mostrar que não há IVs para essa categoria, mas você puder ver uma lista de VIs ao clicar no ícone do gráfico, verifique a coluna com o nome do tópico de observação na lista exibida. Verifique se o valor de todos os IVs listados na coluna do tópico de observação, por exemplo, voltado para a Internet, é `falso`. Este valor neste exemplo indica que não há IVs voltados para a Internet para este tópico de observação.

Para iniciar a correção ou quando surgir uma necessidade crítica dos registros que estão em um tópico de observação, você pode criar um esforço de correção a partir de um tópico de observação. Para obter mais informações, consulte Criar um esforço de correção no Espaço do gerenciador de vulnerabilidades.

Informações relacionadas

Lista de itens relacionados e visualizações em um tópico de observação

Usar tópicos de observação no Vulnerability Manager Workspace

Criar um tópico de observação no Espaço do gerenciador de vulnerabilidades

Editar ou excluir um tópico de observação

Desativar ou ativar um tópico de observação

Lista de itens relacionados e visualizações em um tópico de observação

A partir da versão 18.0, você pode criar tópicos de observação que são categorizados em quatro módulos, Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação e Resultados de testes de configuração. As guias de itens relacionados em um tópico de observação são diferentes para cada módulo.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

O painel de navegação na página principal contém os seguintes módulos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidades do host: exibe os tópicos de observação que incluem os itens vulneráveis do host.
- Vulnerabilidades do contêiner: exibe os tópicos de observação que incluem os itens vulneráveis do contêiner.
- Vulnerabilidades da aplicação: exibe os tópicos de observação que incluem os itens vulneráveis da aplicação.
- Configuração Resultados de testes: exibe os tópicos de observação que incluem os itens de configuração.
- Inativo: exibe os tópicos de observação inativos de todos os quatro módulos.

A tabela a seguir mostra as guias de itens relacionados que estão disponíveis para diferentes módulos de tópico de observação:

Tópico de observação e itens relacionados

Tópico de observação	Guias de itens relacionados
Vulnerabilidades do host	Visão geral, ICs afetados, vulnerabilidades distintas e itens vulneráveis
Vulnerabilidades do contêiner	Visão geral, ICs afetados, vulnerabilidades distintas e itens vulneráveis
Vulnerabilidades de aplicação	Visão geral e itens vulneráveis
Resultados de testes de configuração	Visão geral, ICs afetados, testes de configuração distintos e resultados de testes de configuração

A tabela a seguir fornece uma descrição das guias de itens relacionados e das visualizações em um tópico de observação.

Guias de itens relacionados e visualização em um tópico de observação

Guia e visualização de itens relacionados	Descrição
Visão geral	
Itens vulneráveis ativos ao longo do tempo	Número de itens vulneráveis (IVs) ativos ao longo do tempo. Você pode monitorar as tendências desses dados nos últimos 30 dias. Você também pode filtrar os dados usando os filtros Categoria de ativo .
IVs em esforços de correção	Número de IVs ativos do total de IVs que já estão nos esforços de correção ativos.
Esforços de correção ativos	Lista dos esforços de correção ativos.
Impactados ICs	
ICs distintos	Número de itens de configuração (ICs) (ativos) afetados por essas vulnerabilidades.
IVs por classe de IC	Número de itens vulneráveis (IVs) para cada Configuration Management Database (CMDB) classe de IC.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias de itens relacionados e visualização em um tópico de observação

Guia e visualização de itens relacionados	Descrição
	Nota: Este widget aparece somente para os tópicos de observação no módulo de vulnerabilidades de host, aplicação e contêiner.
Problemas de configuração por classe de IC	Número de ICs para cada Configuration Management Database (CMDB) classe de IC. **Nota:** Este widget aparece somente para os tópicos de observação no módulo Problemas de configuração.
IVs voltados para a Internet	Número de VIs ativos do número total de VIs para seus ativos que estão expostos à Internet. **Nota:** Este widget aparece somente para os tópicos de observação no módulo de vulnerabilidades de host, aplicação e contêiner.
Problemas de configuração voltados para a Internet	Número de ICs ativos do número total de ICs para seus ativos que estão expostos à Internet. **Nota:** Este widget aparece somente para os tópicos de observação no módulo Problemas de configuração.
Vulnerabilidades distintas	
IVs com explorações existentes	IVs ativos com explorações conhecidas.
Vulnerabilidades distintas	Número de vulnerabilidades individuais distintas que estão associadas aos seus ativos. As vulnerabilidades distintas podem ser filtradas com base no tipo de problema.
IVs com vulnerabilidades de PCI	Número de ativos individuais e distintos que têm IVs ativos com vulnerabilidades do Setor de cartões de pagamento (PCI).
Itens vulneráveis	
Itens vulneráveis de host	Lista de todos os itens vulneráveis de host. Você pode filtrar esta lista para que somente os registros que você deseja ver sejam exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias de itens relacionados e visualização em um tópico de observação

Guia e visualização de itens relacionados	Descrição
	Nota: Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades do host.
Itens vulneráveis da aplicação	Lista de todos os itens vulneráveis da aplicação. Você pode filtrar esta lista para que somente os registros que você deseja ver sejam exibidos. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades da aplicação.
Itens vulneráveis de contêiner	Lista de todos os itens vulneráveis de contêiner. Você pode filtrar esta lista para exibir somente os registros que deseja ver. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades do contêiner.
Guia**Visão geral** em um tópico de observação no módulo Resultados de testes de configuração	
Resultados de testes de configuração ativos ao longo do tempo	Número de resultados de testes de configuração ativos ao longo do tempo. Você pode monitorar as tendências desses dados nos últimos 30 dias.
Resultados de testes de configuração em esforços de correção	Número de resultados de testes de configuração ativos do número total de registros que já estão nos esforços de correção ativos.
Esforços de correção ativos	Lista dos esforços de correção ativos.
Guia**Testes de configuração distintos** em um tópico de observação no módulo Resultados de testes de configuração	
Resultados de testes de configuração via criticidade de teste	Resultados de testes de configuração baseados na criticidade dos problemas.
Testes de configuração distinta	Número de testes de configuração distintos.
Guia**Resultados de testes de configuração** em um tópico de observação no módulo Resultados de testes de configuração	Lista de resultados de testes de configuração.

Você pode adquirir os detalhes mais recentes de um tópico de observação selecionando o botão **Atualizar**. O status da atualização mais recente e o carimbo de data/hora são exibidos abaixo do nome do tópico de observação. Quando você atualiza um tópico de observação, todos os detalhes do tópico de observação, incluindo os gráficos e os esforços

Tradução automática

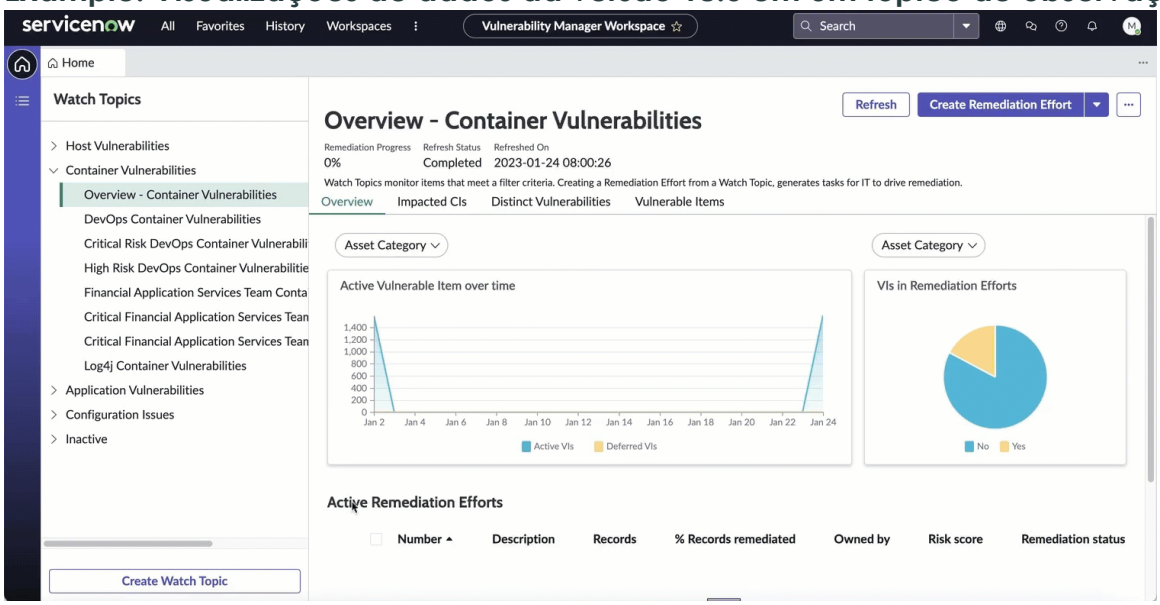
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de correção, são atualizados. Um tópico de observação é atualizado automaticamente quando é criado ou atualizado.

Nota: Como você não pode atualizar um tópico de observação inativo, o botão **Atualizar** está inativo para um tópico de observação inativo.

Clique em um gráfico de dados em qualquer um dos widgets para exibir informações adicionais sobre os registros.

Example: Visualizações de dados da versão 18.0 em um tópico de observação



Visão geral dos esforços de correção

Um Esforço de correção é um conjunto de registros associados a um tópico de observação. Os registros listados em um esforço de correção são estáticos. Eles não são atualizados por novos dados de importação ou mudanças feitas nos tópicos de observação.

Com **Ativo** selecionado na lista **Esforços** de correção, clique em um link de esforço de correção para abri-lo.

Os itens de lista relacionados no registro do esforço de correção permitem que você exiba o andamento e o status geral da correção nos registros associados a ele.

- Na guia **Visão geral**, monitore os registros associados a este esforço de correção que foram encerrados ao longo do tempo. À direita do registro, clique no ícone de filtro no gráfico para ver os filtros aplicados à visualização de dados.
- Na guia **Detalhes**, exiba detalhes sobre o esforço de correção, incluindo o tópico de observação associado e o status (Ativo ou Inativo). Você pode desativar um esforço de correção nesta página. Se você desativar o esforço de correção antes que todos os registros sejam encerrados, todos os registros ativos se tornarão disponíveis para serem adicionados a novos esforços de correção.
- Na guia **Tarefas** de correção, exiba as Tarefas de correção associadas a este esforço de correção. Veja a porcentagem de registros associados a esta tarefa que foram corrigidos.
- Na guia **Itens vulneráveis**, exiba os registros associados a este esforço de correção. Quando todos os registros em uma tarefa de correção são concluídos e encerrados, o esforço de correção muda para Inativo. Quando um esforço de correção está inativo, todos os registros encerrados associados ao esforço de correção não ficam disponíveis para serem adicionados a novos esforços de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> **Nota:** A partir da versão 18.0, a guia **Itens vulneráveis** aparece para os esforços de correção associados aos tópicos de observação nos módulos Vulnerabilidades do host, Vulnerabilidades da aplicação e Vulnerabilidades do contêiner.

- Na guia **Resultados de testes de configuração**, exibe os Resultados de testes de configuração associados ao Esforço de correção.

> **Nota:** A partir da versão 18.0, a guia **Resultados de testes de configuração** aparece para os esforços de correção associados aos tópicos de observação no módulo Resultados de testes de configuração.

Para obter mais detalhes e ações de IU que você pode executar em um esforço de correção, consulte Usar registros de esforço de correção.

Informações relacionadas

Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades

Criar um esforço de correção no Espaço do gerenciador de vulnerabilidades

Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades

Criar um esforço de correção recorrente nos Espaços de resposta a vulnerabilidades

Transferir registros para esforços de correção nos espaços Resposta a vulnerabilidades

Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades

Os estados dos registros e suas tarefas de correção (RTs) associadas serão afetados se os registros forem adiados, resolvidos, reabertos e transferidos para outros esforços de correção (REs).

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Como criar esforços de correção

O modo como os estados e ciclos de vida dos esforços de correção, tarefas de correção e registros são afetados depende de como um esforço de correção é criado, quando é criado e se é desativado.

Na lista no canto superior direito de um tópico de observação, você pode criar um esforço de correção clicando em **Criar um** esforço de correção ou **Criar esforço recorrente**. Você pode criar um esforço de correção recorrente por tópico de observação. Se você criar um esforço de correção recorrente, os esforços de correção subsequentes para o tópico de observação associado serão criados automaticamente com base nos critérios definidos. Em qualquer um dos casos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para facilitar a correção, somente registros ativos são adicionados aos esforços de correção.
- Todos os registros em novos esforços de correção são colocados em novas tarefas de correção. Os registros podem existir em várias tarefas de correção, mas somente um registro pode ser associado a um esforço de correção.

Nota: Um esforço de correção é desativado automaticamente quando não há registros ativos.

Transferindo registros ou transferência de registros

Você pode transferir registros de um esforço de correção para outro ao criar um esforço de correção marcando a caixa de seleção **Transferir registros correspondentes de outros esforços de correção ativos**. Para obter mais informações sobre como transferir os registros, consulte Transferir registros para esforços de correção nos espaços Resposta a vulnerabilidades. Se os registros forem transferidos de um esforço de correção ou transferidos para esforços de correção recorrentes:

Para um novo esforço de correção no mesmo tópico de observação

- Todas as Tarefas de correção do Esforço de correção antigo são movidas para o novo Esforço de correção.
- Novas Tarefas de correção são criadas com base nos critérios de agrupamento escolhidos para os registros que anteriormente não faziam parte de nenhuma Tarefa de correção.
- O Esforço de correção antigo está desativado.

Para um novo esforço de correção em um tópico de observação diferente

Todos os registros do Esforço de correção antigo são movidos para o novo Esforço de correção e as Tarefas de correção são criadas com base nos critérios de agrupamento escolhidos.

- Se todos os registros nas Tarefas de correção associadas ao Esforço de correção antigo forem transferidos, essas Tarefas de correção serão encerradas/canceladas.
- Se apenas um subconjunto de registros for transferido, as Tarefas de correção associadas ao antigo Esforço de correção serão divididas e permanecerão ativas.

As Tarefas de correção encerradas associadas ao Esforço de correção antigo não são afetadas.

Nota: Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. No entanto, você pode transferir registros de esforços de correção não recorrentes existentes para novos esforços de correção. Consulte Transferir registros para esforços de correção nos espaços Resposta a vulnerabilidades para obter mais informações sobre como transferir registros.

Painéis no Vulnerability Manager Workspace

No Vulnerability Manager Workspace, você pode exibir os painéis na IU Next Experience e usar esses painéis para rastrear e analisar as vulnerabilidades.

Funções necessárias:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Acesse os painéis em Vulnerability Manager Workspace navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades** e selecionando o ícone **Painéis**. O painel padrão é exibido com base na sua função.

A tabela a seguir mostra o painel padrão que é exibido para uma função específica.

Painel padrão

Painel padrão	Função
Painel unificado	sn_vul_cmn_vulnerability_admin ou sn_vul_cmn_vulnerability_analyst
Painel de PA de vulnerabilidade	sn_vul_vulnerability_admin ou sn_vul_vulnerability_analyst
Visão geral da aplicação	sn_vul_app_sec_manager
Visão geral do contêiner	sn_vul_container_vulnerability_admin ou sn_vul_container_analyst

Você pode exibir os seguintes painéis para as tarefas que deseja executar selecionando-os no menu suspenso da página Painéis.

Painéis no Espaço do gerenciador de vulnerabilidades

Painel	Descrição
Gestão de vulnerabilidade (PA)	Rastreie o volume, o desempenho e o andamento das vulnerabilidades do host, desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consulte Painel Gestão de vulnerabilidade do (PA).
Aprovações de vulnerabilidade	Exiba o número de solicitações de aprovação aprovadas, rejeitadas e pendentes para você. Para obter mais informações, consulte Usando os painéis padrão Resposta a vulnerabilidades.
Painel do CISO	Revela a postura geral de segurança da sua organização, incluindo a vulnerabilidade e os incidentes de segurança. Para obter mais informações, consulte Painel Gestão de vulnerabilidade do CISO.
Visão geral da gestão de vulnerabilidade do contêiner	Rastreie o volume, o desempenho e o andamento das vulnerabilidades do contêiner, desde a análise e detecção iniciais até a contenção ou correção. Para

Tradução automática

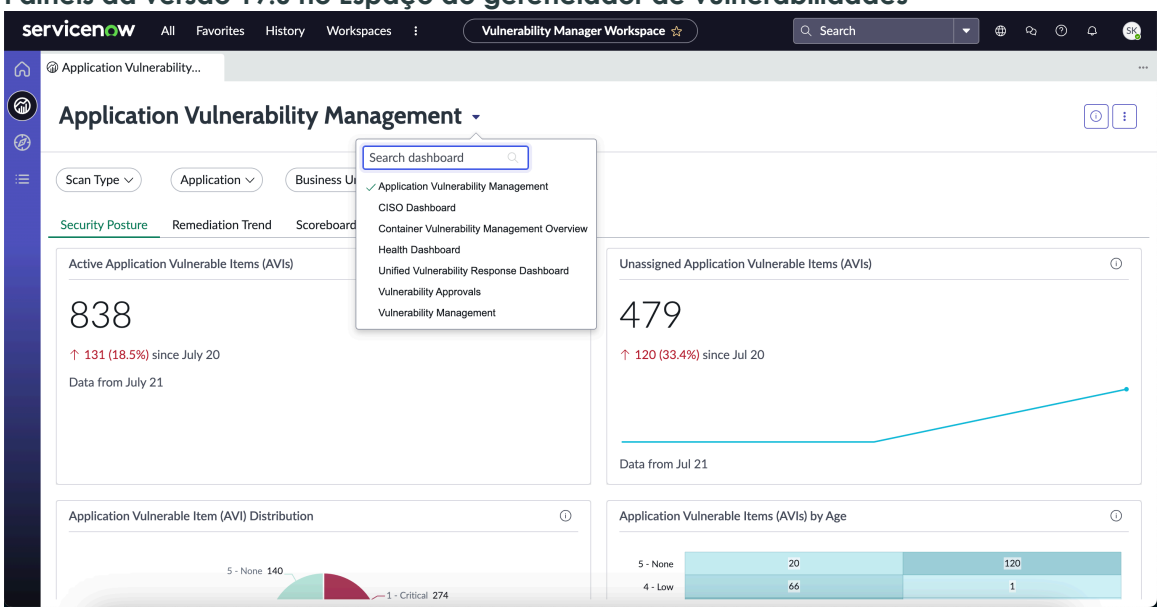
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painéis no Espaço do gerenciador de vulnerabilidades

Painel	Descrição
	obter mais informações, consulte Painel do Contêiner de Resposta a vulnerabilidades.
Painel de gestão de vulnerabilidades de aplicações	Rastreie o volume, o desempenho e o andamento das vulnerabilidades da aplicação desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consulte Gestão de vulnerabilidades de aplicações Painel do (PA).
Painel da Resposta a vulnerabilidades unificado	Fornece visibilidade de vários scanners de vulnerabilidade e ferramentas de segurança para fornecer uma exibição abrangente das vulnerabilidades e riscos de uma organização. Para obter mais informações, consulte Soluções de análise e emissão de relatórios para o Painel unificado da Resposta a vulnerabilidades.
Painel de integridade da Resposta a vulnerabilidades	Exibe a pontuação de integridade geral da aplicação Resposta a vulnerabilidades. Para obter mais informações, consulte Painel de Integridade da Resposta a vulnerabilidades do SecOps.

A imagem a seguir mostra a página Painéis no Vulnerability Manager Workspace.

Painéis da versão 19.0 no Espaço do gerenciador de vulnerabilidades



Você também pode criar um painel personalizado selecionando o ícone ⋮ e selecionando **Criar novo painel**.

Visão geral de listas

A exibição de lista no espaço do Gerenciador de vulnerabilidades permite que os gerentes e analistas de vulnerabilidade e segurança exibam o andamento da correção nos registros,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

analisem os registros da Resposta a vulnerabilidades e exibam o status de suas solicitações de aprovação e exceções.

Essas listas e links fornecem acesso fácil a registros e tarefas. Ele contém duas guias:

- Guia**Listas** : exibe as listas padrão para esforços de correção, tarefas de correção, itens vulneráveis, soluções, exceções e resultados de testes de configuração.
- Guia**Minhas listas** : exibe todas as listas que você renomeou na guia Lista e todas as listas que você cria.

  Você também pode criar sua própria lista para monitorar o andamento da correção. Para obter mais informações, consulte Criar uma lista personalizada de registros.

Guia Listas

As seguintes listas são exibidas:

- Esforços de correção (REs) - Mostra os REs ativos e todos os REs atribuídos aos seus grupos.
- Tarefas de correção (VULs) - Mostra as Tarefas de correção ativas e todas as Tarefas de correção atribuídas aos seus grupos.

  Nota: A partir da versão 18.0, a lista de tarefas de correção mostra as tarefas de correção criadas na IU clássica e no espaço de trabalho para Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicações, Contêiner de Resposta a vulnerabilidadese Conformidade de configurações.

- Itens vulneráveis de host - Mostra os itens vulneráveis (VIs) de host ativos e todos os IVs de host do módulo de vulnerabilidades de host.
- Itens vulneráveis da aplicação - Mostra os itens vulneráveis da aplicação (AVITs) ativos e todos os AVITs do módulo Vulnerabilidades da aplicação.
- Itens vulneráveis de contêiner - Mostra os itens vulneráveis de contêiner ativos (CVITs) e todos os CVITs do módulo Vulnerabilidades de contêiner.
- Resultados de testes de configuração - Mostra os resultados de testes de configuração ativos e todos os resultados de testes de configuração do módulo Resultados de testes de configuração.

  Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

  Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

- Soluções - Mostra todas as soluções para itens vulneráveis.
- Exceções - mostra estados de aprovação para todas as solicitações de falso-positivo e exceção de seus grupos.
- Aprovações - Mostra as solicitações de aprovação atribuídas a você para processamento. Para processar suas aprovações no espaço, consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Bibliotecas - Mostra as seguintes bibliotecas, políticas e testes.
  - CVEs - mostra todas as vulnerabilidades e exposições comuns (CVEs) de Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicaçõese Contêiner de Resposta a vulnerabilidades.
  - TPEs - Mostra todas as entradas de terceiros (TPEs) de Resposta a vulnerabilidades.
  - CWEs — Mostra todas as Enumerações de Pontos Fracos Comuns (CWEs) de Resposta a vulnerabilidades, Resposta a vulnerabilidades de aplicaçõese Contêiner de Resposta a vulnerabilidades.
  - Vulnerabilidades da aplicação - Mostra todas as entradas de vulnerabilidade da aplicação de terceiros.
  - Grupos de teste - Mostra todos os Conformidade de configurações grupos de teste. Você pode exibir a porcentagem de conformidade de IC e a conformidade dos resultados de testes de um grupo de teste na exibição de registro.
  - Testes - Mostra todos os testes de Conformidade de configurações. Você pode exibir a porcentagem de conformidade dos resultados de testes de um teste na exibição de registro.
  - Controles de remuneração - mostra todos os controles de remuneração que podem ser usados para solicitações de redução de risco. Você pode adicionar um controle de remuneração clicando em **Novo**. Para obter mais informações sobre como adicionar um controle de remuneração, consulte Adicionar um controle de compensação à biblioteca.

> **Nota:** A lista Controles remuneratórios aparece a partir da v20.0 de Resposta a vulnerabilidades.

Informações relacionadas

Use a exibição de lista no espaço do gerenciador de vulnerabilidades

Visão geral da edição em massa

No Vulnerability Manager Workspace, o recurso de edição em massa permite que você atualize vários itens vulneráveis simultaneamente (VITs, AVITs, CVITs ou TRs), simplificando o processo de gestão e correção.

Com a edição em massa, você pode selecionar várias vulnerabilidades e aplicar mudanças consistentes, como atribuir proprietários de correção, atualizar status, adicionar anotações de trabalho, solicitar exceções e solicitar falso-positivo. Isso economiza tempo e esforço, eliminando a necessidade de editar itens vulneráveis individualmente, proporcionando um gerenciamento eficiente e consistente de vulnerabilidades.

O recurso de edição em massa está disponível para:

- itens vulneráveis de host (VITs) a partir de v21.0 de Resposta a vulnerabilidades.
- itens vulneráveis de aplicação (AVITs) e itens vulneráveis de contêiner (CVITs) a partir da v22.0 de Resposta a vulnerabilidades.
- resultados de testes (TRs) a partir da v23.0 de Resposta a vulnerabilidades.

Você pode executar as seguintes tarefas usando o recurso de edição em massa no Vulnerability Manager Workspace:

- Atribuir registros a um grupo de atribuição em massa
- Solicitar exceção em massa no Espaço do gerenciador de vulnerabilidades
- Remover atribuições de itens vulneráveis de host em massa

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Edição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades
- Fechar registros em massa no Vulnerability Manager Workspace

Noções básicas sobre controles de remuneração para redução de risco

Controles de compensação são as medidas tomadas para reduzir o risco representado por vulnerabilidades que não podem ser corrigidas imediatamente. Eles podem ser usados para reduzir a probabilidade ou o impacto de uma exploração bem-sucedida.

Nota: O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

A aplicação de controles de compensação pode ajudar a reduzir o risco de uma vulnerabilidade.

A tabela a seguir mostra os casos de uso para controles de compensação:

Casos de uso para controles de compensação

Caso de uso	Controle de remuneração
Uma vulnerabilidade em um servidor Web que permite que invasores executem código arbitrário.	Implemente um WAF (Web application firewall, firewall da aplicação web) para bloquear solicitações mal-intencionadas para o servidor web.
Uma vulnerabilidade em um sistema operacional que permite que invasores escalem privilégios para raiz.	Implemente um controle de aplicação para restringir a execução de aplicações no sistema host.
Uma vulnerabilidade em um servidor de banco de dados que permite que invasores acessem dados confidenciais.	Implemente a segmentação de rede para isolar o servidor de banco de dados de outros hosts e sistemas críticos.

Para obter mais informações sobre o impacto dos controles de compensação na pontuação de risco de um item vulnerável e na tarefa de correção, consulte Impacto dos controles de remuneração na pontuação de risco e na data de vencimento.

Informações relacionadas

- Adicionar um controle de compensação à biblioteca
- Associar controles de remuneração a CVEs ou TPEs para solicitações de redução de risco
- Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Soluções de análise e emissão de relatórios para o Painel unificado da Resposta a vulnerabilidades

O Painel unificado da Resposta a vulnerabilidades é um painel agregado centralizado que fornece visibilidade de vários scanners de vulnerabilidade e ferramentas de segurança para fornecer uma exibição abrangente das vulnerabilidades e riscos de uma organização.

Funções necessárias

As funções e tarefas a seguir estão associadas a esta Solução. Eles são necessários para exibir e compartilhar os relatórios:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Informações relacionadas

Soluções de análise e relatório

Painel da Resposta a vulnerabilidades unificado

O painel da Resposta unificada a vulnerabilidades fornece uma exibição abrangente das vulnerabilidades e riscos de uma organização. As vulnerabilidades relacionadas à infraestrutura, nuvem, aplicações e contêineres podem ser visualizadas em um painel centralizado para melhor visibilidade e correção.

Funções necessárias de Now Platform

As funções a seguir estão associadas a esta solução. Eles são necessários para exibir, editar e compartilhar os relatórios:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

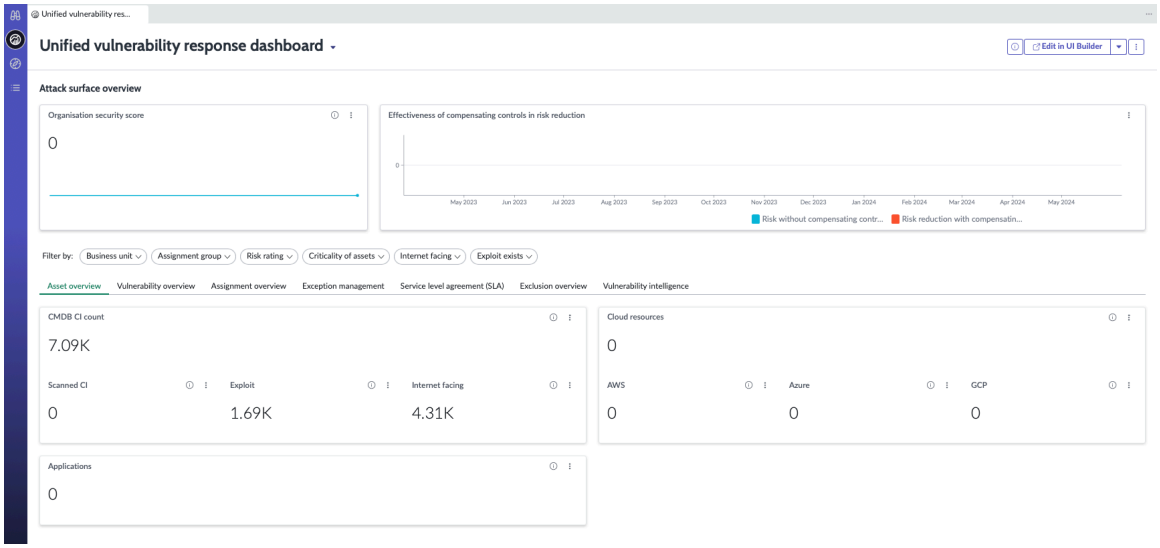
Acessar o painel da Resposta unificada a vulnerabilidades

Para abrir o painel, navegue até:

- **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades** e selecione o ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir o Painel da Resposta a vulnerabilidades unificada, selecione a lista suspensa ao lado do nome do painel.
- **Espaços** > **Espaço de Análise da plataforma** > **Painéis** > **Painel da Resposta a vulnerabilidades unificado**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
• Gerenciadores de vulnerabilidades • Analistas de vulnerabilidade	• Fornece visibilidade em tempo real dos riscos presentes na infraestrutura, aplicações, configurações e contêineres. Permite que os gerentes de vulnerabilidade e os analistas de vulnerabilidade priorizem e corrijam as vulnerabilidades em tempo hábil. • Fornece uma visão geral da superfície de ataque de ativos críticos, que pode ser usada para rastrear o andamento e os esforços de correção. • Fornece uma visão geral dos riscos em unidades de negócios (BUs). Você pode usar filtros para selecionar BUs e comparar o andamento para realocar recursos, conforme necessário. O acesso no nível da função deve ser fornecido ao chefe da UN. • Fornece visibilidade sobre o possível impacto por BUs. Você pode usar o filtro Vulnerabilidade e exposição comum (CVE) para identificar exposições em toda a organização. • Fornece visibilidade sobre as pontuações de EPSS obtidas por entradas vulneráveis que existem no catálogo CISA KEV para itens vulneráveis de aplicação, host e contêiner.

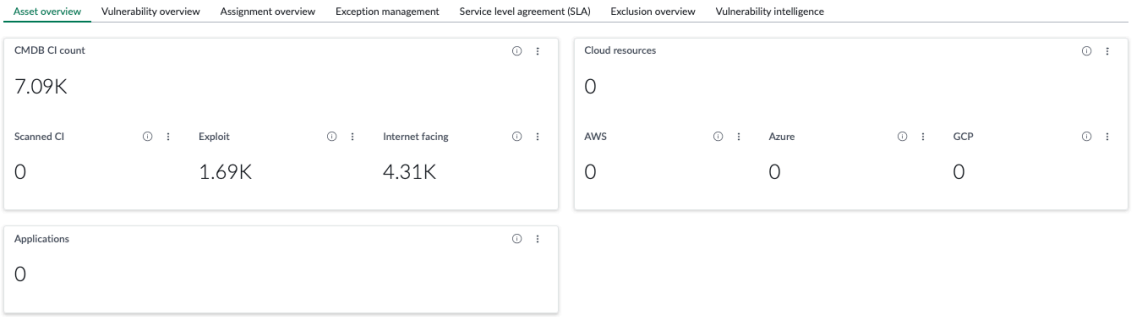
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias do Painel da Resposta unificada a vulnerabilidades

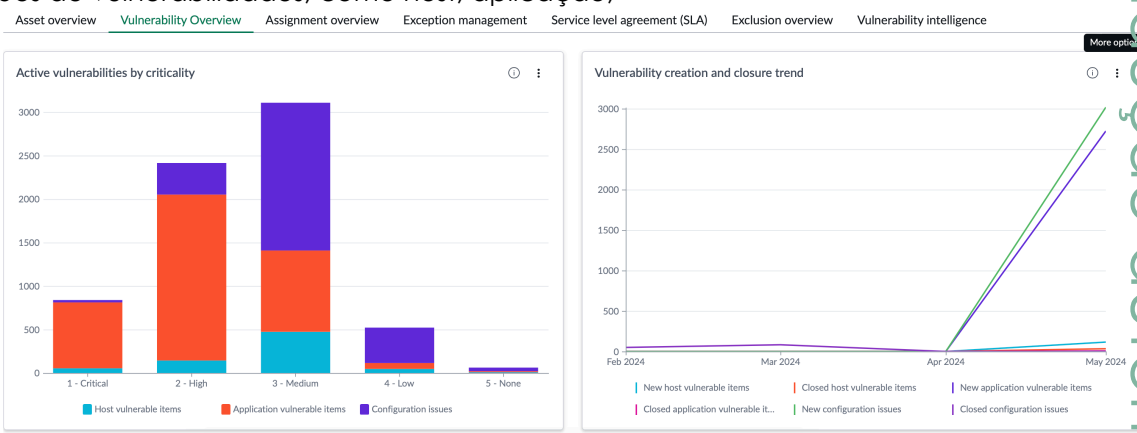
Este painel permite que você veja as vulnerabilidades ou problemas que estão presentes em hosts, nuvem, configurações, aplicações e contêineres. Você pode exibir as vulnerabilidades com base na unidade de negócios, grupo de atribuição, classificação de risco, criticidade e se existe uma exploração para as vulnerabilidades.

A guia **Visão geral** do ativo fornece o status geral dos itens de configuração (ICs) no



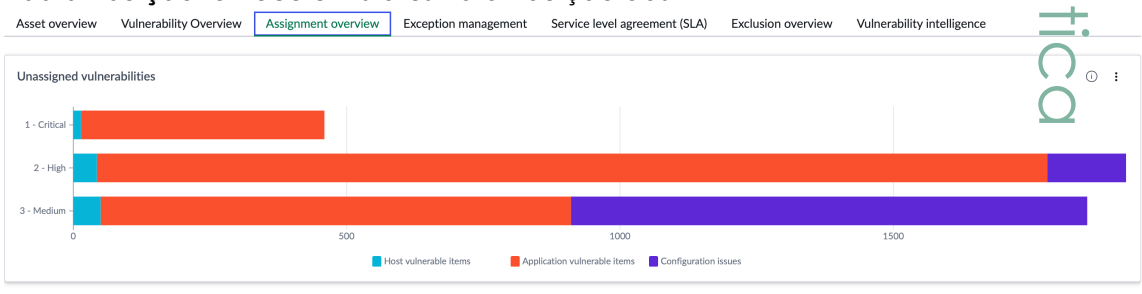
sistema.

A guia **Visão geral da vulnerabilidade** fornece um status sobre os tipos de vulnerabilidades, como host, aplicação,



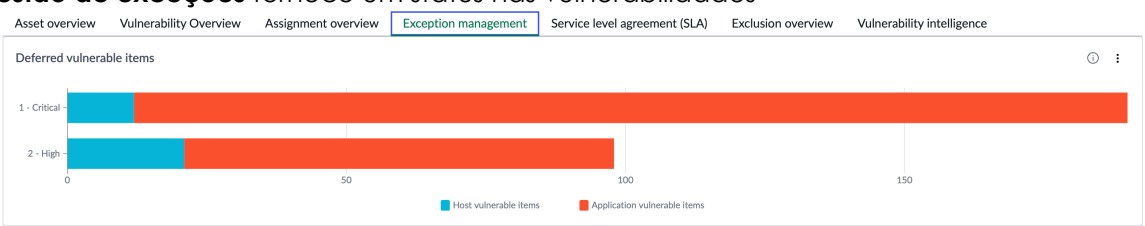
contêiner.

A guia **Visão geral da atribuição** fornece um status na atribuição das



vulnerabilidades.

A guia **Gestão de exceções** fornece um status nas vulnerabilidades



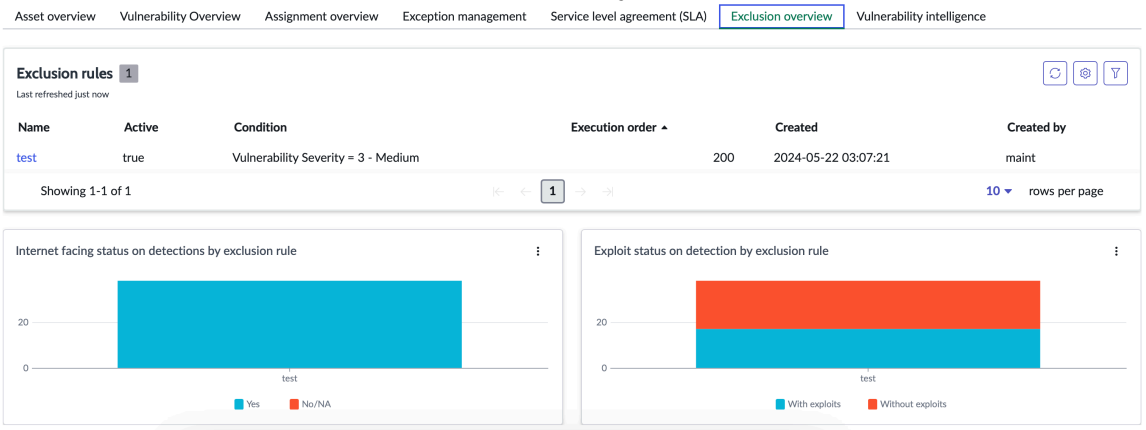
adiadas.

Tradução automática

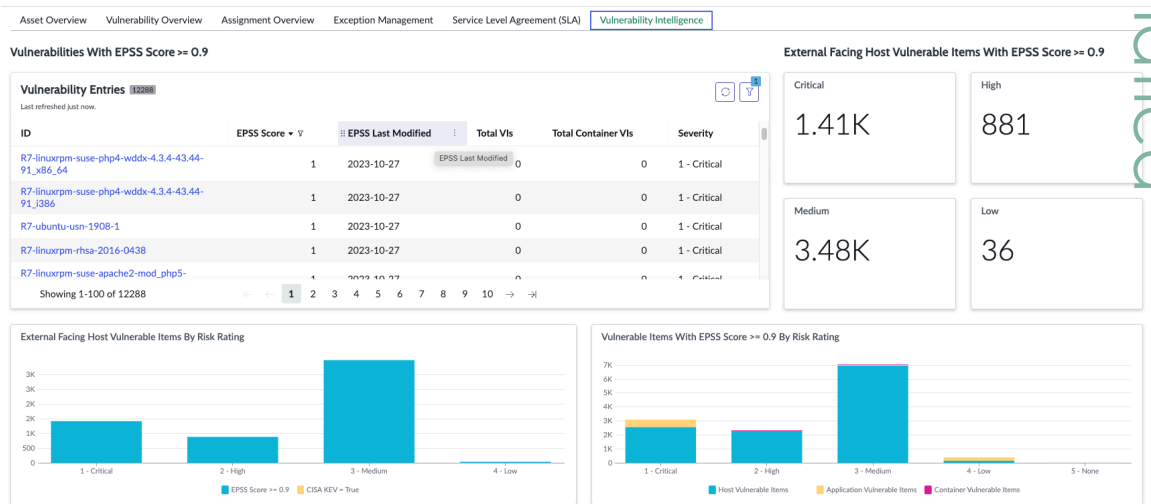
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia **Acordo de nível de serviço (ANS)** fornece um status no acordo de nível de serviço atingido por diferentes grupos de atribuição.

A guia **Visão geral da exclusão** fornece um status das regras de exclusão que você criou, bem como as que afetam as detecções que são voltadas para a Internet e têm explorações disponíveis.



A guia **Inteligência de vulnerabilidade** fornece um status nas pontuações de EPSS obtidas por vulnerabilidades com o sinalizador CISA KEV verdadeiro e Pontuação de EPSS >= 0,9 para itens vulneráveis de aplicação, host e contêiner.



Filtros

Você pode filtrar os widgets com base no seguinte:

- Unidade de negócios
- Grupo de atribuição

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pontuação de risco
- Criticidade de ativos
- Voltado para a internet
- Explorar itens existentes

Quando um filtro é selecionado, os dados em todos os widgets são atualizados. No entanto, se um filtro não for aplicável a um widget, um símbolo de cruz será mostrado ao lado do nome do filtro.

Nota: Somente filtros de Unidade de negócios e Grupo de atribuição estão disponíveis em Tokyo. Todos os filtros estão disponíveis de Utah em diante.

Indicadores

Ativos verificados

Indicador de fórmula para ativos verificados nos últimos 60 dias. Contém ativos de item descoberto verificados, ativos de versão da aplicação verificados, ativos de imagem de contêiner descobertos verificados como indicadores de contribuição.

Ativos - Existe exploração

Indicador de fórmula para ativos em que há exploração nas vulnerabilidades. Contém Ativos de host - Existe exploração, Ativos de aplicação - Existe exploração, Ativos de contêiner - Existe exploração como indicadores de contribuição.

Ativo de infraestrutura – Voltado para a internet

Indicador para buscar a contagem de ativos voltados para a internet.

Itens descobertos com base no tipo de recurso de nuvem

Indicador para buscar a contagem de ativos com uma categoria de ativo, como nuvem.

Imagens base

Indicador para buscar a contagem de imagens de base.

Tipo de ativo de KEVs de CISA

Indicador de fórmula, que fornece a contagem de itens vulneráveis de contêiner e host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro. Contém CISA existe CVR e CISA existe itens de vulnerabilidade como indicadores de contribuição.

Itens vulneráveis existentes de CISA - não atribuídos

Indicador de fórmula, que fornece a contagem de itens vulneráveis de contêiner e host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro e os itens vulneráveis não estão atribuídos. Contém itens de vulnerabilidade de contêiner não atribuídos e item de vulnerabilidade de host não atribuído como indicadores de contribuição.

Existem Itens Vulneráveis CISA – Meta não Atingida

Indicador de fórmula, que fornece a contagem de itens vulneráveis de contêiner e host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro e os itens vulneráveis não atingiram o destino. Contém Itens de vulnerabilidade CISA e CVR existem como indicadores de contribuição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

VITs de host ativo

Contagem de itens vulneráveis de host (VITs) ativos.

VITs da aplicação ativos

Contagem de itens vulneráveis de aplicação ativos (AVITs).

VITs de contêiner ativo

Contagem de itens vulneráveis de contêiner ativos (CVITs).

Novos VITs

Contagem de VITs abertos em um dia.

Novos AVITs

Contagem de AVITs abertos em um dia.

Novos CVITs

Contagem de CVITs abertos em um dia.

Novos Resultados de testes

Contagem de resultados de testes (TRs) que foram criados em um dia.

AVITs encerrados

Contagem de VITs encerrados em um dia.

VITs encerrados

Contagem de AVITs encerrados em um dia.

CVITs encerrados

Contagem de CVITs encerrados em um dia.

Resultados de testes fechados

Contagem de TRs encerrados em um dia.

Problemas de configuração em aberto – Resultados de testes

Contagem de todos os resultados de testes abertos, que estão em estado de falha.

Pontuação de risco da organização

Pontuação de risco de uma organização da tabela de pontuação de risco da aplicação de acúmulo.

Itens vulneráveis de aplicação não atribuídos

AVITs sem grupo de atribuição ou atribuídos a.

Item Vulnerável de Host Não Atribuído

VITs sem grupo de atribuição ou atribuídos a.

Itens vulneráveis de contêiner não atribuídos

CVITs sem grupo de atribuição ou atribuídos a.

Problemas de configuração não atribuídos

TRs sem grupo de atribuição ou atribuídos a.

VITs adiados

VITs no estado adiado.

AVITs adiados

AVITs no estado adiado.

CVITs adiados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

CVITs no estado adiado.

ANS de host – Encerrado

Idade média encerrada de VITs encerrados.

ANS de aplicação – Encerrado

Idade média encerrada de AVITs encerrados.

ANS de contêiner – Encerrado

Idade média de encerramento de CVITs encerrados.

ANS de Resultado de testes – Aprovado

Idade média de encerramento de TRs aprovados.

ANS de host – Encerrado (crítico e alto)

Idade média de encerramento de VITs críticos e altos encerrados.

ANS de aplicação – Encerrado (crítico e alto)

Idade média de encerramento de AVITs críticos e altos.

ANS de contêiner – Encerrado (crítico e alto)

Idade média de encerramento de CVITs críticos e altos encerrados.

ANS do resultado de testes – Aprovado (crítico e alto)

Idade média de encerramento de TRs críticos e altos aprovados.

MTTR agregado

Idade média de encerramento de VITs, AVITs, CVITs e TRs.

ANS não Atingido

Idade média de encerramento de VITs, AVITs, CVITs e TRs encerrados e com meta não atingida.

Vulnerabilidades com pontuações de EPSS >= 0,9

Contagem de entradas de vulnerabilidade com pontuações de EPSS maiores ou iguais a 0,9.

Detalhamentos

- Tipo de VIT (unificado)
- Voltado para a internet (unificado)
- Classificação de risco (unificada)
- Existe exploração (unificada)
- Tipo de recurso de nuvem do item descoberto (unificado)
- Existe CISA (unificado)
- Classe do CMDB (unificada)
- Unidade de negócios (unificada)
- Essencial para os negócios (unificado)
- Motivo adiado (unificado)
- Grupo de atribuição (unificado)
- Status de correção (unificado)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Guia Visão geral do ativo

Título	Tipo	Descrição
Visão geral da superfície de ataque	Pontuação única	Número que representa a pontuação agregada da segurança de uma organização.
Contagem de IC do CMDB	Pontuação única	Número de ICs na organização que estão registrados e rastreados no Configuration Management Database (CMDB). Fornece um detalhamento dos seguintes ICs: • ICs verificados: número de ICs verificados • Exploração: número de explorações disponíveis • Voltados para a Internet: número de ICs voltados para a Internet
Recurso de Nuvem	Pontuação única	Número de ICs com categoria de ativo, como nuvem. Fornece um detalhamento dos seguintes ativos de nuvem: • AWS • Azure • GCP
Imagem do Docker	Pontuação única	Número de imagens do Docker, incluindo o número de imagens de base.

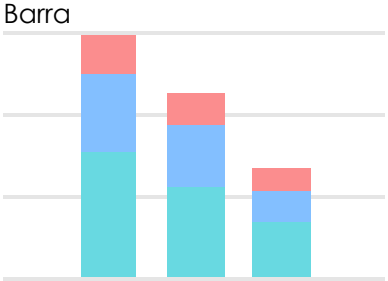
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral do ativo

Título	Tipo	Descrição
Aplicações	Pontuação única	Número de aplicações na organização.

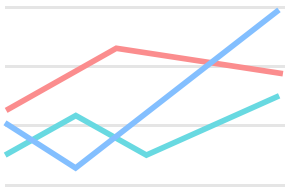
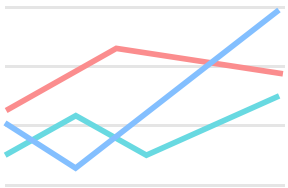
Guia Visão geral da vulnerabilidade

Título	Tipo	Descrição
KEVs de CISA	Gráfico de Pizza	Número de vulnerabilidades associadas ao catálogo CISA e ao sinalizador CISA como verdadeiro. Fornece um detalhamento com base no seguinte: • Vulnerabilidade CISA: tipos de vulnerabilidades com sinalizador CISA como verdadeiro • ICs do host - Voltados para a Internet: ICs voltados para a Internet • VITs não atribuídos: VITs não atribuídos com sinalizador CISA como verdadeiro • VITs não atingiram o objetivo: VITs que não atingiram o objetivo com o sinalizador CISA como verdadeiro
Vulnerabilidades ativas por criticidade	Barra 	Número de VITs, AVITs e CVITs ativos com base na criticidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

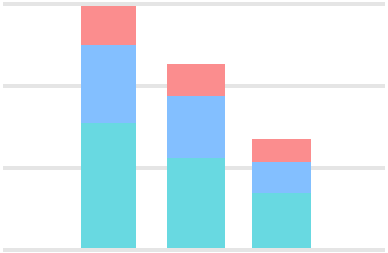
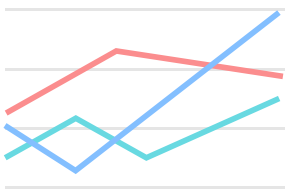
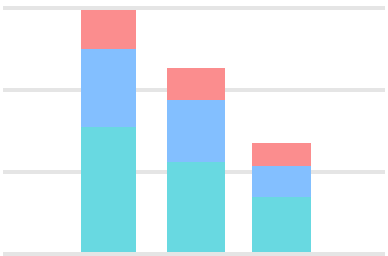
Guia Visão geral da vulnerabilidade

Título	Tipo	Descrição
Tendência de criação e fechamento de vulnerabilidade	Linha 	Número de vulnerabilidades novas e encerradas para todas as aplicações. Fornece uma tendência dos últimos três meses.
Configuração incorreta por plataforma de nuvem	Linha 	Número de problemas de configuração com base na classificação de risco de cada ativo em nuvem.
Conformidade de nuvem	Tabela	Lista de recursos com a categoria de ativo como nuvem junto com os seguintes detalhes: • Nome do recurso • Classe • Problemas de vulnerabilidade: número de problemas presentes no recurso que são agregados com base na classificação de risco. • Problemas de configuração: número de recursos com problemas de configuração junto com a classificação de risco. • Conta em nuvem: ID da conta em nuvem. • Região da nuvem: local dos recursos de nuvem. • Provedor de nuvem: nome do provedor de nuvem.

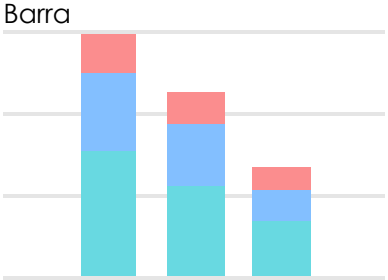
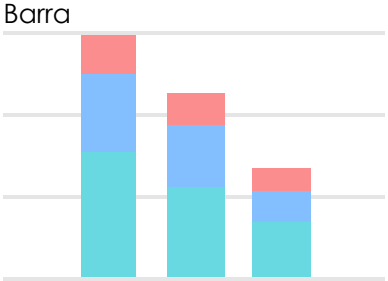
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da atribuição

Título	Tipo	Descrição
VITs não atribuídos	Barra 	Número de vulnerabilidades que não estão atribuídas a nenhum grupo ou indivíduo junto com a classificação de risco.
MTTR por grupo de atribuição – 10 principais	Linha 	Tempo médio gasto por um grupo de atribuição para identificar e corrigir vulnerabilidades ou problemas de segurança. São exibidos os 10 principais grupos de atribuição que têm o maior tempo médio de correção.
10 principais grupos de atribuição sem ANS (vulnerabilidade crítica e alta)	Barra 	10 principais grupos de atribuição que não cumpriram a data prevista de correção de vulnerabilidades críticas e altas.

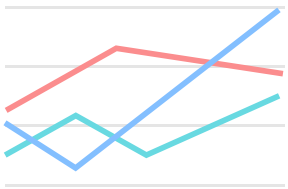
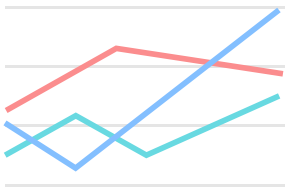
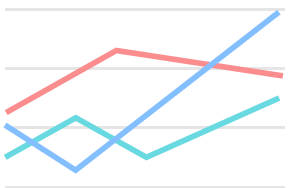
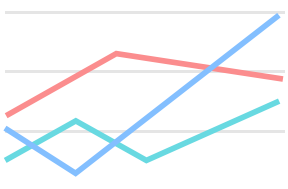
Guia Gestão de exceções

Título	Tipo	Descrição
VITs adiados	Barra 	Número de vulnerabilidades no estado adiado com base na classificação de risco.
VITs críticos e altos adiados por grupo de atribuição	Barra 	Número de vulnerabilidades com classificações de risco crítico e alto no estado adiado que é categorizado com base nos grupos de atribuição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Acordo de nível de serviço (ANS)

Título	Tipo	Descrição
Vulnerabilidade do host: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades do host. Fornece uma tendência dos últimos 10 meses.
Problemas de conformidade: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir problemas de conformidade. Fornece uma tendência dos últimos 10 meses.
Vulnerabilidade da aplicação: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades da aplicação. Fornece uma tendência dos últimos 10 meses.
Vulnerabilidade da contêiner: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades de contêiner. Fornece uma tendência dos últimos 10 meses.

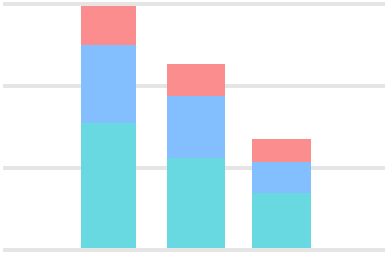
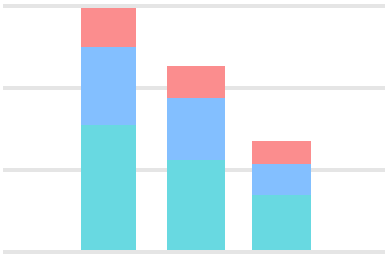
Guia Visão geral da exclusão

Título	Tipo	Descrição
Regras de exclusão	Tabela	Lista de todas as regras de exclusão que você criou.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da exclusão

Título	Tipo	Descrição
Regras de exclusão v/s Voltado para a Internet	Barra 	Regras de exclusão que afetam as detecções que pertencem a ativos voltados para a Internet.
Regras de exclusão v/s Exploração existe	Barra 	Regras de exclusão que afetam as detecções vulneráveis a explorações existentes.

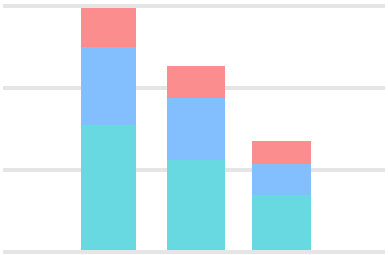
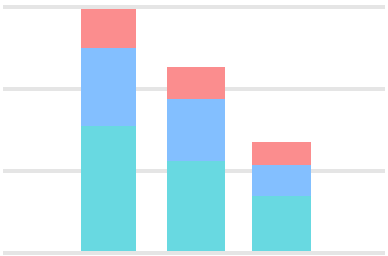
Guia Inteligência para vulnerabilidades

Título	Tipo	Descrição
Vulnerabilidades com Pontuação EPSS>= 0,9	Tabela	Exibição de lista completa de todas as entradas vulneráveis (CVEs ou TPEs) que têm uma pontuação EPSS maior ou igual a 0,9 junto com os seguintes detalhes. • ID: ID de CVE da vulnerabilidade • Pontuação de EPSS • Última modificação de EPSS • CISA KEV BOD 22-01: indica se a entrada existe no CISA KEV BOD (diretriz operacional de vinculação 22-01) • Total de IVs: contagem total de IVs existentes para esta entrada de vulnerabilidade. • Total de VIs de contêiner: contagem total de VIs de contêiner existentes

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Inteligência para vulnerabilidades

Título	Tipo	Descrição
		para esta entrada de vulnerabilidade. • Gravidade
Itens vulneráveis do host externo com pontuação EPSS >= 0,9	Pontuação única	Número que indica a contagem agregada de itens vulneráveis de host voltados externamente com uma pontuação de EPSS maior ou igual a 0,9. Fornece pontuações únicas classificadas por severidade da classificação de risco.
Itens vulneráveis de host voltados externamente por avaliação de risco	Barra 	Número de itens vulneráveis de host voltados externamente por classificação de risco. As barras de pilha são categorizadas por Pontuação EPSS >=0,9 e CISA KEV = Verdadeiro.
Itens vulneráveis com pontuação de EPSS >= 0,9 por avaliação de risco	Barra 	Número de vulnerabilidades com pontuação EPSS maior ou igual a 0,9 classificadas por classificação de risco. Fornece um detalhamento por itens vulneráveis de host, itens vulneráveis de aplicação e itens vulneráveis de contêiner.

Trabalhos agendados para coleta de dados

Os trabalhos de coleta de dados coletam pontuações automaticamente para detalhamentos e indicadores automatizados. Os seguintes trabalhos agendados são executados para coletar pontuações em novos dados automaticamente.

⚠ **Aviso:** Por padrão, os seguintes trabalhos de coleta de dados são desativados no sistema de base:

- Coleta diária de dados do painel unificado
- Coleta de dados semanais do painel unificado
- Coleta de dados históricos do painel unificado

Antes de habilitar os trabalhos, consulte a base de conhecimento .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho agendado	Frequência	Descrição
Coleta de dados históricos do painel unificado	Uma vez	Coleta pontuações e snapshots de registros existentes.
Coleta de dados semanais do painel unificado	Semanalmente	Coleta dados semanalmente.
Coleta diária de dados do painel unificado	Diariamente	Coleta dados todos os dias.
Acumular pontuações de risco para a organização	Diariamente	Coleta a pontuação de risco agregada de uma organização.
Preencher contagens diárias de conformidade em nuvem	Diariamente	Coleta dados para conformidade na nuvem.
Trabalho diário de EPSS	Diariamente	Coleta dados de EPSS do First.org.

Uma nova tabela de pontuação de risco da aplicação de acúmulo [sn_vul_cmn_rollup_app_risk_score] é criada no escopo comum de vulnerabilidade. Esta tabela é preenchida usando as seguintes calculadoras de acúmulo por meio dos trabalhos agendados todos os dias.

Nome da calculadora de acúmulo	Descrição
Acúmulo de pontuação de risco da organização	Acumula as pontuações de risco de todos os itens vulneráveis e problemas de configuração em uma organização. Ele fornece uma pontuação de risco geral para uma organização.
Acúmulo do item vulnerável	Acumula as pontuações de risco de todos os itens vulneráveis em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo de item vulnerável da aplicação	Acumula as pontuações de risco de todos os itens vulneráveis da aplicação em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo do item vulnerável de contêiner	Acumula as pontuações de risco de todos os itens vulneráveis de contêiner em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo do resultado de testes	Acumula as pontuações de risco de todos os resultados de testes em uma organização para contribuir com a pontuação de risco geral de uma organização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da calculadora de acúmulo	Descrição
Acumular pontuações de EPSS de NVDs para TPEs	Acumula pontuações de EPSS de NVDs para TPEs, para contribuir com a pontuação de risco geral de uma organização.

Monitorar e gerenciar itens vulneráveis e resultados de testes no Vulnerability Manager Workspace

O Vulnerability Manager Workspace permite monitorar itens vulneráveis (VITs, AVITs e CVITs) e Resultados de testes usando tópicos de observação e rastrear e gerenciar o andamento de correção criando esforços de correção.

Criar e aplicar filtros para visualizar o resumo dos registros ativos

Como gerente e analista de vulnerabilidades, você pode filtrar registros para visualizar seu resumo no Vulnerability Manager Workspace.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Página inicial**.
2. Na página inicial, selecione o ícone de ícone de engrenagem em qualquer uma das guias Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação ou Resultados de testes de configuração.
3. No modal Filtros salvos, preencha os campos.

Modal de filtros salvos

Campo	Descrição
Nome do filtro	Nome do filtro
Condições	Condição para listar os registros cujas visualizações você deseja ver.

4. Selecione **Salvar**.
   O filtro criado aparece no menu suspenso **Exibir por**.
5. Selecione o filtro criado no campo **Exibir por** para exibir as visualizações dos registros filtrados.
   Para obter mais informações sobre os widgets, consulte Visão geral da página inicial.
6. Para atualizar ou excluir um filtro:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Selecione o ícone de Ícone de engrenagem .

b. No formulário Filtros salvos, selecione **Usar filtros existentes** e preencha os campos e selecione **Atualizar**.

Formulário Filtros salvos

Campo	Descrição
Selecionar filtro	Lista de filtros existentes.
Nome do filtro	Nome descritivo do filtro.
Condições	As condições do filtro existente. Edite a condição de um novo conjunto de registros.

c. Para excluir um filtro, selecione **Excluir**.

Usar tópicos de observação no Vulnerability Manager Workspace

Use tópicos de observação em Vulnerability Manager Workspace para exibir vulnerabilidades que são filtradas dos dados importados a partir dos critérios definidos por você. Use essas informações para determinar como as vulnerabilidades em cada tópico de observação podem afetar seu ambiente.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Nos tópicos de observação, você pode realizar as seguintes tarefas:

- Monitore o número de esforços de correção e os registros de itens vulneráveis para ver o andamento da correção de vulnerabilidades.
- Edite ou exclua os tópicos de observação existentes e crie tópicos.
- Crie os esforços de correção e entregue automaticamente as tarefas de correção para suas equipes de TI somente para as vulnerabilidades que você deseja corrigir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

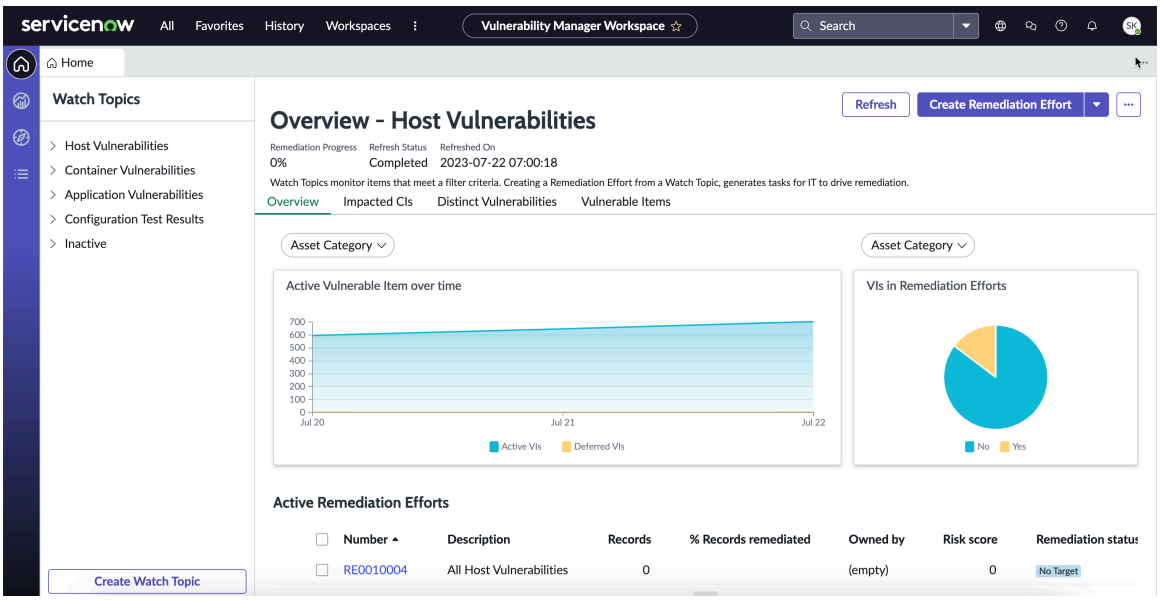
Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Selecione um tópico de observação.

   Quando você seleciona um tópico de observação, a guia **Visão geral** é exibida por padrão.

   Para obter mais informações sobre os tópicos de observação, consulte Visão geral dos tópicos de observação.

   ### Guia Visão geral da versão 19.0 na página inicial do Espaço do gerenciador de vulnerabilidades

   Os painéis são dinâmicos e os novos dados de vulnerabilidade são atualizados após a importação.

3. Selecione uma **guia Itens relacionados** para exibir mais dados.

   Para atualizações na lista de itens relacionados e visualizações em um tópico de observação a partir da versão 18.0, consulte Lista de itens relacionados e visualizações em um tópico de observação.

4. Execute as ações de IU na página Tópicos de observação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
Criar um tópico de observação	Crie seu próprio tópico de observação usando seu próprio conjunto de condições para as vulnerabilidades que você considera importantes. Para obter mais informações sobre como criar um tópico de observação, consulte Criar um tópico de observação no Espaço do gerenciador de vulnerabilidades.
Editar ou excluir um tópico de observação existente	Para obter mais informações sobre como editar ou excluir um tópico de observação, consulte Editar ou excluir um tópico de observação.
Desativar ou ativar um tópico de observação	A partir da versão 18.0, você pode desativar ou ativar um tópico de observação. Para obter mais informações sobre como desativar ou ativar um tópico de observação, consulteDesativar ou ativar um tópico de observação.
Atualizar um tópico de observação	A partir da versão 18.0, você pode adquirir os detalhes mais recentes de um tópico de observação selecionando o botão **Atualizar**. O status da atualização mais recente e o carimbo de data/hora são exibidos abaixo do nome do tópico de observação. ◦ Um tópico de observação é atualizado automaticamente quando é criado ou atualizado. ◦ Quando você atualiza um tópico de observação, todos os detalhes do tópico de observação, incluindo os gráficos e os esforços de correção, são atualizados. **Nota:** Como você não pode atualizar um tópico de observação inativo, o botão **Atualizar** está inativo para um tópico de observação inativo.
Criar um esforço de correção	◦ Crie um esforço de correção. Um esforço de correção contém as tarefas de correção atribuídas às suas equipes de TI. Você pode usar esta ferramenta para orientar e rastrear o andamento da correção da atribuição até a resolução. ◦ Quando você cria um esforço de correção, todos os itens vulneráveis ativos são extraídos automaticamente se ainda não fizerem parte de um esforço de correção

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	existente para esse tópico de observação. ◦ As tarefas de correção são atribuídas às equipes de TI automaticamente com base no grupo de atribuição de VI. ◦ Um exemplo de um esforço de correção do tópico de observação Vulnerabilidades nos servidores Windows pode ser Vulnerabilidades nos servidores Windows no segundo trimestre de 2021. As tarefas de correção neste esforço são atribuídas aos grupos de atribuição listados nos registros associados.
Criar um esforço recorrente	Crie esforços de correção recorrentes em uma programação que ajude a rastrear as vulnerabilidades que podem exigir sua atenção imediata e contínua. Para obter mais informações sobre a criação de esforço recorrente, consulte Criar um esforço de correção recorrente nos Espaços de resposta a vulnerabilidades. **Nota:** A partir da versão 18.0, você não pode criar um esforço recorrente para um tópico de observação inativo.
Refinar filtros para uma coluna em uma lista	Passe o mouse sobre o título de uma coluna e clique no menu de três pontos verticais para definir os filtros dessa coluna. Por exemplo, digamos que você queira filtrar mais os itens de configuração associados aos registros. Você pode selecionar a coluna Item de configuração para exibir as condições de filtro disponíveis. Você pode definir condições para filtrar seus ativos para que você veja somente os ativos que contêm os dados de PCI.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Filtrar itens ou corresponder itens de uma linha em uma coluna. Por exemplo, digamos que você queira exibir somente os registros que têm uma vulnerabilidade específica. Com a guia da lista de itens relacionados a Itens vulneráveis selecionada, na lista de registros, selecione a linha de um registro na coluna Resumo. Selecione o menu de três pontos verticais exibido e selecione uma das seguintes opções:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	◦ **Mostrar correspondência**: mostra todos os outros registros que têm esta vulnerabilidade. ◦ Remover do**filtro**: mostra todos os registros que não têm esta vulnerabilidade.

5. Opcional: Selecione um registro para exibir mais detalhes.

Criar um tópico de observação no Espaço do gerenciador de vulnerabilidades

Os gerentes e analistas de vulnerabilidade podem criar tópicos de observação usando um conjunto de condições para filtrar subconjuntos de itens vulneráveis que desejam monitorar.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Na guia Visão geral dos tópicos de observação, um relatório de tendências atualizado todas as noites, junto com outros relatórios, mostra o status atual dos registros desse tópico de observação.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
A página inicial (principal) é exibida com os tópicos de observação atuais.

2. Opcional: Como alternativa, à direita do botão Criar esforço de correção, clique nos três pontos e, em seguida, edite para modificar um tópico de observação existente.

Nota: Você pode notar um atraso antes que os dados atuais sejam exibidos para um tópico de observação depois de alterar a filtragem.

3. No canto inferior esquerdo da página, clique em **Criar tópico**de observação .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No modal exibido, preencha os campos.
   Para obter mais informações sobre os campos Criar modal de tópico de observação, consulteCampos de formulário Criar tópico de observação.
5. A partir da versão 18.0, você pode definir condições para a categoria de registro selecionada.

Opção no menu suspenso Categoria	Etapas
Vulnerabilidades do host	Na **Condição de item vulnerável**, defina condições para identificar as vulnerabilidades do host. As vulnerabilidades do host são detectadas com base nas condições definidas.
Vulnerabilidades de aplicação	Na **Condição de item vulnerável da aplicação**, defina condições para identificar as vulnerabilidades do host. As vulnerabilidades da aplicação (ou AVITs) são detectadas com base nas condições definidas.
Vulnerabilidades do contêiner	Na **Condição de item vulnerável de contêiner**, defina condições para identificar as vulnerabilidades do host. As vulnerabilidades do contêiner (CVITs) são detectadas com base nas condições definidas.
Resultados de testes de configuração	Na **Condição de resultados de testes de configuração**, defina condições para identificar os problemas de configuração. Os resultados de testes de configuração são detectados com base nas condições definidas.

Nota: Se você não definir nenhuma condição no tópico de observação, nenhum dado será extraído para o painel.

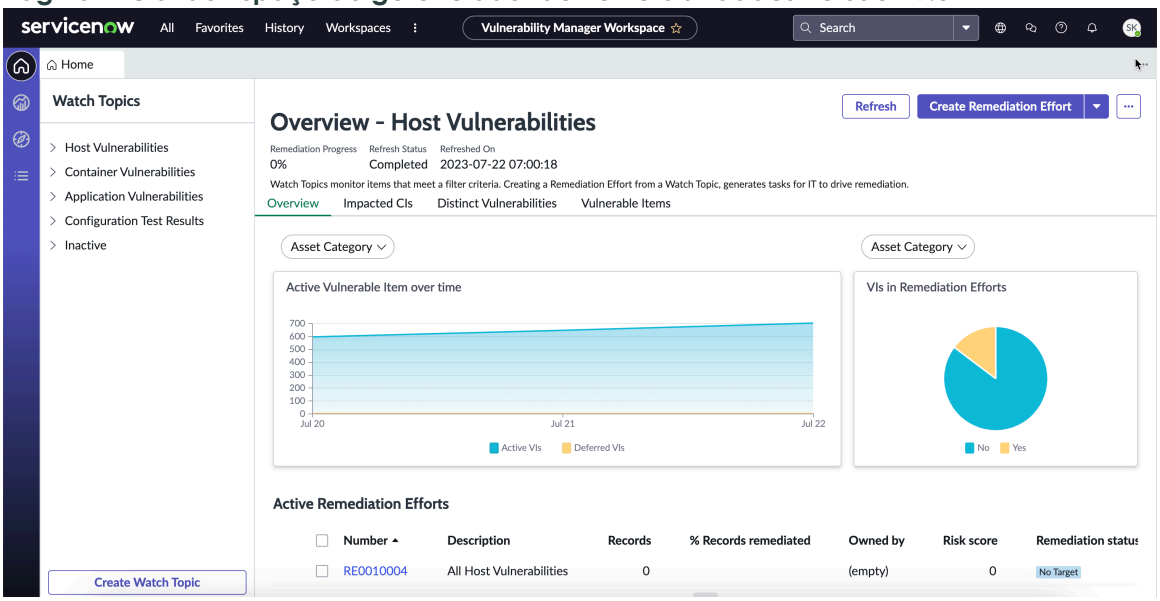
6. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seu novo tópico de observação é exibido na página inicial de. A partir da versão 18.0, os tópicos de observação são categorizados por tipo de registro no painel de navegação.

Página inicial do Espaço do gerenciador de vulnerabilidades versão 19.0



O que Fazer Depois

Crie um esforço de correção.

Editar ou excluir um tópico de observação

Como administrador ou analista de vulnerabilidades, você pode editar ou excluir um tópico de observação existente.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Se você editar um tópico de observação existente:

- Os dados no painel são atualizados para refletir suas mudanças.
- Os registros que estão atualmente nos Esforços de correção existentes permanecem inalterados.
- Os registros que não estão em Esforços de correção são exibidos com base nos critérios inseridos no construtor de condições.

Se você excluir um tópico de observação antes que todos os registros associados sejam corrigidos, os registros exibidos com esse tópico de observação não serão afetados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   A página inicial (principal) é exibida com os tópicos de observação atuais.
2. Abra o tópico de observação que você deseja editar.
3. Clique nos três pontos e clique em **Editar**.

   Nota: Você não pode editar um tópico de observação inativo.

4. No modal Editar tópico de observação, modifique os campos.
5. Clique em **Enviar**.

   Nota: Você pode notar um atraso antes que os dados atuais sejam exibidos para um tópico de observação depois de alterar a filtragem.

   Você também pode editar os esforços de correção recorrentes existentes. Se houver um esforço de correção recorrente para um tópico de observação, **Editar esforço recorrente** estará disponível no menu. Selecione esta opção para editar o esforço recorrente.

   As mudanças feitas e salvas no registro do esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

6. Opcional: Para excluir um tópico de observação, selecione o menu de três pontos no tópico de observação e selecione **Excluir**.

Desativar ou ativar um tópico de observação

A partir da versão 18.0, você pode desativar ou ativar um tópico de observação.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

- Todos os tópicos de observação inativos são exibidos no módulo **Inativo** no painel de navegação.
- Você não pode criar um esforço de correção ou um esforço de correção recorrente para um tópico de observação inativo.
- Você não pode atualizar um tópico de observação inativo.
- Os detalhes de um tópico de observação inativo e os esforços de correção associados não são atualizados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   A página inicial (principal) é exibida com os tópicos de observação atuais.
2. Abra o tópico de observação que você deseja desativar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique nos três pontos e clique em **Desativar**.
   O tópico de observação aparece no módulo Inativo.
4. Para ativar um tópico de observação, selecione um tópico de observação no módulo Inativo, selecione o menu de três pontos e selecione **Ativar**.
   O tópico de observação ativado é movido para o módulo apropriado no painel de navegação.

Usar registros de esforço de correção

Quando os gerentes de vulnerabilidade e analistas criam esforços de correção (REs), as Tarefas de correção (VUL) são atribuídas automaticamente às equipes de TI para correção.

Antes de Iniciar

Você precisa criar um esforço de correção antes de usá-lo para monitorar o andamento da correção nas Tarefas de correção.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Procedimento

1. Se não estiver selecionado, no canto superior esquerdo, clique no ícone Lista.

   A exibição de lista com registros de Esforço de correção ativos é exibida.

2. Na página principal de exibição de lista, com Esforços de correção ativos selecionados nas listas filtradas, clique em um registro para abri-lo.
   O registro é exibido. Você pode exibir as tarefas de correção e registros que estão associados ao esforço de correção selecionado.
3. Consulte a tabela a seguir para ver as ações que você pode executar no registro de esforço de correção.

   Depois de criar um registro, pode levar alguns minutos para que as tarefas de correção e um grande número de registros sejam exibidos.

Ação de IU	Descrição
Adicionar um marcador	À direita do cabeçalho, clique no pequeno ícone de marcador. Você pode adicionar um texto que ajude a identificar este registro. Por exemplo, você pode adicionar um marcador informando que este registro tem PCI ou outros dados críticos.
Adicionar uma anotação de trabalho ao registro	Na extrema direita da tela, clique no ícone **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
Atualizar o registro	Na guia **Detalhes**, para todos os campos editáveis, clique em um campo para selecioná-lo, faça as mudanças e clique em **Salvar** para atualizar o registro.
Quando exibido, clique no ícone de filtro para refinar os dados na página exibida	Com qualquer uma das guias Tarefas de correção, Itens vulneráveis our Resultados de testes de configuração selecionadas, à extrema direita, clique no ícone de filtro para mostrar os filtros que se aplicam à guia. No painel exibido, clique **em Exibição avançada** para adicionar ou alterar as condições de filtro dos itens na página. Clique em **Atualizar** para salvar suas mudanças. Por exemplo, na guia **Itens vulneráveis**, talvez você prefira adicionar o campo Idade e inserir um intervalo para exibir somente registros de um período específico. Os registros que correspondem às condições definidas são exibidos na lista.
Refinar filtros para itens em uma coluna	Selecione uma coluna e clique no menu de três pontos verticais para expandi-la e inserir condições para refinar e agrupar os dados na coluna.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Digamos, por exemplo, que você queira exibir somente registros que tenham uma vulnerabilidade específica. Na lista de registros, selecione a linha do registro na coluna **Resumo**. Clique no menu de pontos vertical exibido e escolha uma: ◦ **Mostrar correspondência** - mostra todos os outros registros que têm esta vulnerabilidade. ◦ **Filtrar** - mostra todos os registros que não têm esta vulnerabilidade.

4. Nas guias Tarefas de correção, Itens vulneráveis e Resultados de testes de configuração, você pode fazer uma busca detalhada em registros individuais de Tarefa de correção (VUL), Item vulnerável (VIT) e Resultado de testes (CTR) .

O que Fazer Depois

Se você quiser criar uma tarefa de correção sob demanda a partir de um esforço de correção, consulte Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades. Você também pode Criar uma lista personalizada de registros para ajudá-lo a monitorar o andamento da correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um esforço de correção no Espaço do gerenciador de vulnerabilidades

Um registro de esforço de correção é uma lista estática de registros que você cria a partir de um tópico de observação no espaço do Gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você usa esforços de correção para entregar as tarefas que as equipes de TI usam para corrigir vulnerabilidades. A partir da v16.1:

- Você pode editar os esforços de correção existentes.
- Crie esforços de correção que são criados automaticamente nas datas e horas que você definir.
- Transfira registros de esforços de correção existentes para um novo esforço de correção.

A partir da versão 18.0, como você não pode criar um esforço de correção para um tópico de observação inativo, o botão **Criar** esforço de correção está inativo.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Na página principal (Inicial), selecione um tópico de observação para o qual você deseja criar um esforço de correção.
3. Para exibir os registros associados ao tópico de observação selecionado, no cabeçalho do registro, clique no **Itens vulneráveis** guia.

   Os registros são exibidos.

   No cabeçalho da guia Itens vulneráveis, você pode exibir o número total de registros que este tópico de observação tem.

   As seguintes colunas e dados são exibidos:

Colunas na guia Itens vulneráveis

Coluna	Descrição
Número	O número do registro.
Resumo	Descrição da vulnerabilidade.
Item de configuração	O ativo associado à vulnerabilidade.
Pontuação de risco	Pontuação de risco quantificado que separa os registros em Crítico, Alto, Médio, Baixo e Nenhum.
Estado	Status do registro.
Status da Correção	Status de correção de um registro.
Grupo de atribuição	Grupos de atribuição responsáveis pela correção. A atribuição de registros a grupos é baseada nas regras de atribuição que você cria.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
Esforço de correção	Se estiver atribuído a um esforço de correção, cada registro listará seu esforço de correção atribuído. Depois de ser adicionado a um esforço de correção, um registro não será adicionado a nenhum outro esforço de correção criado.
Grupo de atribuição	Grupos de atribuição responsáveis pela correção. A atribuição de registros a grupos é baseada nas regras de atribuição que você cria.
Esforço de correção	Se estiver atribuído a um esforço de correção, cada registro listará seu esforço de correção atribuído. Depois de ser adicionado a um esforço de correção, um registro não será adicionado a nenhum outro esforço de correção criado.
Na tarefa de correção	Se `verdadeiro`, este valor indica que um registro já está em uma tarefa de correção. Os registros podem estar em várias tarefas de correção, mas um registro pode ser adicionado somente a um esforço de correção.
Explorar itens existentes	Indica se existe uma exploração conhecida para um registro.
Aberto pela última vez	Data em que o registro foi aberto pela última vez em seu Now Platform. Se o registro foi fechado e reaberto em seguida, esta é a última vez em que o registro foi reaberto.

4. Para criar um esforço de correção, clique em **Criar**esforço de correção .

   Quando você cria um esforço de correção, os registros que já estão nos esforços de correção existentes não são adicionados a nenhum novo esforço de correção criado a partir deste tópico de observação.

   Conforme os registros são atualizados ou novos registros são criados em tópicos de observação, você pode criar esforços de correção.

5. Como alternativa, você pode Criar um esforço de correção recorrente nos Espaços de resposta a vulnerabilidades.

   O botão **Editar** está disponível no menu para esforços de correção existentes. Você tem a opção de modificar os campos e condições de um modal que é exibido. As mudanças feitas e salvas no registro do esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

6. Na etapa 1 do modal Criar esforço de correção, preencha os campos.

   No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente e ajuda a localizá-lo e rastreá-lo na lista de esforços.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção.

A partir da versão 17.1, ao criar um esforço de correção para tópicos de observação que contêm vulnerabilidades de host, você pode atualizar automaticamente itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, marque a caixa de seleção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.

Nota: A partir da versão 18.0, esta caixa de seleção aparece na etapa 2.

7. Na etapa 2, Geração de tarefa, escolha um método na lista para agrupar os registros nas tarefas de correção geradas a partir deste esforço de correção após sua criação.

Opção	Descrição
Por grupo de atribuição	Registros com o mesmo grupo de atribuição são agrupados em uma Tarefa de correção.
Por grupo de atribuição e item de configuração	Registros com o mesmo grupo de atribuição e item de configuração são agrupados em uma tarefa de correção.
Por grupo de atribuição e (teste de configuração ou vulnerabilidade)	Registros com o mesmo grupo de atribuição e item de configuração são agrupados em uma tarefa de correção.
Nenhum (nenhuma tarefa de correção foi criada).	Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades. **Nota:** A partir da versão 18.0, a opção **Nenhum** não está disponível.

Nota: Para a versão 18.0, a opção **Nenhum** não está disponível.

8. Na etapa 3, Transferir, verifique quantos registros você deseja adicionar ao esforço de correção e veja quantos registros estão disponíveis para transferência de outros esforços de correção ativos.

Se não houver novos registros ativos a serem adicionados, o seguinte texto será exibido:

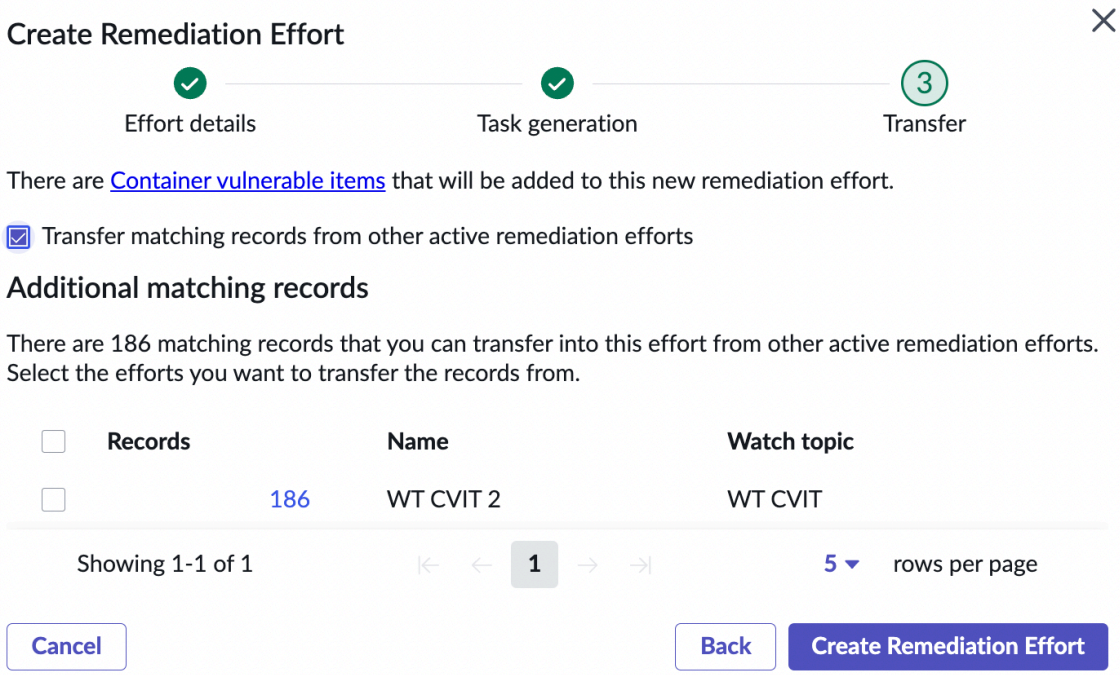
```
Não há registros ativos disponíveis que você possa adicionar a este novo esforço de correção.
```

Todos os registros adicionais que estão disponíveis para transferência para este esforço são listados em `Registros correspondentes adicionais` .

A partir da versão 18.0, marque a caixa de seleção **Transferir registros correspondentes de outros esforços de correção ativos** e marque as caixas de seleção dos registros que você deseja transferir de outros esforços de correção ativos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão 18.0 - Criar esforço de correção



Depois de clicar em **Criar esforço**de correção , em alguns momentos, o novo esforço de correção será exibido. Dependendo do número de registros, pode levar algum tempo para preencher o novo registro. Uma mensagem indica se o registro ainda está sendo preenchido.

O novo esforço de correção é criado com todos os registros que estão disponíveis no tópico de observação usado para criá-lo, além de todos os registros que você selecionou para transferência de esforços existentes.

Se você selecionar registros para transferir de um esforço existente e o esforço existente transferir todos os registros para o novo esforço, o esforço de correção do qual você moveu os registros será encerrado. Para obter mais informações sobre como as Tarefas de correção associadas aos Esforços de correção são afetadas pela transferência de registros, consulte Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades.

Nota: Se não houver registros disponíveis no tópico de observação ou registros selecionados para transferência, o botão **Criar esforço** de correção será desativado.

O trabalho agendado *Populate Efforts* é executado a cada 10 minutos para preencher os dados nos widgets com base na condição selecionada.

Clique na guia Progresso da correção para exibir o andamento da correção. Clique em qualquer item para exibir detalhes, incluindo tipo de registro, pontuação de risco, classificação de risco, porcentagem de registros corrigidos, registros em estado adiado e não adiado e número total de registros, condições usadas no tópico de observação e status de correção. As informações de Status de correção, como Meta de correção e Status de correção, são acumuladas da tabela Itens vulneráveis. A pontuação de risco de registro mais alta é acumulada a partir da tabela Calculadoras de vulnerabilidade, enquanto a pontuação de risco é acumulada a partir da **Calculadoras de acúmulo de vulnerabilidades** > **Agregar esforço de correção**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia Tarefas de correção exibe as tarefas para todos os tipos de problemas. Os campos são preenchidos quando os seguintes trabalhos agendados são executados. Eles são executados automaticamente a cada 15 minutos:

- Acumular valores de item vulnerável da aplicação para vulnerabilidade e grupo.
- Acumular valores de item vulnerável de contêiner para vulnerabilidade e grupo.
- Acumule valores de resultado de testes para testar o grupo de resultados e o teste de configuração.
- Acumular valores de item vulnerável para vulnerabilidade e grupo.

Na exibição Listas, você pode exibir os Esforços de correção, Tarefas de correção, Itens vulneráveis, Resultados de testes de configuração e assim por diante. Você pode abrir uma tarefa de correção ou um item vulnerável e exibir a página Detalhes. Clique nas reticências Mais ações e clique em **Iniciar investigação** para resolver uma tarefa de correção.

9. Opcional: Você também pode editar os esforços de correção recorrentes existentes.

   (Optional) Se houver um esforço de correção recorrente para um tópico de observação, **Editar esforço recorrente** estará disponível no menu no canto superior direito de um tópico de observação. Escolha esta opção para editar o esforço recorrente.

   As mudanças feitas e salvas no registro do esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades

Crie uma tarefa de correção sob demanda a partir de um esforço de correção. Se você criar uma tarefa de correção sob demanda, escolha os registros que deseja adicionar manualmente.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Para a versão 18.0 de Resposta a vulnerabilidades, não é possível criar uma Tarefa de correção na exibição de registro de um Esforço de correção.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. No canto superior esquerdo do espaço com a página inicial exibida, clique no ícone de exibição de **lista** para exibir a página principal de lista.
3. Em Esforços de correção, clique em **Ativo** ou **Todos**.
4. Na lista exibida, clique em um registro para abri-lo.
   A guia de visão geral do registro é exibida.
5. Clique na guia **Itens vulneráveis**.
   A lista de registros é exibida.
6. Para criar uma nova tarefa de correção, na coluna Número, selecione os registros que você deseja adicionar.
7. Clique **em Criar tarefa de correção**.
8. No modal exibido, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Insira um texto que possa ajudá-lo a identificar facilmente essas tarefas de correção em suas tarefas de correção existentes.
Grupo de atribuição	Escolha um grupo de atribuição para as tarefas. Use o filtro para ajudá-lo a localizar o grupo desejado.

9. Clique em **Criar**.
10. A nova tarefa de correção é exibida com os registros ativos selecionados.

Criar um esforço de correção recorrente nos Espaços de resposta a vulnerabilidades

Você pode criar e programar esforços de correção recorrentes que são gerados automaticamente nas datas e horas definidas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar automaticamente esforços de correção recorrentes em uma programação que ajuda a rastrear vulnerabilidades que podem surgir e exigir atenção imediata e contínua.

A partir da versão 18.0, como não é possível criar um esforço de correção recorrente para um tópico de observação inativo, a opção **Criar esforço recorrente** está inativa. Se você desativar um tópico de observação que tenha um esforço recorrente já programado, um novo esforço de correção não será criado até que o tópico de observação seja ativado. Além disso, os detalhes da **Recorrência de esforço** e da **Data da próxima recorrência** desaparecem no canto superior direito. Depois de ativar o tópico de observação, um esforço de correção será criado na próxima programação.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Na página principal (Inicial), selecione um tópico de observação para o qual você deseja criar um esforço de correção recorrente.

   Você pode criar um esforço de correção recorrente por tópico de observação.

   Nota: Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. No entanto, você pode transferir registros de esforços de correção não recorrentes existentes para novos esforços de correção. Consulte Transferir registros para esforços de correção nos espaços Resposta a vulnerabilidades para obter mais informações sobre como transferir registros.

3. Em um tópico de observação, no canto superior direito da lista Criar esforço de correção, selecione **Criar esforço recorrente**.

   O modal Criar esforço recorrente é exibido.

4. Na etapa 1, Detalhes do esforço, preencha os campos obrigatórios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente que ajuda a localizá-lo e rastreá-lo na lista de esforços.

No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção. Por exemplo, `Vulnerabilidades em ativos voltados externamente`.

A partir da versão 17.1, ao criar um esforço de correção para tópicos de observação que contêm vulnerabilidades de host, você pode atualizar automaticamente itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar a opção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.

Nota: A partir da versão 18.0, esta caixa de seleção aparece na etapa 2.

5. Clique em **Avançar**.
   Os detalhes da geração da tarefa são exibidos.
6. Na etapa 2, Geração de tarefa, escolha um método na lista para agrupar os itens vulneráveis nas tarefas de correção geradas a partir deste esforço de correção após sua criação.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum (nenhuma tarefa de correção foi criada). Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades.

     Nota: Para a versão 18.0 de Resposta a vulnerabilidades, a opção **Nenhum** não está disponível.
7. Clique em **Avançar** para continuar.
8. Na etapa 3, Recorrência, selecione a frequência.

Opção	Descrição
Trimestralmente (a cada 3 meses)	Programa o esforço de correção uma vez a cada três meses. **Nota:** Se o mês selecionado tiver apenas 30 dias, o esforço de correção será criado nessa última data do mês.
Mensalmente	Programa o esforço de correção uma vez por mês.
Semanalmente	Programa o esforço de correção uma vez por semana. **Nota:** Esta opção está disponível a partir da versão 19.0 de Resposta a vulnerabilidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Diariamente	Programa o esforço de correção todos os dias. **Nota:** Esta opção está disponível a partir da versão 19.0 de Resposta a vulnerabilidades.

a. Defina a programação de recorrência.

Use as listas para selecionar o mês/dia/hora/minuto em que você deseja que o esforço de correção seja criado. O fuso horário para programação é, por padrão, o seu fuso horário.

Nota: Se você tiver muitas vulnerabilidades, talvez prefira definir a criação para fora do horário comercial.

Se você quiser que o trabalho seja criado no último dia do mês, o trabalho agendado criará o esforço de correção recorrente no último dia do mês. Uma mensagem será exibida se o mês não tiver 31 dias.

b. Opcional: Selecione **Transferir vulnerabilidades** para vulnerabilidades ativas neste esforço de correção para levar adiante em cada esforço de correção subsequente que for criado.

9. Clique **em Programar recorrência**.
É exibida uma mensagem informando que o registro de correção recorrente foi criado. O novo esforço de correção não é exibido imediatamente, ele é criado quando você o programou. Ele é exibido em suas listas depois de ser criado pelo trabalho agendado.

A data em que o esforço de correção será criado é mostrada no tópico de observação correspondente. Para obter mais informações sobre como as Tarefas de correção associadas aos Esforços de correção são afetadas pela transferência de registros, consulte Ciclos de vida dos esforços de correção, tarefas de correção e registros nos Espaços de resposta a vulnerabilidades.

Transferir registros para esforços de correção nos espaços Resposta a vulnerabilidades

Você pode transferir registros de esforços de correção existentes para novos esforços de correção.

Antes de Iniciar

Se você se deparar com uma ameaça de dia zero ou uma vulnerabilidade muito crítica que deseja resolver rapidamente, convém consolidar todos os registros ativos que já possui para esta vulnerabilidade em um esforço de correção. No entanto, cada registro só pode estar em um esforço e os registros podem se sobrepor entre tópicos de observação. Portanto, para coletar todos eles, você precisa transferir esses registros de vários esforços existentes para um esforço de correção.

Digamos, por exemplo, que você criou um esforço de correção que contém uma vulnerabilidade de alta prioridade. Como esta vulnerabilidade é difundida e pode afetar outras áreas em seu ambiente, você pode ter registros associados a esta vulnerabilidade já em esforços de correção existentes. Para combinar esses registros para que estejam todos em um esforço de correção, você pode transferir todos os registros dos esforços de correção existentes para um novo esforço de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. Para obter mais informações, consulte Criar um esforço de correção recorrente nos Espaços de resposta a vulnerabilidades.

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Na página principal (Inicial), selecione um tópico de observação para o qual você deseja criar um esforço de correção recorrente.
3. Clique **em Criar esforço**de correção .
   O modal Criar esforço de correção é exibido.
4. Na etapa um, Detalhes do esforço, preencha os campos obrigatórios.

   No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente que ajuda a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção. Por exemplo, `Vulnerabilidades ativas do Log4J`.

   a. No campo Nome, insira um nome para o novo esforço de correção.
      Por padrão, o nome do tópico de observação é exibido.

   b. No campo Descrição, insira o texto que ajudará você a localizar facilmente esse esforço de correção na lista de esforços de correção.

   A partir da versão 17.1, ao criar um esforço de correção para tópicos de observação que contêm vulnerabilidades de host, você pode atualizar automaticamente itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar a opção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.

   Nota: A partir da versão 18.0, esta caixa de seleção aparece na etapa 2.

5. Clique em **Avançar**.
   Os detalhes da geração da tarefa são exibidos.
6. Na etapa 2, Geração de tarefa, escolha um método na lista para agrupar os registros nas tarefas de correção geradas a partir deste esforço de correção após sua criação.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum (nenhuma tarefa de correção foi criada). Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Criar uma tarefa de correção sob demanda no Espaço do gerenciador de vulnerabilidades.

     Nota: Para a versão 18.0, a opção **Nenhum** não está disponível.

7. Clique em **Avançar**.

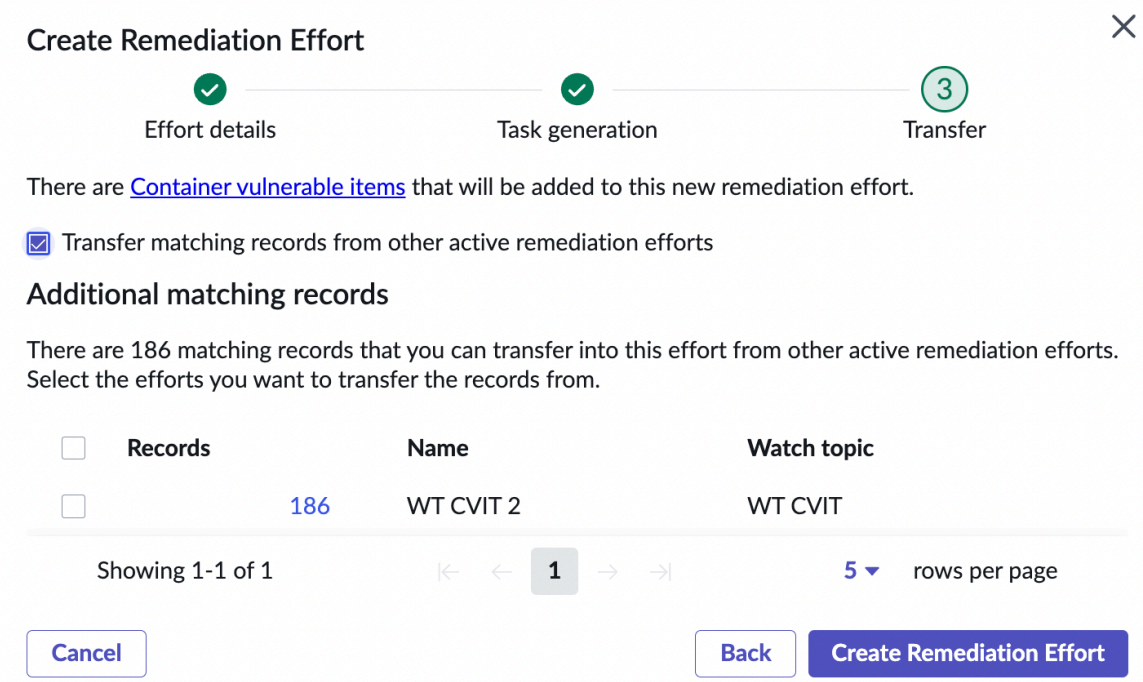
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Na etapa 3, Transferir, verifique quantos registros serão adicionados ao esforço de correção e veja quantos registros estão disponíveis para transferência de outros esforços de correção ativos.
9. Para transferir registros de outros esforços, na lista, marque as caixas de seleção dos registros desejados.

   A partir da versão 18.0, marque a caixa de seleção **Transferir registros correspondentes de outros esforços de correção ativos** e marque as caixas de seleção dos registros que você deseja transferir de outros esforços de correção ativos.

Versão 18.0 - Criar esforço de correção



10. Clique **em Criar esforço**de correção .

    Depois de alguns momentos, o novo esforço de correção será exibido. Dependendo do número de registros, isso pode levar algum tempo. Uma mensagem indica que o registro está sendo preenchido.

    O novo esforço de correção é criado com todos os registros que estão disponíveis no tópico de observação usado para criá-lo, além de todos os registros que você selecionou para transferência de esforços existentes.

    Se você selecionar registros para transferir de um esforço existente e o esforço existente transferir todos os registros para o novo esforço, o esforço de correção do qual você moveu os registros será encerrado.

    Nota: Se não houver registros disponíveis no tópico de observação nem registros selecionados para transferência, o botão **Criar esforço** de correção será desativado.

    Para obter mais informações sobre como as Tarefas de correção associadas aos Esforços de correção são afetadas pela transferência de registros, consulte Transferência de registros ou transferênciade registros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar um controle de compensação à biblioteca

Como gerente ou analista de vulnerabilidade, adicione uma lista de controles compensatórios à biblioteca Controles de compensação no Espaço do gerente de vulnerabilidades, que pode ser aplicada para a redução de risco de itens vulneráveis e tarefas de correção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Alguns controles de compensação usados com frequência são enviados com o sistema de base. Você pode exibir esses controles de compensação navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Listas** > **Bibliotecas** > **Controles de remuneração**. Você pode ativar ou desativar esses controles de compensação de acordo com seus requisitos.

Nota: O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista em Bibliotecas, selecione **Controles de remuneração**.
3. Clique em **Nova**.
4. No formulário Criar controles de remuneração, preencha os campos.

Campos de formulário Criar controles de remuneração

Campo	Descrição
Nome	Nome do controle de remuneração, que aparece como uma opção no menu suspenso **Controles de remuneração** do modal de exceção Solicitar.
Descrição	Informações resumidas que fornecem detalhes sobre o controle de remuneração.
Ativo	Status do controle de remuneração. Somente controles ativos aparecem no menu suspenso **Controles de remuneração** do modal Solicitar exceção.

5. Selecione **Salvar**.
6. Na lista Controles de remuneração em Bibliotecas, selecione o controle de remuneração desejado e selecione **Editar**, ative ou desative um controle de remuneração e clique em **Salvar** para modificar os controles de remuneração.
   Todos os controles de remuneração ativos aparecem como uma opção no menu suspenso **Controles de remuneração** do modal Solicitar exceção para solicitações de redução de risco.

O que Fazer Depois

A partir da v21.0 de Resposta a vulnerabilidades, você pode associar controles de compensação a CVEs ou TPEs depois de adicionar controles de compensação à biblioteca. Para obter mais informações sobre como associar controles de remuneração, consulte Associar controles de remuneração a CVEs ou TPEs para solicitações de redução de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

- Noções básicas sobre controles de remuneração para redução de risco
- Desabilitar ou habilitar a redução de risco para um CVE ou TPE
- Associar controles de remuneração a CVEs ou TPEs para solicitações de redução de risco
- Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Associar controles de remuneração a CVEs ou TPEs para solicitações de redução de risco

Como gerente de vulnerabilidade ou analista, você pode associar controles de compensação relevantes a uma entrada de vulnerabilidade comum (CVE) ou entrada de terceiros (TPE) no espaço do gerente de vulnerabilidade, que pode ser usado para reduzir o risco representado por uma vulnerabilidade.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

- Se você não associar controles de remuneração a um CVE ou TPE, todos os controles ativos serão exibidos no campo Selecionar controles de remuneração do formulário Solicitar exceção.
- Se você associar um controle de remuneração a um CVE, esse controle de remuneração será associado automaticamente ao TPE, que é mapeado para o CVE.

Nota: O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Listas, em Bibliotecas, abra uma das seguintes opções para as quais você deseja associar os controles:
   - **CVE** da lista de CVEs.
   - **TPE** da lista de TPEs.
3. Selecione **Associar controles**.

   Nota: O botão **Associar controles** aparece somente quando a redução de risco está habilitada para um CVE ou TPE. Em outras palavras, você pode associar controles de remuneração somente quando a redução de risco estiver habilitada para um CVE ou TPE. Se o botão **Associar controles** não estiver visível, selecione **Habilitar redução de risco**.

4. No modal Associar controles, selecione os controles de compensação que podem ser aplicados a vulnerabilidades associadas ao CVE ou TPE para redução de risco.
5. Selecione **Enviar**.
   - Os controles de remuneração associados aparecem na guia Controles de remuneração aplicáveis na exibição de registro do CVE e do TPE.
   - Enquanto um proprietário de correção solicita a redução de risco, esses controles de remuneração associados aparecem no campo Selecionar controles de remuneração no modal Solicitar exceção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

- Noções básicas sobre controles de remuneração para redução de risco
- Desabilitar ou habilitar a redução de risco para um CVE ou TPE
- Adicionar um controle de compensação à biblioteca
- Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Como Gerente e Analista de Vulnerabilidades, você pode desabilitar ou habilitar as solicitações de redução de risco para as vulnerabilidades do host em uma Entrada de Vulnerabilidade Comum (CVE) ou Entrada de Terceiros (TPE) no Espaço do Gerenciador de Vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A redução de risco para um CVE e TPE está habilitada por padrão.

Nota: O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   Na página Listas, em Bibliotecas, abra uma das seguintes opções para as quais você deseja desabilitar as solicitações de redução de risco:
   - **CVE** da lista de CVEs.
   - **TPEs** da lista de TPEs.
2. Selecione **Desabilitar redução de risco**.
   O responsável pela correção não pode solicitar a redução de risco dos itens vulneráveis de host relacionados a este CVE ou TPE. Em outras palavras, a caixa de seleção Solicitar redução de risco não aparece quando o **motivo** é selecionado como `Controle de mitigação no local` no modal de exceção de solicitação.
3. Para habilitar as solicitações de redução de risco para itens vulneráveis de host, selecione **Habilitar redução de risco**.

Informações relacionadas

- Noções básicas sobre controles de remuneração para redução de risco
- Adicionar um controle de compensação à biblioteca
- Associar controles de remuneração a CVEs ou TPEs para solicitações de redução de risco
- Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Verificar novamente registros e tarefas de correção no Espaço do gerenciador de vulnerabilidades

Para verificar se suas tarefas e registros de correção foram resolvidos entre os ciclos de verificação programados, inicie novas verificações a partir de seu Now Platform sob demanda.

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Os scanners Rapid7 e Qualys são desativados por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem nos registros de item vulnerável e de tarefa de correção após a próxima importação, e **Verificar novamente** está disponível como uma ação de IU.

A nova verificação é compatível com registros e tarefas de correção com as seguintes integrações no Espaço do gerenciador de vulnerabilidades. Consulte os seguintes tópicos para obter mais informações:

- Verificar novamente Rapid7 itens vulneráveis dos espaços Resposta a vulnerabilidades
- Verificar novamente Qualys itens vulneráveis dos espaços Resposta a vulnerabilidades
- Verificar novamente itens vulneráveis Tenable.io e Tenable.sc dos espaços Resposta a vulnerabilidades

Para iniciar novas verificações no espaço do Gerenciador de vulnerabilidades a partir de registros de item vulnerável e tarefa de correção, os registros exigem um scanner compatível como origem.

Você pode preferir criar uma lista filtrada que exiba registros por origem. Consulte Criar uma lista personalizada de registros para obter um exemplo de como criar uma lista.

Reavaliar as propriedades de correção dos registros no Vulnerability Manager Workspace

A partir da v23.0 da Resposta a vulnerabilidades, avalie as atribuições, a data da meta de correção, as tarefas de correção e a pontuação de risco de um conjunto de registros (VITs, AVITs, CVITs ou TRs) no Vulnerability Manager Workspace.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host
- sn_vul.app_sec_manager para itens vulneráveis da aplicação
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner
- sn_vulc.vulnerability_analyst e sn_vulc.admin para resultados de testes de configuração

Por Que e Quando Desempenhar Esta Tarefa

Antes da versão 23.0 da Resposta a vulnerabilidades, era necessário aplicar as regras a todos os registros para obter as atribuições mais recentes, datas de meta de correção, pontuações de risco e tarefas de correção, o que era um processo demorado. A partir da versão 23.0, você pode avaliar e atualizar seletivamente essas propriedades para registros

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

específicos, reduzindo assim o tempo de processamento. Além disso, você pode refinar o processo de correção com base nessas propriedades atualizadas.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis da aplicação
   - Itens vulneráveis de contêiner
   - Resultados de testes de configuração
3. Marque a caixa de seleção dos registros desejados e selecione o botão **Reavaliar**.
4. No modal Reavaliar e atualizar propriedades de correção, selecione as propriedades que você deseja atualizar para os registros selecionados.

Propriedade	Descrição
Atribuições	Atualiza as atribuições no campo Grupo de atribuição de acordo com as Regras de atribuição mais recentes.
Pontuação de risco	Atualiza a pontuação de risco no campo Pontuação de risco de acordo com as Regras de pontuação de risco mais recentes.
Tarefas de correção	Atualiza as tarefas de correção de acordo com as regras de tarefa de correção mais recentes.
Data da meta de correção	Atualiza a data da meta de correção de acordo com as Regras de meta de correção mais recentes.

Nota: Quando você seleciona uma propriedade, suas propriedades dependentes são selecionadas automaticamente.

5. Selecione **Aplicar**.

Resultados

As propriedades são atualizadas para os registros selecionados. Você pode verificar nas **Anotações de trabalho** dos registros os valores anteriores e mais recentes das propriedades de correção atualizadas.

Use a exibição de lista no espaço do gerenciador de vulnerabilidades

A exibição de lista no espaço do Gerenciador de vulnerabilidades permite que os gerentes e analistas de vulnerabilidade e segurança exibam o andamento da correção nos registros, analisem os registros da Resposta a vulnerabilidades e exibam o status de suas solicitações de aprovação e exceções.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço para gerentes de vulnerabilidades**.
2. Na parte superior esquerda do espaço com a página inicial exibida, clique no ícone **Lista**.
3. Opcional: Clique em **Minhas listas** para criar uma lista.
   Para obter mais informações sobre como criar uma lista, consulte Criar uma lista personalizada de registros.
4. Consulte a tabela a seguir para ver as ações que você pode executar na página Lista.

Ação de IU	Descrição
Abrir um esforço de correção	
À esquerda da coluna Número com uma lista exibida, passe o mouse sobre uma linha e clique no pequeno ícone de informações **(i)** de um registro.	Detalhes sobre os registros são exibidos no painel do lado direito da página. Os detalhes incluem: ◦ Grupo de atribuição ◦ Vulnerabilidade ◦ Atribuído a ◦ Descrição resumida ◦ Descrição Você pode editar os campos. Se a caixa de seleção Ativo for exibida, você poderá ativar ou desativar o registro. Clique em **Atualizar** para salvar suas mudanças.
Atualizar lista	Com o ícone de atualização no canto superior direito da página, recarregue a página atual.
Redefinir larguras	Clique no ícone de engrenagem para ajustar as larguras das colunas nas listas. Uma cópia da lista original é salva em **Suas listas**.
Copiar a URL da página exibida	Copie o URL para uso em outro lugar.
Exportar a página	No modal, insira o arquivo e os tipos de entrega e clique em **Exportar**.
Refine os filtros para os dados na página.	Selecione uma coluna e expanda o menu de três pontos verticais para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, talvez você prefira filtrar a coluna Grupo de atribuição da lista de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	tarefas de correção ativas por um grupo de atribuição específico.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ◦ Mostrar correspondência - exibe somente itens que correspondem à célula selecionada na coluna. ◦ Remover do filtro — Filtra os itens da coluna que correspondem à célula selecionada na coluna.

5. Crie um item vulnerável de aplicação das listas **Ativo** ou **Todos** em *Application Vulnerable items* clicando no botão **Novo** no canto superior direito.

Criar uma lista personalizada de registros

Você pode criar uma lista personalizada no espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Selecione o ícone **Lista** e clique em **Minhas listas**.
3. Selecione **Nova lista**.
4. No modal Nova lista, clique em **Iniciar a partir de existente** e pesquise na lista de seleção Lista uma lista existente para usar como modelo.
5. Edite o Nome da Lista.
6. Adicionar filtros.
   Por exemplo, você pode criar uma lista de registros ativos para um scanner específico que deseja monitorar para novas verificações. Você pode usar os filtros: `Ativo é verdadeiro` e `Origem contém (nome do seu scanner)`.
7. Edite as colunas que você deseja exibir na lista.
8. Clique em **Criar**.
   Sua nova lista será exibida.
9. Como alternativa, clique em **Criar o seu próprio**, insira um nome e, em seguida, **Selecionar origem**.
10. Comece a digitar no campo e selecione nas origens exibidas para sua nova lista.
11. Clique em **Criar**.
    Sua nova lista será exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você sair do módulo de lista, a lista exibida ao sair será a lista que você vê ao retornar.

12. Para excluir uma lista, com a lista exibida, clique no ícone de engrenagem no canto superior direito da página.

Atualizar uma tarefa de correção no Espaço do gerenciador de vulnerabilidades

O botão **Atualizar status** é usado para que os registros sejam inspecionados para ver se há registros adicionais que pertençam a uma tarefa de correção (VUL, AVUL, CVUL ou CRG). Use-o se uma atualização for garantida fora do trabalho agendado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, na lista Tarefas de correção, abra qualquer registro nos estados Aberto ou Sob investigação.
3. Selecione o menu de três pontos e selecione a opção **Atualizar status**.

Resultados

Os respectivos novos registros aparecem nas guias Itens vulneráveis , Itens vulneráveis de aplicação, Itens vulneráveis de contêiner ou Resultados de testes de configuração.

Habilitar ou desabilitar a importação de resultados de testes para um grupo de testes Qualys

A partir da v23.0 de Resposta a vulnerabilidades, controle a importação dos resultados de testes para os testes em um grupo de testes Qualys usando o botão **Habilitar/Desabilitar importação**, que está disponível na exibição de registro do grupo de teste.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Listas**.
2. Nas Bibliotecas, na lista Grupos de teste, abra um grupo de teste Qualys na exibição de registro.
3. Desabilite a importação dos resultados de testes associados a um grupo de testes Qualys selecionando o botão **Desabilitar importação**.
   Na próxima ingestão de dados, os resultados de testes não serão importados para o grupo de testes Qualys.
   O valor no campo **Importação desabilitada** muda para *verdadeiro*.
4. Opcional: Habilite a importação dos resultados de testes selecionando o botão **Habilitar importação**.

Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace

Aprove ou rejeite solicitações enviadas por proprietários de correção.

Antes de Iniciar

Funções necessárias:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informação adicional
Aprovações de falso-positivo	Um	• Função granular sn_vul.false_positive_approver para itens vulneráveis (VITs). • Função sn_vul.app_false_positive_approver para itens vulneráveis da aplicação (AVITs) • Função sn_vul_container.false_positive_approver para itens vulneráveis de contêiner (CVITs) • sn_vulc.false_positive_approver para resultados de testes de configuração Ou Os aprovadores devem estar no grupo de usuários Aprovador de falso-positivo.	-
Aprovações de exceção (adiamentos)	Dois	• É necessário um aprovador no grupo de aprovadores - nível 1 • É necessário um aprovador no grupo de aprovadores - nível 2	Uma solicitação de exceção para um registro ou tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. A solicitação de exceção requer dois níveis de aprovadores. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de segundo nível e fica visível na fila do aprovador 2.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informação adicional
Aprovações não atribuídas	É necessário um aprovador no grupo Aprovador – Nível 1	• sn_vul.unassign_appr para AVITs e VITs • sn_vul_container.una para CVITs • sn_vulc.unassign_app para problemas de configuração (ICs)	**Nota:** Por padrão, uma configuração de aprovação é fornecida e um grupo de aprovação não atribuído é criado. Os usuários (Aprovador não atribuído - Nível 1) deste grupo podem aprovar a solicitação. Este grupo contém uma função de aprovador não atribuído, sn_vul.unassign_approver, por padrão. Você pode modificar ou criar um novo grupo e atualizar a configuração de aprovação. Para configurar regras de aprovação, navegue até o respectivo módulo Regras de aprovação, selecione qualquer uma das regras de aprovação a seguir e navegue até a configuração de aprovação na guia **Configurações** de aprovação: • *Vulnerable item field change request* para um item vulnerável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos EUA e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informação adicional
Aprovações de redução de risco	Dois	• É necessário um aprovador no grupo de aprovadores - nível 1 • É necessário um aprovador no grupo de aprovadores - nível 2	O fluxo de aprovação para redução de risco é igual às aprovações de exceção (adiamentos).

Consulte Resposta a vulnerabilidades personas e funções granulares e Atribua as funções de persona Resposta a vulnerabilidades usando o Assistente de configuração para obter mais informações sobre como atribuir funções de persona a usuários e usuários a grupos.

Nota: Adicione usuários aos grupos de aprovação antes de enviar solicitações de aprovação. Se você criar solicitações antes de adicionar usuários aos grupos de aprovação, as solicitações talvez não fiquem visíveis para os usuários que têm a permissão de aprovação.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   Se um aprovador não tiver acesso ao espaço, as aprovações poderão ser processadas em **Resposta a vulnerabilidades** > **Minhas aprovações** no ambiente clássico.
2. Selecione o ícone de exibição de lista (ícone de exibição List).
   A página Lista é exibida.
3. Na lista filtrada de Aprovações, selecione **Atribuído a mim**.
4. Localize uma solicitação que você deseja processar e selecione o link na coluna Estado.
   O registro de Aprovação de Mudança do Estado de Vulnerabilidade (VCA#) é exibido.
5. Escolha uma das seguintes opções para aprovar ou rejeitar a solicitação.

Opção	Descrição
Clique na guia Detalhes, insira o texto no campo Comentários e clique em Rejeitar	◦ Uma mensagem é exibida indicando que há uma aprovação rejeitada para o registro de Aprovação de Mudança de Estado de Vulnerabilidade. ◦ O estado no registro de Aprovação de mudança do estado de vulnerabilidade muda para Rejeitado. ◦ O estado na tarefa de correção ou no registro permanece o mesmo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	◦ O registro de Aprovação de Mudança do Estado de Vulnerabilidade não é mais exibido na exibição da lista de Aprovações no espaço.
Nas guias **Solicitação** ou **Detalhes**, clique em Aprovar	◦ Uma mensagem é exibida indicando que o registro de Aprovação de Mudança de Estado de Vulnerabilidade foi aprovado. ◦ O estado na tarefa de correção ou nas transições de registro para Adiado. ◦ Registros ativos na transição das tarefas de correção para adiados. ◦ O registro de Aprovação de Mudança do Estado de Vulnerabilidade não é mais exibido na exibição da lista de Aprovações.

Tradução automática

Configurar notificações por e-mail nos espaços Resposta a vulnerabilidades

Identifique usuários para lembretes automáticos por e-mail enviados a usuários no grupo de usuários responsáveis pela correção.

Antes de Iniciar

Função necessária: administrador

Este recurso gera automaticamente um resumo de e-mail para usuários do grupo de usuários responsáveis pela correção. Adicione todos os usuários que você deseja que recebam notificações por e-mail, conforme descrito em Use o resumo de e-mail nos Espaços de resposta a vulnerabilidades.

Verifique se os usuários têm um endereço de e-mail ativo inserido no registro de usuário e se você os adicionou ao grupo de usuários responsáveis pela correção.

Se você quiser mudar a frequência de entrega, o dia ou a hora dos e-mails, ou desativar o recurso, siga estas etapas.

Procedimento

1. Navegar até **Todos** > **Trabalhos agendados**.
2. Localize **Gerar resumo de correção** e clique nele para abrir o registro.

   Você pode preferir deixar os campos em suas configurações padrão até verificar se as notificações estão sendo enviadas. Por padrão, os e-mails são enviados semanalmente às segundas-feiras de manhã às 9h no fuso horário da instância que está executando o trabalho.

3. Modifique os campos no formulário.
   Para obter mais informações sobre os campos de formulário, consulteGerar campos de formulário de resumo de correção.
4. Clique em **Atualizar**.

O que Fazer Depois

Caso você tenha verificado que todas as informações listadas anteriormente estão corretas e você tenha usuários no grupo de usuários responsáveis pela correção, mas os e-mails

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

não sejam enviados conforme o esperado, verifique se há canais ativados para receber notificações por e-mail. Consulte Criar canais de notificação .

Corrigindo itens vulneráveis e resultados de testes no Vulnerability Manager Workspace

No Vulnerability Manager Workspace, você pode corrigir itens vulneráveis e resultados de testes do em um tópico de observação definindo uma condição e pode rastrear o andamento da correção criando esforços de correção.

Como usar a edição em massa no Vulnerability Manager Workspace

No Vulnerability Manager Workspace, você pode atualizar o estado dos registros, solicitar exceções e falso-positivos e atribuir registros a um grupo de atribuição de vários itens vulneráveis (VITs, AVITs ou CVITs) simultaneamente usando o recurso de edição em massa.

O recurso de edição em massa está disponível para:

- itens vulneráveis de host (VITs) a partir de v21.0 de Resposta a vulnerabilidades.
- itens vulneráveis de aplicação (AVITs) e itens vulneráveis de contêiner (CVITs) a partir da v22.0 de Resposta a vulnerabilidades.
- resultados de testes a partir da v23.0 de Resposta a vulnerabilidades.

Atualizar o estado de registros em massa no Vulnerability Manager Workspace

Atualize o estado de vários registros (VITs, AVITs ou CVITs) simultaneamente de acordo com o andamento da correção usando o recurso de edição em massa no Vulnerability Manager Workspace.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host
- sn_vul.app_sec_manager para itens vulneráveis da aplicação
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
3. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo **Seleção de registro**.
   - Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** no campo **Seleção de registro**.
4. Selecione o botão **Edição em massa**.
5. No modal de edição em massa, preencha os campos a seguir para atualizar o estado dos registros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ Somente itens selecionados: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ Todos os itens vulneráveis que correspondem ao filtro: selecione esta opção se quiser atualizar os registros filtrados. ◦ Tarefa de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção. ◦ Entrada de vulnerabilidade: selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecionar o CVE no campo **Entrada de vulnerabilidade**. **Nota:** Registros com IC inválido ou IC desativado não são atualizados.
Estado	Mude para o **Estado** no registro. As opções são: ◦ Não atualizar ◦ Aberto ◦ Sob Investigação ◦ Aguardando Implementação ◦ AdiadoSolicitar exceção em massa no Espaço do gerenciador de vulnerabilidades ◦ FechadoEdição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades ◦ Resolvido **Nota:** Somente os registros para os quais a transição de estado é válida são atualizados.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Selecione **Editar**.

Um trabalho assíncrono de edição em massa atualiza os registros selecionados.

Edição em massa de itens vulneráveis de host com patches e soluções

Recomende um patch ou solução para vários itens vulneráveis de host simultaneamente usando o recurso de edição em massa no Vulnerability Manager Workspace.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin e qualquer função com a função granular sn_vul.bulk_edit.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

No modal de edição em massa, ao adicionar uma solução preferencial e um patch, você também pode cancelar a atribuição ou atribuir vários itens vulneráveis de host (VITs) a um grupo de atribuição simultaneamente.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.

   Nota: Os registros selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.

2. Na página Lista, em Itens vulneráveis de host, abra a lista Ativo ou Todos.
3. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo **Seleção de registro**.
   - Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** no campo **Seleção de registro**.
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo Seleção de registro do modal de edição em massa.
   - Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** no campo Seleção de registro do modal de edição em massa.
4. Selecione o botão **Edição em massa**.
5. No modal de edição em massa, preencha os campos para recomendar um patch ou solução para vários itens vulneráveis de host.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ Somente itens selecionados: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ Todos os itens vulneráveis que correspondem ao filtro: selecione esta opção se quiser atualizar os registros filtrados. ◦ Tarefa de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção. ◦ Entrada de vulnerabilidade: selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecionar o CVE no campo **Entrada de vulnerabilidade**. **Nota:** ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros (VITs) no estado Aberto, Sob investigação ou Aguardando implementação são atualizados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	Mudança para o **Estado** dos itens vulneráveis de host. Você pode adicionar a solução preferencial e o patch somente ao escolher os seguintes estados. ◦ Não atualizar ◦ Aberto ◦ Sob Investigação ◦ Aguardando Implementação
Solução preferencial	Solução que é direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa. Selecione a mudança para o campo **Solução preferencial** no item vulnerável. As opções são de uma lista de pesquisa de soluções preferenciais disponíveis para os VITs selecionados. **Nota:** ◦ O conjunto de soluções preferenciais disponíveis é uma interseção de todas as possíveis soluções das vulnerabilidades em todos os VITs selecionados. ◦ Ao selecionar **Seleção de registro** > **Entrada de Vulnerabilidade** para uma edição em massa, todos os VITs da vulnerabilidade serão definidos para a solução preferencial selecionada. **Nota:** Esta operação não define a **solução preferencial** no nível de entrada de vulnerabilidade. Definir a **solução preferencial** no nível de entrada de vulnerabilidade definiria a **solução preferencial** para todos os novos VITs daqui em diante. A edição em massa modifica somente o conjunto atual de VITs. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir a **solução preferencial**. ◦ O número total de soluções que podem ser mostradas na lista de pesquisa é limitado a 170. Se houver mais de 170 soluções, uma mensagem de aviso será exibida. O valor atualizado é mostrado na exibição de lista de itens vulneráveis.
Patch preferencial	Patch destinado a corrigir todos os itens de vulnerabilidade selecionados para edição em massa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Você deve instalar a Orquestração de patches para exibir a lista de patches preferenciais. ◦ O conjunto de patches preferenciais disponíveis é uma interseção de todos os possíveis patches em todos os VITs selecionados. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir o **patch preferencial**. ◦ O número total de patches que podem ser mostrados na lista de pesquisa é limitado a 170. Se houver mais de 170 patches, uma mensagem de aviso será exibida.
Cancelar atribuição	Todos os itens selecionados não estão atribuídos ao grupo de atribuição e ao proprietário de correção. **Nota:** ◦ Este campo aparece quando você seleciona o Estado como Não atualizar. ◦ Quando você cancela a atribuição de registros, é criada uma tarefa de correção que é enviada para aprovação. Para obter mais informações, consulte Remover atribuições de itens vulneráveis de host em massa.
Grupo de atribuição	Grupo de atribuição para os registros. Todos os grupos de atribuição ativos aparecem neste campo. **Nota:** Este campo é desativado quando você marca a caixa de seleção Não atribuir.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Selecione **Editar**.

Resultados

Um trabalho assíncrono de edição em massa atualiza os itens vulneráveis de host (VITs) selecionados. A solução preferencial e o patch são adicionados aos itens vulneráveis de host (VITs) relevantes. Abra um item vulnerável de host e exiba a solução e o patch preferenciais na seção Correção da guia Detalhes.

Atribuir registros a um grupo de atribuição em massa

Atribua vários registros (VITs, AVITs, CVITs ou TRs) simultaneamente a um grupo de atribuição usando o recurso de edição em massa no Vulnerability Manager Workspace.

Antes de Iniciar

Função necessária:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
   - Resultados de testes de configuração
3. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo Seleção de registro.
   - Aplique filtros se quiser usar a opção de **filtro Todos os registros correspondentes** no campo Seleção de registro.
4. Selecione o botão **Edição em massa**.
5. No formulário, preencha os campos para atribuir os registros a um grupo de atribuição.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ *Somente itens selecionados*: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ *Todos registros que correspondem ao filtro*: selecione esta opção se quiser atualizar os registros filtrados. ◦ *Tarefa*de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção. ◦ *Entrada de vulnerabilidade*: selecione esta opção se quiser atualizar os registros específicos para uma vulnerabilidadey e, em seguida, selecionar um CVE ou TPE no campo **Entrada de vulnerabilidade**. **Nota:** Este campo aparece para itens vulneráveis de host, itens vulneráveis de aplicação e itens vulneráveis de contêiner.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ *Teste de configuração*: selecione esta opção se quiser atualizar os resultados de testes específicos para um teste e, em seguida, selecionar um teste no campo **Teste de configuração**. **Nota:** Esta opção aparece somente para resultados de testes de configuração. **Nota:** ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros nos estados Aberto, Sob investigação, Aguardando implementação ou Adiado são atualizados.
Grupo de atribuição	Grupo de atribuição para os registros. Todos os grupos de atribuição ativos aparecem neste campo. **Nota:** Este campo é desativado quando você marca a caixa de seleção Cancelar atribuição para VITs.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Clique **em Editar**.

Resultados
Abra um registro para o qual você atualizou o grupo de atribuição e navegue até a guia Visão geral. O grupo de usuários ao qual o registro está atribuído aparecerá no campo **Grupo de atribuição**.

Remover atribuições de itens vulneráveis de host em massa

Remova a si mesmo ou seus grupos dos campos **Atribuído a** e **Grupo de atribuição** em itens vulneráveis de host (VITs) ou tarefas de correção (VUL) se você determinar que os registros não estão dentro do seu escopo de correção ou se achar que os registros foram incorretos atribuídos a você ou aos seus grupos.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst e sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
O recurso Cancelar atribuição é aplicável a registros em qualquer estado diferente de Encerrado ou Resolvido. Quando você remove atribuições de itens vulneráveis de host usando o recurso de edição em massa, somente os registros relevantes são atualizados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, em Itens vulneráveis de host, abra a lista Ativo ou Todos.
3. Execute uma das seguintes ações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo #unique_785_Connect_42_record-slection-field-unassign.
- Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** ao campo #unique_785_Connect_42_record-slection-field-unassign.

4. Selecione o botão **Edição em massa**.
5. No formulário, preencha os campos para remover atribuições em massa.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ Somente itens selecionados: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ Todos os itens vulneráveis que correspondem ao filtro: selecione esta opção se quiser atualizar os registros filtrados. ◦ Tarefa de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção. ◦ Entrada de vulnerabilidade: selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecionar o CVE no campo **Entrada de vulnerabilidade**. **Nota:** ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros nos estados Aberto, Sob investigação, Aguardando implementação ou Adiado são atualizados.
Estado	Selecione o estado como Não atualizar.
Cancelar atribuição	Todos os itens vulneráveis selecionados não estão atribuídos ao grupo de atribuição e ao proprietário de correção. **Nota:** ◦ Este campo aparece quando você seleciona o Estado como Não atualizar. ◦ Quando você cancela a atribuição de registros, é criada uma tarefa de correção que é enviada para aprovação.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Clique **em Editar**.
Uma tarefa de correção é criada com os itens vulneráveis de host (VITs) selecionados.

Sua solicitação é enviada para aprovação e o aprovador recebe uma notificação por e-mail sobre sua solicitação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O estado dos itens vulneráveis de host (VITs) e da tarefa de correção (VUL) muda para Em revisão. Se uma tarefa de correção for atualizada com este recurso, os campos**Atribuído a** e **Grupo de atribuição** em todos os VITs associados também serão limpos após a aprovação da sua solicitação.

Resultados

No Espaço do gerenciador de vulnerabilidades, na página Lista, navegue até **Solicitações de exceção** > **Todos** e abra o registro de aprovação de mudança de estado correspondente (VCA#) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado de aprovação	Resultado
Aprovado	Os campos **Atribuído a** e **Grupo de atribuição** de todos os itens vulneráveis de host são limpos.
Rejeitado	Os campos **Atribuído a** e **Grupo de atribuição** de todos os itens vulneráveis de host não são atualizados.

No **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da sua solicitação.

Solicitar exceção em massa no Espaço do gerenciador de vulnerabilidades

Solicite uma exceção para vários registros (VITs, AVITs, CVITs ou TRs) simultaneamente usando o recurso de edição em massa em vez de selecionar cada registro manualmente.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Quando você solicita uma exceção para um ou mais registros do modal de edição em massa, uma tarefa de correção é criada com os registros selecionados.

Nota: Os Itens vulneráveis de aplicação (AVITs) dos scanners com o parâmetro **Gerenciar exceções na ServiceNow** definido como falso não são atualizados.

- Se você selecionar AVITs de vários scanners, alguns com o parâmetro **Gerenciar exceções na ServiceNow** definido como verdadeiro e outros definidos como falso, os AVITs vinculados aos scanners com o parâmetro **Gerenciar exceções na ServiceNow** definido como falso não serão atualizados.
- Se você selecionar AVITs somente dos scanners com o parâmetro **Gerenciar exceções na ServiceNow** definido como falso, a opção *Adiar* não aparecerá no campo **Estado** no modal de edição em massa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra a lista Ativo ou Todos em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
   - Resultados de testes de configuração
3. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção *Somente itens selecionados* no campo Seleção de registro.
   - Aplique filtros se quiser usar a opção de *filtro Todos os registros correspondentes* no campo Seleção de registro.
4. Selecione o botão **Edição em massa**.
5. No formulário, preencha os campos a seguir para solicitar uma exceção para vários registros (VITs, AVITs, CVITs ou TRs) simultaneamente.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ *Somente itens selecionados*: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ *Todos os registros correspondentes ao filtro*: selecione esta opção se quiser atualizar os registros filtrados. ◦ *Tarefa*de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção. ◦ *Entrada de vulnerabilidade*: selecione esta opção se quiser atualizar os registros específicos para uma vulnerabilidade e, em seguida, selecionar um CVE ou TPE no campo **Entrada de vulnerabilidade**. **Nota:** Este campo aparece para itens vulneráveis de host, itens vulneráveis de aplicação e itens vulneráveis de contêiner. ◦ *Teste de configuração*: selecione esta opção se quiser atualizar os resultados de testes específicos para um teste e, em seguida, selecionar um teste no campo **Teste de configuração**. **Nota:** Esta opção aparece somente para resultados de testes de configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros no estado Aberto, Sob investigação ou Aguardando implementação são atualizados.
Estado	Selecione o estado *Adiado* para solicitar uma exceção para os registros selecionados. **Nota:** ◦ Quando você seleciona essa opção, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ◦ Quando você adia registros, uma tarefa de correção é criada e essa tarefa é enviada para aprovação.
Motivo	Motivo para adiar registros: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Redução do controle no local ◦ Outro **Nota:** O campo **Motivo** aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Breve nota descrevendo os motivos da solicitação de adiamento. Essas informações são refletidas no campo **Descrição** da tarefa de correção criada para uma solicitação de adiamento. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.
Até	Data até a qual o registro permanece adiado. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado.
Informação adicional	Outras informações necessárias. Essas informações são refletidas no campo Informações adicionais na guia Visão geral da tarefa de correção criada para solicitações de adiamento e falso-positivo encerradas. Se sua solicitação de adiamento for aprovada, essas informações adicionais serão exibidas como notas de adiamento para o VIT e a tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Clique **em Editar**.
7. No modal Responder ao questionário, responda às perguntas e clique em **Enviar**.

   Uma tarefa de correção é criada contendo os registros selecionados. Sua solicitação é enviada para aprovação e o Estado dos registros muda para Em revisão.

   Nota: O modal Responder ao **questionário** aparece somente quando o questionário está habilitado para solicitações de exceção no formulário Gestão de exceções. Para obter mais informações sobre como configurar um questionário para solicitações de exceção, consulte Configurar Gestão de exceções para Resposta a vulnerabilidades, Configurar Gestão de exceções para Resposta a vulnerabilidades de aplicaçõese Configurar Gestão de exceções para Contêiner de Resposta a vulnerabilidades.

   O aprovador recebe uma notificação por e-mail sobre sua solicitação.

Resultados

No Espaço do gerenciador de vulnerabilidades, na página Lista, navegue até **Exceções** > **Todos**, abra o registro de aprovação de mudança de estado correspondente (VCA#) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado de aprovação	Resultado
Aprovado	O estado da Tarefa de correção muda para Adiado com o Motivo fornecido como subestado. O estado e o motivo são revertidos para os registros.
Rejeitado	O estado da Tarefa de correção e de seus registros não muda.

No **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da sua solicitação.

Edição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades

Marque um ou mais registros (VITs, AVITs, CVITs ou TRs) como falso-positivos simultaneamente usando o recurso de edição em massa do Espaço do gerenciador de vulnerabilidades em vez de selecionar cada item manualmente.

Antes de Iniciar

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host (VITs)
- sn_vul.app_sec_manager para itens vulneráveis da aplicação (AVITs)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner (CVITs)
- sn_vulc.admin para resultados de testes de configuração (TRs)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Quando você gera uma solicitação de falso-positivo para um ou mais registros do modal de edição em massa, uma tarefa de correção é criada com os registros selecionados.

Nota: Quando você gera uma solicitação de falso-positivo para os Itens vulneráveis de aplicação (AVITs) usando o recurso de edição em massa, os AVITs dos scanners com o parâmetro **Gerenciar falso-positivo com** a ServiceNow definido como falso não são atualizados.

- Se você selecionar AVITs de vários scanners, alguns com o parâmetro **Gerenciar falso-positivo com a Servicenow** definido como verdadeiro e outros definidos como falso, os AVITs vinculados aos scanners com o parâmetro **Gerenciar falso-positivo com a Servicenow** definido como falso não serão atualizados.
- Se você selecionar AVITs somente dos scanners com o parâmetro **Gerenciar falso-positivo com a ServiceNow** definido como falso, a opção *Falso-positivo* não aparecerá no campo **Motivo** no modal de edição em massa.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista**.

   Nota: Os registros selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.

2. Na página Lista, abra a lista Ativa ou Todas em uma das seguintes listas:
   - Itens vulneráveis de host
   - Itens vulneráveis de contêiner
   - Itens vulneráveis da aplicação
   - Resultados de testes de configuração
3. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção *Somente itens selecionados* no campo **Seleção de registro**.
   - Aplique filtros se quiser usar a opção de *filtro Todos os registros correspondentes* no campo **Seleção** de registro.
4. Selecione o botão **Edição em massa**.
5. No formulário, preencha os campos para solicitar falso-positivo para vários registros.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ *Somente itens selecionados*: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ *Todos os registros correspondentes ao filtro*: selecione esta opção se quiser atualizar os registros filtrados. ◦ *Tarefa*de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ *Entrada de vulnerabilidade*: selecione esta opção se quiser atualizar os registros específicos para uma vulnerabilidade e, em seguida, selecionar um CVE ou TPE no campo **Entrada de vulnerabilidade**. **Nota:** Este campo aparece para itens vulneráveis de host, itens vulneráveis de aplicação e itens vulneráveis de contêiner. ◦ *Teste de configuração*: selecione esta opção se quiser atualizar os resultados de testes específicos para um teste e, em seguida, selecionar um teste no campo **Teste de configuração**. **Nota:** Esta opção aparece somente para resultados de testes de configuração. **Nota:** ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros no estado Aberto, Sob investigação ou Aguardando implementação são atualizados.
Estado	Selecione o estado **Fechado**.
Motivo	Selecione o motivo como Falso-positivo. **Nota:** ◦ Quando você seleciona essa opção, os campos Descrição resumida e Informações adicionais são exibidos. ◦ Uma tarefa de correção é criada quando você marca os registros como falso-positivos e essa tarefa é enviada para aprovação. **Nota:** O campo **Motivo** aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Breve nota descrevendo os motivos da solicitação de falso-positivo encerrado. Essas informações são refletidas no campo **Descrição** da tarefa de correção criada para uma solicitação de falso-positivo encerrado. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado-Falso-positivo.
Informação adicional	Outras informações necessárias. Essas informações são refletidas no campo Informações adicionais na guia Visão geral da tarefa de correção criada para a solicitação Falso-positivo fechado. Se sua solicitação de falso-positivo for aprovada, essas informações adicionais serão exibidas como anotações para o VIT e a tarefa de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado-Falso-positivo.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Clique **em Editar**.
7. No modal Responder ao questionário, responda às perguntas e selecione **Enviar**. Uma tarefa de correção é criada com os registros selecionados. Sua solicitação é enviada para aprovação e o Estado da tarefa de correção muda para Em revisão.

   Nota: O modal Responder ao **questionário** aparece somente quando o questionário está habilitado para solicitações de falso-positivo no formulário Gestão de exceções. Para obter mais informações sobre como configurar um questionário para solicitações de falso-positivo, consulte Configurar Gestão de exceções para Resposta a vulnerabilidades, Configurar Gestão de exceções para Resposta a vulnerabilidades de aplicaçõese Configurar Gestão de exceções para Contêiner de Resposta a vulnerabilidades.

   O aprovador recebe uma notificação por e-mail sobre sua solicitação.

Resultados

No Espaço do gerenciador de vulnerabilidades, na página Lista, navegue até **Exceções** > **Todos**, abra o registro de aprovação de mudança de estado correspondente (VCA#) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado de aprovação	Resultado
Aprovado	O estado da Tarefa de correção muda para Encerrado com o Motivo como Falso-positivo. O estado e o motivo são revertidos para os registros.
Rejeitado	O estado da Tarefa de correção e de seus registros não muda.

No **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da sua solicitação.

Fechar registros em massa no Vulnerability Manager Workspace

Feche vários registros (VITs, AVITs ou CVITs) simultaneamente usando o recurso de edição em massa no Vulnerability Manager Workspace.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager ou sn_vul_container.vulnerability_admin

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, abra a lista Ativa ou Todas em uma das seguintes listas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Itens vulneráveis de host
- Itens vulneráveis de contêiner
- Itens vulneráveis da aplicação

3. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção Somente itens selecionados no campo **Seleção de registro**.
   - Aplique filtros se quiser usar a opção de filtro Todos os itens vulneráveis que correspondem no campo **Seleção de registro**.
4. Selecione o botão **Edição em massa**.
5. No formulário, preencha os campos para fechar os registros selecionados.

Campos modais de edição em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ◦ Somente itens selecionados: selecione esta opção se quiser atualizar os registros selecionados usando a caixa de seleção. ◦ Todos os itens vulneráveis que correspondem ao filtro: selecione esta opção se quiser atualizar os registros filtrados. ◦ Tarefa de correção: selecione esta opção se quiser atualizar os registros em uma tarefa de correção e selecionar a tarefa de correção desejada no campo **Tarefa** de correção. ◦ Entrada de vulnerabilidade: selecione esta opção se quiser atualizar os registros específicos para uma entrada vulnerável comum (CVE) e selecionar o CVE no campo **Entrada de vulnerabilidade**. **Nota:** ◦ Registros com IC inválido ou IC desativado não são atualizados. ◦ Somente os registros no estado Aberto, Sob investigação ou Aguardando implementação são atualizados.
Estado	Selecione o estado como Encerrado.
Motivo	Motivo para fechar registros: ◦ Falso-positivo **Nota:** Quando você seleciona esta opção para marcar os registros como falso-positivos, os campos Motivo, Descrição resumida e Informações adicionais são exibidos. Para obter mais informações sobre edição em massa para falso-positivo, consulte Edição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades. ◦ Cancelado(a) ◦ Fixo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os motivos Cancelado e Fixo não são aplicáveis a CVITs.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

6. Clique **em Editar**.

   Um trabalho assíncrono de edição em massa atualiza os registros relevantes.

Solicitar exceções para tarefas de correção e registros do Vulnerability Manager Workspace

A partir do Vulnerability Manager Workspace, os gerentes e analistas de vulnerabilidade podem solicitar exceções e falso-positivos para uma tarefa de correção (VUL, AVUL, CVUL ou CRG) e registrar (VIT, CVIT, AVIT ou TR). Você também pode dividir uma tarefa de correção e criar solicitações de mudança.

Função necessária:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para itens vulneráveis de host
- sn_vul.app_sec_manager para itens vulneráveis da aplicação
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin para itens vulneráveis de contêiner
- sn_vulc.admin para resultados de testes de configuração

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

No Vulnerability Manager Workspace, você pode executar o seguinte nos registros e nas tarefas de correção:

- Divida uma tarefa de correção (VUL, AVUL, CVUL e CRG).
- Solicite uma exceção para um registro (VIT, AVIT, CVIT ou CTR) ou tarefa de correção (VUL, AVUL, CVUL ou CRG).
- Solicite uma exceção à política para registros (VIT, AVIT ou CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG).
- Crie uma solicitação de mudança para a tarefa de correção (VUL, CVUL ou CRG).
- Solicite um falso-positivo para o registro (VIT, AVIT ou CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG).

Nota: Você pode gerar solicitações de falso-positivo para um conjunto de resultados de testes e tarefa de correção (CRG) a partir da v22.0 de Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você inicia essas ações de IU a partir de registros no Vulnerability Manager Workspace, da mesma forma que os proprietários de correção executam essas tarefas no Espaço de correção de problemas de TI.

Consulte os seguintes tópicos para obter mais informações:

- Solicitar um falso-positivo no Espaço de correção de problemas de TI
- Solicitar uma exceção no Espaço de correção de problemas de TI
- Solicitar redução de risco no Espaço de correção de problemas de TI
- Dividir uma tarefa de correção no Espaço de correção de problemas de TI
- Criar uma solicitação de mudança no Espaço de correção de problemas de TI
- Solicitar uma exceção usando GRC: Gestão de políticas e conformidade no Espaço de correção de problemas de TI
- Solicitar falso-positivo para um conjunto de resultados de testes

Informações relacionadas

Visão geral da Gestão de exceções

Conformidade de configurações Visão geral da Gestão de exceções

Solicitar exceção em massa no Espaço do gerenciador de vulnerabilidades

Edição em massa de falso-positivo no Espaço do gerenciador de vulnerabilidades

Tradução automática

Solicitar uma extensão para um item vulnerável adiado no espaço do Gerenciador de vulnerabilidades

Solicite uma extensão para um item vulnerável adiado antes que ele atinja a data de vencimento adiada até. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão do ambiente clássico.

Use o mesmo procedimento para solicitar uma extensão para um item vulnerável de aplicação, item vulnerável de contêiner, grupo de resultados de testes e uma tarefa de correção.

Procedimento

1. Navegar até **Espaços** > **Espaços do gerenciador de vulnerabilidades**.
2. Selecione Listas.
3. Em Itens vulneráveis de host, selecione **Todos**.
4. Filtre a lista selecionando adiado na coluna Estado.
5. Selecione um item vulnerável adiado.

   Nota: O botão Solicitar extensão fica visível somente quando o estado do item vulnerável é Adiado.

6. Selecione o botão **Solicitar extensão**.
7. Preencha os campos no formulário, conforme o apropriado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Controle de mitigação em vigor ◦ Outro
Informação adicional	Insira outras informações relevantes.

8. Selecione **Solicitar extensão**.
   Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

   Nota:
   - A solicitação passa por dois níveis de aprovação.
   - Se um item vulnerável adiado for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

9. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Informações de referência do Espaço para gerentes de vulnerabilidade

Os tópicos a seguir fornecem links, informações de referência, além de dados de campo nos formulários e registros encontrados nos espaços do Gerenciador de vulnerabilidades.

Campos de formulário Criar tópico de observação

A tabela a seguir descreve os campos no formulário Criar tópico de observação no Espaço do gerenciador de vulnerabilidades.

Campo	Descrição
Nome	Nome do tópico de observação, por exemplo, `IVs críticos`.
Pertencente a	O nome do usuário proprietário do tópico de observação.
Ordem de exibição	Insira um valor entre 100 e 1000. 100 é o valor padrão. Valores inferiores começando com 100 são exibidos em ordem crescente nas listas.
Grupo responsável	O nome do grupo proprietário do tópico de observação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Ative ou desative o tópico de observação. O padrão é selecionado (ativo).
Lista de observação	Adicione nomes de usuários que recebem notificações e podem exibir o tópico de observação.
Descrição	Texto que descreve o tópico de observação. Este texto é exibido no campo Descrição quando você cria um esforço de correção a partir deste tópico de observação.
Categoria	Tipo de registro para o qual o tópico de observação está sendo criado. **Nota:** O campo **Categoria** aparece a partir da versão 18.0.
Visualização	Clique em **Visualizar** para ver uma lista de quantos registros suas condições de filtro retornam. **Nota:** A partir da versão 18.0, o botão **Visualizar** não está disponível.

Informações relacionadas

Criar um tópico de observação no Espaço do gerenciador de vulnerabilidades

Campos do formulário de exceção de solicitação do GRC

A tabela a seguir mostra as descrições de campo do formulário de exceção de solicitação do GRC.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não estiver selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção começa. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
	Nota: O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

Gerar campos de formulário de resumo de correção

A tabela a seguir mostra os campos no formulário Gerar resumo de correção.

Gerar campos de resumo de correção

Campo	Descrição
Caixa de seleção ativa	Esta caixa de seleção está ativada por padrão. Se você não quiser enviar notificações por e-mail, desative este campo.
Executar	Semanal é o padrão. Escolha uma opção na lista.
Dia	Segunda-feira é o padrão. Escolha uma opção na lista.
Hora	Defina um horário para entregar os e-mails. Selecione um fuso horário se quiser um fuso horário diferente do usado pela instância que executa o trabalho.

Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

A partir da v20.0 da Resposta a vulnerabilidades, como responsável pela correção, você pode solicitar a redução de risco de um item vulnerável de host ou tarefa de correção. E o gerente ou analista de vulnerabilidade pode aprovar essas solicitações de redução de risco.

Para obter mais informações sobre como solicitar a redução de risco e aprovar a aprovação da redução de risco, consulte Solicitar redução de risco no Espaço de correção de problemas de TI e Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace, respectivamente.

Quando uma solicitação de redução de risco é aprovada, a pontuação de risco é reduzida de acordo com o **valor desejado** (classificação de risco) no registro de aprovação de mudança de estado (VCA#). A pontuação de risco mais alta da classificação de risco desejada é atribuída ao registro quando sua solicitação de redução de risco é aprovada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O exemplo a seguir mostra como a Pontuação de risco e a Pontuação de risco original são atualizadas quando os controles de compensação são aplicados. As pontuações de risco mais altas padrão das classificações de risco são usadas no exemplo a seguir.

Impacto dos controles de remuneração na pontuação de risco e na pontuação de risco original

Cenário	Pontuação de risco	Pontuação de risco	Pontuação de risco original (Pontuação de risco calculado)
Dados anteriores à v20.0	2 - Alto	80	O campo não está disponível antes da v20.0.
Após o upgrade para v20.0	2 - Alto	80	Nulo
A pontuação de risco calculado muda para 90 durante a ingestão	1 - Crítico	90	Nulo
Quando você aplica controles de remuneração	3 – Médio	69	90
A pontuação de risco calculado muda para 70 durante a ingestão	3 – Médio	69	70
A pontuação de risco calculado muda para 50 durante a ingestão	3 – Médio	50	50
A pontuação de risco calculado muda para 80 durante a ingestão	3 – Médio	50	80
Quando os controles de remuneração expiram em **Até a data para redução de risco**	2 - Alto	80	Nulo

Impacto dos controles de compensação em uma tarefa de correção

Quando sua solicitação de redução de risco é aprovada para uma tarefa de correção, o impacto dos controles de compensação em seus itens vulneráveis é o seguinte:

- Os controles de remuneração aplicados na tarefa de correção são aplicados em seus itens vulneráveis (exceto aqueles no estado Fechado) que têm pontuação de risco maior do que a pontuação de risco correspondente ao **valor desejado** na aprovação de mudança de estado de uma tarefa de correção. E a pontuação de risco desses itens vulneráveis é reduzida de acordo com o **valor desejado**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A **data Até para redução de risco** permanece inalterada para os itens vulneráveis nos quais um controle de compensação já foi aplicado. Ele não é atualizado com a **data Até para redução de risco** da Tarefa de correção.
- A **data Até para redução de risco** é revertida para os itens vulneráveis somente quando um controle compensatório não é aplicado em nenhum item vulnerável anteriormente. Se você aplicar os controles compensatórios na tarefa de correção novamente, a **data Até para redução de risco** não será revertida para os itens vulneráveis, já que a **data Até existente para redução de risco** dos itens vulneráveis terá prioridade.
- Quando um novo item vulnerável é adicionado a uma tarefa de correção na qual os controles compensatórios já estão aplicados, o risco não é revertido para o item vulnerável.

Impacto de um controle de remuneração em um item vulnerável

Quando sua solicitação de redução de risco é aprovada para um item vulnerável:

- Its nova pontuação de risco é exibida no campo **Pontuação de risco** e a pontuação de risco antiga (pontuação de risco calculada) é movida para o campo **Pontuação de risco original**. Esta mudança é válida até a data especificada no campo **Até a data para redução de risco**.
- Quando um item vulnerávelnerável tem controles de remuneração já aplicados, durante a ingestão:
  - Se a pontuação de risco calculada for maior do que a pontuação de risco, a pontuação de risco permanecerá a mesma e a pontuação de risco original será atualizada com a pontuação de risco calculada.
  - Se a pontuação de risco calculada for menor do que a pontuação de risco, a pontuação de risco e a pontuação de risco original serão atualizadas com a pontuação de risco calculada.
- Se um item de configuração(IC) for alterado para um item vulnerável ao qual um controle de compensação já foi aplicado:
  - O IC é atualizado para um item vulnerável por padrão, já que a propriedade do sistema *sn_sec_cmn.update_on_ci_change* está definida como verdadeira.

    O controle de remuneração ainda é aplicável ao item vulnerável.
  - O item vulnerável será encerrado e um novo item vulnerável será criado se a propriedade do sistema *sn_sec_cmn.update_on_ci_change* estiver definida como falsa.

    O controle de remuneração aplicado ao item vulnerável antigo é aplicado ao novo item vulnerável e a **data Até para redução de risco**, a Pontuação de **risco original e a Pontuação** de **risco** permanecem as mesmas.
- Quando um item vulnerável é reaberto pelo scanner e o controle de compensação já está aplicado a ele, o mesmo controle de compensação é aplicado depois que ele é reaberto.

Informações relacionadas

Noções básicas sobre controles de remuneração para redução de risco

Adicionar um controle de compensação à biblioteca

Associar controles de remuneração a CVEs ou TPEs para solicitações de redução de risco

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

#unique_126_Connect_42_li-risk-reduction-vmws

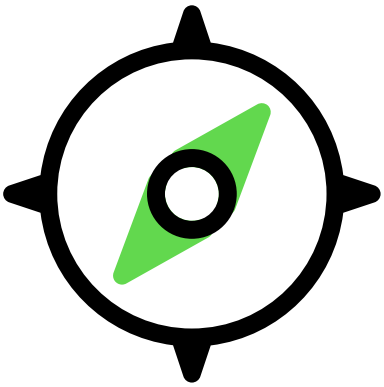
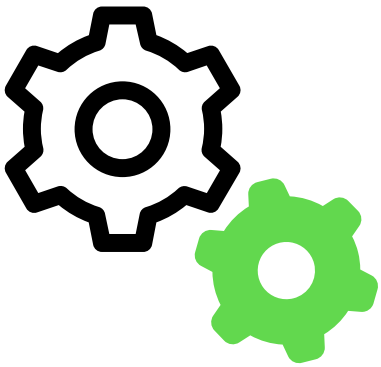
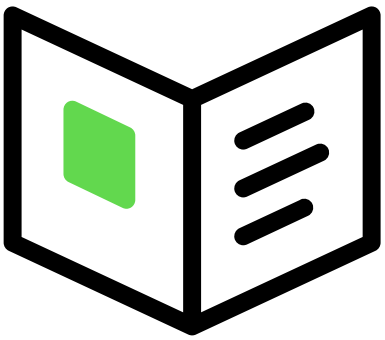
Espaço de correção de problemas de TI

As equipes de TI visualizam tarefas e informações centradas em TI, como soluções e itens de configuração afetados. As equipes de TI podem economizar tempo na resolução de vulnerabilidades criando facilmente solicitações de mudança, verificando novamente itens vulneráveis e enviando solicitações de exceção no espaço de correção de TI.

Visão geral

Demonstração do espaço de correção de TI v18.0

Iniciar

Explorar	Corrigir	Referência
		
Saiba mais sobre o Espaço de correção de TI	Saiba como corrigir vulnerabilidades e erros de configuração no IT Remediation Workspace	Saiba mais sobre as informações adicionais necessárias para usar o Espaço de correção de TI

Tradução automática

Solucionar problemas e obter ajuda

- Operações de segurança na comunidade da ServiceNow
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorar o Espaço de correção de problemas de TI

O Espaço de correção de problemas de TI se destina a proprietários de correção de TI e grupos de TI. Ele é composto por exibições iniciais e de lista, bem como visualizações de dados nas quais você pode clicar que permitem ver as tarefas de correção atribuídas a você e quantos registros atribuídos a você têm soluções.

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_chamion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

O Espaço de correção de problemas de TI consiste nas seguintes páginas principais, listas e formulários:

Página principal (Inicial)

A página inicial inicial consiste em uma lista de tarefas de correção atribuídas a você e quais registros atribuídos a você têm soluções.

Você pode clicar em uma tarefa de correção para exibir os detalhes e iniciar uma investigação. Na exibição Listas, você pode exibir os Esforços de correção, Tarefas de correção, Itens vulneráveis, Resultados de testes de configuração e assim por diante. Você pode abrir uma tarefa de correção e clicar em **Atribuir a mim** para atribuir a tarefa a você mesmo e iniciar a investigação.

Nota: Se você não atribuir a tarefa a si mesmo na tarefa de correção, não poderá exibir nenhuma ação de IU no nível do item vulnerável.

Clique nas reticências Mais ações e clique em **Iniciar investigação** para resolver uma tarefa de correção.

Um cartão de pontuação adicional, **ICs vulneráveis**, é exibido na exibição inicial. A visualização de dados de ICs vulneráveis mostra itens de configuração que têm IVs atribuídos a você ou a seus grupos. Para obter mais informações, consulte Exibir itens de configuração com vulnerabilidades no Espaço de correção de problemas de TI.

A página exibida inclui as seguintes informações:

- Tarefas de correção ativas atribuídas a você.
- Registros atribuídos a você que têm soluções preferenciais.
- A lista de tarefas de correção atribuídas a você.

Para obter mais informações sobre o que você pode fazer nesta página, consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI.

Página Painéis

A página de painéis consiste no painel de correção de vulnerabilidade. Para obter mais informações sobre a página Painéis, consulte Visão geral dos painéis.

Página da lista

Essa exibição consiste em páginas de lista padrão e personalizadas para Tarefas de correção, Itens vulneráveis, Soluções e Solicitações de exceção atribuídas a você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Listas: listas padrão de Tarefas de correção, Itens vulneráveis de host, Itens vulneráveis de aplicação, Itens vulneráveis de contêiner e Resultados de testes de configuração atribuídos a você e seu grupo, Soluções e Solicitações de exceção.
- Minhas listas - Esta exibição mostra todas as listas que você renomeou na página principal Lista e todas as listas que você cria.

A exibição de lista é exibida com links para trabalhos atribuídos a você e seus grupos, itens vulneráveis atribuídos a você e seus grupos, soluções e suas solicitações de exceção.

Você também pode criar suas próprias listas para ajudá-lo a monitorar o andamento da correção.

As listas de **ICs vulneráveis** são exibidas na exibição de lista. A lista Soluções será exibida se a aplicação Gestão de soluções para vulnerabilidades estiver instalada. Este cartão mostra dados de solução, soluções potenciais e preferenciais de fornecedores terceirizados sobre seus itens vulneráveis.

Para obter mais informações sobre o que você pode fazer nesta página, consulte Use a exibição de lista no Espaço de correção de problemas de TI.

Exibir um exemplo de fluxo de trabalho no Espaço de correção de problemas de TI

Veja um exemplo de um fluxo de trabalho de ponta a ponta no Espaço de correção de problemas de TI. Veja como os especialistas em TI podem usar o espaço para monitorar itens vulneráveis críticos e corrigir as vulnerabilidades atribuídas a eles.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_chamion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Procedimento

Clique na imagem a seguir para exibir as etapas do fluxo de trabalho.
Demonstração do espaço de correção de TI

A imagem inclui as seguintes tarefas:

- Na página inicial (Página principal do responsável pela correção de TI), exiba as tarefas de correção atribuídas a você. Alterne entre o trabalho atribuído a você e seu grupo. Consulte as tarefas de correção que têm soluções.
- Clique na exibição de **lista** para ver as listas do trabalho atribuído.
- Na exibição de lista com a lista **Atribuído ao meu grupo** selecionada, identifique e atribua o trabalho a você mesmo.
- Em um registro de tarefa de correção em aberto:
  - Clique na guia **Visão geral** para ver os itens vulneráveis (IVs) e os itens de configuração (ICs) afetados que estão associados ao registro.
  - Clique na guia **Soluções** para ver as soluções preferenciais e potenciais.
  - Clique na guia **Detalhes** para modificar os campos editáveis.
  - Clique nas ações de IU: **Marcar como falso positivo**, **Criar mudança**, **Dividir tarefa**, **Solicitar exceção**. Siga os avisos nas caixas de diálogo para ajudá-lo na correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral dos painéis

A página Painéis no Espaço de correção de problemas de TI fornece o painel de correção de vulnerabilidade na IU Next Experience, que pode ser usado para se concentrar nas tarefas de correção e nos itens vulneráveis.

Como proprietário de correção (sn_vul.remediation_owner), você pode acessar o painel de correção de **vulnerabilidade** navegando até **Espaços** > **Espaço de correção de TI** e selecionando o ícone Painéis. Para obter mais informações sobre o painel Correção de vulnerabilidades, consulte Usando os painéis padrão Resposta a vulnerabilidades.

Você pode criar um painel personalizado selecionando o ícone ⋮ e selecionando **Criar novo painel**.

Usando o Espaço de correção de problemas de TI

O Espaço de correção de TI fornece uma lista consolidada de vulnerabilidades de host, vulnerabilidades de aplicação, vulnerabilidades de contêiner e erros de configuração atribuídos a você e seu grupo. Você pode usar este espaço para corrigir e solicitar exceções para vulnerabilidades e erros de configuração.

Use o resumo de e-mail nos Espaços de resposta a vulnerabilidades

Use notificações por e-mail para exibir o andamento da correção e lembrá-lo quando as tarefas estiverem se aproximando ou já tiverem passado do ANS.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_chamion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Como proprietário de correção, entre em sua área de trabalho e veja sua notificação por e-mail como um resumo do seu trabalho. Veja o que você realizou, o que está se aproximando e o que está atrasado. Use a notificação para ajudá-lo a organizar e priorizar suas ações de correção críticas. Clique em um link no e-mail para acessar diretamente o seu espaço. As notificações podem ajudar os especialistas em TI a visualizar rapidamente o status de seu trabalho. Como gerenciador de vulnerabilidades, ajude seus especialistas em TI a acessar a plataforma diretamente do serviço de e-mail para tarefas de correção.

Consulte Configurar notificações por e-mail nos espaços Resposta a vulnerabilidades para obter mais informações sobre como configurar este recurso.

O e-mail, por padrão, mostra as tarefas que você fechou, o total de tarefas ativas atribuídas a você e seus grupos, recém-atribuídas, VITs fechadas e outras informações.

Procedimento

1. Navegue até o seu e-mail, localize uma notificação e clique para abri-la.
   A notificação é exibida com informações sobre seu status de trabalho.
2. Clique **em Ir para o espaço** para navegar até sua área de trabalho.

Use a exibição de lista no Espaço de correção de problemas de TI

Com a exibição de lista no Espaço de correção de problemas de TI, você pode exibir tarefas de correção e registros atribuídos a você e seus grupos. Você também pode rastrear suas solicitações de exceção e falso-positivo para tarefas de correção, itens vulneráveis e resultados de testes e exibir soluções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Clique no ícone Lista.
   A exibição de lista é exibida.
   - Clique em uma lista filtrada para exibir o número total de tarefas de correção ativas ou registros atribuídos a você ou ao seu grupo. Consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI para obter mais informações sobre o que você pode fazer com esses registros.
   - Exiba o número total de IVs atribuídos a você ou aos seus grupos que têm soluções. Clique no cartão **Soluções preferenciais em VIs** para exibir a lista.
   - Veja os ICs vulneráveis atribuídos a você e seus grupos que têm vulnerabilidades sobre eles na guia **ICs vulneráveis** ou na lista de ICs vulneráveis atribuídos a você e seu grupo na exibição de lista.
3. Opcional: Clique **em Minhas listas**.

   (Optional) Para criar uma nova lista, siga estas etapas:

   a. No canto inferior esquerdo da página, clique em **Nova lista**.

   b. No modal Nova lista, clique em **Iniciar a partir de existente** e pesquise na lista de seleção Lista uma lista existente para usar como modelo.

   c. Edite o Nome da Lista.

   d. Adicionar filtros.
   Por exemplo, você pode criar uma lista de itens vulneráveis ativos para um scanner específico que deseja monitorar. Por exemplo, você pode usar os filtros: `Ativo é verdadeiro`e A `origem contém (nome do seu scanner)`.

   e. Edite as colunas que você deseja exibir na lista.

   f. Clique em **Criar**.
   Sua nova lista será exibida.

   g. Como alternativa, clique em **Criar o seu próprio**, insira um nome e, em seguida, **Selecionar origem**.

   h. Comece a digitar no campo e selecione nas origens que são exibidas para sua nova lista.

   i. Clique em **Criar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sua nova lista será exibida.

Nota: Se você sair do módulo de lista, a lista exibida ao sair será a lista que você vê ao retornar. Para excluir as listas personalizadas que você cria, com a lista exibida, à direita do painel, clique no ícone de engrenagem.

4. Consulte a tabela a seguir para saber o que você pode fazer na exibição de lista.

Tarefa	Descrição
Clique em Minhas listas	Crie novas listas e exiba as listas que você criou. No modal exibido, crie outra versão de uma lista existente ou uma nova. As listas que você cria são exibidas na guia Minha lista. Para excluir uma lista, com a lista exibida, na extrema direita da página, clique no ícone de engrenagem.
Atribuir registros de tarefa de correção a você mesmo	Na guia Listas com **Atribuído ao meu grupo** selecionado, clique em um registro de tarefa de correção (VUL) para abri-lo. No registro exibido, clique em **Atribuir a mim**. Esta opção só estará disponível se uma tarefa de correção ainda não estiver atribuída a você.
Abrir uma tarefa de correção (VUL)	Com um registro de tarefa de correção exibido, clique em um item da lista relacionada para abrir e exibir os seguintes detalhes: ◦ Visão geral - Exiba o andamento da correção e outros detalhes da tarefa de correção. ◦ Soluções - Exiba as soluções preferenciais e potenciais que você pode usar para corrigir a vulnerabilidade. Na guia Soluções, os itens da lista relacionada secundária mostram as Soluções preferenciais e Possíveis soluções. ◦ Detalhes — Mais informações de visão geral, incluindo a vulnerabilidade associada. Você pode editar esses campos. ◦ Solicitações de mudança - Exiba as solicitações de mudança associadas ao registro. ◦ Aprovações solicitadas - Exiba as aprovações solicitadas. Se não houver aprovações de solicitação de mudança, este item de lista relacionado não será exibido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	◦ Aprovações de mudança de estado - exibe as solicitações de falso-positivo e de exceção associadas a este registro. Se não houver solicitações, este item da lista relacionada não será exibido. Os registros abertos permanecem exibidos como guias até que você os feche. Consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI para saber o que você pode fazer a partir do registro da tarefa de correção.
Abrir um registro de item vulnerável (VIT)	Com um registro de item vulnerável exibido, clique em um item da lista relacionada para abrir e exibir os seguintes detalhes: ◦ Visão geral - O ativo afetado, a vulnerabilidade associada, a detecção inicial e outros detalhes sobre o estado e a data de destino. ◦ Detalhes - Mais informações de visão geral, incluindo a solução preferencial, se disponível. Você pode editar esses campos. ◦ Detecções - Primeiro encontrado, último encontrado, endereço IP, porta, protocolo e informações de prova, se disponíveis. ◦ Serviços afetados - Criticidade dos negócios, grupo de suporte e serviço ◦ Tarefas de correção - As tarefas de correção às quais este IV está associado. Os registros de VIT abertos permanecem exibidos como guias até que você os feche. Consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI para saber o que você pode fazer a partir do registro da tarefa de correção.
Definir filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, em uma lista de itens vulneráveis selecionados, talvez você prefira classificar a coluna Classificação de risco para que somente os itens críticos sejam exibidos.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	◦ Mostrar correspondência — Exibe somente itens que correspondem à célula selecionada na coluna. ◦ Remover do filtro — Filtra os itens da coluna que correspondem à célula selecionada na coluna.
Na exibição de lista, à esquerda da coluna Número com uma lista exibida, passe o mouse sobre uma linha e clique no pequeno ícone de informações (i) de um registro.	Detalhes sobre os registros são exibidos no painel do lado direito da página.

Usar registros no Espaço de correção de problemas de TI

Use registros para ajudá-lo a exibir o andamento da correção e o impacto dos itens vulneráveis em seus ativos.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Procedimento

1. Em sua instância Now Platform, navegue até **Espaços** > **Espaço de correção de TI**.
   A página principal inicial é exibida.
2. Navegue até um registro de item vulnerável e abra-o na página inicial inicial ou na exibição de lista.

   A guia de detalhes inclui informações no cabeçalho do formulário na parte superior que estão relacionadas à natureza da vulnerabilidade, por exemplo, `CVE-2013-5014 detectado em LINUX-DAL-4331`. No cabeçalho do formulário, os valores de Estado, Classificação de risco e Data de meta de correção são exibidos.
3. Consulte a tabela a seguir para ver as ações de IU que você pode executar no registro da tarefa de correção.

Tarefa	Descrição
Clique em um link de Itens relacionados	◦ Visão geral - Exiba detalhes como estado, classificação de risco, pontuação de risco, origem, último encontrado, status de correção, vulnerabilidade associada, item de configuração afetado e informações de detecção inicial. ◦ Detalhes - Mais informações de visão geral, incluindo a solução preferencial. Você pode editar esses campos. ◦ Detecções - Exibir informações de detecção importadas de seus scanners.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	◦ Serviços afetados - Exiba os serviços afetados pela vulnerabilidade. ◦ Tarefas de correção - exibe as outras tarefas de correção associadas a este item vulnerável. Os registros abertos do VIT permanecem exibidos como guias nas guias de registro até que você os feche.
Clique em um link para abrir um registro	Na lista exibida em registros abertos dos links de itens relacionados, veja mais detalhes sobre as tarefas de correção, detecções e serviços afetados.
Clique em uma ação de IU	◦ Atribuir a mim - Esta opção só será exibida se a tarefa de correção ainda não estiver atribuída a você. ◦ Marcar como falso-positivo - Relate quando um scanner encontrar uma vulnerabilidade, mas você determinar que não existe nenhuma vulnerabilidade. Envie uma solicitação. ◦ Se o item vulnerável estiver atribuído a você, será possível verificar novamente o VI. ◦ Resolver — Resolver este item vulnerável. As tarefas de correção associadas fazem a transição para Resolvido quando todos os seus IVs são Resolvidos. ◦ Exceção de solicitação - Se uma data de destino for aprovada e você souber que precisa de mais tempo para resolver a vulnerabilidade, envie uma solicitação. ◦ Salvar - Salve as mudanças e atualize o registro.
Adicionar uma anotação de trabalho ou anexar um arquivo	Na extrema direita da tela, clique no ícone **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.
Definir filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, com o item relacionado Detecções selecionado, talvez você prefira classificar a coluna para que somente as úl-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	timas detecções encontradas a partir de uma determinada data sejam exibidas.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ◦ Mostrar correspondência - exibe somente itens que correspondem à célula selecionada na coluna. ◦ Remover do filtro — Filtra os itens da coluna que correspondem à célula selecionada na coluna.

Usar registros de tarefa de correção no Espaço de correção de problemas de TI

As tarefas de correção são criadas e atribuídas automaticamente a partir dos esforços de correção. As equipes de TI e os responsáveis pela correção podem exibir as tarefas de correção no Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Quando os gerentes e analistas de vulnerabilidade criam esforços de correção para orientar a correção, as tarefas de correção são criadas automaticamente e atribuídas a equipes de TI com base no grupo que está associado aos registros em um esforço de correção.

Veja os ICs vulneráveis atribuídos a você e seus grupos que têm vulnerabilidades sobre eles na guia **ICs vulneráveis** ou na lista de ICs vulneráveis atribuídos a você e seu grupo na exibição de lista.

Procedimento

1. Em sua instância Now Platform, navegue até **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
   A página principal inicial é exibida.
2. Na seção Tarefas de correção, clique em um registro de tarefa de correção (VUL) para abri-lo.
3. Opcional: Como alternativa, você pode clicar no ícone Lista no canto superior esquerdo da página inicial para ver todas as tarefas de correção e registros (trabalho) atribuídos a você e seus grupos.
   Para obter mais informações sobre como usar a exibição de lista, consulte Use a exibição de lista no Espaço de correção de problemas de TI.
4. Na página inicial ou na exibição de lista, clique em um registro de tarefa de correção (VUL) para abri-lo.

   A imagem a seguir mostra as seções de um registro de tarefa de correção e os dados que estão disponíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Entre as guias **Soluções** e **Solicitações de mudança** nas guias da lista relacionada mostradas na imagem a seguir, você pode clicar na guia **Detalhes** para atualizar algumas das informações no registro, como grupo de atribuição, por exemplo. Clique em **Salvar** para aplicar suas mudanças.

A guia de detalhes inclui informações no cabeçalho do formulário na parte superior que estão relacionadas à natureza da tarefa, por exemplo, `Vulnerabilidades nos servidores XYZ (San Diego)`. No cabeçalho do formulário, são exibidos os valores de Estado, Classificação de risco, Grupo de atribuição, Status da correção e a porcentagem de registros ativos que você corrigiu.

5. Consulte a tabela a seguir para ver as ações de IU que você pode executar a partir do registro da tarefa de correção.

Tarefa	Descrição
Clique em um link de itens relacionados	◦ Visão geral: exiba o andamento da correção com % de IVs corrigidos, o estado, a classificação de risco, o grupo de atribuição, os ICs afetados e outros detalhes da tarefa. Para ver os ICs afetados, consulte a imagem após a tabela. ◦ Soluções - Exiba as soluções preferenciais e potenciais que você pode usar para corrigir a vulnerabilidade. No registro que é exibido, os itens da lista relacionada secundária mostram as Soluções preferenciais e Possíveis soluções. Veja as imagens abaixo da tabela. ◦ Detalhes — Mais informações de visão geral, incluindo a vulnerabilidade associada. Você pode editar esses campos. ◦ Solicitações de mudança - Exiba as solicitações de mudança associadas ao registro. ◦ Aprovações solicitadas - Exiba os envios de solicitações de mudança. Se não houver solicitações de aprovação de solicitação de mudança, este item de lista relacionado não será exibido. ◦ Aprovações de mudança de estado - exibe as solicitações de falso-positivo e de exceção associadas a este registro. Se não houver solicitações, este item da lista relacionada não será exibido. Os registros abertos permanecem exibidos como guias até que você os feche.
Clique em um link para abrir um registro	Na lista exibida em registros abertos dos links de itens relacionados, veja mais detalhes sobre os registros, as vulnerabilidades associadas, ICs afetados (ativos), dados de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	detecção, serviços afetados e registrosassociados.
Clique em uma ação de IU	◦ Atribuir a mim - Esta opção só será exibida se a tarefa de correção ainda não estiver atribuída a você. ◦ Marcar como falso positivo - Envie uma solicitação se, por exemplo, um scanner encontrar uma vulnerabilidade, mas você determinar que não existe nenhuma vulnerabilidade. ◦ Criar mudança - Você pode criar uma nova solicitação de mudança ou adicionar esta tarefa de correção a uma solicitação de mudança existente. ◦ Dividir tarefa - Identifique um subconjunto de IVs que você deseja incluir em uma nova tarefa de correção ◦ Exceção de solicitação - Envie uma solicitação se uma data de destino for aprovada e você souber que precisa de mais tempo para resolver a vulnerabilidade. ◦ Resolver - Resolva este RT. A tarefa de correção faz a transição para Resolvido e todos os seus IVs fazem a transição para Resolvido. ◦ Salvar - Salve as mudanças e atualize o registro.
Adicionar uma anotação de trabalho ou anexar um arquivo	Na extrema direita da tela, clique no ícone **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel. Você também pode carregar um arquivo.
Definir filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu vertical de três pontos para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, com o item relacionado à visão geral selecionado, talvez você prefira classificar a coluna Classificação de risco para que somente os itens críticos sejam exibidos.
Filtrar uma coluna por uma linha selecionada	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	◦ Mostrar correspondência - exibe somente itens que correspondem à célula selecionada na coluna. ◦ Remover do filtro - filtra os itens da coluna que correspondem à célula selecionada na coluna.

A guia Soluções mostra as informações da solução preferencial e potencial que melhor corresponde à vulnerabilidade associada ao registro da tarefa. Soluções são patches que suas equipes de TI aplicam para resolver vulnerabilidades.

Se a aplicação Gestão de soluções de vulnerabilidade estiver instalada, as Soluções preferenciais serão as soluções de maior substituição aplicadas a registros. A lista de soluções se baseia nos registros na tarefa de correção.

Para exibir as soluções, no registro da tarefa de correção, navegue até **Soluções** > **Soluções preferenciais**.

Possíveis soluções. Todas as soluções disponíveis para IVs nesta tarefa. Navegar até **Soluções** > **Soluções potenciais**.

Você pode exibir os ICs (ativos) afetados por esta vulnerabilidade no registro da tarefa de correção navegando até **Visão geral** > **ICs afetados**.

Atribuir uma tarefa de correção ou registro a si mesmo no Espaço de correção de problemas de TI

Atribua uma tarefa de correção (VUL, AVUL, CVUL ou CRG) ou registro (VIT, AVIT, CVIT ou TR) a si mesmo na página Lista no espaço Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Esta opção só está disponível em registros de tarefa de correção que ainda não foram atribuídos a você.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI** > **Exibição em lista** > **Atribuído ao meu grupo**.
2. Clique em uma tarefa de correção (VUL, AVUL, CVUL ou CRG) para abri-la.
3. Nos botões de ação de IU à direita, clique em **Atribuir a mim**.

   O botão **Atribuir a mim** só estará disponível se o registro ainda não estiver atribuído a você.

   A tarefa de correção é exibida na lista Atribuído a mim em Tarefas de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Você também pode atribuir um registro [(VIT, AVIT, CVIT ou TR) a si mesmo seguindo as mesmas etapas de um registro aberto.
   O botão **Atribuir a mim** só estará disponível se o registro ainda não estiver atribuído a você.

Exibir itens de configuração com vulnerabilidades no Espaço de correção de problemas de TI

As seguintes melhorias foram adicionadas às tarefas de correção com a versão 16.1 da aplicação Resposta a vulnerabilidades.

Antes de Iniciar
Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

A função itil ou cmdb_read também será necessária se você quiser exibir dados de IC nos espaços.

Por Que e Quando Desempenhar Esta Tarefa
Consulte os itens de configuração (IC) atribuídos a você que têm vulnerabilidades. Clique em Cartão de pontuação de **ICs vulneráveis**. Clique na lista Filtro no canto superior esquerdo para alternar entre **Atribuído a mim** e **Atribuído aos meus grupos**. Na exibição de lista, clique nos links.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
   A página principal inicial é exibida.
2. Como alternativa, você pode exibir essas listas nos links na exibição de lista ou navegando até seus módulos, por exemplo, **Todos** > **Resposta a vulnerabilidades** > **Tarefas de correção**.
3. Escolha um para continuar.
   Dependendo do que estiver selecionado na alternância de filtro, exiba as listas dos seguintes registros atribuídos a você ou a você e seus grupos.

Opção	Descrição
Tarefas de correção atribuídas	Tarefas de correção (RT). Para obter mais informações sobre as ações que você pode realizar em um RT, consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI.
Solução preferencial em VIs	Registros que têm soluções preferenciais mapeadas para eles. Se a aplicação Gestão de soluções de vulnerabilidade estiver instalada, as Soluções preferenciais serão as soluções de maior substituição aplicadas aos registros. A lista de soluções é baseada nos registros no registro da tarefa de correção. Para ver o que você pode fazer com os registros de solução, consulte Usar regis-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	tros de tarefa de correção no Espaço de correção de problemas de TI.
ICs Vulneráveis	(IC)s com vulnerabilidades. Após o preenchimento inicial, este cartão de pontuação mostra contagens atualizadas de seus ICs vulneráveis depois que novos IVs com vulnerabilidades são adicionados ou quando há mudanças de estado nos IVs existentes. Consulte as etapas a seguir para saber como exibir este registro e o que você pode fazer nesta lista.

4. Clique no cartão de pontuação de **ICs vulneráveis**.

   A lista de registros de IC é exibida.

5. Clique em um item de configuração para abrir seu registro.
   O registro é exibido.

   As listas relacionadas permitem que você exiba detalhes e vários registros associados. Os novos dados disponíveis neste registro com esta versão incluem:

   - Uma linha do tempo que mostra a atividade recente neste registro.
   - Todas as solicitações de mudança associadas a este IC.
   - Navegue facilmente até os cartões de pontuação e exiba as tarefas de correção, itens vulneráveis e soluções preferenciais associadas a este IC.
   - Vocêpode navegar até os cartões de pontuação e exibir os patches preferenciais associados a este IC. Patches preferenciais são os patches associados aos itens vulneráveis. A guia Patches na Lista relacionada exibe os patches instalados e ausentes para os ICs.
   - Informações sobre o IC que incluem Classe, Local, Voltado para a Internet, Ambiente e Cronograma de manutenção.

Criar uma solicitação de mudança no Espaço de correção de problemas de TI

A partir de uma tarefa de correção (VUL, CVUL ou CRG), crie uma solicitação de mudança. Como alternativa, adicione uma tarefa de correção a uma solicitação de mudança existente.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host
- sn_vul.app_security_campion para itens vulneráveis de contêiner
- sn_vulc.remediation_owner para resultados de testes de configuração

Nota: A função itli será necessária se você quiser enviar solicitações de mudança do Espaço de correção de problemas de TI.

Por Que e Quando Desempenhar Esta Tarefa

Pode haver vários motivos para você criar uma solicitação de mudança para uma tarefa de correção. Normalmente, isso ocorre porque sua investigação requer intervenção manual para corrigir as vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre as solicitações de mudança e a criação de solicitações de mudança no ambiente clássico, consulte Gestão de mudanças para Resposta a vulnerabilidades.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Na página Lista, na lista Tarefa de correção, localize uma tarefa de correção para a qual você deseja criar uma solicitação de mudança.
3. Nos botões de ação de IU à direita, expanda a lista e escolha uma:
   - Clique **em Criar mudança**
   - **Adicionar a uma mudança existente**
4. Para criar uma nova solicitação de mudança, no modal exibido, preencha os campos. Para mais informações sobre campos de formulário, consulte Criar campos de formulário de solicitação de mudança.
5. Selecione **Criar solicitação de mudança**.
   O registro da tarefa de correção é exibido e uma mensagem indica que a solicitação de mudança foi criada com sucesso.

   Clique no link relacionado Solicitações de mudança em um registro para exibir todas as solicitações de mudança associadas ao registro.
6. Como alternativa, para adicionar esta tarefa de correção a uma solicitação de mudança existente, siga estas etapas.

   a. Clique na seta para baixo para expandir a lista no botão **Criar mudança**.

   b. Selecione **Adicionar à mudança existente**.

   c. No modal exibido, clique no ícone de pesquisa para exibir a lista de solicitações de mudança existentes.

   d. Para adicionar condições à lista para enfocar a lista de solicitações de mudança, no canto superior direito do modal, clique no ícone de filtro (funil).

   e. No novo painel exibido, clique **em Exibição avançada**.

   f. Use o Construtor de condições para criar suas condições.

   g. Selecione **Atualizar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

h. Na lista, clique em uma solicitação de mudança para selecioná-la.
Um modal atualizado é exibido com sua escolha.

i. Opcional: No modal, marque a caixa de seleção Adicionar ICs ao CR para adicionar itens de configuração de todos os itens vulneráveis ativos à solicitação de mudança.

j. Selecione **Adicionar mudança**.
O registro de correção é exibido e uma mensagem indica que a solicitação de mudança foi criada com sucesso e enviada para aprovação.

- Clique no link **Exibir mudança** na mensagem para abrir o registro de solicitação de mudança (CHG).
- Selecione o link do menu do item relacionado às **solicitações de mudança** no registro da tarefa de correção para exibir todas as solicitações de mudança associadas ao registro.

Como alternativa, no ambiente clássico, navegue até **Autoatendimento** > **Minhas solicitações**. Depois de enviar a mudança e ela ser implementada, se a sincronização de estado estiver habilitada, a tarefa de correção será movida automaticamente para `Resolvido`. Para obter mais informações sobre estados e sincronização de estado em solicitações de mudança, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção.

Dividir uma tarefa de correção no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, identifique um subconjunto de itens vulneráveis ou resultados de testes e crie uma nova tarefa de correção para eles.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Você pode selecionar itens vulneráveis individuais na lista exibida na guia Itens vulneráveis e movê-los para uma nova tarefa de correção.

Os casos de uso para dividir IVs de tarefas de correção existentes em novas tarefas podem incluir os seguintes exemplos:

- Você deseja criar uma solicitação de mudança ou solicitações de mudança para um grupo dividido.
- Você deseja reatribuir um grupo dividido a outro usuário em seu grupo de atribuição.
- Você solicita um adiamento ou uma exceção para um grupo dividido porque sabe que algumas vulnerabilidades em itens de configuração (ICs) específicos não podem ser corrigidas até a data prevista.

Para obter mais informações sobre solicitações de mudança e dividir uma tarefa de correção no ambiente clássico e para versões de Resposta a vulnerabilidades anteriores à v15.0, consulte Dividir uma tarefa de correção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da v19.0 de Resposta a vulnerabilidades, você pode dividir tarefas em grupos de resultados de testes.

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

A partir da versão 18.0, você pode dividir tarefas para itens de vulnerabilidade de aplicação e itens de vulnerabilidade de contêiner.

Procedimento

1. Com uma tarefa de correção exibida, clique na guia **Itens vulneráveis**, se ainda não estiver selecionada.
2. Na lista, selecione os IVs que você deseja mover para uma nova tarefa de correção.
3. Clique **em Dividir tarefa**.
4. Na caixa de diálogo exibida, o número de IVs selecionados na lista é exibido.
5. Clique **em Dividir tarefa** novamente.
   A mensagem de confirmação a seguir é exibida com um link para a nova tarefa de correção.

   Como alternativa, você pode usar o construtor de condições para filtrar IVs.
6. Localize uma tarefa de correção que você deseja dividir.
7. Nos botões de ação de IU à direita, clique em **Dividir tarefa**.
   Depois de alguns momentos, o construtor de condições é exibido.
8. No modal exibido, use o Construtor de condições para identificar o subconjunto de itens vulneráveis que você deseja a adicionar a uma nova tarefa de correção.
9. Clique **em Dividir tarefa**.
   Se uma mensagem exibir que nenhum item vulnerável corresponde às suas condições, você deverá ajustar os critérios e clicar em **Dividir tarefa** novamente. Edite o campo de descrição resumida conforme necessário. Este campo pode ajudá-lo a encontrar sua nova tarefa de correção depois que ela for criada.

   Se os IVs corresponderem às suas condições, o número de VIs correspondentes será exibido em uma mensagem, conforme mostrado na imagem anterior.
10. Opcional: Clique no link **Visualizar itens** para exibir os IVs que correspondem às suas condições de filtro.
    A nova tarefa de correção é exibida como uma nova guia na parte superior do registro.

Solicitar um falso-positivo no Espaço de correção de problemas de TI

Gere uma solicitação de falso-positivo para item vulnerável de host (VIT), item vulnerável de aplicação (AVIT), item vulnerável de contêiner (CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG) no Espaço de correção de problemas de TI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa
Um falso-positivo é uma condição em que o scanner relata que existe uma vulnerabilidade no sistema, mas, na verdade, não há vulnerabilidade. Pode haver vários motivos, como classificação incorreta, lógica ou algoritmo inadequados no scanner.

Para obter mais informações sobre como solicitar um falso-positivo para um conjunto de resultados de testes, consulte Solicitar falso-positivo para um conjunto de resultados de testes.

Procedimento
1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Localize uma tarefa de correção (VUL, AVUL, CVUL ou CRG) ou item vulnerável (VIT, AVIT ou CVIT) que você deseja marcar como falso-positivo.
3. Nos botões de ação de IU à direita, selecione **Marcar como falso-positivo**.
4. Na caixa de diálogo exibida, insira as informações sobre a solicitação e selecione **Solicitar aprovação**.
5. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação ao aprovador e selecione **Enviar**.

   Nota: O modal Responder questionário aparece somente quando a caixa de seleção **Habilitar questionário para marcar como falso-positivo** está marcada no formulário Configuração de gestão de exceções. Para obter mais informações, consulte Configurar Gestão de exceções para Resposta a vulnerabilidades,Configurar Gestão de exceções para Resposta a vulnerabilidades de aplicações, Configurar Gestão de exceções para Contêiner de Resposta a vulnerabilidadese Configurar Gestão de exceções para Conformidade de configurações.

   O estado do item vulnerável (VIT, AVIT ou CVIT) ou da tarefa de correção (VUL, AVUL ou CVUL) muda para Em revisão.

   Sua solicitação é enviada para aprovação e o aprovador recebe uma notificação por e-mail sobre sua solicitação.

Resultados
Você receberá uma notificação por e-mail após a aprovação ou rejeição da sua solicitação.

O que Fazer Depois
No Espaço de correção de TI, na página Lista, navegue até **Solicitações de exceção** > **Minhas solicitações** e abra o registro de aprovação de mudança de estado correspondente (VCA#) e verifique o status da sua solicitação na coluna Estado de aprovação:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado de aprovação	Registro (VIT, AVIT ou CVIT)	Tarefa de correção (VUL, AVUL, CVUL ou CRG)
Aprovado	O estado do registro muda para encerrado com o motivo como falso-positivo.	O estado das transições da tarefa de correção para encerrado com o motivo como falso-positivo. O estado é revertido para os registros na tarefa de correção. Navegue até a guia Detalhes de uma Tarefa de correção e defina a data de vencimento para falso-positivo no campo **Até**, se necessário. A tarefa de correção será revertida para o estado Aberto após a data especificada e o estado será revertido para os resultados de testes.
Rejeitado	O estado do registro não muda.	O estado da tarefa de correção e seus registros são revertidos para o estado anterior.

No **Fluxo de atividades** de um registro ou tarefa de correção, você pode exibir todo o fluxo de trabalho da solicitação de falso-positivo.

Informações relacionadas

Falso-positivo visão geral

Solicitar falso-positivo para um conjunto de resultados de testes

A partir da v22.0 de Resposta a vulnerabilidades, você pode gerar uma solicitação de falso-positivo para um conjunto de resultados de testes em uma tarefa de correção, no Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária: sn_vulc.remediation_owner

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Na página Lista, abra uma Conformidade de configurações Tarefa de correção.
3. No item relacionado Visão geral, na guia Resultados de testes, selecione os resultados de testes que você deseja marcar como falso-positivos.

Nota: Você pode solicitar um falso-positivo para um conjunto de resultados de testes em uma Tarefa de correção somente quando:

- Pelo menos um resultado de testes selecionado está no estado Ativo.
- A Tarefa de correção tem pelo menos dois resultados de testes.
- Todos os resultados de testes não estão selecionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione o botão **Marcar como falso-positivo** na guia Resultados de testes de configuração.
5. Na caixa de diálogo exibida, insira as informações sobre a solicitação e selecione **Solicitar aprovação**.
6. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação ao aprovador e selecione **Enviar**.

   Nota: O modal Responder questionário aparece somente quando a caixa de seleção **Habilitar questionário para marcar como falso-positivo** está marcada no formulário Configuração de gestão de exceções. Para obter mais informações sobre como um questionário é configurado, consulte Configurar Gestão de exceções para Conformidade de configurações.

   Os resultados de testes selecionados são movidos para uma nova tarefa de correção e sua solicitação é enviada para aprovação. O número da tarefa aparece no **Fluxo de atividades** da antiga Tarefa de correção. O aprovador recebe uma notificação por e-mail sobre sua solicitação.

Resultados

Você receberá uma notificação por e-mail sobre a aprovação ou rejeição da sua solicitação.

No **Fluxo de atividades** de um resultado de testes ou tarefa de correção, você pode exibir todo o fluxo de trabalho da solicitação de falso-positivo.

O que Fazer Depois

1. Em Espaço de correção de problemas de TI, na página Lista, navegue até **Solicitações de exceção** > **Minhas solicitações**.
2. Abra o registro de aprovação de mudança de estado correspondente (VCA#) e verifique o status da sua solicitação na coluna Estado de aprovação:

Estado de aprovação	Resultado
Aprovado	O estado da nova tarefa de correção muda para Encerrado com o motivo como Falso-positivo.
Rejeitado	O estado da nova tarefa de correção muda para Aberto.

3. Depois que a solicitação for aprovada, navegue até a guia Detalhes da nova Tarefa de correção e defina a data de vencimento como falso-positivo no campo **Até**, se necessário.

   A tarefa de correção será revertida para o estado Aberto após a data especificada e o Estado será revertido para os resultados de testes.

Solicitar uma exceção no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, solicite uma exceção para uma tarefa de correção.

Antes de Iniciar

Função necessária:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Ou você pode determinar que uma tarefa de correção não pode ser resolvida até a data de destino. Quando sua correção não pode estar em conformidade com uma política de segurança ou gestão de vulnerabilidades, padrão ou diretriz publicada, você pode solicitar uma exceção.

Você pode solicitar exceções para tarefas de correção e itens vulneráveis do Espaço de correção de TI atribuídos a você.

A partir da versão 19.0 de Resposta a vulnerabilidades, você pode solicitar exceções para resultados de testes .

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

A partir da versão 18.0, você pode solicitar exceções para itens de vulnerabilidade da aplicação e itens de vulnerabilidade de contêiner.

Para obter mais informações sobre como solicitar exceções no ambiente clássico, consulte Solicitar uma exceção para uma tarefa de correção.

Procedimento

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Espaço de correção de TI**.
2. Localize uma tarefa de correção para a qual você deseja solicitar uma exceção.
3. Nos botões de ação de IU à direita, clique em **Solicitar exceção**.
4. Na caixa de diálogo exibida, preencha a data de término da exceção, selecione um motivo na lista e adicione outras informações necessárias.
5. Clique **em Solicitar exceção**.
6. No modal Responder ao **questionário**, responda às perguntas e clique em **Enviar**.

   Nota: A partir da versão 18.0, você pode responder ao questionário para fornecer informações adicionais sobre sua solicitação para o aprovador. O modal Responder **questionário** aparece somente quando a caixa de seleção **Habilitar questionário para solicitar exceção** está marcada no formulário **Configuração de gestão de exceções**.

   Uma mensagem exibe que sua solicitação foi enviada com sucesso para aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma solicitação de exceção para uma tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de nível 2.

- O registro da tarefa de correção ou as transições de VI para Em revisão enquanto a solicitação de exceção está aberta.
- O registro da tarefa de correção ou as transições de VI para Adiado se a solicitação for aprovada.
- O registro de solicitação de exceção é encerrado depois que sua solicitação de exceção é aprovada.

Para exibir o status de suas solicitações de aprovação, em Solicitações de exceção na página Lista, clique em **Minhas solicitações**. O número da solicitação (VCA#) é exibido quando você abre o VI ou o registro da tarefa de correção na lista.

- Se a solicitação for rejeitada, o registro de solicitação (VCA#) exibirá **Rejeitado** na coluna Estado de aprovação na Exibição de lista em Minhas solicitações.
- Você deve enviar uma nova solicitação de exceção se ainda quiser adiar este item.

Solicitar uma exceção usando GRC: Gestão de políticas e conformidade no Espaço de correção de problemas de TI

Solicite uma exceção à política para o item vulnerável de host (VIT), item de vulnerabilidade da aplicação (AVIT), item vulnerável de contêiner (CVIT) ou tarefa de correção (VUL, AVUL, CVUL ou CRG) do Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária:

- sn_vul.remediation_owner para itens vulneráveis de host (VITs)
- sn_vul_container.remediation_owner para itens vulneráveis da aplicação (AVITs)
- sn_vul.app_security_campion para itens vulneráveis de contêiner (CVITs)
- sn_vulc.remediation_owner para resultados de testes de configuração (TRs)

Por Que e Quando Desempenhar Esta Tarefa

Nota: A partir da v19.0 de Resposta a vulnerabilidades, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. No navegador de aplicações, selecione o ícone de lista (ícone de).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na página Lista, em Itens vulneráveis de host, Itens vulneráveis de aplicação, Itens vulneráveis de contêiner ou Tarefas de correção, selecione o registro para o qual você deseja solicitar uma exceção.
   O registro selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
4. Selecione o botão **Solicitar exceção**.
5. No formulário, preencha os campos.
   Para mais informações sobre campos de formulário, consulte Solicitar campos de formulário de exceção para exceções às políticas.
6. Selecione **Solicitar exceção**.
7. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação e selecione **Enviar**.

   Nota: O modal Responder ao questionário aparece somente quando os detalhes do questionário são adicionados ao respectivo registro de integração.

   É exibida uma mensagem informando que sua solicitação foi enviada com sucesso para aprovação.

   Para obter mais informações sobre a integração de exceção à política e a transferência entre o responsável pela correção e o gerente de conformidade, consulte Configuração opcional da Gestão de políticas e conformidade .

Solicitar redução de risco no Espaço de correção de problemas de TI

A partir da v20.0 de Resposta a vulnerabilidades, você pode solicitar a redução no risco de um item vulnerável de host ou uma tarefa de correção no Espaço de correção de problemas de TI.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
A partir de v21.0 de Resposta a vulnerabilidades:

- Você pode solicitar a redução de risco para uma tarefa de correção se os itens de vulnerabilidade estiverem associados a uma mesma Entrada de vulnerabilidade comum (CVE) ou Entrada de terceiro (TPE) para a qual a redução de risco está habilitada.
- Você não pode solicitar a redução de risco para uma tarefa de correção com itens vulneráveis associados a diferentes CVEs, mesmo que a redução de risco esteja habilitada para CVEs.

Nota: O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Na página Lista, abra um item vulnerável de host ou uma tarefa de correção.
3. Selecione o menu de três pontos e selecione **Solicitar exceção**.
4. No pop-up Solicitar exceção, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar modal de exceção

Campo	Descrição
Motivo	Motivo da sua solicitação de exceção. Selecione *Controle de mitigação no local* para solicitação de redução de risco. Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Solicitação de adiamento	Difere o registro. Este campo é selecionado por padrão. **Nota:** Este campo aparece somente quando a opção *Controle de mitigação no local* está selecionada no campo **Motivo**.
Solicitação de redução de risco	Permite que você solicite a redução da pontuação de risco. **Nota:** Esta caixa de seleção aparece somente quando a opção *Controle de mitigação no local* está marcada no campo **Motivo**.
Classificação de risco atual	Gravidade atual do risco. **Nota:** Este campo aparece somente quando a caixa de seleção **Solicitar redução de risco** está marcada.
Classificação de risco desejado	Nova classificação de risco que você deseja atribuir ao registro. A pontuação de risco mais alta neste intervalo de classificação de risco é aplicada ao registro quando sua solicitação é aprovada. **Nota:** Este campo aparece somente quando a caixa de seleção **Solicitar redução de risco** está marcada.
Selecionar controles de remuneração	Motivo da sua solicitação para reduzir a classificação de risco.
Até	Data em que a solicitação de adiamento ou redução de risco expira. Quando a solicitação de exceção expira:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ O registro é revertido para o estado Aberto. ◦ Os controles de compensação expiram. ◦ A pontuação calculada substituirá uma pontuação reduzida.
Observações de justificativas	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita.

5. Selecione **Solicitar exceção**.
6. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação e selecione **Enviar**.

   Nota: O modal Responder ao questionário aparece somente quando o questionário está habilitado para gerenciamento de exceções. Para obter mais informações, consulte Configurar Gestão de exceções para Resposta a vulnerabilidades.

   Uma mensagem será exibida informando que sua solicitação foi enviada com sucesso para aprovação. Uma notificação é enviada ao aprovador sobre sua solicitação.

   - Se você solicitar um adiamento e redução de risco:
     - Duas aprovações de mudança de estado (VCA#) são criadas para adiamento e redução de risco.
     - O estado do registro muda para Em revisão.
   - Se você solicitar somente redução de risco:
     - Uma aprovação de mudança de estado (VCA#) é criada.
     - O estado não muda.

   Na aprovação ou rejeição da sua solicitação, você receberá uma notificação.

   Para obter mais informações sobre como a **data Até da redução de risco** é atualizada para uma tarefa de correção e item vulnerável quando uma solicitação de redução de risco é aprovada, consulte Impacto dos controles de remuneração na pontuação de risco e na data de vencimento.

O que Fazer Depois

Você receberá uma notificação quando sua solicitação for aprovada ou rejeitada pelo aprovador. Para obter mais informações sobre o processo de aprovação, consulte Aprovar ou rejeitar solicitações no Vulnerability Manager Workspace.

Informações relacionadas

Noções básicas sobre controles de remuneração para redução de risco

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Adicionar um controle de compensação à biblioteca

Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações a partir de Espaço de correção de problemas de TI em seu Now Platform sob demanda.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

A nova verificação é compatível com as seguintes integrações no Espaço de correção de problemas de TI. Consulte os seguintes tópicos para obter mais informações:

- Verificar novamente Qualys itens vulneráveis dos espaços Resposta a vulnerabilidades
- Verificar novamente Rapid7 itens vulneráveis dos espaços Resposta a vulnerabilidades
- Verificar novamente itens vulneráveis Tenable.io e Tenable.sc dos espaços Resposta a vulnerabilidades

Funções necessárias: sn_vul.remediation_owner para Espaço de correção de problemas de TI.

Verificar novamente Qualys itens vulneráveis dos espaços Resposta a vulnerabilidades

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações no produto Qualys sob demanda a partir de Espaço de correção de problemas de TI em sua instância Now Platform.

Antes de Iniciar

Para iniciar uma nova verificação do produto Qualys no ambiente clássico, consulte Iniciar nova verificação para Qualys Vulnerability Integration.

Os scanners Qualys são desativados por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto de scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto ativado é exibido no campo Origem nos registros de item vulnerável e de tarefa de correção após a próxima importação, e **Verificar novamente** está disponível como uma ação de IU.

Para obter mais informações sobre como configurar o scanner Qualys, consulte Configurar dispositivos scanner e Configurações e modificações avançadas da Qualys.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode iniciar novas verificações sob demanda para itens vulneráveis e tarefas de correção que tenham o produto Qualys como origem do Espaço de correção de problemas de TI em seu Now Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Qualys.
- Para iniciar novas verificações no espaço de correção de TI a partir de registros de item vulnerável e tarefa de correção, esses registros devem ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para Espaço de correção de problemas de TI.
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin do Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção que foi atribuída a você e abra-o.

   Nota: Se você escolher um esforço de correção para iniciar uma nova verificação, todos os IVs associados a esse registro serão verificados.

2. No canto superior direito do registro, clique em **Verificar novamente**.
3. No modal Verificar novamente, escolha um perfil de opção.
   Um perfil de opção é necessário quando você inicia uma verificação de [Qualys a partir do seu Now Platform®. Os perfis de opção contêm Qualys configurações de verificação.

Opção	Descrição
Usar perfil de opção padrão	Este é o perfil de opção definido como padrão para a instância de integração. Você seleciona este perfil ao configurar o scanner Qualys. Para obter mais informações, consulte Configurar dispositivos scanner.
Especificar perfil de opção	Na lista Perfil de opção, escolha um perfil a ser usado na verificação. Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

4. No modal Verificar novamente, clique em **Solicitar nova verificação**.
   A mensagem `A solicitação de verificação está sendo processada` é exibida.
5. Clique no link **Exibir status** na mensagem para exibir o andamento da verificação.

   O registro de verificação (VSCAN#) é exibido. Abaixo do cabeçalho do registro com o número de verificação, as listas de itens relacionados exibem as seguintes informações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A lista Detalhes exibe o número de verificação da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
- A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias são concluídas, o estado da verificação primária muda para Concluído.
- A lista de origem exibe o item vulnerável usado para a verificação, o item de configuração e a vulnerabilidade associados, o estado do VI e seu status de correção.

Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou.

Todos os IVs que fizeram ou farão a transição para Encerrado/Corrigido são importados com a próxima importação agendada das Qualys integrações.

Verificar novamente Rapid7 itens vulneráveis dos espaços Resposta a vulnerabilidades

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações no produto Rapid7 sob demanda no Espaço de correção de TI em sua instância Now Platform.

Antes de Iniciar

Para iniciar uma nova verificação do produto no ambiente clássico, consulte Iniciar nova verificação para a integração de vulnerabilidade Rapid7. Este tópico também inclui informações sobre como programar verificações com os parâmetros de integração na instância de integração Rapid7.

Os scanners Rapid7 são desativados por padrão na aplicação Resposta a vulnerabilidades. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou tarefas de correção que tenham a aplicação Rapid7 como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o produto de scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto ativado é exibido no campo Origem nos registros de item vulnerável e de tarefa de correção após a próxima importação, e **Verificar novamente** está disponível como uma ação de IU.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode iniciar novas verificações sob demanda para itens vulneráveis e tarefas de correção que tenham o produto Rapid7 InsightVM como origem do Espaço de correção de TI em seu Now Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Rapid7.
- Para iniciar novas verificações no espaço de correção de TI a partir de registros de item vulnerável e tarefa de correção, esses registros precisam ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para o espaço de correção de TI
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin do Espaço do gerenciador de vulnerabilidades

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção que foi atribuída a você e abra-o.

   Nota: Se você escolher um esforço de correção para iniciar uma nova verificação, todos os IVs associados a esse registro serão verificados.

2. No canto superior direito do registro, clique em **Verificar novamente**.
3. No modal Confirmar nova verificação, clique em **Solicitar nova verificação**.
   A mensagem `A solicitação de verificação está sendo processada` é exibida.
4. Clique no link **Exibir status** na mensagem para exibir o andamento da verificação.

   O registro de verificação (VSCAN#) é exibido. Abaixo do cabeçalho do registro com o número de verificação, as listas de itens relacionados exibem as seguintes informações:

   - A lista Detalhes exibe o número de verificação da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
   - A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias são concluídas, o estado da verificação primária muda para Concluído.
   - A lista de origem exibe o item vulnerável usado para a verificação, o item de configuração e a vulnerabilidade associados, o estado do VI e seu status de correção.

   Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

   O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou.

   Todos os IVs que fizeram ou farão a transição para Encerrado/Corrigido são importados com a próxima importação agendada das Rapid7 integrações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar novamente itens vulneráveis Tenable.io e Tenable.sc dos espaços Resposta a vulnerabilidades

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações nos produtos Tenable.io e Tenable.sc sob demanda no Espaço de correção de TI em sua instância Now Platform.

Antes de Iniciar

Para iniciar uma nova verificação dos produtos Tenable.io e Tenable.sc do ambiente clássico de Resposta a vulnerabilidades, consulte Iniciar nova verificação para a integração Tenable.sc e Iniciar nova verificação para a integração Tenable.io.

Para executar novas verificações a partir do seu Now Platform, você precisa das suas credenciais da Tenable. Para obter mais informações sobre como configurar seus scanners Tenable.io e Tenable.sc e importar suas credenciais da Tenable, consulte Configurar a Integração de vulnerabilidade da Tenable usando o Assistente de configuração.

- Você pode iniciar novas verificações sob demanda para itens vulneráveis e tarefas de correção que tenham o produto Tenable.io ou Tenable.sc como origem do Espaço de correção de TI em seu Now Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Tenable.io ou Tenable.sc.
- Para iniciar novas verificações em Espaço de correção de problemas de TI a partir de registros de item vulnerável e tarefa de correção, esses registros devem ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para o Espaço de correção de problemas de TI
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin do Espaço do gerenciador de vulnerabilidades

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção que foi atribuída a você e abra-o.

   Nota: Se você escolher um esforço de correção para iniciar uma nova verificação, todos os IVs associados a esse registro serão verificados.

2. No canto superior direito de um registro, clique em **Verificar novamente**.
   Você será solicitado a escolher a instância ou as instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pelas integrações de credencial de verificação Tenable.io e Tenable.sc.
3. No modal, clique no ícone de pesquisa.

   Em Selecionar um modal de credencial de verificação exibido, use os filtros nos títulos das colunas para selecionar o nome, a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Consulte a tabela a seguir para obter mais informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
Nome	Escolha o nome das credenciais desejadas. Passe o mouse sobre o título da coluna. Use o menu vertical de três pontos no título da coluna para filtrar os nomes das suas credenciais.
Instância de integração	Escolha um Tenable.io ou, se for Tenable.sc, a instância de integração Tenable.sc a partir da qual você deseja iniciar a nova verificação. Todas as suas instâncias de integração para Tenable.io ou Tenable.sc são exibidas. Se houver um VI em mais de uma instância de integração, você poderá usar este filtro para limitar ou expandir as instâncias que deseja verificar. **Nota:** Se você optar por verificar novamente os IVs de um registro de tarefa de correção para uma única instância de integração, somente os VIs ativos que estão associados a essa tarefa de correção, para essa instância, usando as credenciais selecionadas serão verificados.
Tipo	Estas são as credenciais de scanner disponíveis importadas dos produtos Tenable.io ou Tenable.sc. Passe o mouse sobre o título da coluna. Use o menu vertical de três pontos no título da coluna para abrir o modal e selecionar os tipos de credenciais desejados.

4. No modal Nova verificação atualizado, clique em **Solicitar nova verificação**.
   A mensagem `A solicitação de verificação está sendo processada` é exibida.
5. Clique no link **Exibir status** na mensagem para exibir o andamento da verificação.

   O registro de verificação (VSCAN#) é exibido. Abaixo do cabeçalho do registro com o número de verificação, as listas de itens relacionados exibem as seguintes informações:

   - A lista Detalhes exibe o número de verificação da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
   - A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias são concluídas, o estado da verificação primária muda para Concluído.
   - A lista de origem exibe o item vulnerável usado para a verificação, o item de configuração e a vulnerabilidade associados, o estado do VI e seu status de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sua instância Now Platform® rastreia o status da nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

O tempo limite não interrompe a verificação. O tempo limite se refere a quando o Now Platform® parou de rastrear seu status de nova verificação, não quando a nova verificação real parou.

Todos os IVs que fizeram ou farão a transição para Encerrado/Corrigido são importados com a próxima importação agendada das integrações Tenable.io ou Tenable.sc.

Espaço de correção de problemas de TI informações de referência

Os tópicos a seguir fornecem links, informações de referência, além de dados de campo nos formulários e registros encontrados em Espaço de correção de problemas de TI.

Criar campos de formulário de solicitação de mudança

A tabela a seguir mostra os campos e sua descrição no formulário Criar solicitação de mudança.

Campo	Descrição
Tipo de mudança	Normal – Normal é o padrão. Padrão- dois campos adicionais são exibidos: Categoria de mudança padrão - Selecione uma categoria na lista Modelo de mudança padrão – Selecione um modelo na lista de seleção a ser usado nesta solicitação de mudança Emergência - Prioridade crítica
Adicionar ICs à solicitação de mudança	O padrão é habilitado. Se habilitada, a solicitação de mudança adicionará todos os itens de configuração (IC) que pertencem aos itens vulneráveis ativos neste esforço de correção adicionados a esta solicitação de mudança.
Prioridade	Alto é o padrão. Selecione uma prioridade na lista.
Grupo de atribuição	Por padrão, o grupo de atribuição é obtido do tópico de observação. Clique no ícone de pesquisa e, no modal, escolha outro grupo de atribuição.
Data de término planejada	Clique no ícone de calendário para selecionar uma data de término planejada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuído a	O usuário atual é atribuído por padrão à tarefa de correção. Clique no ícone de pesquisa e escolha outro usuário no modal.
Descrição resumida	A descrição resumida é obtida da tarefa de correção. Clique no texto para editá-lo.
Descrição	A descrição é obtida da tarefa de correção. Clique no texto para editá-lo.
Justificativa	A justificativa obtida da tarefa de correção. Clique no texto para editá-lo.
Plano de implementação	Preenchido previamente com informações da solução preferencial, se disponíveis. Exiba a solução ou insira um plano de justificativa.

Informações relacionadas

Criar uma solicitação de mudança no Espaço de correção de problemas de TI

Solicitar campos de formulário de exceção para exceções às políticas

A tabela a seguir mostra os campos que você deve preencher no formulário Solicitar exceção para exceções às políticas.

Formulário Solicitar exceção

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não estiver selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção começa. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção à política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção à política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criação de uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
	Este campo deve ser preenchido pelo responsável pela correção.

Informações relacionadas

Solicitar uma exceção usando GRC: Gestão de políticas e conformidade no Espaço de correção de problemas de TI

Solicitar campos de formulário de exceção para redução de risco

A tabela a seguir mostra os campos que você deve preencher no formulário Solicitar exceção para solicitações de redução de risco.

Formulário Solicitar exceção

Campo	Descrição
Motivo	Motivo da sua solicitação de exceção. Selecione *Controle de mitigação no local* para solicitação de redução de risco. Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Solicitação de adiamento	Difere o registro. Este campo é selecionado por padrão. **Nota:** Este campo aparece somente quando a opção *Controle de mitigação no local* está selecionada no campo **Motivo**.
Solicitação de redução de risco	Permite que você solicite a redução da pontuação de risco. **Nota:** Esta caixa de seleção aparece somente quando a opção *Controle de mitigação no local* está marcada no campo **Motivo**.
Classificação de risco atual	Gravidade atual do risco. **Nota:** Este campo aparece somente quando a caixa de seleção **Solicitar redução de risco** está marcada.
Classificação de risco desejado	Nova classificação de risco que você deseja atribuir ao registro. A pontuação de risco mais alta neste intervalo de classificação de risco é

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Solicitar exceção

Campo	Descrição
	aplicada ao registro quando sua solicitação é aprovada. **Nota:** Este campo aparece somente quando a caixa de seleção **Solicitar redução de risco** está marcada.
Selecionar controles de remuneração	Motivo da sua solicitação para reduzir a classificação de risco.
Até	Data em que a solicitação de adiamento ou redução de risco expira. Quando a solicitação de exceção expira: • O registro é revertido para o estado Aberto. • Os controles de compensação expiram. • A pontuação calculada substituirá uma pontuação reduzida.
Observações de justificativas	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita.

Explorar o espaço de avaliação de vulnerabilidade

O Espaço de avaliação de vulnerabilidade foi projetado para que o gerenciador de eventos de vulnerabilidade execute a avaliação de exposição e gerencie proativamente eventos de vulnerabilidade críticos, especialmente durante os eventos de vulnerabilidade críticos, como um evento de dia zero.

Depois que uma vulnerabilidade crítica é identificada, os gerentes de eventos de vulnerabilidade podem avaliar o possível impacto e o risco associados à vulnerabilidade. Os analistas podem analisar o sistema, as aplicações ou os componentes de rede afetados para entender a gravidade e os possíveis vetores de ataque na organização.

O Espaço de avaliação de vulnerabilidade contém:

Página Avaliação de exposição

Fornece visibilidade detalhada dos ativos expostos a vulnerabilidades e software vulnerável. A funcionalidade de avaliação de exposição fornece:

- Visibilidade dos ativos afetados para vulnerabilidade e software afetado
- Capacidade de executar avaliações autônomas para um único CVE ou software vulnerável
- Visibilidade dos ativos afetados para CVEs de vulnerabilidades exploradas conhecidas da CISA
- Visibilidade para exposição de ativos e modelo de descoberta adicionais.
- Capacidade de criar itens vulneráveis

Página Avaliação de vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A página Avaliação de vulnerabilidade na qual você pode lidar com eventos de crise de vulnerabilidade, desde a avaliação até a resolução, usando o fluxo de trabalho Gestão de crises de vulnerabilidade. O fluxo de trabalho permite rastrear eventos de vulnerabilidade de interesse, analisar o risco associado a eles, executar avaliação de exposição em vários inventários (por exemplo, inventário de instalações de software) e declará-lo como uma crise para maior engajamento de resposta. Você pode associar o registro de avaliação de vulnerabilidade a um incidente de segurança grave e permitir que a equipe de resposta a incidentes de segurança responda à crise.

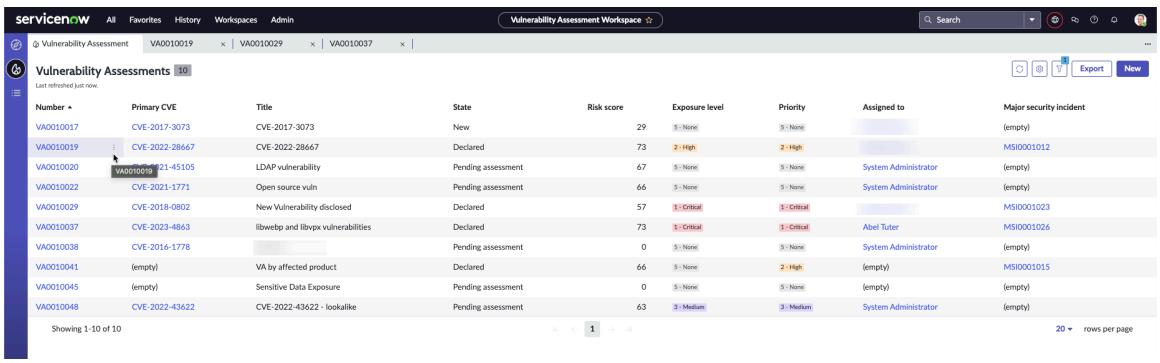
- Criar e modificar avaliações de vulnerabilidade para eventos de vulnerabilidade críticos
- Registrar atributos principais da vulnerabilidade para calcular o risco
- Realizar avaliação de vulnerabilidade para determinar o nível de exposição e a prioridade
- Declarar a avaliação de vulnerabilidade como um evento crítico
- Associe a avaliação de vulnerabilidade a um incidente de segurança grave vinculando, propondo ou promovendo a avaliação de vulnerabilidade a um incidente de segurança grave.

Página da lista

A página Lista compreende uma biblioteca que contém:

- CVEs
- TPEs
- CWEs

A imagem a seguir mostra a página inicial do Espaço de avaliação de vulnerabilidade.



Explorando a avaliação de exposição

A avaliação de exposição usa a estrutura de enumeração de plataforma comum (CPE), que faz parte do sistema de vulnerabilidades e exposições comuns (CVEs), para avaliar a exposição de vulnerabilidade de seus ativos ao software de vulnerabilidade. Esta avaliação é realizada usando um modelo de descoberta de software.

Ao empregar um algoritmo de correspondência, os CPEs relevantes são associados e mapeados para o modelo de descoberta de software, permitindo a identificação de possíveis exposições.

Você pode usar a avaliação de exposição por CVE ou software para identificar a exposição a possíveis vulnerabilidades para os seguintes cenários:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidades que podem não ser identificadas por verificadores tradicionais
- Vulnerabilidades de dia zero antes que o scanner forneça a assinatura para detecção de vulnerabilidades

A avaliação de exposição fornece um aviso antecipado para corrigir essas vulnerabilidades e melhorar a maturidade do programa de gestão de vulnerabilidades.

Pré-requisitos para avaliação de exposição

Versões disponíveis

Aplicação	Versão
Plug-in Gestão de crises de vulnerabilidade	1.0
Resposta a vulnerabilidades	20,0
Resposta a vulnerabilidades com NVD	1,3
Integração de Resposta a vulnerabilidades com CISA	1.2
Vulnerability Response Integration with NVD **Nota:** Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.	1,3
Gestão de ativos de software	Plug-inPlug-in Software Asset Management Foundational ou Software Asset Management Professional

Compatibilidade e requisitos do sistema

A aplicação Resposta a vulnerabilidades está disponível no ServiceNow Store. A aplicação Gestão de ativos de software do ITSM (com.snc.asset_management) é necessária para o módulo Avaliação de exposição. Esta aplicação gerencia todos os seus ativos e licenças de software, e a versão SAM Foundation desta aplicação faz parte da aplicação Resposta a vulnerabilidades que você baixa do ServiceNow Store.

Importante: A aplicação Avaliação de exposição funciona com os seguintes plug-ins:

- Plug-in Software Asset Management Foundational (com.snc.sams)
- Software Asset Management Professional (com.snc.pa.samp)
- Plug-in de Gestão de ativos de software (com.snc.software_asset_management)

Para verificar se a aplicação SAM Foundation está instalada em sua instância, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e pesquise por com.snc.asset_management. Se a aplicação não estiver instalada, selecione **Instalar**. Como a aplicação Avaliação de exposição de vulnerabilidade requer acesso aos dados de ativos em sua instância Now Platform®, as aplicações de gestão de ativos devem ter dados para fazer referência. A tabela Modelos de descoberta de software (cmdb_sam_sw_discovery_model) e as instalações de software (cmdb_sam_sw_install) exigem dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de algoritmo correspondentes para modelos de descoberta de software

A aplicação Software Asset Management Professional permite que você edite um modelo de descoberta de software para normalizar manualmente o software descoberto que não foi totalmente normalizado (parcialmente normalizado, fornecedor normalizado ou correspondência não encontrada) no formulário Modelos de descoberta de software para que ele possa ser reconciliado. A partir da versão 20.0 do Resposta a vulnerabilidades, o oferece suporte ao modelo de descoberta normalizado que vem do Software Asset Management Professional. Os campos a seguir são usados para o algoritmo de correspondência para modelos de descoberta de software.

CPE (modelo de software)	SAM Foundations	SAM profissional
Fornecedor	Chave primária	Chave primária
Produto	Nome para exibição	Nome para exibição
Versão	Fornecedor descoberto	Fornecedor descoberto
Edição	Produto Descoberto	Produto Descoberto
	Versão descoberta	Versão descoberta
		Fornecedor Normalizado
		Produto normalizado
		Versão normalizada

Nota: A aplicação SAM Professional não faz parte do produto principal Resposta a vulnerabilidades do ServiceNow Store e requer uma assinatura separada.

Propriedade do sistema

Para processar as vulnerabilidades exploradas pela CISA automaticamente para avaliação de exposição, defina a propriedade do sistema *sn_vul_analyst.enable_exposure_for_cisa* como *true*. O valor padrão é *false*.

Trabalhos agendados

A seguir estão os trabalhos agendados.

Nome do trabalho programado	Descrição
Verificar possível exposição a vulnerabilidades	Processa os CVEs delta, o software e as instalações para obter a exposição. **Nota:** Este trabalho agendado é executado a cada 12 horas. Ele é executado por um período mais longo do que os outros trabalhos agendados.
Inserir CVE explorado CISA na configuração de exposição	Sob demanda. Insere os CVEs CISA na tabela Configuração de exposição para calcular a exposição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do trabalho programado	Descrição
Executar avaliação de exposição para CVEs configurados	Sob demanda. Calcula a exposição de todos os registros de CVE na tabela Configuração de exposição.
Executar exposição de software	Sob demanda. Calcula a exposição de todos os registros de software na tabela Configuração de exposição.

Termos principais

- Pontuação de**confiança:** uma pontuação de confiança é uma medida da confiabilidade no fornecimento de uma recomendação para um campo. Quanto maior a pontuação, mais confiável será a recomendação. Para obter exemplos de cálculos, consulte Exemplo de cálculo de pontuação de confiança.
- **Contagem de instalação de software:** número de ativos de software afetados pela vulnerabilidade.
- Modelo de**software: modelo** de software associado ao produto. Faça o detalhamento ativo do modelo de software para ver o resultado do modelo de software. Para obter mais informações, consulte Plug-in Software Asset Management Foundational modelos de descoberta e instalações de software .

O campo **Contagem de instalações de software** fornece o número total de instalações de software, independentemente do status ativo ou inativo no modelo de descoberta. A partir da v22.0 de Resposta a vulnerabilidades, uma nova propriedade do sistema, *sn_vul.filter_inactive_sw_installs*, foi introduzida para determinar se as instalações de software inativas devem ser filtradas para avaliação de exposição. Por padrão, a propriedade está habilitada no sistema de base. Quando o filtro está habilitado, somente as instalações ativas são exibidas.

O campo **Modelo de descoberta** mostra especificamente a contagem de instalações de software ativas, já que as inativas são filtradas com base no filtro ativo=verdadeiro padrão na tabela Modelo de descoberta de software. A contagem neste campo deve corresponder à contagem filtrada exibida no campo **Contagem de instalação de software**. A contagem no campo **Instalação de software** persiste mesmo se você atualizar a propriedade do sistema. Para obter a contagem atualizada, você deve executar os trabalhos agendados *Run exposure assessment for configured CVEs* e *Run software exposure that updates the count*.

Avaliação de exposição por CVE

A avaliação de exposição usa vulnerabilidades e exposições comuns (CVEs) para avaliar a exposição de seus ativos usando o modelo de descoberta de software. Você pode usar a avaliação de exposição por CVE para identificar a exposição a possíveis vulnerabilidades.

Para obter informações sobre como avaliar a exposição por CVE, consulte:

- Adicionar CVEs para avaliar a exposição
- Criar VIs para CVEs para avaliação de exposição
- Ativar ou desativar CVEs para avaliação de exposição
- Exportar ICs afetados para avaliação de exposição
- Exemplo de cálculo de pontuação de confiança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar CVEs para avaliar a exposição

Adicione vulnerabilidades e exposições comuns (CVEs) à lista de configuração de exposição de CVEs na avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione **Adicionar**.
3. Na caixa de diálogo Adicionar CVE, selecione os CVEs que deseja adicionar à lista e selecione a opção **Adicionar**.
   CVEs que já estão na lista não são adicionados novamente. O restante é adicionado à lista de CVEs.

   Nota: Selecione o ícone de filtro para navegar até a **exibição avançada** e especifique os CVEs que deseja exibir.

4. Para avaliar o impacto dos CVEs que já estão na lista:

   a. Marque a caixa de seleção dos CVEs que você deseja reavaliar.

   b. Selecione o botão **Reavaliar**.
      Os detalhes atualizados aparecem nas respectivas colunas.

Criar VIs para CVEs para avaliação de exposição

Crie itens vulneráveis (VIs) na página Avaliação de exposição. Os gerentes de eventos de vulnerabilidade analisam essa lista de IVs e recomendam soluções e patches que ajudam a equipe de TI a corrigir essas vulnerabilidades.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Depois que a exposição é avaliada, a lista da possível avaliação é exibida no registro de avaliação de exposição com a contagem de itens de configuração (ICs). Você pode selecionar os registros e, na ação de lista, selecionar **Criar itens vulneráveis** para criar itens vulneráveis (IVs) para os ICs em que o software vulnerável está presente e nas CVEs (Common Vulnerability and Exposures, vulnerabilidades e exposições comuns). Os IVs são criados em segundo plano. Este processo pode levar algum tempo. Depois que os itens forem criados, você poderá navegar até a tabela VI para exibir os registros criados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione os CVEs necessários e selecione a opção **Criar itens vulneráveis**.
3. Na caixa de diálogo Criar itens vulneráveis, selecione a opção **Criar itens vulneráveis**.
4. Selecione o link **Exibir status** para exibir o status do trabalho em segundo plano usado para criar os IVs.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar ou desativar CVEs para avaliação de exposição

Para o processamento delta de um CVE, você pode ativá-lo, adicionando-o à lista ativa de CVEs.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione os CVEs ativos necessários e selecione a opção **Desativar**.
   Os CVEs estão desativados.

   Nota: Para ativar o software, siga o mesmo processo e selecione a opção **Ativar**.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exportar ICs afetados para avaliação de exposição

Você pode rastrear a lista de ativos afetados para um novo CVE exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma planilha do Excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione o modelo de descoberta para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados na coluna **Instalado em**.
3. Selecione a opção **Exportar**.
4. Na caixa de diálogo Exportar, selecione o Tipo de arquivo e o Tipo de entrega para exportar os ICs relacionados.
5. Selecione a opção **Exportar**.

Exemplo de cálculo de pontuação de confiança

Exemplo de cálculo da confiança de uma vulnerabilidade de dia zero com base nas informações de CVE (Common Vulnerability and Exposures, vulnerabilidades e exposições comuns).

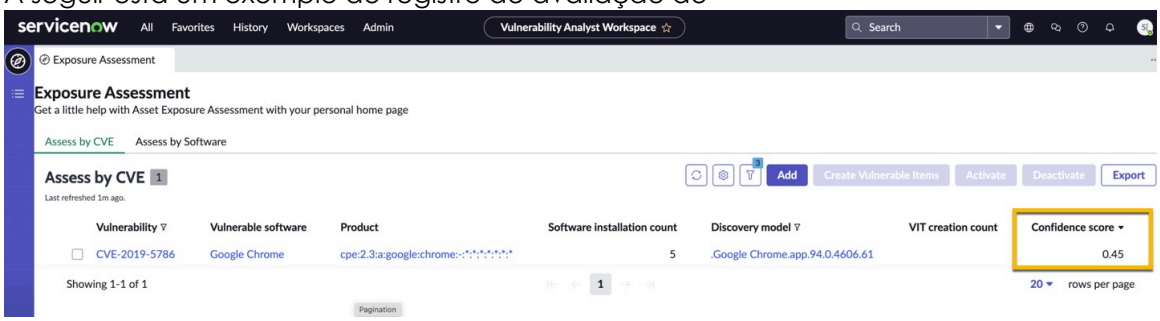
A seguir está um exemplo de cálculo da pontuação de confiança a partir das informações de Enumeração de Plataforma Comum (CPE) de **CVE-2019-5786**.

Nota: Para exibir os CPEs, você pode agrupar a coluna Vulnerabilidade por vulnerabilidade. Para obter detalhes sobre como exibir os detalhes do software vulnerável, consulte Exibir detalhes do software vulnerável.

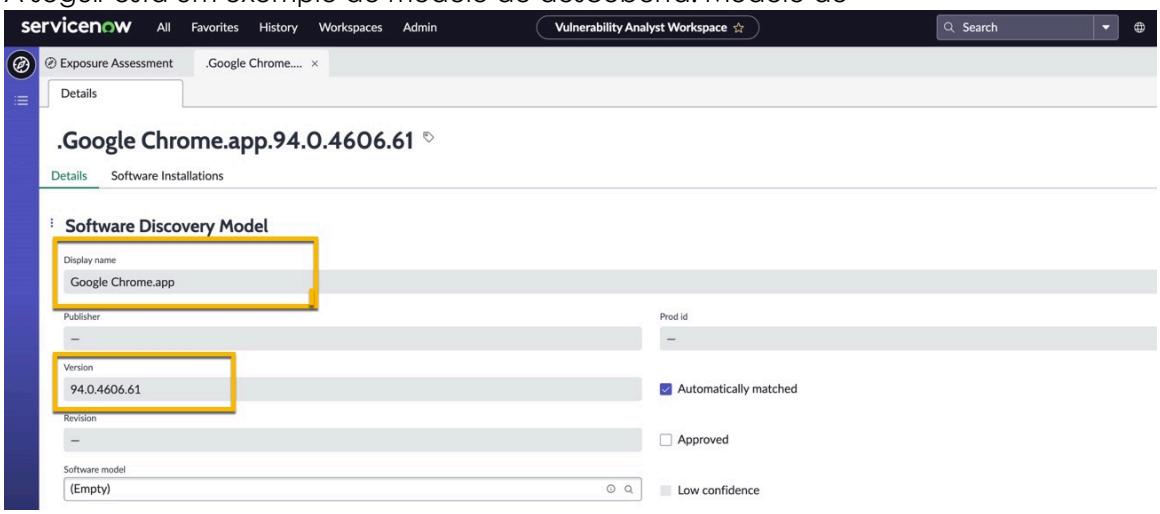
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está um exemplo de registro de avaliação de



A seguir está um exemplo de modelo de descoberta: Modelo de



Como calcular a pontuação de confiança

O intervalo de pontuação de confiança é de 0 a 1. Com base nas informações do CPE, a pontuação de confiança é calculada usando a seguinte fórmula:

```
((BASE SCORE) + (publisher score) +(product score) + (version score) +
 (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

```
.45
```

Nota: Para consultar os valores usados para calcular a pontuação de confiança, consulte Tabelas de referência de pontuação de confiança para avaliação de exposição.

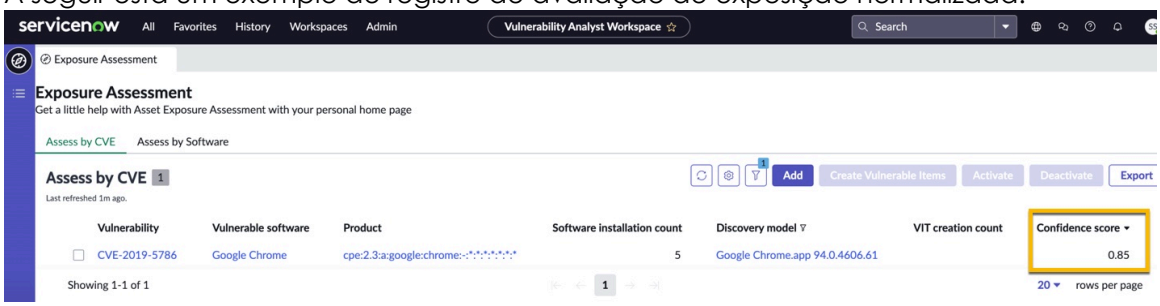
Como calcular a pontuação de confiança quando o modelo de software corresponde ao modelo de descoberta normalizado

Se você estiver usando o modelo de descoberta normalizado, as informações adicionais disponíveis para o modelo de descoberta de software fornecerão uma pontuação de confiança aprimorada. A seguir está o cálculo de amostra:

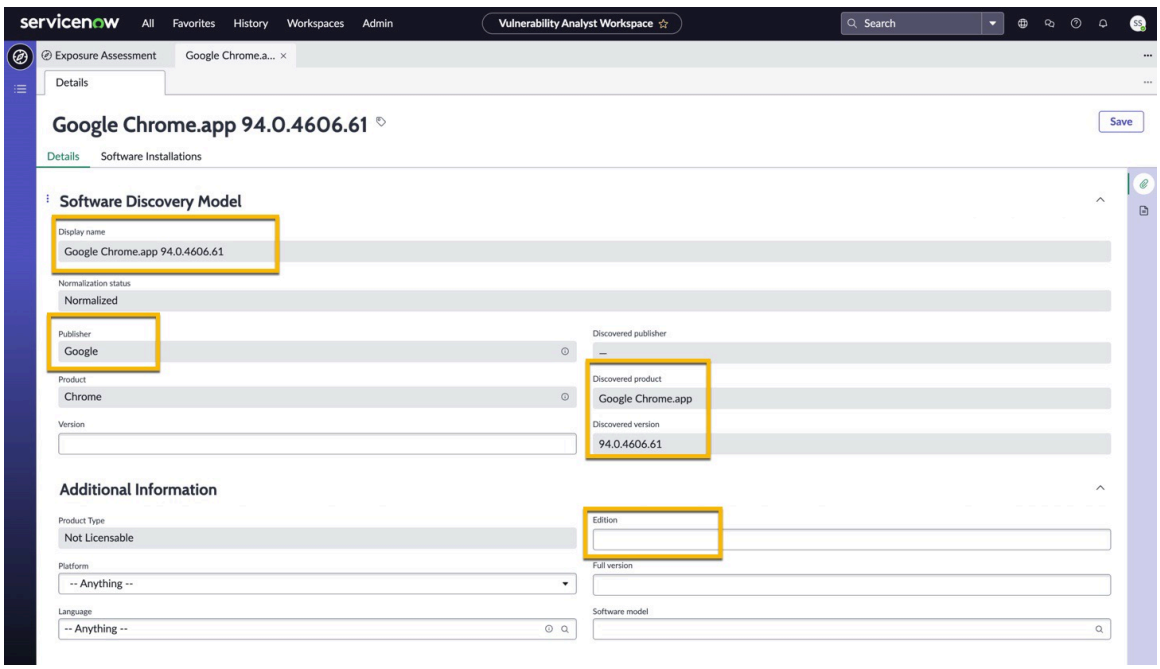
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está um exemplo de registro de avaliação de exposição normalizada.



A seguir está um exemplo de modelo de descoberta normalizada.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) +
 (edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Nota: Para consultar os valores usados para calcular a pontuação de confiança, consulte Tabelas de referência de pontuação de confiança para avaliação de exposição.

Exibir detalhes do software vulnerável

Exiba os detalhes do software vulnerável, neste caso, o Google Chrome. É correspondido com o modelo de descoberta e a Enumeração de plataforma comum (CPE). Esta versão de CPE afeta todas as versões do Google Chrome.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** e digite *sn_vul_software.LIST*.
2. Na lista de softwares vulneráveis, pesquise por **cpe:2.3:a:google:chrome:-:*:*:*:*:*:*:*** para exibir as informações.

Tabelas de referência de pontuação de confiança para avaliação de exposição

Valores de referência usados para calcular a pontuação de confiança.

Tabelas de referência

Tabela de referência do cálculo de pontuação de confiança

Segmento de software vulnerável	Segmento do modelo de descoberta	Pontuação	Segmento de correspondência exata do modelo de descoberta	Pontuação de correspondência exata
Fornecedor	Nome de exibição	15	Fornecedor	5
Modelo	Nome de exibição	15	Modelo	5
Versão	Nome de exibição	10	Versão	5
Edição	Nome de exibição	3	Edição normalizada	2
Nome de exibição	Nome de exibição	10	Nome de exibição	5

Tabela de resumo da pontuação de confiança

Pontuação	Valor
Soma de todas as pontuações	75
Pontuação base **Nota:** Pontuação mínima atribuída a todos os modelos de descoberta correspondentes.	25
Pontuação total	100

Avaliação de exposição por software

Avaliação de exposição para vulnerabilidades de dia zero, quando as vulnerabilidades e exposições comuns (CVEs) para o ativo ou item de configuração não estão disponíveis. Ele usa as informações do software para avaliar a exposição, usando o modelo de descoberta de software.

Para obter informações sobre como avaliar a exposição por software, consulte:

- Adicionar software para avaliação de exposição
- Criar VIs para software para avaliação de exposição

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ativar ou desativar o software para avaliação de exposição
- Exportar ICs afetados para software no espaço de avaliação de vulnerabilidade

Adicionar software para avaliação de exposição

Adicione um novo software ao módulo Avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software** > **Adicionar**.
2. No formulário, preencha os campos.

Campo	Descrição
Fornecedor	Fornecedor do software.
Produto	Nome do produto do software.
Versão	Versão do produto de software.
Edição	Edição do software

> **Nota:** Se você tentar adicionar exposição a um software que existe na tabela com o status "falso", um registro duplicado não será criado. O status do software existente é atualizado para "verdadeiro".

3. Selecione a opção **Adicionar**.
4. Para avaliar o impacto do software que já está na lista:
   a. Marque a caixa de seleção do software que você deseja reavaliar.
   b. Selecione o botão **Reavaliar**.
   Os detalhes atualizados aparecem nas respectivas colunas.

Criar VIs para software para avaliação de exposição

Crie itens vulneráveis (VIs) na página Avaliação de exposição. Os gerentes de eventos de vulnerabilidade analisam essa lista de IVs e recomendam soluções e patches que ajudam a equipe de TI a corrigir essas vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Selecione os registros para os quais você deseja criar IVs.
3. Selecione a opção **Criar itens vulneráveis**.
4. Na caixa de diálogo Criar itens vulneráveis, selecione uma das opções:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidade Existente
- Nova Vulnerabilidade

5. Selecione a opção **Criar itens vulneráveis**.

Ativar ou desativar o software para avaliação de exposição

Para interromper o processamento delta do software, você pode optar por desativá-lo, removendo-o da lista ativa de software.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Para desativar, selecione o software ativo necessário e selecione a opção **Desativar**.
   O software está desativado.

   Nota: Para ativar o software, siga o mesmo processo e selecione a opção **Ativar**.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exportar ICs afetados para software no espaço de avaliação de vulnerabilidade

Você pode rastrear a lista de ativos afetados do novo software exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma planilha do Excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Selecione o modelo de descoberta para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados na coluna **Instalado em**.
3. Selecione a opção **Exportar**.
4. Na caixa de diálogo Exportar, selecione o Tipo de **arquivo e o Tipo** de **entrega** para exportar os ICs relacionados.
5. Selecione a opção **Exportar**.

Explorando a avaliação de vulnerabilidade

O Espaço de avaliação de vulnerabilidade foi projetado para que o Gerenciador de eventos de vulnerabilidade crie um evento de vulnerabilidade e execute a avaliação de vulnerabilidade, especialmente durante a análise de vulnerabilidade de dia zero.

Você pode usar o espaço de avaliação de vulnerabilidades para gerenciar vulnerabilidades críticas, como:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidades de dia zero de severidade crítica ou alta
- Novas informações sobre ameaças identificadas para uma vulnerabilidade
- Exploração rápida de uma vulnerabilidade de gravidade crítica ou alta.

Espaço de avaliação de vulnerabilidade e Gestão de crises de vulnerabilidade

Como um gerenciador de eventos de vulnerabilidade, identifique e crie um registro de eventos de vulnerabilidade para vulnerabilidades de interesse. Depois de criar o evento vulnerável, você pode executar a avaliação de risco, atualizar manualmente os atributos de risco e calcular a pontuação de risco automaticamente. Usando o Espaço de avaliação de vulnerabilidade, você pode executar as seguintes ações para lidar com eventos de crise de vulnerabilidade desde o início até a resolução.

- Criar um registro de avaliação de vulnerabilidade
- Modificar o registro de avaliação de vulnerabilidade
- Executar uma avaliação de vulnerabilidade
- Revisar os detalhes da avaliação
- Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade
- Adicionar ICs afetados ao registro de avaliação
- Criar itens vulneráveis para o IC afetado ou o componente de software afetado
- Vincule o registro de avaliação de vulnerabilidade ao incidente de segurança grave em Gestão de incidentes graves de segurança

Pré-requisitos para avaliação de vulnerabilidade

Versões disponíveis

Aplicação	Versão
Plug-in Gestão de crises de vulnerabilidade	1.0
Resposta a vulnerabilidades	20,0
Resposta a vulnerabilidades com NVD **Nota:** Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.	1.4.2
Integração de Resposta a vulnerabilidades com CISA	1.2
Modelo de dados para SBOM	1.1.2
Lista de materiais de software Núcleo	2.0.2
Gestão de ativos de software	Plug-inPlug-in Software Asset Management Foundational ou Software Asset Management Professional
Gestão de incidentes graves de segurança	2.2.5

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos agendados

A seguir estão os trabalhos agendados.

Nome do trabalho programado	Descrição
Avaliação de vulnerabilidade	Atualiza a tabela de itens de configuração afetados e a origem do IC se itens vulneráveis (VITs ou AVITs) forem criados após a avaliação. **Nota:** Este trabalho agendado é executado diariamente. Ele é executado por um período mais longo do que os outros trabalhos agendados.

Informações relacionadas

Gestão de crises de vulnerabilidade

Criar um registro de avaliação de vulnerabilidade

Crie registros de avaliação para vulnerabilidades de interesse. Depois de criar a avaliação, você pode iniciar a avaliação de risco inicial, atualizar manualmente o registro e calcular a pontuação de risco automaticamente.

Antes de Iniciar

Você precisa fazer parte do grupo de atribuição do gerenciador de eventos de avaliação de vulnerabilidade do sistema de base para poder executar as tarefas associadas à avaliação de vulnerabilidade. Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar um registro de avaliação de vulnerabilidade para vulnerabilidades de interesse associando o registro de evento a um CVE primário ou a um produto afetado.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o ícone **Avaliação de vulnerabilidade**.
3. Selecione **Novo**.
4. Insira um título apropriado no campo **Título**.
5. Opcional: Selecione um CVE primário para associar ao novo registro de avaliação no campo **CVE primário**.

   Nota: Todos os detalhes preliminares no registro de avaliação são preenchidos com base no produto selecionado ou criado ou no CVE primário associado ao registro.

6. Selecione **Enviar**.
   O registro de avaliação de vulnerabilidade com o título que você inseriu é criado e exibido em uma nova guia de avaliação de vulnerabilidade. Por padrão, o registro de avaliação de vulnerabilidade é exibido na guia **Detalhes**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Por padrão, os detalhes do CVE primário associado/mapeado são exibidos.

- Se nenhum CVE primário for selecionado durante a criação do registro de evento de avaliação de vulnerabilidade, um registro padrão será criado.
- Se o CVE primário tiver CVEs associados, os CVEs relacionados serão preenchidos na guia **Entradas de vulnerabilidade**. Você pode adicionar mais CVEs associados na guia **Entradas de vulnerabilidade**.

7. Navegue até a guia **Produtos afetados**.

a. Selecione **Novo**.

b. No formulário, preencha os campos.

Campo	Descrição
Fornecedor	Fornecedor do software. Este é um campo obrigatório.
Produto	Nome do produto do software. Este é um campo obrigatório.
Versão	Versão do produto de software.
Edição	Edição do software

Nota: Se você tentar adicionar vulnerabilidades a um software existente na tabela com o status "falso", um registro duplicado não será criado. O status do software existente é atualizado para "verdadeiro".

c. Selecione **OK**.

8. Selecione **Salvar**.

Atualizar o registro de limpeza automática da avaliação de vulnerabilidade

Atualize o registro de limpeza automática da avaliação de vulnerabilidade.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

No sistema de base, o período de retenção de registros de avaliação de vulnerabilidade é definido como 6 meses. Se qualquer estado de registro de avaliação de vulnerabilidade estiver fechado, os registros de avaliação de vulnerabilidade serão armazenados somente até o período de retenção definido e os registros relacionados a essa avaliação serão removidos após 6 meses de todas as tabelas relacionadas.

Procedimento

1. Navegar até **Todos** > **Limpezas automáticas**.

2. Abra o registro com a tabela sn_vul_analyst_vulnerability_assessment.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Marque a caixa de seleção **Ativo** para ativar a opção de limpeza automática para o registro de avaliação de vulnerabilidade.
4. Clique em **Atualizar**.

Modificar o registro de avaliação de vulnerabilidade

Atualize o registro de avaliação de vulnerabilidade, publique sua criação. Com base nos valores do campo, você pode calcular a pontuação de risco.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

Depois que o CVE primário é adicionado à avaliação de vulnerabilidade, o registro é movido para um estado de avaliação pendente. Você pode adicionar outros CVEs relacionados na guia **Entradas de vulnerabilidade**ou adicionar os produtos afetados por esta vulnerabilidade na guia **Produtos afetados**. Você pode fazer modificações adicionais nos campos de **avaliação de risco** e a **pontuação** de risco do registro de avaliação é atualizada automaticamente de acordo.

Procedimento

1. Navegar até **Todos** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de vulnerabilidade**.
2. Na guia **Detalhes**, atualize os campos.

Campo	Descrição
Título	Título que descreve o registro do evento de vulnerabilidade .
CVE primário	CVE primário que você associou ao registro do evento.
Estado	Estado atual do registro do evento.
Prioridade	Prioridade do registro do evento em uma escala de 1 a 5.
Origem do alerta	Origem do possível evento de vulnerabilidade.
Pontuação de risco	Pontuação de risco calculada automaticamente. Não editável por padrão.
Nível de exposição	O nível de exposição do evento de vulnerabilidade em uma escala de 1 a 5.
Grupo de atribuição	O grupo de atribuição ao qual o registro de evento está atribuído.
Atribuído a	O usuário ao qual o registro de evento está atribuído.
Descrição	Descrição detalhada do registro do evento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegue até a guia **Entradas de vulnerabilidade** para adicionar CVEs associados ou relacionados.
   a. Selecione **Novo**.
   b. Pesquise o registro no campo de **entrada Vulnerabilidade**.
   c. Selecione o registro de vulnerabilidade que você deseja associar ao registro de avaliação.
   d. Opcional: Selecione **Procurar** para navegar e anexar um arquivo.
   e. Selecione **Salvar**.
   Os registros de vulnerabilidade selecionados são adicionados ao registro de avaliação e exibidos na guia **Entradas de vulnerabilidades**.
4. Opcional: Adicione produtos afetados.
5. Adicionar link relacionado ao registro de avaliação.
6. Modifique os **atributos de risco** do CVE primário associado ao registro de evento de avaliação de vulnerabilidade.

Campo	Descrição
Corrupção de memória	Indica se este registro de evento pode corromper a memória.
Executável de código remoto	Indica se a execução remota de código é possível.
Escalação de privilégio local	Indica se existe uma vulnerabilidade de escalação de privilégio local.
Acesso não autorizado	Indica se existe uma vulnerabilidade de acesso não autorizado.
DDOS	Indica se o possível evento pode envolver a negação de serviço distribuída.
Complexidade de ataque	Indica a complexidade do anexo. As opções são Baixo, Médio ou Alto.
Vetor de ataque	Indica o possível caminho ou método de ataque. As opções são: Rede, Rede adjacente, Local, Física, Nenhuma.
Privilégios necessários (PN):	Indica o nível de privilégios de que um invasor precisa para explorar a vulnerabilidade. As opções são Nenhum, Baixo ou Alto.
Interação do usuário	Indica se a interação do usuário é necessária para explorar a vulnerabilidade.
Impacto da confidencialidade	Indica a medida do possível impacto na confidencialidade da vulnerabilidade. As opções são Nenhum, Baixo ou Alto

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Mudança de escopo	Indica se o escopo da avaliação foi alterado.
Impacto na disponibilidade	Indica o possível impacto na disponibilidade de uma vulnerabilidade de uso indevido explorada com sucesso. Disponibilidade se refere à acessibilidade dos recursos de informações. As opções são Nenhum, Baixo ou Alto
Impacto na integridade	Indica o possível impacto na integridade de uma vulnerabilidade de uso indevido explorada com sucesso. A integridade se refere à confiabilidade e à veracidade garantida das informações. As opções são Nenhum, Baixo ou Alto
Nível de correção	Indica o status ou a disponibilidade de correção para a vulnerabilidade. As opções são Correção oficial, Correção temporária, Solução alternativa, Indisponível, Não definido.
Maturidade do código de exploração	Indica a probabilidade de a vulnerabilidade ser explorada com base no estado existente das técnicas de exploração e na disponibilidade do código. As opções são Não comprovado, Prova de conceito, Funcional, Altoe Não definido.
Confiança do relatório	Indica o quanto você tem certeza de que a vulnerabilidade existe.

Tradução automática

7. Insira comentários relevantes no campo **Compor**.
   - Insira suas anotações de trabalho no campo Anotações de **trabalho (privadas)**.
   - Insira seus comentários (visíveis para todos) no campo **Comentários**.
8. **Salve** o registro de avaliação.
   Com base nas atualizações feitas nos campos de **atributo de risco** do CVE primário ou do produto afetado associado ao registro de avaliação, o campo de **pontuação de risco** é atualizado automaticamente.

> **Nota:** Para modificar as regras ou critérios da calculadora de pontuação de risco do sistema de base, navegue até **Todos** > **Calculadoras de avaliação de vulnerabilidade** > **Calculadora de risco da avaliação de vulnerabilidade** > **Regra de risco de avaliação de vulnerabilidade**. Você pode adicionar critérios e modificar a ponderação do nível de campo para os critérios existentes, conforme necessário.

O que Fazer Depois

Execute uma avaliação inicial do registro de eventos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Excluir CVEs associados ou produtos afetados do registro de avaliação de vulnerabilidade

Exclua um registro de evento de vulnerabilidade se ele não for mais necessário.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Você pode excluir CVEs ou produtos afetados associados ao registro de avaliação de vulnerabilidade. Você só pode excluir entradas de vulnerabilidade/CVEs associados ou produtos afetados se eles estiverem nos estados de avaliação **Novo** ou **Pendente**.

Procedimento
1. Navegar até **Todos** > **Espaços** > **Avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação de vulnerabilidade.
3. Selecione a guia **Entradas de vulnerabilidade** ou a guia **Produtos afetados**.
4. Selecione o CVE associado ou o registro do produto afetado.
5. Selecione **Excluir**.

> **Nota:** O botão **Excluir** é exibido somente para um registro de avaliação quando ele está nos estados **Novo** ou **Avaliação Pendente**.

Adicionar link relacionado ao registro de avaliação

Adicione links e informações adicionais relacionados ao registro de avaliação.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento
1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione a entrada de registro de avaliação.
3. Selecione a guia **Links relacionados**.
4. Insira uma descrição relevante no campo **Descrição**.
5. Insira o URL no campo **Link**.
6. Selecione **OK**.
   O link relacionado é adicionado e listado na guia Links relacionados.

Realizar uma avaliação

Depois de criar o registro de avaliação de vulnerabilidade e atualizar os campos de atributo de risco, execute uma avaliação do registro de evento.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Execute uma avaliação inicial depois que um evento para uma vulnerabilidade de interesse tiver sido criado e determinado como apresentando risco aos sistemas e dados. O objetivo desta atividade é analisar ainda mais a ameaça atualizando a avaliação de risco com uma avaliação de exposição detalhada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de vulnerabilidade**.
2. Selecione o registro relevante na lista de registros de eventos de avaliação de vulnerabilidade.
3. Selecione **Avaliar** para executar a avaliação de vulnerabilidade.
   O trabalho em segundo plano do evento Resposta a vulnerabilidades - Avaliação de vulnerabilidade do processo é iniciado e uma notificação relevante é exibida.
4. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
5. Selecione **Salvar**.

   A guia **Avaliações** exibe detalhes da avaliação. Quando a avaliação é processada, os VITs ou AVITs associados às entradas vulneráveis ou CVEs são exibidos nos **Itens vulneráveis** ou na guia **Itens vulneráveis da aplicação**.

Resultados

- Itens vulneráveis ou TPEs relacionados aos CVEs associados são obtidos durante a avaliação. Os ICs relacionados aos itens vulneráveis também são identificados e exibidos na tabela Itens de configuração afetados.
- Se os ICs associados não existirem na tabela de ICs afetados, os ICs identificados serão adicionados à tabela e o valor do campo **Tem item vulnerável** será definido como **Verdadeiro**e o valor do campo **Origem** será definido como Scanner.
- Se o IC já existir na tabela de ICs afetados, somente o valor do campo **Tem item vulnerável** será definido como **Verdadeiro** e o valor dos Campos de **origem** do IC permanecerá o mesmo de quando o registro de avaliação foi criado.
- Se itens vulneráveis forem criados após a avaliação, um trabalho agendado de avaliação de vulnerabilidade será executado para atualizar a tabela de ICs afetados e a origem do IC.

O que Fazer Depois

- Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade
- Adicionar ICs afetados ao registro de avaliação
- Criar itens vulneráveis para o IC afetado ou o componente de software afetado
- Adicionar link relacionado ao registro de avaliação

Informações relacionadas

Guia Avaliação

Guia Visão Geral

Guia Avaliação

Revise os resultados da avaliação na guia de avaliação. Depois de executar uma avaliação do evento de vulnerabilidade, o registro é correlacionado aos dados de Lista de materiais de software e Gestão de ativos de software e exibido com visualizações.

A guia de avaliação preenche os dados (se disponíveis) com base no registro de avaliação que você cria e correlaciona os detalhes com as avaliações dos dados dos componentes Gestão de ativos de software e Lista de materiais de software no CMDB.

Tradução automática

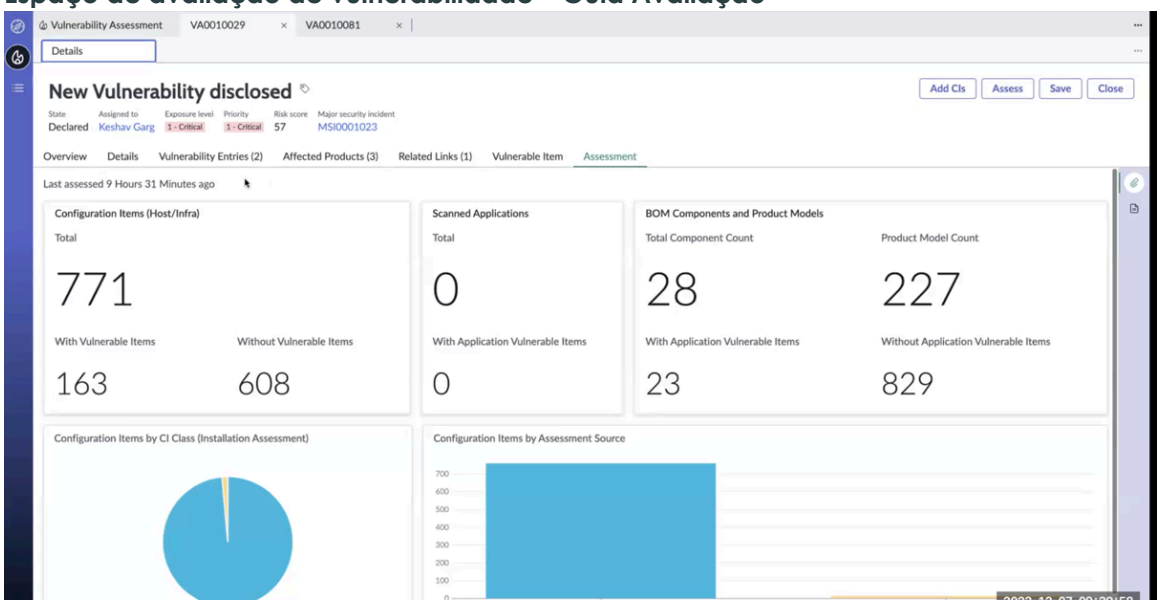
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como a avaliação funciona

Ao selecionar o botão **Avaliar**, uma avaliação de todos os CVEs relacionados e produtos afetados usando dados Gestão de ativos de software e SBOM é iniciada. Um trabalho em segundo plano é acionado e, quando a avaliação é processada, os VITs ou AVITs associados às entradas vulneráveis ou CVEs são exibidos nas guias Itens vulneráveis e **Itensvulneráveis da aplicação**.

- Todos os itens vulneráveis ou TPEs relacionados ao CVE são identificados.
- Os itens de configuração (ICs) relacionados aos itens vulneráveis também são identificados e exibidos na tabela de itens de configuração afetados.
- Se os ICs não estiverem presentes na tabela de ICs afetados, os ICs identificados serão adicionados à tabela e o sinalizador **Tem item vulnerável** será transformado em verdadeiro, e o valor do campo **Origem** será definido como Scanner.
- Se o IC já existir na tabela de itens de configuração afetados, somente o sinalizador **Tem item vulnerável** será definido como verdadeiro e a **Origem** permanecerá inalterada desde quando o registro de avaliação foi criado.
- Se itens vulneráveis forem criados após a avaliação, um trabalho agendado de avaliação de vulnerabilidade será executado para atualizar a tabela de ICs afetados e a origem do IC.
- No espaço de avaliação, você pode exibir carimbos de data/hora para ver a última avaliação dos eventos. A guia **Avaliação** fica visível somente quando as novas avaliações são criadas. Se a avaliação estiver no estado em andamento, o status da última avaliação aparecerá como a avaliação está em andamento. Para exibir o status de avaliação atualizado, você precisa atualizar a página. Depois que a avaliação for concluída, o usuário poderá ver todas as guias relacionadas a essa avaliação.

Espaço de avaliação de vulnerabilidade – Guia Avaliação



Os detalhes da avaliação são exibidos para os seguintes widgets.

- Itens de configuração (host/infraestrutura)
- Aplicações escaneadas
- Componentes da BOM e modelos de produto

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Itens de configuração por classe de IC (avaliação de instalação)
- Itens de configuração por origem de avaliação: exibe a lista de itens de configuração afetados.

Visualizações de dados

Nome	Tipo	Descrição
Itens de configuração (host/ infraestrutura)	Pontuação única	Exibe a contagem de ICs com e sem IVs. O widget Itens de configuração exibe a contagem total de ICs associados ao registro de avaliação. O widget exibe ainda os itens de configuração com itens vulneráveis e sem itens vulneráveis.
Aplicações escaneadas	Contagem	Contagem total de candidaturas verificadas com AVITs. **Nota:** Você pode exibir a contagem de aplicações verificadas para CVEs primários e secundários.
Componentes da BOM e modelos de produto	Pontuação única	Contagem total de componentes, contagem de modelo de produto, com itens vulneráveis de aplicação, sem contagem de itens vulneráveis de aplicação.
Itens de configuração por origem de avaliação	Barras empilhadas	Itens de configuração afetados empilhados pela origem da avaliação.
Itens de configuração por classe de IC (avaliação de instalação)	Gráfico de Pizza	Itens de configuração empilhados por classe de IC.

Guia Visão Geral

A visão geral dos detalhes da avaliação é exibida na guia Visão geral. Depois de executar a avaliação inicial, o registro é correlacionado aos dados de Lista de materiais de software e Gestão de ativos de software e exibido com visualizações.

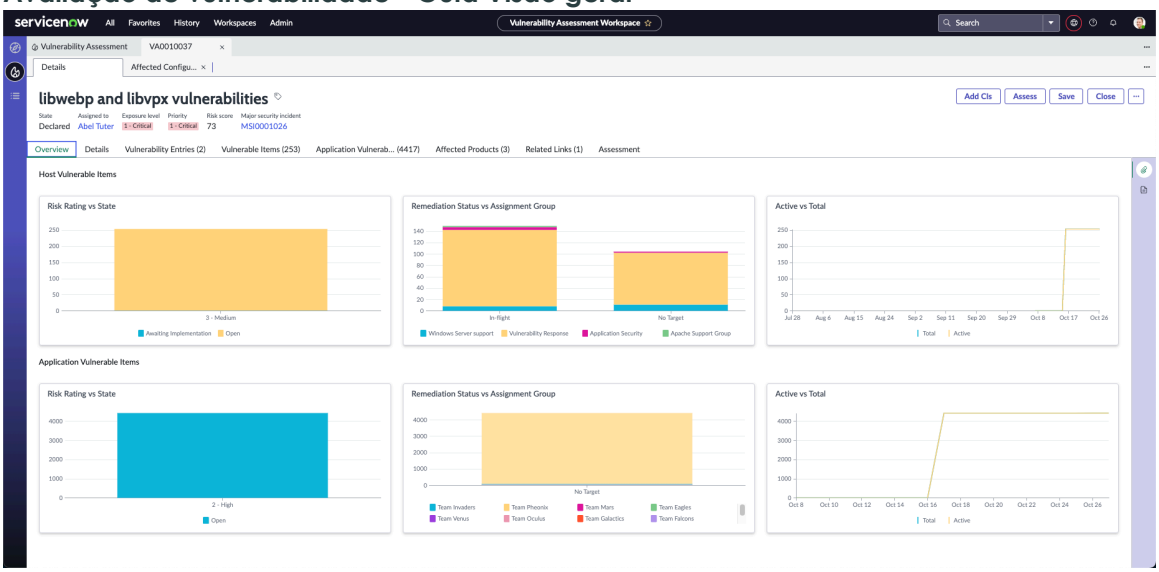
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão Geral

A guia Visão geral preenche os dados (se disponíveis) com base no registro de avaliação que você cria e correlaciona os detalhes com as avaliações de dados Gestão de ativos de software e Lista de materiais de software no CMDB. O

Avaliação de vulnerabilidade - Guia Visão geral



Os detalhes da avaliação são exibidos para os seguintes widgets.

- Itens vulneráveis de host (host/infraestrutura)
  - Classificação de risco x estado
  - Status de correção x Grupo de atribuição
  - Ativo x Total
- Itens vulneráveis da aplicação
  - Classificação de risco x estado
  - Status de correção x Grupo de atribuição
  - Ativo x Total

Visualizações de dados

Itens vulneráveis de host

Nome	Tipo	Descrição
Classificação de risco x estado	Barras empilhadas	Estado dos itens vulneráveis empilhados por sua classificação de risco.
Status de correção x Grupo de atribuição	Barras empilhadas	Status de correção do item vulnerável empilhado por seu grupo de atribuição.
Ativo x Total	Lista e linha	Total de itens vulneráveis associados a esta entrada versus itens vulneráveis ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Itens vulneráveis da aplicação

Nome	Tipo	Descrição
Classificação de risco x estado	Barras empilhadas	Estado dos itens vulneráveis da aplicação empilhados por sua classificação de risco.
Status de correção x Grupo de atribuição	Barras empilhadas	Status de correção do item vulnerável da aplicação empilhado por seu grupo de atribuição.
Ativo x Total	Lista e linha	Total de itens vulneráveis da aplicação associados a esta entrada versus itens vulneráveis ativos.

Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade

Atribua manualmente a prioridade e o nível de exposição ao registro de avaliação de vulnerabilidade.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione um registro de avaliação de vulnerabilidade.
3. Navegue até **Atributos de risco** na guia **Detalhes**.
4. Selecione uma **Prioridade** na lista de opções.
5. Selecione um **Nível de exposição** na lista de opções.
6. Selecione **Salvar**.

Adicionar ICs afetados ao registro de avaliação

Adicione manualmente os ICs em sua organização que você acha que devem estar associados ao registro de avaliação de vulnerabilidade, mas não são exibidos nos ICs afetados após a avaliação inicial.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Adicione ICs que você sabe que podem ter sido afetados, mas não aparecem após a conclusão da avaliação. Você só pode adicionar ICs quando o registro de avaliação está no estado de avaliação **Declarado** ou **Pendente**.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação necessário na lista.
3. Selecione **Adicionar ICs**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione os itens de configuração na caixa de diálogo Itens de configuração.
5. Selecione **Adicionar ICs**.
   O trabalho em segundo plano da Resposta a vulnerabilidades - Adicionar itens de configuração ao evento é iniciado e uma notificação relevante é exibida.
6. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.

Resultados
Os registros são adicionados à tabela Itens de configuração afetados com a **Origem** como *Manual*.

O que Fazer Depois
Navegue até a guia **Avaliação** e atualize o widget **Itens de configuração (Host/ Infraestrutura)** para exibir os ICs que você adicionou.

Criar itens vulneráveis para o IC afetado ou o componente de software afetado

Crie itens vulneráveis (VIs) ou itens vulneráveis de aplicação (AVITs) no Espaço de avaliação de vulnerabilidade. Os analistas de vulnerabilidade analisam a lista de IVs e recomendam soluções e patches que ajudam a equipe de TI a corrigir essas vulnerabilidades.

O gerenciador de eventos de vulnerabilidade deve ser capaz de selecionar um, muitos ou todos os resultados da pesquisa de exposição para criar itens de vulnerabilidade.

- Item vulnerável da aplicação para resultados de avaliação SBOM que não têm AVITs associados
- Itens vulneráveis para itens de configuração que não têm VITs associados
- Associe o CVE primário aos itens de vulnerabilidade.

Criar IVs para itens de configuração sem itens vulneráveis associados

Crie VITs de itens vulneráveis para itens de configuração identificados por meio da avaliação de vulnerabilidade, mas não tenham VITs associados ao registro.

Antes de Iniciar
Função necessária: administrador

Procedimento
1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliações**.
2. Selecione o registro de avaliação para o qual você precisa criar o VIT.
3. Selecione a guia **Avaliação**.
4. Selecione **Sem** contagem de itens de **configuração no widget Itens de configuração (infraestrutura do host)**.
5. Selecione os Itens de configuração para os quais você deseja criar VITs na lista **Itens de configuração afetados**.
6. Selecione **Criar item vulnerável**.
   O trabalho em segundo plano Resposta a vulnerabilidades - Criar VITs manuais Avaliação de vulnerabilidade é iniciado e uma notificação relevante é exibida.
7. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
   Itens vulneráveis para os itens de configuração afetados que você selecionou são criados.

   O widget **Itens de configuração (Infraestrutura do host)** agora exibirá o mesmo IC na contagem **Com itens vulneráveis**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar itens vulneráveis de aplicação (AVITs) para modelos de produtos afetados ou componentes sem itens vulneráveis de aplicação associados

Crie itens vulneráveis de aplicação (AVITs) para produtos afetados ou itens de componentes identificados por meio da avaliação de vulnerabilidade, mas não tenham AVITs associados ao registro.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliações**.
2. Selecione o registro de avaliação para o qual você precisa criar o VIT.
3. Selecione a guia **Avaliação**.
4. Selecione **Sem contagem de itens vulneráveis de aplicação** no widget **Componentes da lista de materiais e Modelos de produto**.
5. Selecione os modelos de produto afetados para os quais você deseja criar AVITs na lista **Modelos de produtos afetados**.
6. Selecione **Criar item vulnerável da aplicação**.
   O trabalho em segundo plano Resposta a vulnerabilidades - Criar VITs manuais Avaliação de vulnerabilidade é iniciado e uma notificação relevante é exibida.
7. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
   Itens vulneráveis de aplicação para os itens de modelos de produto afetados que você selecionou são criados. para o CVE primário associado ao registro.

   Os **componentes da lista de materiais e o widget de modelos de produto** agora exibirão o mesmo modelo de produto ou componente na contagem de **itens vulneráveis da aplicação**.

Vincule o registro de avaliação de vulnerabilidade ao incidente de segurança grave em Gestão de incidentes graves de segurança

Você pode vincular, propor ou promover o registro de avaliação para um Incidente grave de segurança, desde que tenha acesso à aplicação Gestão de incidentes graves de segurança.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode mover o registro de avaliação para ser associado a um incidente de segurança grave existente, criar um novo MSI a partir do registro de avaliação ou promover o registro de avaliação de vulnerabilidade a um incidente de segurança grave. Aproveite os recursos Gestão de incidentes graves de segurança, como as integrações com Microsoft Teams e Microsoft SharePoint.

Você também pode exibir o link para incidentes de segurança graves no Espaço do gerenciador de vulnerabilidades para itens vulneráveis. O link MSIM será associado à avaliação vulnerável que será mostrada nos itens de vulnerabilidade e também nos outros espaços de Resposta a vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação que você deseja vincular a um incidente de segurança grave.
3. Selecione o ícone **Mais ações**, na guia **Detalhes**.
4. Selecione uma das seguintes opções.

Opção	Descrição
Link para o incidente de segurança grave	Selecione o registro do MSI existente na lista de Incidentes de segurança graves. O registro de avaliação de vulnerabilidade está vinculado ao incidente de segurança grave existente.
Propor como incidente de segurança grave	Insira os seguintes detalhes e selecione **Propor**. ◦ Data de detecção ◦ Justificativa ◦ Impacto potencial
Promover como incidente de segurança grave	Insira os seguintes detalhes e selecione **Promover**. ◦ Data de detecção ◦ Data de resolução estimada ◦ Justificativa ◦ Impacto potencial

5. Selecione **Salvar**.

O que Fazer Depois

Selecione o registro MSI para abrir o registro na exibição Gestão de incidentes graves de segurança.

Informações relacionadas

Vincular a Incidente grave de segurança

Propor como um Incidente grave de segurança

Promover para um Incidente grave de segurança

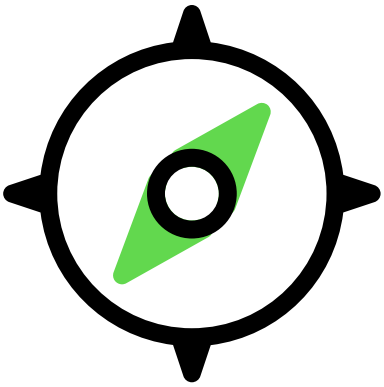
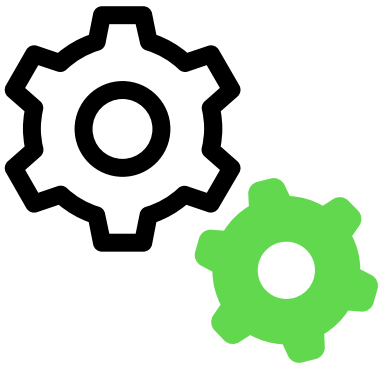
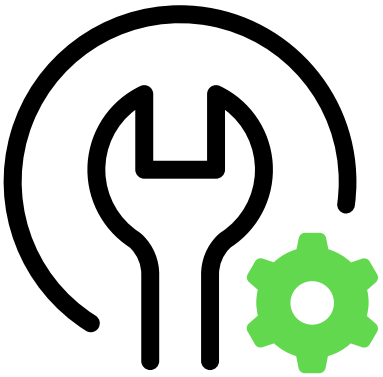
Lista de materiais de software

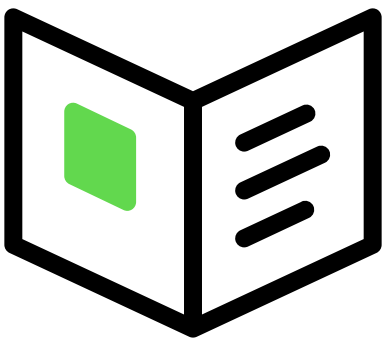
Exiba uma lista dos componentes de software de código aberto e de terceiros que você está usando no desenvolvimento de aplicações. Obtenha informações sobre licenças de software, informações de versão e vulnerabilidades conhecidas em seus componentes nos arquivos Lista de materiais de software (SBOM) que você carrega em sua instância.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Primeiros passos

Explorar	Configurar	Uso
		
Saiba mais sobre SBOM conceitos e recursos.	Configure SBOM aplicações.	Saiba como importar SBOM componentes e exibir dados no espaço.

Referência

Veja detalhes sobre SBOM formulários, campos, tabelas e propriedades.

Tradução automática

Solucionar problemas e obter ajuda

- Comunidade das Operações de segurança
- CycloneDX - Lista de materiais de software (SBOM) .
- SPDX .
- Pesquise artigos de erros conhecidos no Portal de erros conhecidos .
- Contato Suporte e atendimento ao cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exploração do Lista de materiais de software

Identifique os componentes usados nas aplicações da sua organização a partir de Lista de materiais de software (SBOM) arquivos que você carrega em sua instância. Entenda todos os riscos associados ao uso de software de código aberto para ajudá-lo a determinar sua possível exposição e corrigir vulnerabilidades.

Versões Lista de materiais de software disponíveis

Versão de lançamento	Notas de versão
Modelo de dados para SBOM v 2.0, v1.4, v1.3, v1.1, v1.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão Notas de versão Resposta a vulnerabilidades de aplicações
SBOM Núcleo v4.0, v3.0, v2.1, v2.0, v1.0	
SBOM Resposta v4.0, v3.2, v3.1, v3.0, v2.0	

Caso de uso do SBOM

A partir das versões listadas na tabela, há suporte para casos de uso de operações de desenvolvimento de software (DevOps) para carregar SBOM arquivos de pipelines de integração contínua e entrega/implantação contínua (IC/CD). Para obter mais informações, consulte Carregando Lista de materiais de software para arquivos de DevOps SBOM.

Versão de lançamento	Aplicação
v1.4 e posterior	Modelo de dados para SBOM
v3.0 e posterior	SBOM Núcleo
v4.0 e posterior	SBOM Resposta

Componentes de terceiros e de código aberto oferecem muitas vantagens para a criação e a liberação rápidas de seus projetos de software. No entanto, em alguns casos, há riscos associados ao uso de componentes acessíveis publicamente, como os seguintes:

- Falta de visibilidade na integridade do componente
- Vulnerabilidades no software de código aberto
- Inteligência de pacote para software de código aberto

Três Lista de materiais de software aplicações permitem que você exiba um inventário preciso de seus componentes de software e riscos associados:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Modelo de dados para SBOM
- SBOM Núcleo
- SBOM Resposta

Você pode carregar seus arquivos de lista de materiais de software por meio de uma API ou manualmente. Exiba os arquivos importados como entidades, que são inventários das bibliotecas de componentes de terceiros usadas em seu software, incluindo quaisquer dependências transitivas.

Para obter mais informações sobre o que está incluído nos inventários de software nos SBOMs CycloneDX e SPDX, consulte CycloneDX - Software Bill of Materials (SBOM) e SPDX .

Modelo de dados para SBOM

Esta aplicação fornece as tabelas usadas para armazenar dados de SBOM.

SBOM Núcleo

A partir da v3.0 do SBOM Core, carregue, analise e processe seus arquivos de lista de materiais de software nos padrões CycloneDX e SPDX. Consulte a tabela a seguir para obter os formatos de arquivo e versões compatíveis com esses produtos. Exiba entidades de lista de materiais (BOM) e um inventário de seus componentes de software. Uma entidade de lista de materiais é o componente de nível raiz em um arquivo SBOM. Por exemplo, para um SBOM CycloneDX, o componente listado nos metadados é considerado a entidade da lista de materiais.

Versão do SBOM Core	Versões compatíveis de CycloneDx e SPDX
v4.0	XML e JSON no CycloneDx (versões 1.0 - 1.6) JSON em SPDX (versões 2.2-2.3)
v3.0	XML e JSON no CycloneDX (até a versão 1.4, inclusive) XML no SPDX (até e incluindo v2.3)

Consulte a seção intitulada Como usar a REST API em Carregando Lista de materiais de software arquivos usando uma REST API para obter mais informações sobre melhorias para oferecer suporte ao formato CycloneDX.

A partir da versão 4.0 do SBOM Core, você pode carregar SBOM arquivos para o Now Platform® de seus repositórios GitHub.

Determine se SBOM arquivos gerados em seus pipelines de IC/CD (integração contínua e entrega/implantação contínuas) foram enfileirados com sucesso em sua instância Now Platform®.

- Proteja seus ambientes de componentes potencialmente prejudiciais durante os ciclos de desenvolvimento de software com GitHub Ações que você inicia em seu ambiente GitHub.
- Obtenha todas as GitHub Ações necessárias para SBOM upload no GitHub Marketplace.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SBOM Resposta

Exiba seu inventário de componentes e avalie sua exposição a riscos no espaço SBOM. Você pode identificar se há vulnerabilidades conhecidas associadas a componentes de software e exibir informações de licenciamento e versão junto com outros detalhes.

Consulte a tabela a seguir para obter mais informações sobre cada aplicação ServiceNow® SBOM.

Aplicações necessárias para SBOM

ServiceNow **aplicativo**	**Descrição**
Modelo de dados para SBOM	Esta aplicação é necessária. Inclui as tabelas, ACLs e funções necessárias para ler SBOM dados.
SBOM **Núcleo**	Esta aplicação é necessária. Inclui a API necessária para carregar SBOM documentos e a lógica de negócios necessária para analisar e importar os dados desses documentos para sua instância. A partir da versão 2.1, você pode exibir um inventário dos componentes de software no espaço SBOM.
SBOM **Resposta**	A partir da versão 4.0 da resposta SBOM, você pode exibir os componentes identificados como obsoletos ou abandonados como "Fora de conformidade" na interface PaCE (Policy as Code Engine), que está disponível no espaçoSBOM. • Determine se os componentes estão obsoletos ou abandonados com o trabalho agendado Executar políticas de PaCE para resposta de SBOM. O trabalho agendado está desativado por padrão. • Exiba os componentes identificados como obsoletos ou abandonados como fora de conformidade na interface PaCE que está disponível no espaço do SBOM. SBOM A resposta requer a aplicação Resposta a vulnerabilidades. Instale a aplicação Resposta a vulnerabilidades antes de instalar a resposta SBOM. Exiba seu inventário de componentes e avalie sua exposição a riscos no espaço SBOM. Configure regras para criar itens vulneráveis de aplicação (AVITs) automaticamente e corrija-os com o fluxo de trabalho da Resposta a vulnerabilidades da aplicação. As integrações OSV.dev e Deps.dev são incluídas quando você instala o SBOM Response.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações necessárias para SBOM

ServiceNow **aplicativo**	**Descrição**
	• OSV.dev é uma API de código aberto que fornece informações de inteligência de vulnerabilidade para uma determinada versão de um pacote ou biblioteca. • Deps.dev é uma API de código aberto que fornece uma lista de versões para um determinado pacote ou biblioteca.

A instalação da inteligência de vulnerabilidade de terceiros compatível e outras integrações permite que você exiba as contagens de componentes considerados obsoletos e abandonados, bem como informações sobre se você pode corrigir vulnerabilidades associadas aos componentes. As aplicações ServiceNow® e integrações de terceiros listadas na tabela a seguir são compatíveis com a aplicação SBOM. Essas aplicações fornecem dados de vulnerabilidade aprimorados, inteligência de vulnerabilidade e outras informações importantes que podem ajudá-lo a exibir e priorizar as vulnerabilidades associadas aos arquivos SBOM. Todas essas aplicações e integrações estão disponíveis no ServiceNow Store.

Aplicações de terceiros compatíveis com SBOM

Aplicação	**Descrição**
Resposta a vulnerabilidades	Necessário se você instalar a aplicação SBOM Response. Resposta a vulnerabilidades de aplicações recursos são instalados com Resposta a vulnerabilidades. Esses recursos permitem o acesso ao Espaço do gerenciador de vulnerabilidades na aplicação Resposta a vulnerabilidades e ao fluxo de trabalho de vulnerabilidade para ajudá-lo a corrigir itens vulneráveis da aplicação (AVITs).
Vulnerability Response Integration with NVD	Exiba dados aprimorados de vulnerabilidade e gravidade do NVD. Se você instalou o SBOM Response, poderá exibir os dados importados das integrações do NVD e do CWE para aprimorar todos os dados de vulnerabilidade encontrados nos dados do SBOM. Para obter mais informações, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.
Veracode Vulnerability Integration	A versão 4.3 do Veracode Vulnerability Integration inclui os seguintes aprimoramentos com arquivos Veracode SBOM :

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de terceiros compatíveis com SBOM

Aplicação	Descrição
	• Se você instalou o SBOM Response, terá a opção de incluir vulnerabilidades encontradas por Veracode nos arquivos SBOM carregados. • Veracode é mapeado para o campo **Origem** para registros na tabela Lista de materiais [sn_sbom_doc] para os arquivos Veracode SBOM que você carrega. Importe listas de materiais de software com o Veracode Vulnerability Integration. Se você já tiver esta integração instalada, também poderá carregar dados Veracode SBOM importados nos formatos CycloneDX (JSON e XML) e SPDX (XML) a partir da versão v3.0 do SBOM Core.

Instalar as aplicações compatíveis com Lista de materiais de software

Baixe e ative as aplicações necessárias para a aplicação Lista de materiais de software (SBOM) antes de carregar arquivos.

Antes de Iniciar

Funções necessárias: administrador para download, instalação e ativação de todas as aplicações e atribuições de função em sua instância.

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Baixe as aplicações [SBOM necessárias da instância ServiceNow Store para sua instância ServiceNow.

   Essas aplicações permitem que você carregue e importe SBOM arquivos para sua instância. Você pode exibir os dados do componente no SBOM Workspace que começa com v2.1 do SBOM Core.

   - Modelo de dados para SBOM
   - SBOM Núcleo

   Para obter mais informações sobre como baixar e ativar aplicações, consulte o seguinte:

   - Operações de segurança e a ServiceNow Store
   -

2. Opcional: Se você quiser exibir seus dados [SBOM no espaço SBOM, exibir a inteligência de vulnerabilidade de terceiros importada, avaliar sua exposição a riscos e corrigir vulnerabilidades com os fluxos de trabalho da Resposta a vulnerabilidades da aplicação e da Resposta a vulnerabilidades, baixe as seguintes aplicações:

   - Resposta a vulnerabilidades e suas dependências
   - Vulnerability Response Integration with NVD
   - SBOM Resposta

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre essas e outras aplicações SBOM compatíveis, consulte Exploração do Lista de materiais de software.

3. Depois de baixar as aplicações, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
4. Localize as SBOM aplicações que você baixou e selecione **Instalar** para ativá-las junto com suas dependências.

   Uma mensagem é exibida depois que uma aplicação é ativada com sucesso. Ative as aplicações na seguinte ordem:

   - Resposta a vulnerabilidades e suas dependências
   - Vulnerability Response Integration with NVD
   - Modelo de dados para SBOM
   - SBOM Núcleo
   - SBOM Resposta, que inclui as integrações OSV.dev e Deps.dev

   Consulte Como configurar as integrações Deps.dev e OSV.dev para Lista de materiais de software para obter mais informações sobre como configurar essas aplicações de integração depois de instalar o SBOM Response.

5. Opcional: Ative integrações navegando até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e selecionando **Instalar**.

   (Optional) Para obter mais informações sobre essas integrações e os recursos que elas fornecem, consulte Exploração do Lista de materiais de software.

   - Vulnerability Response Integration with Veracode. Para obter mais informações, consulte Instalar a ServiceNow Integração de resposta a vulnerabilidades com Veracode.
   - Vulnerability Response Integration with NVD, que é necessária se você quiser exibir os dados aprimorados de vulnerabilidades associadas aos componentes carregados. Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.
   - Integração do CWE Comprehenctive 2000. Consulte Configure e execute o trabalho agendado para atualizar registros de CWE para obter mais informações sobre como ativar este trabalho agendado.

   Uma mensagem é exibida depois que uma aplicação é ativada com sucesso.

6. Atribua as seguintes funções aos usuários.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
7. Opcional: Atribua usuários ao grupo de gerentes de App-Sec se você estiver criando itens vulneráveis de aplicação para vulnerabilidades em seus dados SBOM importados.

   (Optional) Usuários atribuídos ao grupo de gerentes de App-Sec priorizam e gerenciam itens vulneráveis da aplicação. Os usuários neste grupo herdam muitas das funções

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

necessárias para ler e editar registros e configurar as aplicações compatíveis com a aplicação Resposta a vulnerabilidades de aplicações e seus fluxos de trabalho de correção.

O que Fazer Depois
Carregue seus arquivos SBOM. Para obter mais informações, consulte Carregar Lista de materiais de software arquivos manualmente e Carregando Lista de materiais de software arquivos usando uma REST API.

Como configurar as integrações Deps.dev e OSV.dev para Lista de materiais de software

Você pode editar alguns dos parâmetros das integrações Deps.dev e OSV.dev. Há duas integrações de gatilho de código que são usadas estritamente para fluxos de trabalho internos.

Integrações de gatilho de código para fluxos de trabalho internos

A partir da v3.2 do SBOM Response, as melhorias de desempenho incluíram a adição de duas integrações para OSV.dev e Deps.dev:

- Integração de OSV (gatilho de código sob demanda)
- Integração Deps.dev (gatilho de código sob demanda)

Essas integrações são iniciadas automaticamente por fluxos de trabalho internos e são somente para uso interno. Você não deve iniciar essas integrações sob demanda com o botão **Executar agora** em seus registros de integração.

Configurando a programação de execução para Deps.dev

Se instalada, a integração Deps.dev será ativada (caixa de seleção Ativo marcada no registro de integração) por padrão e programada para ser executada semanalmente. Você pode editar a programação e iniciar o trabalho agendado sob demanda a partir do registro de integração. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Integrações** > **Integração Deps.dev**. A função sn_vul.app_configure_integrations é necessária para editar a programação desta integração.

A integração Deps.dev é usada para identificar componentes que estão nos estados **Obsoleto** e **Abandonado**. A versão de um componente obsoleto está mais de duas versões principais atrás da versão mais recente e dois anos atrás da versão mais recente. Um componente abandonado não foi atualizado por mais de dois anos. Os limites de dois anos e duas versões podem ser editados com as propriedades do sistema. Para editar esses parâmetros, navegue até **Todos** > **Propriedades do sistema** > **Todas as Propriedades** e localize os seguintes registros:

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Os valores de limite para abandonados e obsoletos estão em meses. O valor de limite para a versão é numérico.

Configurando OSV.dev

Se instalada, a integração do OSV.dev será ativada (caixa de seleção Ativa marcada no registro de integração) por padrão. No entanto, você deve iniciá-la sob demanda a partir do registro de integração. Navegar até **Todos** > **Resposta a vulnerabilidades** > **Integrações** >

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

OSV.dev Integration - Abrangente. A função sn_vul.app_configure_integrations é necessária para editar a programação desta integração.

Nota: Você pode configurar o parâmetro de integração *batchSize* do OSV.dev na Integração de vulnerabilidades de código aberto. O padrão é 75 Purls por chamada de API.

Você pode preferir deixar este valor em sua configuração padrão. Alterar o valor pode afetar o desempenho.

Usando o Lista de materiais de software Workspace

As aplicações SBOM permitem que você carregue arquivos e exiba detalhes de entidades e inventários de componentes no espaço Lista de materiais de software (SBOM).

As aplicações SBOM permitem que você execute as seguintes tarefas:

1. Carregue arquivos com uma API ou manualmente.

   Consulte Carregando Lista de materiais de software arquivos usando uma REST API e Carregar Lista de materiais de software arquivos manualmentee Carregando Lista de materiais de software para arquivos de DevOps SBOM para obter mais informações.

2. Revise os componentes da lista de materiais carregados no espaço. A forma como você revisa os componentes depende das aplicações instaladas.

   Para obter mais informações, consulte Exibição de relatórios e painéis no espaço Lista de materiais de software.

3. Avalie sua exposição a riscos e crie itens vulneráveis de aplicação para componentes que tenham vulnerabilidades associadas.
   - Identifique se há vulnerabilidades conhecidas associadas a componentes de software.
   - Revise os detalhes aprimorados da inteligência de vulnerabilidade, como informações de versão, disponibilidade de versões fixas e informações de licenciamento para ajudá-lo a resolver itens vulneráveis.

   Para obter mais informações, consulte Exibição de relatórios e painéis no espaço Lista de materiais de software e Criação de regras para itens vulneráveis de aplicação no espaço Lista de materiais de software.

Carregando Lista de materiais de software arquivos usando uma REST API

Revise as informações a seguir antes de carregar arquivos Lista de materiais de software usando uma API.

Como usar a REST API

Para carregar um arquivo SBOM com uma API, a função sn_sbom_core.sbom_ingest é necessária.

Carregar API.

Esta API é usada para carregar e ingerir um arquivo SBOM (CycloneDX/SPDX) em sua instância.

A versão 4.0 do SBOM Core é compatível com:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- XML e JSON no CycloneDx (versões 1.0 - 1.6).
- JSON em SPDX (versões 2.2-2.3)

- **Nota:** Arquivos com mais de 32 MB podem não ser carregados corretamente.

Método HTTP: (POST)

URL da API:<host_name> `/api/sbom/core/upload`

Nota: <host_name>é o nome da sua instância ServiceNow .

Todos os parâmetros de solicitação abaixo são opcionais. o corpo da solicitação é o conteúdo do arquivo SBOM. Se você estiver usando o DevOps como parte do processo de desenvolvimento, o valor de "requestedBy" deve ser "devops". Consulte Carregando Lista de materiais de software para arquivos de DevOps SBOM para obter informações gerais sobre DevOps. Se o valor de "requestedby" for "devops" (operações de desenvolvimento), estes parâmetros serão obrigatórios:

- buildId
- lifecycleStage

Além disso, se "requestedBy" for "devops", os dados para fetchVulenrabilityInfo e fetchPackageInfo serão incluídos.

- buildId- cadeia de caracteres que você envia
- lifecycleStage- dois valores, produção ou pré-produção
- fetchVulenrabilityInfo- t/f
- fetchPackageInfo-t/f

Parâmetros de solicitação	Valores possíveis	Descrição
productModelId	SYS ID	SYS ID do modelo de produto a ser mapeado com a aplicação raiz de determinado SBOM.
businessApplicationId	SYS ID	SYS ID da aplicação de negócios a ser mapeada com a aplicação raiz de determinado SBOM.
businessApplicationName	O nome da sua aplicação de negócios	Nome da aplicação de negócios a ser mapeada com a aplicação raiz de determinado SBOM.
sbomSource	Um produto como Vericode, por exemplo	A origem do arquivo SBOM.
requestedBy	Uma ferramenta ou nome de uma metodologia, Jenkins. Se você usar "devops", buildId e lifecycleStage serão obrigatórios.	Carregamento solicitado por

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de solicitação	Valores possíveis	Descrição
buildId	Um solicitante de cadeia de caracteres envia.	ID da compilação do SBOM.
lifecycleStage	produção ou pré_produção	Fase do ciclo de vida da entidade.
fetchVulenrabilityInfo	T/F	Se verdadeiro, aciona a integração de inteligência de vulnerabilidade.
Informações do fetchPackage	T/F	Se verdadeiro, aciona a integração de inteligência de pacote.

Resposta da API de upload: incluiu "status" com sucesso/falha, "message" (cadeia de caracteres), "bomRecordId" (este é o SYS ID do SBOM que é retornado por meio da API de upload para um carregamento de SBOM bem-sucedido.

```
{
"result": {
"status": "success",
"message": "Queued for processing.",
"bomRecordId": "f207059b4393c290629aa597cbb8f247"
}
}
```

API de status

Esta API obtém o status e o resumo de um SBOM que está na fila para ingestão.

- URL da API: `/api/sbom/core/upload/status`
- Método HTTP (GET)

Parâmetros de solicitação	Valores possíveis	Descrição
bomRegistroId	SYS ID	ID do registro de SBOM que é retornado por meio da API de upload para um carregamento de SBOM bem-sucedido.

Exemplo de resposta padrão da API de status.

```
{
   "result": {
      "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
      "uploadStatus": "processed",
      "additionalInfoStatus": "not_requested",
      "uploadSummary": {
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
        "components": {
           "added": 0,
           "removed": 0,
           "total": 70
        }
      }
    }
}
```

Exemplo de resposta da API Status com parâmetros adicionais. Se você solicitou fetchVulenrabilityInfo para esse SBOM, receberá o detalhamento da vulnerabilidade como parte da resposta.

```
{
 "result": {

  "bomRecordId": "93af349b4393c290629aa597cbb8f258",

  "uploadStatus": "processed",

  "additionalInfoStatus": "complete",

  "uploadSummary": {

    "components": {

     "added": 0,

     "removed": 0,

     "total": 3

   },

   "vulnerabilityInfo": {

    "critical": 0,

    "high": 0,

    "medium": 0,

    "low": 0,

    "none": 0

   }

  },

  "buildId": "1"

 }

}
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você solicitou fetchPackageInfo para esse SBOM, obterá contagens obsoletas e abandonadas como parte da resposta.

Depois que um SBOM é processado com sucesso, o local onde você exibe os registros carregados depende das aplicações que você está usando.

- Se você estiver usando a resposta SBOM, o registro de entidade da lista de materiais será exibido na lista de status de ingestão SBOM no módulo Fila da lista de materiais no espaço SBOM.
- Se você estiver usando o SBOM Core, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**.

Melhorias nos padrões SBOM compatíveis e informações de uso geral

A versão 4.0 do SBOM Core é compatível com:

- XML e JSON no CycloneDx (versões 1.0 - 1.6).
- JSON em SPDX (versões 2.2-2.3)

- **Nota:** Arquivos com mais de 32 MB podem não ser carregados corretamente.

A partir da v4.0 do SBOM Core, os seguintes aprimoramentos foram feitos para oferecer suporte aos padrões CycloneDx para as versões 1.0 - 1.6:

- Importe informações adicionais em arquivos SBOM do CycloneDX com a propriedade (sn_sbom_core.collect_properties). Esta propriedade está desativada por padrão. Ative a propriedade para importar informações que geralmente não são compatíveis. Todas as informações importadas dessas propriedades são carregadas na tabela Propriedade do componente SBOM [sn_sbom_comp_property] para o seguinte:
  - Arquivos SBOM carregados
  - Metadados
  - Vulnerabilidades individuais
  - Componentes
- Exiba os dados do componente importado para licenças declaradas e concluídas para arquivos SBOM nas versões 1.4 e posteriores do CycloneDX em dois novos campos de licença:
  - **Declarado**
  - **Concluído**
- O suporte à análise de SBOM foi estendido para os seguintes tipos de componente do CycloneDX:
  - Versão 1.5: plataforma, dados, driver de dispositivo, modelo de aprendizado de máquina
  - Versão 1.6: Criptográfica

A versão 3.0 do SBOM Core é compatível com:

- XML e JSON no CycloneDx (até e incluindo a versão 1.4).
- JSON em SPDX (até e incluindo v2.3).

Se o usuário de chamada for autenticado com sucesso e tiver a função sn_sbom_core.sbom_ingest na instância ServiceNow, você poderá acessar a API de fora da instância para carregar os dados SBOM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que os dados são carregados, eles são analisados. Antes que os dados sejam analisados, os seguintes requisitos são verificados:

- Os dados de entrada são verificados para garantir que sejam JSON ou XML válidos.
- O formato da lista de materiais é compatível. A partir da versão 2.1 do SBOM Core, os formatos CycloneDX (JSON e XML) e SPDX (XML) são compatíveis.
- Os campos mínimos estão disponíveis para que os dados possam ser analisados.

Depois que essas verificações são verificadas, uma entrada é feita na tabela Lista de materiais [sn_sbom_doc] com dados de entrada SBOM como um anexo.

A regra de negócio *Process BOM file* é acionada automaticamente como resultado da inserção de registro e da análise de dados.

Nota: Esta regra de negócio é ativada durante a instalação do SBOM Core por padrão.

Todos os componentes listados em SBOM têm um `tipo`definido.

- Os componentes para os quais os arquivos SBOM foram carregados são considerados entidades da lista de materiais.
- Os componentes listados como `type=library` são considerados componentes de terceiros.

Informações relacionadas

Exibição do status de carregamento de Lista de materiais de software arquivos

Exibição de relatórios e painéis no espaço Lista de materiais de software

Carregar Lista de materiais de software arquivos manualmente

Carregar Lista de materiais de software (SBOM) arquivos manualmente.

Antes de Iniciar

Função necessária: sn_sbom_core.sbom_ingest

Procedimento

1. Carregar arquivos manualmente.

   O método usado para carregar seus arquivos depende se você tem as aplicações SBOM Core ou SBOM Response instaladas.

   A partir da v4.1 do SBOM Core, os seguintes formatos de arquivo SBOM são compatíveis:

   - XML e JSON no CycloneDX (versões 1.0- 1.6).
   - JSON em SPDX (versões 2.2 - 2.3).

Opção	Descrição
Se você instalou o SBOM Core	**a.** Navegar até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**. **b.** Na lista Lista de materiais, selecione **Novo**. **c.** Selecione o link **Clique para adicionar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Você pode carregar apenas um arquivo SBOM de cada vez. **d.** Selecione **Escolher arquivo** e localize o arquivo desejado. O nome do arquivo é exibido na página Escolher um arquivo de anexo. **e.** Selecione **OK**.
Se você instalou SBOM Resposta	**a.** Navegar até **Todos** > **Espaços** > **Espaço de SBOM** > **Fila de lista de materiais**. **b.** Selecione **Carregar lista**de materiais . **c.** Selecione **Procurar** e localize o arquivo desejado. Você pode carregar apenas um arquivo SBOM de cada vez. **d.** Selecione **Carregar**. O arquivo é exibido na caixa de diálogo Carregar SBOM Arquivo. **e.** Selecione **Carregar** novamente.

2. Opcional: Carregar SBOM arquivos importados pelo Veracode Vulnerability Integration.

Nota: Você pode carregar Veracode arquivos nos formatos CycloneDX (JSON e XML) e SPDX (XML) somente se tiver instalado e ativado a integração [Veracode com Resposta a vulnerabilidades de aplicações. Consulte Veracode Vulnerability Integration para obter mais informações.

Resultados
Depois que um SBOM é processado com sucesso, o local onde você exibe o status de carregamento depende das aplicações que você está usando.

- Se você estiver usando a resposta SBOM, o registro de entidade da lista de materiais será exibido na lista de status de ingestão SBOM no módulo Fila da lista de materiais no espaço SBOM.
- Se você estiver usando o SBOM Core, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**.

Informações relacionadas

Carregando Lista de materiais de software arquivos usando uma REST API

Carregando Lista de materiais de software para arquivos de DevOps SBOM

Gere e carregue Lista de materiais de software SBOM arquivos para software em toda a integração contínua e ciclos de desenvolvimento de implantação contínua.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SBOMs e operações de desenvolvimento de software

SBOM arquivos podem ser gerados em vários estágios em todo o ciclo de vida de desenvolvimento da integração contínua de software e implantação contínua (IC/CD). A maioria das operações de desenvolvimento de software (DevOps) nas organizações usa algum tipo de processo de IC/CD para ajudá-las a identificar e evitar erros custosos que podem surgir após a versão. Em todo o pipeline de IC/CD, o DevOps pode gerar arquivos SBOM e verificar proativamente se há vulnerabilidades e componentes em risco. Essas verificações podem ajudar as organizações a obter melhor qualidade de software e evitar manutenções dispendiosas posteriormente. Gerar arquivos SBOM é essencial para implementar e automatizar com sucesso avaliações de compilação precisas durante o desenvolvimento de IC/CD.

O carregamento de arquivos SBOM de pipelines de desenvolvimento é compatível a partir das seguintes versões das aplicações SBOM.

Versões compatíveis

Aplicação	Versões compatíveis
Modelo de dados para SBOM	v2.0, v1.4
SBOM Núcleo	v4.0, 3.0
SBOM Resposta	v3.2, 3.1

Casos de uso

Gerar arquivos SBOM e enviá-los por meio da API de carregamento do SBOM como parte do pipeline de compilação do DevOps pode fornecer contagens para o seguinte para determinar se o pipeline deve ser bem-sucedido ou falhar:

- Componentes adicionados
- componentes removidos
- Informações de vulnerabilidades
- Informações do pacote (componentes abandonados/obsoletos)

As políticas e regras de DevOps para o sucesso ou a falha de um pipeline podem ser definidas pelas contagens de vulnerabilidades e pelos limites de contagem de componentes obsoletos e abandonados que são recebidos da API SBOM Status.

Para um pipeline com falha, os usuários do DevOps podem acessar informações sobre a compilação com falha em sua instância ServiceNow® para ajudá-los a entender melhor a causa raiz e a origem das vulnerabilidades.

Consulte Carregando Lista de materiais de software arquivos usando uma REST API para obter mais informações sobre parâmetros (POST) e (GET) e URLs para as APIs de upload e status.

Separação de domínios

Todas as tabelas nas aplicações SBOM são separadas por domínio.

Exibição de relatórios e painéis no espaço Lista de materiais de software

Os analistas de vulnerabilidade visualizam arquivos de lista de materiais de software carregados em registros, visualizações de dados, bem como inteligência de vulnerabilidade aprimorada no espaço Lista de materiais de software (SBOM).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Requisitos para exibir dados

Núcleo de SBOM

A partir da v2.1 da aplicação SBOM Core, você pode exibir as entidades da lista de materiais e uma lista de componentes carregados na página inicial (principal) e no módulo Componentes no espaço SBOM. Antes da v2.1, navegar até **Núcleo de SBOM** > **Status de ingestão da lista de materiais** para exibir os componentes.

Resposta de SBOM

A aplicação SBOM Response fornece visualizações de dados com informações detalhadas sobre entidades da lista de materiais, entidades com vulnerabilidades e itens vulneráveis da aplicação ativos na página inicial (principal) do espaço SBOM. O espaço com a resposta SBOM inclui os seguintes módulos:

- Página inicial - Visualizações de dados e detalhes de vulnerabilidade aprimorados.
- Componentes — Informações de versão e correção dos componentes.
- Regras de criação de AVIT (item vulnerável da aplicação) — Condições para quando os itens vulneráveis da aplicação (AVITs) são criados.
- Fila da lista de materiais - Status e histórico de carregamento de arquivo.
- Lista — Registros AVIT para seus componentes vulneráveis e bibliotecas (NVD, CWE e vulnerabilidades da aplicação).

Os tópicos a seguir fornecem mais informações sobre como localizar detalhes sobre seus componentes no Lista de materiais de software Workspace.

- #unique_854
- Revisando o módulo Componentes no espaço Lista de materiais de software
- Exibição do status de carregamento de Lista de materiais de software arquivos
- Verificação de vulnerabilidades em uma entidade Lista de materiais de software

Revisando o módulo Componentes no espaço Lista de materiais de software

O módulo Componentes no espaço Lista de materiais de software (SBOM) exibe informações atuais sobre combinações vulneráveis, obsoletas, abandonadas e de alto risco para os componentes importados.

Exibição do módulo Componentes

Funções necessárias:

- A partir da v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

Navegar até **Espaços** > **Espaço de SBOM** > **Componentes**.

O que você pode ver no módulo depende das aplicações instaladas.

A partir da v3.2 da resposta SBOM, os dados importados não são calculados e preenchidos por consultas em tempo real. As pontuações nas páginas Inicial e Componentes são atualizadas uma vez por dia com melhorias de desempenho para emissão de relatórios. Esta melhoria pode fornecer tempos de carregamento mais rápidos para os cartões de pontuação nos módulos Página inicial e Componentes no espaço SBOM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Essas melhorias não têm impacto sobre como ou onde os dados são armazenados.

Aplicação instalada	Descrição
Se você instalou o SBOM Core	A partir da versão 2.1, um inventário de todos os componentes carregados inclui as seguintes informações: • Nome • Descrição • Versão • Contagem de entidades da lista de materiais
Se você instalou SBOM Resposta	A partir da v3.1 da Resposta SBOM, selecione um gráfico ou um número no gráfico para exibir uma lista de registros associados. Todos os componentes A lista de componentes **obsoletos** e **abandonados**, bem como aqueles com pelo menos uma vulnerabilidade em sua contagem total de componentes. Essas contagens podem ajudá-lo a identificar componentes que requerem sua atenção. Esses subconjuntos de componentes podem não corresponder à contagem total de componentes porque todos os seus componentes podem não se encaixar nessas categorias. • A versão de um componente obsoleto está mais de duas versões principais atrás da versão mais recente e dois anos atrás da versão mais recente. • Um componente abandonado não foi atualizado por mais de dois anos. • Componentes vulneráveis são componentes que têm vulnerabilidades com uma severidade **Alta** ou superior. Combinações de alto risco Componentes de alto risco podem exigir sua atenção

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	imediata. A integração Deps.dev, que é instalada quando você instala a aplicação SBOM Response, fornece a inteligência de pacotes para componentes nos estados **Obsoleto** e **Abandonado**. As combinações importadas de alto risco são compostas por componentes obsoletos e abandonados com pelo menos uma vulnerabilidade grave (**Crítica** ou **Alta**) que você pode corrigir com atualizações, substituições ou outro tipo de reparo. O status **Completamente corrigível** significa que um componente tem uma versão disponível que pode corrigi-lo. A porcentagem do número total de componentes de alto risco que têm versões corrigíveis é anotada. Componentes vulneráveis que podem ser corrigidas Totais e detalhamentos dos componentes com vulnerabilidades **Críticas**, **Altas**, **Médias**e **Baixas** e se algumas ou todas as vulnerabilidades podem ser corrigidas. Se um componente tiver mais de uma vulnerabilidade, a vulnerabilidade mais crítica terá precedência. O status de fixability: • Concluído - Há versões de correção para todas as vulnerabilidades associadas à versão atual do componente. • Parcial - há uma versão de correção para pelo menos uma, mas não todas as vulnerabilidades associadas à versão atual do componente. Componentes por licença Totais e detalhamentos de componentes por licenças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	A lista de componentes nas visualizações permite que você veja o nome, a descrição, a versão e as contagens de entidade. No painel direito, você pode exibir um histórico de versões. A versão atual é realçada no histórico de versões. As colunas Vulnerabilidades e exposição comuns (**CVE**) e **Fixabilidade** também são exibidas.

Como avaliar o risco com a inteligência de vulnerabilidade

Consulte Verificação de vulnerabilidades em uma entidade Lista de materiais de software para obter mais informações sobre como revisar dados de inteligência de vulnerabilidade no espaço.

Criação de regras para itens vulneráveis de aplicação no espaço Lista de materiais de software

Antes de poder ver os itens vulneráveis da aplicação (AVITs) no espaço da lista de materiais de software (SBOM), você deve configurar as condições sob as quais os AVITs são criados.

AVITs no espaço SBOM

Se você instalou e ativou a aplicação SBOM Response, os AVITs serão criados para os arquivos SBOM se algum dos dados importados corresponder às condições das regras de criação de AVIT existentes.

As aplicações SBOM Response e Resposta a vulnerabilidades são necessárias para configurar regras para criar itens vulneráveis de aplicação (AVITs) automaticamente e corrigi-los com o fluxo de trabalho Resposta a vulnerabilidades de aplicações. Para obter mais informações, consulte Exploração do Lista de materiais de software.

Você deve adicionar regras de criação de AVIT no espaço SBOM antes de criar AVITs para as vulnerabilidades encontradas nos dados SBOM ingeridos. Os AVITs permitem que você avalie a integridade dos componentes de terceiros em suas aplicações. Um AVIT é criado em sua instância quando uma aplicação é correspondida a um componente que tem uma vulnerabilidade associada.

No espaço SBOM, você pode exibir somente AVITs de SBOM. No entanto, você pode exibir SBOM AVITs junto com outros tipos de itens vulneráveis no Espaço do gerenciador de vulnerabilidades em Resposta a vulnerabilidades. Você pode exibir todos os AVITs que foram criados no espaço SBOM no módulo de lista. O módulo de lista também inclui todas as entradas do NVD e CWE e as vulnerabilidades da aplicação.

Você também pode atribuir AVITs para correção com base em recomendações de listas de vulnerabilidades conhecidas, como o Banco de dados nacional de vulnerabilidades (NVD). Um trabalho agendado é acionado e, se as condições das regras de criação corresponderem aos dados ingeridos, os AVITs serão criados.

Você pode rastrear e corrigir AVITs configurando regras personalizadas.

Consulte Criar uma regra de item vulnerável da aplicação no espaço Lista de materiais de software para obter informações sobre como criar uma regra.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SBOM AVITs em Vulnerability Manager Workspace em Resposta a vulnerabilidades

Você pode exibir todos os SBOM AVITs criados no SBOM Workspace no Vulnerability Manager Workspace se você tiver acesso a ele.

Nota: Para exibir somente SBOM AVITs da lista de Itens vulneráveis de aplicação no Vulnerability Manager Workspace em vez de todos os AVITs, defina a condição **[Source] [is] [SBOM] AND [Scan type] [is] [SBOM-SCA]** na vulnerabilidade da aplicação Tabela Itens [sn_vul_app_vulnerable_item]. Para exibir a tabela, navegue em sua instância até **Todos** e insira **sn_vul_app_vulnerable_item.list** no navegador de filtros.

Para obter mais informações sobre o Espaço do gerenciador de vulnerabilidades, como exibir tópicos de observação, esforços de correção de aplicações e regras de tarefa de correção de aplicações para AVITs configurados na aplicação Resposta a vulnerabilidades no Vulnerability Manager Workspace, consulte Usar tópicos de observação no Vulnerability Manager Workspace.

Tarefas de correção (AVULs) são criadas a partir de AVITs e atribuídas automaticamente a grupos para correção com base em suas regras de atribuição. Para obter mais informações sobre como criar essas regras, consulte os seguintes tópicos:

- Criar ou editar Resposta a vulnerabilidades regras de atribuição
- Criar ou editar Resposta a vulnerabilidades regras de tarefa de correção e Criar um esforço de correção no Espaço do gerenciador de vulnerabilidades.

Exibição do status de carregamento de Lista de materiais de software arquivos

Verifique o status de carregamento dos arquivos da lista de materiais de software (SBOM) que você carrega no módulo Fila da lista de materiais no espaço Lista de materiais de software (SBOM). Rastreie os arquivos que você carregou com sucesso, seu histórico de upload e erros.

Função necessária:

- A partir da v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

1. Exiba o status de carregamento.

   O método usado para exibir o status de carregamento depende das aplicações instaladas.

Opção	Descrição
SBOM Núcleo	**a.** Navegar até **Todos** > **Núcleo de SBOM** > **Status de ingestão da lista de materiais**. **b.** Na lista Lista de materiais, revise as colunas como **Status**, **Tempo de geração da lista**de materiais e colunas **Criado** para obter detalhes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
SBOM Resposta	**a.** Navegar até **Todos** > **Espaço de SBOM** > **Fila de lista de materiais**. **b.** Selecione um cartão de visualização para revisar os seguintes detalhes das categorias dos arquivos carregados: ▪ Atualizações da lista de materiais nos últimos 30 dias: total de entidades da lista de materiais carregadas e analisadas com sucesso nos últimos 30 dias. ▪ Origem de carregamento - Total de arquivos carregados com sucesso SBOM e um detalhamento dos métodos usados para ingeri-los (API ou manual). ▪ Erros de upload por categoria - Cinco principais categorias de erros de upload. Se nenhum dado for exibido nesta visualização, todos os seus arquivos SBOM foram carregados com sucesso.

As informações de status na tabela Lista de materiais [sn_sbom_doc_list] e no módulo Fila da lista de materiais incluem formatos de lista de materiais, status de ingestão e tempo de geração de lista de materiais. A coluna Status para ingestão da lista de materiais inclui os seguintes estados:

- Em fila - SBOM dados foram carregados.
- Processamento - Os dados do componente estão sendo processados como parte da importação.
- Processado — A ingestão de dados foi concluída com sucesso.
- Erro - ocorreu um erro durante o processamento.

Além do status dos arquivos carregados, você pode exibir listas de componentes que você ingeriu selecionando um registro de entidade da lista de materiais.

2. Acesse mais informações sobre erros e status de carregamento selecionando o ícone de ⚙ Ícone de engrenagem e adicionando campos como **Categoria** de **erro e Detalhe**do erro .

Verificação de vulnerabilidades em uma entidade Lista de materiais de software

Determine se há vulnerabilidades associadas aos componentes em um arquivo Lista de materiais de software (SBOM).

As aplicações a seguir devem ser instaladas e ativadas para que você possa exibir as vulnerabilidades e os dados de vulnerabilidade aprimorados:

- SBOM Resposta
- Integração de Resposta a vulnerabilidades com trabalhos do NVD e CWE
- Resposta a vulnerabilidades

Para obter mais informações, consulte Exploração do Lista de materiais de software.

Função necessária:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A partir da v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

1. Navegar até **Todos** > **Espaço de SBOM** > **Componentes**.
2. Antes da versão 3.1 da SBOM Response, as informações de vulnerabilidade eram exibidas por meio de uma visualização ou de um registro de componente.

Método	Ações
Entidades da lista de materiais com visualização de vulnerabilidades	Selecione o gráfico de visualização **Entidades da lista de materiais com vulnerabilidades**. ◦ Se as vulnerabilidades estiverem associadas a este componente, os totais serão exibidos nas colunas CVE e CWE na lista. Um componente pode ter mais de uma vulnerabilidade. Se disponível, você pode verificar a coluna Fixabilidade nesta lista para entradas. ◦ Se nenhuma vulnerabilidade estiver associada a este componente, essas colunas exibirão 0 ou nenhum valor para o componente. Se as colunas CVE, CWE e Fixibilty não forem exibidas, você poderá adicioná-las à página selecionando o ícone de Ícone de engrenagem no canto superior direito da página e **Editar colunas**. Selecione-os na lista da coluna Disponível e clique em **OK**.
Registro de componente	**a.** Selecione um registro na lista abaixo das visualizações. **b.** Selecione a guia **Vulnerabilidades** no registro. **i.** Se nenhum dado for exibido, nenhuma vulnerabilidade relatada será associada ao registro. **ii.** Se os dados forem exibidos, consulte Revisando o módulo Componentes no espaço Lista de materiais de software e siga as etapas no fluxo de trabalho de correção para Resposta a vulnerabilidades de aplicações para resolver a vulnerabilidade. Para obter mais informações, consulte Corrigindo Resposta a vulnerabilidades de aplicações vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como avaliar o risco com a inteligência de vulnerabilidade

A partir da versão 3.1 da Resposta SBOM, veja mais dados de vulnerabilidade aprimorados com a Resposta SBOM nos registros do componente. Os trabalhos agendados SBOM da aplicação Response, Vulnerability Response, National Vulnerability Database (NVD) e Common Weakness Enumeration (CWE) descritos em Aplicações compatíveis devem ser instalados e ativados.

1. Selecione a visualização **Todos os componentes** para exibir a lista de registros associados.
2. Selecione um link na coluna **Nome** para abrir um registro.

   Os estados, **obsoletos**, **abandonados**e **vulneráveis** são exibidos abaixo do nome do componente. Um componente pode ter qualquer combinação desses estados. Se nenhum estado for exibido, o componente não está obsoleto, abandonado ou vulnerável.

   Revise a versão atual e a versão publicada mais recente. No painel direito, você pode exibir um histórico de versões. A versão atual é realçada no histórico de versões e sua localização na lista pode fornecer informações sobre o motivo pelo qual um componente está **obsoleto**, **abandonado**e **vulnerável**. Por exemplo, você pode estar usando uma versão mais antiga de um componente.

3. Selecione as guias relacionadas **Visão geral**, **Hashes**, **Entidades da lista**de materiais , **Vulnerabilidades**e **AVIs** no registro.
   - Visão geral - Um resumo dos detalhes do componente.
   - Entidades da lista de materiais - Uma lista das entidades associadas a este componente.
   - Hashes - Se importados, os hashes serão exibidos.
   - Vulnerabilidades - Informações sobre vulnerabilidades conhecidas associadas a este componente. Se esta lista estiver vazia, não há vulnerabilidades conhecidas.

     Se a lista estiver preenchida, selecione a guia para exibir IDs de vulnerabilidade, resumos e outras informações de vulnerabilidade dos dados de Vulnerabilidades e exposições comuns (CVE) e Enumeração de pontos fracos comuns (CWE) associados a este registro. Os CVEs são divididos por gravidade, e os CWEs são divididos pela probabilidade de o componente ser explorado. Você pode exibir os registros de vulnerabilidade aprimorados nas aplicações Resposta a vulnerabilidades ou Resposta a vulnerabilidades de aplicações selecionando o link do ID de vulnerabilidade.

   - AVIs (AVITs) - Itens vulneráveis de aplicação associados a este componente se você tiver criado regras de criação de AVIT que correspondam o componente a uma vulnerabilidade conhecida. A aplicação Resposta a vulnerabilidades (AVR) relaciona uma vulnerabilidade a uma aplicação para criar um registro AVI. Para obter mais informações, consulte Criação de regras para itens vulneráveis de aplicação no espaço Lista de materiais de software.

Componentes instalados com Lista de materiais de software aplicações

Vários tipos de componentes são instalados com a ativação das aplicações Lista de materiais de software, incluindo tabelas, funções de usuário e trabalhos agendados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
SBOM gravar [sn_sbom_dm.app_write], SBOM criar [sn_sbom_dm.app_create], SBOM ler [sbom_dm.app_read]	Essas funções são instaladas com a aplicação Modelo de dados para SBOM. Eles permitem que você leia, crie e edite registros em SBOM tabelas.	Nenhum(a)
SBOM Ingestões de núcleo [sn_sbom_core.sbom_ingest] e SBOM Administrador de núcleo [sn_sbom_core.admin]	Essas funções são instaladas com a aplicação SBOM Core. A função sn_sbom_core.sbom_ingest permite que você carregue SBOMs manualmente e por meio da REST API. A função sn_sbom_core.admin permite que você crie, leia, edite dados e carregue SBOMs. Esta função também concede acesso aos módulos SBOM Core em sua instância. Ele herda as funções da aplicação Modelo de dados para SBOM.	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read
Analista de SBOM [sn_sbom_resp.sbom_analyst]	Esta função é instalada com a aplicação SBOM Response. Ele herda a função sn_sbom_core.admin e permite que você acesse o espaço SBOM.	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • Tabela sn_sbom_config_rule

Tabelas instaladas com as aplicações SBOM

As tabelas listadas na tabela a seguir são instaladas com a aplicação Modelo de dados para SBOM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de dados para tabelas SBOM

Tabela	Descrição
Documento de SBOM [sn_sbom_doc]	Contém as entidades da lista de materiais que você carregou.
SBOM componente [sn_sbom_component]	Contém SBOM componentes, classificadores e versões importados que estão incluídos no componente primário.
SBOM relacionamento do componente [sn_sbom_comp_relationship]	Contém componentes e suas dependências.
SBOM componente da lista de materiais m2m [sn_sbom_m2m_bom_comp]	Contém os mapeamentos de componentes da lista de materiais.
Licença do SBOM [sn_sbom_license]	Contém os IDs de licença de código aberto usados para componentes.
SBOM fornecedor [sn_sbom_supplier]	Contém a organização que forneceu o componente, que pode ser um fabricante, fornecedor ou reempacotador.
SBOM ID do componente [sn_sbom_comp_id]	Contém os identificadores do componente.
SBOM propriedades do componente [sn_sbom_comp_property]	Contém as propriedades de nome-valor do componente.
SBOM hash [sn_sbom_hash]	Contém algoritmos de hash de componente.
SBOM contato [sn_sbom_contact]	Contém informações de contato do fornecedor.
SBOM referências externas [sn_sbom_comp_external_ref]	Contém componentes, tipos de componente e URLs externos que documentam sistemas, sites e informações que podem ser relevantes, mas não estão incluídos com o SBOM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de dados para tabelas SBOM

Tabela	Descrição
SBOM grupo de pacotes [sn_sbom_pkg_group]	Contém as informações do grupo de pacotes para cada componente. Várias versões de bibliotecas podem ser usadas em aplicações. Versões dos mesmos componentes são agrupadas e adicionadas a esta tabela para evitar a extração dos mesmos dados várias vezes.

As tabelas listadas na tabela a seguir são instaladas com a aplicação de resposta SBOM

SBOM Tabelas de resposta

Tabela	Descrição
SBOM configuração de regra de criação [sn_sbom_config_rule]	Contém regras de criação de AVIT usadas no espaço SBOM.
SBOM vulnerabilidades do componente m2m [sn_sbom_m2m_comp_vuln]	Contém os componentes e as vulnerabilidades associadas.
Informações de correção de vulnerabilidade do componente [sn_sbom_comp_vuln_fix_info]	Contém as versões de correção para cada vulnerabilidade de terceiros associada a uma versão do componente.
Informações do relatório do componente [sn_sbom_comp_report_insight]	Contém informações sobre dados obsoletos, abandonados e de capacidade de correção para componentes.
Importações de integrações de Deps [sn_sbom_deps_integration_import]	Contém informações da lista de versões importadas para um determinado pacote ou biblioteca.
Importações de integrações de OSV [sn_sbom_osv_integration_import]	Contém informações de inteligência de vulnerabilidade para uma determinada versão de um pacote ou biblioteca.
Listas de versão de componentes [sn_sbom_st_version_list]	Contém informações de versão e datas de publicação dos componentes.

Trabalhos agendados

Trabalho	Descrição
Calcular a fixabilidade e a vulnerabilidade do componente	Calcula informações sobre como corrigir componentes com vulnerabilidades e qual é a probabilidade de que você possa corrigir componentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
Novos componentes de integração de OSV	Recupera todas as vulnerabilidades conhecidas publicamente associadas a pacotes (bibliotecas) que foram importados após a última execução de integração.
Integração OSV Abrangente	Recupera todas as vulnerabilidades conhecidas publicamente associadas a todos os pacotes que foram importados.
Integração Deps.dev	Recupera todas as versões publicamente conhecidas de pacotes e usadas com para identificar componentes nos estados **Obsoleto** e **Abandonado**.
Atualizar vuln_based_criticality em componentes da lista de materiais	Atualiza a criticalidade dos componentes com vulnerabilidades.

Criar uma regra de item vulnerável da aplicação no espaço Lista de materiais de software

Configure as condições sob as quais os itens vulneráveis da aplicação (AVITs) são criados automaticamente no módulo Regras de criação de AVI no espaço Lista de materiais de software (SBOM).

Antes de Iniciar

A aplicação de resposta SBOM é necessária se você quiser criar itens vulneráveis da aplicação. Para obter mais informações, consulte Exploração do Lista de materiais de software.

Função necessária: sn_sbom_resp.manage_avi_rule.

Procedimento

1. Navegar até **Espaço de SBOM** > **Regras de criação de AVI**.
2. Selecione **Novo**.
3. Preencha os campos.

Campo	Descrição
Nome	Nome da regra.
Ativo	Indica se a regra de criação está ativada.
Ordem de execução	Ordem na qual as regras são avaliadas. A regra com o menor valor numérico é executada primeiro. Por exemplo, você pode criar regras de prioridade mais alta para itens que precisam de tratamento especial ou onde o risco é crítico, portanto, elas são executadas primeiro. Em seguida, crie regras gerais para itens que não requerem tratamento especial. Por fim, crie uma regra padrão para detectar componentes que tenham vulnerabilidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição da regra para ajudá-lo a diferenciá-la de outras regras.
Condições	Crie as condições sob as quais os itens vulneráveis da aplicação (IVAs) são criados. Por exemplo, você pode selecionar **[Vulnerabilidade > Severidade][é][1-Crítico]** para criar AVITs para componentes que têm vulnerabilidades de alto risco e podem afetar gravemente você. Observe que você pode adicionar mais condições.

4. Selecione **Salvar**.
   Sua regra de criação é executada automaticamente após o próximo carregamento e cria AVIs para componentes que correspondem às suas condições. Você também pode executar a regra sob demanda no módulo Regras de criação de AVI selecionando **Executar agora**.

Resultados
Depois que eles forem criados, você poderá verificar se um AVIT foi criado especificamente para dados SBOM, verificando os valores nos campos **Origem** e **Tipo de verificação** em um registro AVI.

Campo	Valor
Origem	SBOM
Tipo de verificação	SBOM-SCA

Aplicações de gestão de casos de segurança empresarial

As aplicações de gestão de casos de segurança empresarial incluem Security Incident Response, uma solução de orquestração de segurança e resposta de automação (SOAR) que ajuda você a responder rapidamente às ameaças em constante evolução enquanto otimiza e orquestra as operações de segurança corporativa. Ele elimina os erros e o atrito inerentes às transferências manuais entre sistemas, equipes e responsabilidades.

Visão geral
<Video to be added.>

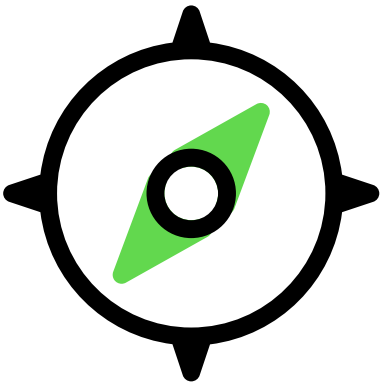
Primeiros passos

As seguintes Security Incident Response aplicações estão disponíveis com assinaturas separadas do ServiceNow® Store. Consulte para obter mais informações sobre como localizar, obter direito e baixar apps em sua instância.

Tradução automática

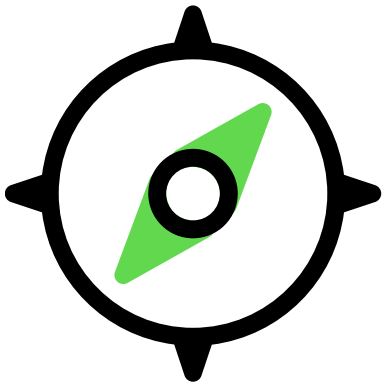
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança



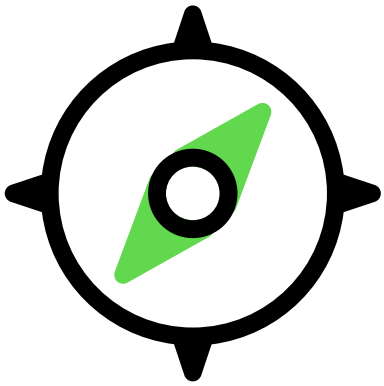
Saiba mais sobre a aplicação Security Incident Response

Gestão de incidentes graves de segurança



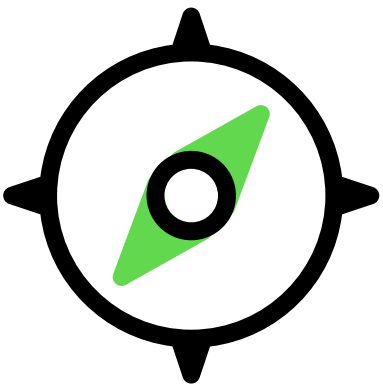
Saiba mais sobre a aplicação Gestão de incidentes graves de segurança

Inteligência contra ameaças



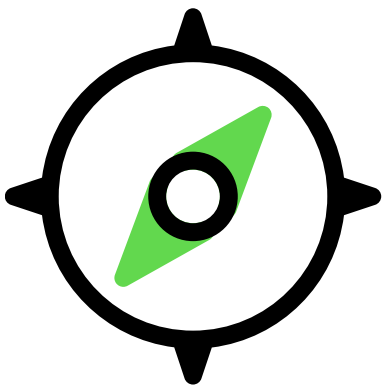
Saiba mais sobre a aplicação Inteligência contra ameaças

Central de segurança de inteligência contra ameaças



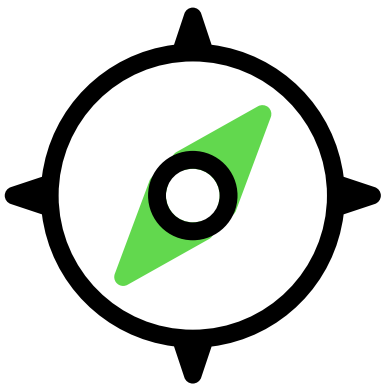
Saiba mais sobre a aplicação Central de segurança de inteligência contra ameaças

Data Loss Prevention Incident Response



Saiba mais sobre a aplicação Data Loss Prevention

Recursos compartilhados de aplicações do Security Incident Response



Saiba mais sobre os recursos compartilhados entre as aplicações do Security Incident Response

Tradução automática

Solucionar problemas e obter ajuda

- Comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

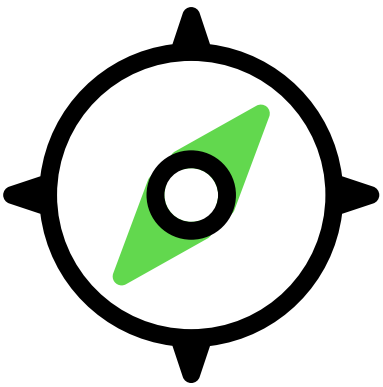
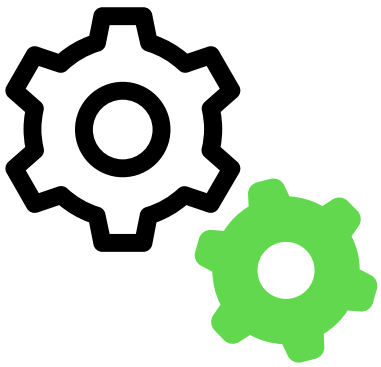
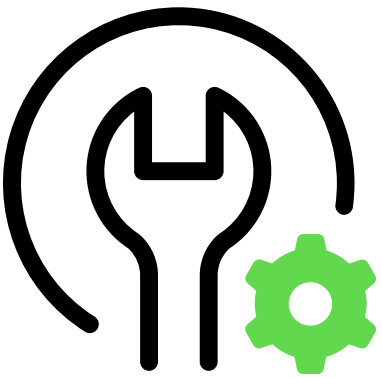
Security Incident Response

A aplicação ServiceNow® Security Incident Response rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão final pós-incidente, a criação e o fechamento do artigo da base de conhecimento.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

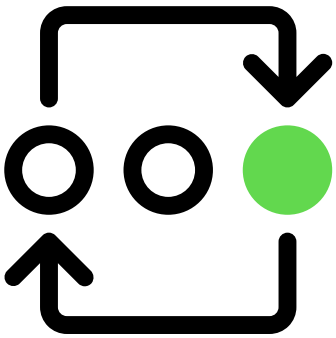
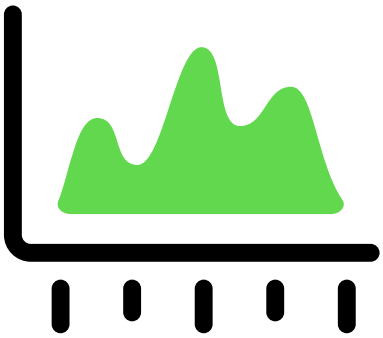
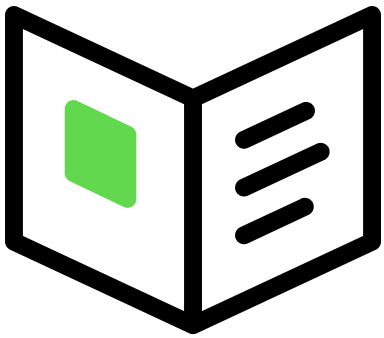
Security Incident Response

Explorar	Instalar e configurar	Administrar
		
Saiba mais sobre os recursos do Security Incident Response	Instalar e configurar a aplicação Security Incident Response	Gerenciar e personalizar seus incidentes de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Incident Response

Integrar	Use o espaço do Security Incident Response	Análise e Emissão de relatórios
		
Estenda a Resposta a incidentes de segurança integrando-a a outras aplicações	Saiba como usar o Security Incident Response e IT Remediation Workspaces	Monitorar o andamento da correção
		
	Obter informações adicionais sobre o Security Incident Response	

Tradução automática

Solicitar um aplicativo Operações de segurança na Store

Se você é um novo cliente Operações de segurança do Patch London 6 ou posterior, visite o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja.

Noções básicas do Security Incident Response

Com Security Incident Response (SIR), gerencie o ciclo de vida de seus incidentes de segurança, desde a análise inicial até a contenção, erradicação e recuperação. O

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Incident Response permite que você obtenha uma compreensão abrangente dos procedimentos de resposta do incidente realizados por seus analistas e entenda as tendências e gargalos nesses procedimentos com painéis e relatórios orientados por análise.

Uma introdução ao Security Incident Response, mostrando como começar a usar a aplicação.

Assista a este vídeo de nove minutos para saber mais sobre o processo SIR, usando Security Incident Response para impedir ataques e exibindo a atividade de segurança no Security Incident Response Explorer.

Integrações integradas com soluções de segurança cibernética de terceiros e integrações desenvolvidas por parceiros da ServiceNow Store permitem a automação e a orquestração da segurança para uma resposta eficiente e precisa a incidentes.

Para proteger suas investigações e manter os incidentes de segurança privados, Security Incident Response fornece os meios para restringir o acesso ao sistema a funções e ACLs relacionadas à segurança específicas. Os administradores que não são de segurança podem ter acesso restrito, a menos que você permita expressamente a entrada.

Nota: Os administradores do sistema de TI [admin] podem representar usuários da ServiceNow. No entanto, ao representar um usuário com uma função de administrador de aplicações para o Security Incident Response, um administrador não pode acessar recursos concedidos por essa função, incluindo incidentes de segurança e informações de perfil. O acesso a módulos e aplicações na barra de navegação também é restrito. Além disso, o administrador não pode mudar a senha de nenhum usuário com uma função de administrador de aplicação para o Security Incident Response.

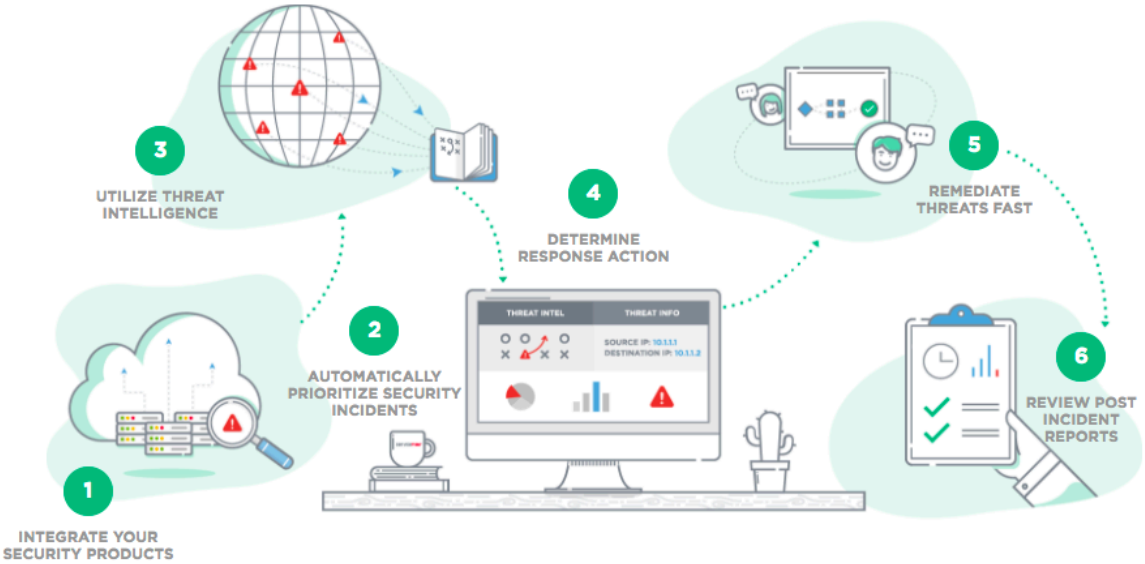
Fluxo de informações do Security Incident Response

O Security Incident Response emprega o seguinte fluxo de informações, desde a integração até a investigação e, em seguida, até a resolução e a revisão.

Nota: Este é um infográfico interativo, então você pode tentar clicar em qualquer um dos ícones ou etapas na imagem para saber mais sobre esse processo ou tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



1. Clique nesta imagem para saber mais sobre integrações SIR
2. Clique nesta imagem para saber mais sobre a criação de incidentes de segurança
3. Clique nesta imagem para saber mais sobre Inteligência contra ameaças
4. Clique nesta imagem para saber mais sobre o Espaço SIR
5. Clique nesta imagem para saber mais sobre os recursos de ataque do MITRE
6. Clique nesta imagem para saber mais sobre as atividades de análise pós-incidente

Descoberta

Os incidentes de segurança podem ser registrados ou criados das seguintes maneiras.

- No formulário de Incidente de segurança
- De eventos gerados internamente ou criados por sistemas externos de monitoramento ou acompanhamento de vulnerabilidades por meio de regras de alerta ou manualmente
- De sistemas externos de monitoramento ou acompanhamento
- Do catálogo de serviços

Análise

Dependendo da exibição selecionada que você está usando (padrão, segurança não relacionada a TI, segurança ITIL e assim por diante), o formulário de incidente de segurança pode mostrar qualquer combinação de vulnerabilidades, incidentes, mudanças, problemas, tarefas no IC afetado e no IC afetado grupos. O sistema pode identificar malware, vírus e outras áreas de vulnerabilidade fazendo referência cruzada ao banco de dados do Instituto Nacional de Padrões e Tecnologia (NIST) ou a outro software de detecção de terceiros. Conforme os incidentes de segurança são resolvidos, você pode usar qualquer incidente para criar um artigo da base de conhecimento de segurança para referência futura.

Realize análises adicionais usando um mapa de serviços de negócio para localizar outros sistemas afetados ou serviços de negócio que podem estar infectados.

Contenção, Erradicação e Recuperação

Ao monitorar e analisar vulnerabilidades, você pode criar e atribuir tarefas a outros departamentos. Você pode usar um mapa de serviços de negócio para criar tarefas,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

problemas ou mudanças para todos os sistemas, documentos, atividades, mensagens SMS, chamadas em ponte afetados e assim por diante.

Revisão

Depois que o incidente for resolvido, outras etapas podem ocorrer antes do fechamento. Você pode executar uma análise pós-incidente. A criação de artigos da base de conhecimento pode ajudar em futuros incidentes semelhantes. Incidentes significativos podem exigir uma revisão de resolução pós-incidente. Esta revisão pode assumir várias formas. Por exemplo:

- Conduzir uma reunião para discutir o incidente e coletar respostas.
- Escreva e distribua para as equipes que trabalharam em um incidente uma lista de perguntas de análise de resolução projetadas para cada categoria ou prioridade de incidente.
- Os gerentes de incidentes podem escrever o relatório e coletar informações por conta própria.

Um relatório de revisão de resolução de incidente pode ser gerado automaticamente, incluindo:

1. um resumo do que foi feito
2. a linha do tempo
3. o tipo de incidente de segurança encontrado
4. todos os incidentes, mudanças, problemas, tarefas, grupos de IC relacionados
5. os detalhes da resolução

Além disso, um sistema automatizado de pesquisa de revisão de resolução de incidentes de segurança está disponível. Ele reúne os nomes de todos os usuários atribuídos a um incidente de segurança e envia uma pesquisa personalizada para coletar dados sobre o tratamento do incidente. Esses dados podem ser disponibilizados em um relatório de revisão de incidente de segurança gerado, que você pode editar em um rascunho final. Dados semelhantes podem ser adicionados a um artigo da base de conhecimento para conter as lições aprendidas e as etapas a serem seguidas para resolver problemas semelhantes no futuro.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Terminologia do Security Incident Response

Os termos a seguir são usados em Security Incident Response.

Termo	Definição
Ativo	Qualquer incidente de segurança que não esteja no estado encerrado ou cancelado.
Bloqueio de administrador	A capacidade de restringir o acesso Security Incident Response ao pessoal com funções e ACLs relacionadas à segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Termo	Definição
Solicitações de segurança de entrada	Solicitações enviadas para demandas de segurança de baixo impacto, como solicitar um novo crachá eletrônico.
Gerenciar atividades pós-incidente	Uma revisão das origens e do tratamento de um incidente de segurança. O produto final é um relatório pós-incidente, que documenta todas as ações realizadas e os motivos para realizá-las.
Tarefas de resposta	Tarefas atribuídas a um incidente de segurança para rastrear ações em resposta à ameaça.
Noções básicas sobre calculadoras de incidentes de segurança	Calculadoras usadas para atualizar valores de registro quando condições pré-configuradas são atendidas.
Mapas de árvore de incidentes de segurança	Tipo de gráfico que mostra hierarquicamente os dados de incidentes de segurança na forma de retângulos aninhados.
Pesquisa de ameaças	Uma solicitação enviada do catálogo de incidentes de segurança para verificar arquivos, URLs e endereços IP em busca de malware.
Verificação de vulnerabilidade	Uma solicitação iniciada a partir do formulário de Incidente de segurança para verificar recursos afetados (servidores, computadores e outros itens de configuração) em busca de vulnerabilidades.

Separação de domínios e Security Incident Response

Separação de domínios é compatível com Security Incident Response. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Visão geral

Na aplicação Security Incident Response, o Domain Separation permite que os provedores de serviço (SPs) padronizem os procedimentos do SOC (Security Operations Center) e do Security Incident Response (SIR) em toda a base de clientes que atendem com custos operacionais reduzidos e uma qualidade de serviço superior. Separar espaços do cliente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínios no Security Incident Response por versões de versão

Versão	Nível de suporte	Anotações
Genebra, Helsinki	Sem suporte	Início da separação de domínios em nível de dados
Istambul	Somente dados	
Jakarta	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos**: suporte a integrações de terceiros com separação de domínio de nível 2 em uma única instância de integração, incluindo integrações de Inteligência contra ameaças
Kingston	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos**: a integração da Pesquisa de detecções para SIR está habilitada com várias instâncias, mas todas as instâncias ainda estão em um único domínio. Exemplo: se houver duas instâncias de uma integração do Splunk configuradas (SplunkCLOUD e SplunkCORP), ambas ainda serão aproveitadas para atividades de resposta a incidentes em um único domínio, onde a implementação foi configurada originalmente.
Londres	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos**: todas as integrações residem em vários domínios
Madri	Nível 2 (Dados, Solicitante, Executante)	Todas as integrações agora podem residir em vários domínios. No exemplo acima, SplunkCloud pode ser domain1 e SplunkCORP domain2.
Nova York	Nível 2 (Dados, Solicitante, Executante)	Todas as integrações residem em vários domínios.
Orlando	Padrão	Todas as integrações residem em vários domínios.
Paris	Padrão	Todas as integrações residem em vários domínios.

O Domain Separation para a aplicação Security Incident Response cobre a seguinte funcionalidade do produto:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os alertas de segurança são direcionados para o domínio apropriado do usuário cujo ID/credencial/escopo gera o incidente e está registrado como um incidente de segurança.
- Os alertas geram "observáveis", que representam propriedades com monitoramento de estado ou eventos mensuráveis: fluxos de trabalho de segurança no domínio do incidente de segurança são usados para orquestrar a resposta.
- As integrações são configuradas no domínio do incidente de segurança para automação de resposta.
- As capacidades são configuradas no domínio do incidente de segurança para automação de resposta. Esses recursos (a partir da versão Kingston) incluem:
  - Pesquisa de ameaças
  - Aprimorar Observável
  - Aprimorar item de configuração
  - Obter processo em execução
  - Obter estatísticas de rede
  - Bloquear Solicitação
  - Isolar host
  - Pesquisa de detecções
  - Pesquisa e Exclusão de E-mails
  - Publicar na Watchlist
- Os resultados da automação de resposta (como Pesquisa de ameaças ou Pesquisa de detecções) são armazenados no domínio do incidente de segurança.
- Outros incidentes de segurança são referenciados cruzadamente no mesmo domínio do incidente de segurança com base em um conjunto compartilhado de observáveis.
- Outros usuários têm referência cruzada no domínio do incidente de segurança.
- Os itens de configuração têm referência cruzada no mesmo domínio do incidente de segurança.
- Tarefas de resposta manual são adicionadas ao domínio do incidente de segurança.
- Artigos da base de conhecimento e livros de execução são referenciados no domínio do incidente de segurança.
- As métricas do Security Incident Response pertinentes a incidentes no domínio são exibidas em painéis e também em relatórios.

Nota: Nos casos anteriores, aplicam-se os princípios abrangentes de visibilidade em domínios separados na NOW Platform. Como sempre, um incidente no domínio primário pode fazer referência a artefatos no domínio secundário, mas não o contrário.

Como o Domain Separation funciona no Security Incident Response

A aplicação Security Incident Response gerencia o ciclo de vida de um incidente de segurança de ponta a ponta. Os seguintes casos de uso reconhecem a separação de domínios:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Ingestão de eventos e alertas** para criar incidentes de segurança para o analista no SOC do cliente ou o MSP responder:
  - Analisadores de e-mail (baseado em plataforma, phishing relatado pelo usuário, personalizado)
  - Eventos/alertas de desduplicação antes da criação do incidente
  - Extração automática de observáveis
  - Aplicações no armazenamento SIEM de terceiros
- **Aprimoramento** de artefatos envolvidos nos incidentes (IP, URLs, domínios, hashes de arquivo):
  - Aprimoramento de ativos (CMDB)
  - Usuários (plataforma)
  - Automação: enriquecimento de observável (por exemplo: WhoIs)
- **Investigar** os incidentes com a ajuda dos artefatos e sua reputação ou associação com ameaças conhecidas
  - Orquestrar: playbooks e artigos da base de conhecimento
  - Automação: pesquisa de ameaças (por exemplo: VirusTotal), pesquisa de detecções (por exemplo: Splunk), obter processos em execução (por exemplo: Carbon Black)
- **Eliminar** os artefatos relacionados a ameaças envolvidos no incidente com base na investigação realizada
  - Orquestrar: playbooks e artigos da base de conhecimento
  - Automação: pesquisa e exclusão de e-mail (por exemplo: Microsoft Exchange), Bloquear IP (por exemplo: firewall da Palo Alto)
- **Medir** a eficiência ou as operações de resposta a incidentes
  - Painéis do Performance Analytics: tendências de produtividade e incidentes
  - Reconstrução de etapas de investigação de incidentes a partir de anotações de trabalho
  - Revisão pós-incidente

Configuração do Domain Separation

A configuração do Domain Separation para Security Incident Response não requer etapas adicionais. Todas as tabelas Security Incident Response adquirem a coluna Domínio depois que a instância é separada por domínio.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os incidentes de segurança em um domínio não podem ser exibidos em outros domínios.
- Os observáveis extraídos do incidente de segurança são colocados no mesmo domínio e não podem ser exibidos de outros domínios.
- Até a versão Kingston, as integrações de terceiros configuradas existem no domínio global e podem ser acessadas por todos os outros domínios na instância.
- Na versão Madrid, as integrações de terceiros podem ser configuradas e ativadas por domínio. Isso significa que a integração ativada e configurada em um domínio não pode ser aproveitada em outro domínio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As automações executadas nos observáveis usando integrações de terceiros (para investigação de ameaças, contenção ou erradicação) colocam seus resultados no domínio do incidente de segurança e os resultados não podem ser exibidos em outro domínio.
- Os fluxos de trabalho de Orquestração criados em um domínio não são visíveis em outro domínio.
- As capacidades (conforme delineadas na lista de funções de capacidades anteriores) que são invocadas permanecem genéricas entre domínios com implementação específica de domínio da capacidade que está sendo chamada. Por exemplo, uma pesquisa de detecções em um IP pode invocar uma implementação Splunk em um domínio e uma implementação QRadar em outro.

Configuração

Todos os aspectos da configuração do produto são autocontidos em um ambiente separado por domínio. A configuração pode ser personalizada para domínios individuais.

Nota: A lógica de negócios e os processos nos itens 2 a 5 abaixo podem ser administrados no domínio do locatário.

As seguintes tarefas devem ser configuradas:

1. Administração do Sistema
   - Atribua funções a usuários e grupos de usuários: funções de usuário instaladas com o Security Incident Response
   - Instale um ou mais plug-ins de integração de terceiros para trabalhar com Security Incident Response: Integrações do Security Incident Response
2. Security Incident Response Administration
   - Adicionar ou revisar funções: Componentes instalados com Security Incident Response
   - Configurar grupos e usuários: Criar um grupo de incidentes de segurança
   - Configurar escalações de incidentes: Escalar um incidente de segurança
   - Configurar calculadoras de pontuação de risco de incidente de segurança: Noções básicas sobre calculadoras de incidentes de segurança
   - Configurar acordos de nível de serviço: Criar um Security Incident Response ANS
   - Configure as definições do processo de incidente de segurança: Noções básicas sobre a definição do processo do Security Incident Response
   - Configurar processos de revisão pós-incidente: Gerenciar atividades pós-incidente
3. Configurações de e-mail de incidente de segurança
   - Definir a caixa de entrada de análise de e-mail: Operações de segurança análise de e-mail
   - Configure analisadores de e-mail para ingestão de alertas: Criar analisadores de e-mail em Operações de segurança
   - Configure regras de correspondência de e-mail para phishing relatado pelo usuário: Criar regras para validar ataques de phishing relatados por usuários
   - Configurar ações de e-mail de entrada:Ações de e-mail de entrada
4. Configurações do playbook de incidente de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Revise e configure documentos do runbook: Criar um runbook do Security Incident Response
- Configure fluxos de trabalho de incidentes de segurança: Operações de segurança funcionalidade comum

5. Configurações de capacidade
   - Bloquear solicitação: Integração de Operações de segurança - Capacidade de solicitação de bloqueio
   - Pesquisa e exclusão de e-mail: Integração de Operações de segurança - Capacidade de pesquisa e exclusão de e-mail
   - Aprimorar item de configuração: Integração de Operações de segurança - Capacidade de IC aprimorada
   - Aprimorar observável: Integração de Operações de segurança - Capacidade de aprimorar observável
   - Obter estatísticas de rede: Capacidade de Integração de Operações de segurança - Obter estatísticas de rede
   - Obter processos em execução: Capacidade de Obter processos em execução da Integração de Operações de segurança
   - Isolar host: Integração de Operações de segurança - Capacidade de isolamento de host
   - Publicar na lista de observação: Integração de Operações de segurança - Capacidade de publicar na lista de observação
   - Pesquisa de detecções: Integração de Operações de segurança - Capacidade de pesquisa de detecções
   - Pesquisa de ameaças: Integração de Operações de segurança - Capacidade de pesquisa de ameaças

Como os domínios de locatário gerenciam seus dados de aplicação próprios

- Os proprietários de domínio de locatário criam suas próprias regras de análise de e-mail para ingerir incidentes de segurança.
- Os proprietários de domínio de locatário podem configurar integrações específicas exclusivamente para uso dentro do domínio.
- Os proprietários de domínio de locatário podem criar seus próprios fluxos de trabalho de resposta a incidentes.
- Os proprietários de domínio de locatário podem criar suas próprias categorias de incidentes, artigos da base de conhecimento de resposta a incidentes e runbooks a serem associados a fluxos de trabalho de resposta a incidentes.
- Os usuários do domínio do locatário criam e encerram seus próprios incidentes de segurança.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Security Incident Response usuários e grupos
- Security Incident Response integrações (a partir da versão Madrid)
- Regras de análise de e-mail para criação de incidentes

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Regras de negócio para consolidar vários eventos ou alertas em um incidente de segurança
- Fluxos de trabalho para orquestração de resposta a incidentes
- Calculadoras de pontuação de risco de incidente de segurança
- Caminho de escalação de incidente de segurança
- ANS de incidente de segurança
- Definições do processo de incidente de segurança
- Processos de análise pós-incidente de segurança

Informações relacionadas

Domain Separation para provedores de serviço

Configuração do Security Incident Response

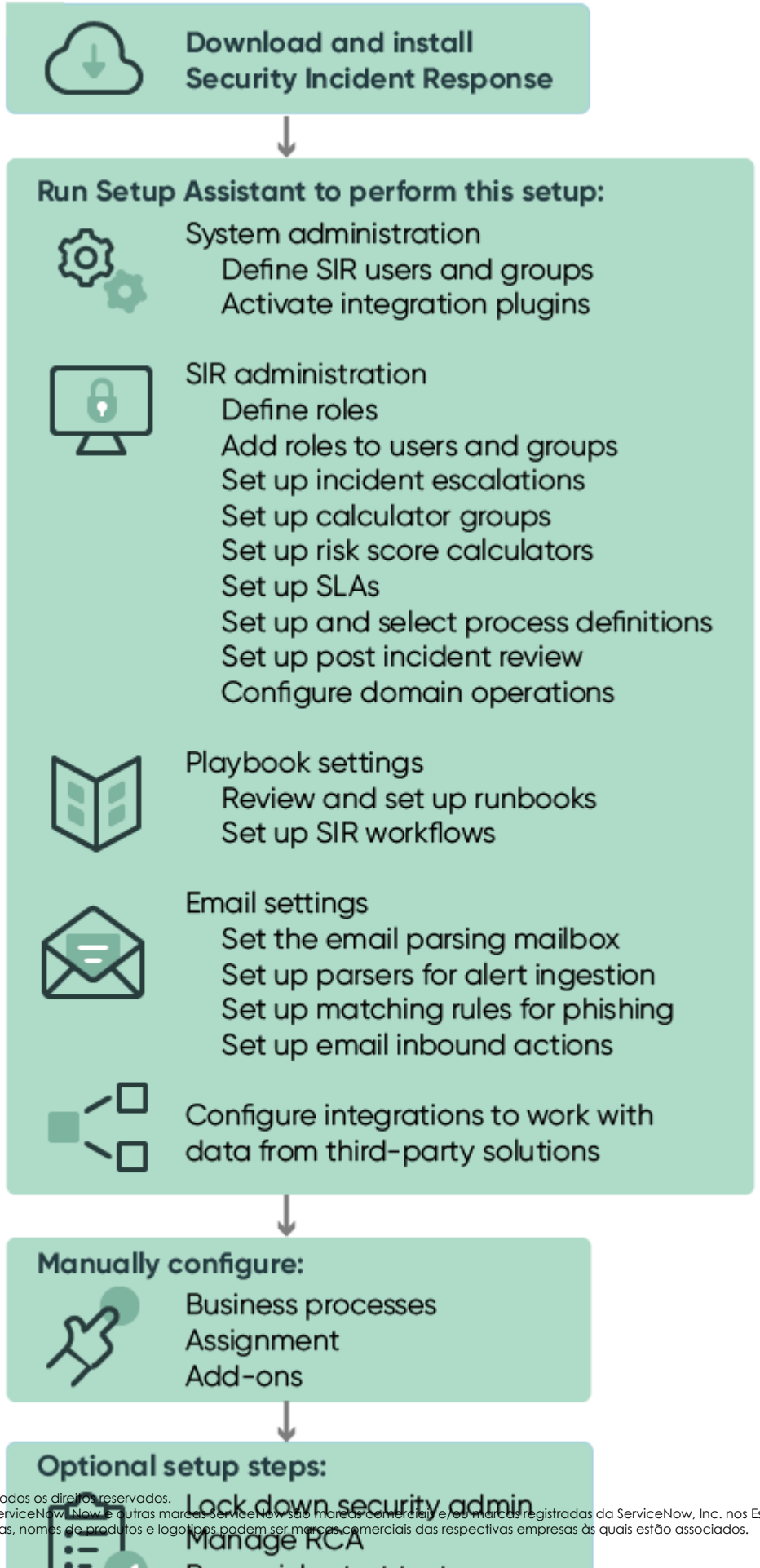
A configuração de Security Incident Response envolve algumas etapas obrigatórias e várias etapas opcionais, dependendo dos seus requisitos específicos. Depois de baixar Security Incident Response de ServiceNow Store e instalá-lo, você está pronto para executar o Assistente de configuração para executar a configuração básica de Security Incident Response e integrações de terceiros.

O Security Incident Response processo de configuração

O diagrama a seguir ilustra o processo de configuração. Ele é separado em dois subprocessos, o download e a configuração da aplicação Security Incident Response.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A primeira etapa de configuração é baixar o Security Incident Response aplicação do ServiceNow Store. Quando o download estiver concluído, vários aplicativos dependentes, incluindo o Assistente de configuração, serão carregados e prontos para uso para configurar Security Incident Response.

Assistente de configuração

O Security Incident Response Assistente de configuração é uma aplicação semelhante a um assistente que orienta você, passo a passo, na configuração da sua instância Security Incident Response de base.

As etapas de configuração são bastante autoexplicativas; no entanto, se você precisar de mais explicações, poderá encontrar assistência adicional na referência do Assistente de configuração. Depois de concluir a configuração usando o Assistente de configuração, você pode executar outros procedimentos de configuração opcionais, conforme necessário. Esses procedimentos incluem opções para:

- Como configurar o ciclo de vida da solicitação
- Como criar catálogos e solicitações
- Configurando notificações
- Configuração de atribuição manual e automática
- Habilitação da base de conhecimento, documentos gerenciados e atividades de tarefa

Um novo e aprimorado espaço de resposta a incidentes de segurança está disponível. Para obter mais informações, consulte Espaço de resposta a incidentes de segurança.

Instalar e configurar Security Incident Response

Antes de executar Security Incident Response em sua instância, você deve baixá-lo do ServiceNow Store e concluir as etapas de configuração.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

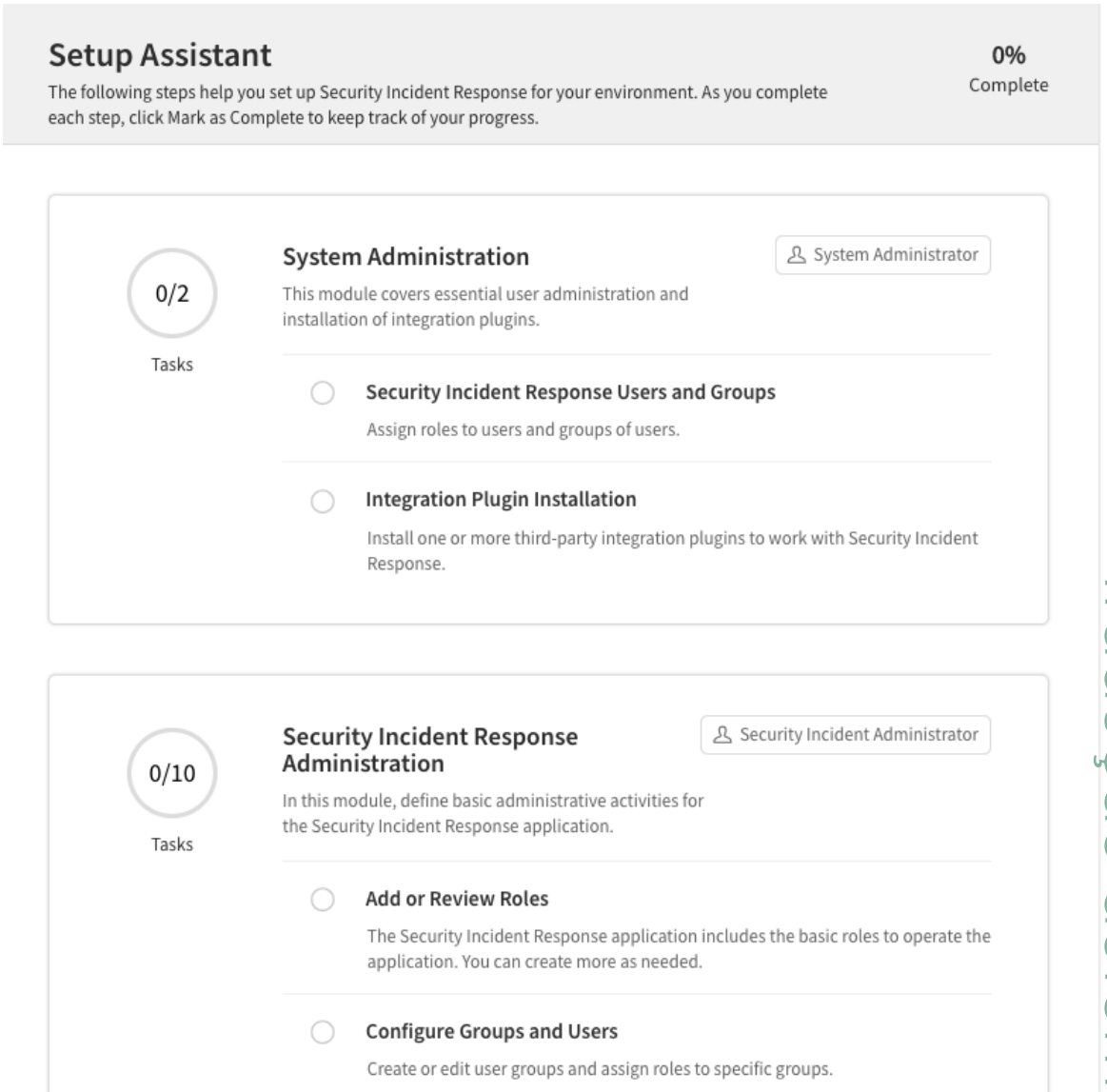
- A instalação da versão Security Incident Response 13.4.5 ou posterior a partir de ServiceNow Store instalará automaticamente a versão Espaço de resposta a incidentes de segurança (sn_si_aw) 1.5.1 ou posterior por padrão. Para obter mais informações sobre as aplicações dependentes, consulte a seção Espaço SIR plug-ins e funções.
- Observe que as versões 1.5.1 e superiores do Espaço de resposta a incidentes de segurança só podem ser instaladas/atualizadas por meio de uma instalação/atualização do Security Incident Response e não podem ser instaladas independentemente.
- Os recursos mais recentes em Security Incident Response estão disponíveis exclusivamente no Espaço de resposta a incidentes de segurança. Instale ou faça upgrade para a versão mais recente Security Incident Response ou Espaço de resposta a incidentes de segurança para acessar e aproveitar recursos como Transferência de turno, Calculadora de pontuação de risco etc.

Procedimento

1. Siga as instruções para download de uma aplicação do ServiceNow Store.
2. Depois de baixar a aplicação Security Incident Response e todas as aplicações dependentes, navegue até **Incidente de segurança** > **Configuração do espaço do analista** > **Assistente de configuração**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Siga as instruções nos formulários para configurar o sistema de base Security Incident Response.
   Para obter informações adicionais sobre algumas das tarefas de configuração mais complicadas, consulte Referência do Assistente de configuração, conforme necessário.

Baixar e instalar o Espaço do analista de segurança

Antes de executar a Security Incident Response nova IU em sua instância, você deve baixá-la do ServiceNow® Store e instalá-la.

Antes de Iniciar

Para garantir uma instalação sem problemas, verifique se você tem as funções ServiceNow necessárias para sua instância. As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

- Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá a função de administrador do Security Incident Response [sn_si.admin].
- O administrador do Security Incident Response [sn_si.admin] supervisiona a configuração e verifica os resultados esperados.

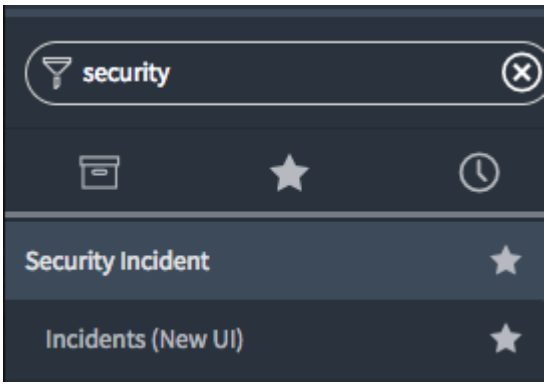
Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Siga as instruções para download de uma aplicação do ServiceNow Store e instale a aplicação **de IU do Security Incident Response**.
2. Depois que a instalação estiver concluída, você poderá abrir o Espaço do analista de segurança navegando até **Incidente de segurança** > **Incidentes (Nova IU)**



Componentes instalados com Security Incident Response

Vários tipos de componentes são instalados com o download e a ativação da aplicação Security Incident Response, incluindo funções de usuário, tabelas, propriedades e trabalhos programados.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Propriedades instaladas

Usuários com a função de administrador do sistema [admin] podem exibir as propriedades. Usuários com a função de administrador de segurança [sn_si.admin] podem modificá-las.

Propriedade	Uso
Hora de início padrão para todos os agentes quando nenhuma programação estiver definida, no formato 08:00 sn_si.default.start.time	• **Tipo**: cadeia de caracteres • **Valor padrão**: 08:00 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Hora de término padrão para todos os agentes quando nenhuma programação estiver definida, no formato 17:00 sn_si.default.end.time	• **Tipo**: cadeia de caracteres • **Valor padrão**: 17:00 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Incluir observáveis do tipo de destino junto com outros observáveis de tipo de contexto no usuário de incidentes de segurança e relacionamentos de IC	Determina se um observável de incidente de segurança com um tipo de contexto de Destino é exibido nas guias **Itens de configuração** ou **Usuários afetados**. Por

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_si.link_dest_ip	padrão, os observáveis com um tipo de contexto de destino são excluídos. Para incluir os observáveis, escolha Sim.
Permitir personalização ao criar um Problema ou uma Solicitação de mudança com base em um Incidente de segurança sn_si.popup	Quando um problema ou uma mudança são criados, esta propriedade abre uma janela pop-up para modificar a solicitação. Se estas propriedades estiverem definidas como **falsas**, o problema ou a solicitação de mudança terá a mesma prioridade, descrição resumida e descrição que o incidente de segurança sem a opção de adicionar ou editar esses campos. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Associe resultados de pesquisa de detecções a ICs no CMDB. sn_si.associate_ci_with_sighting_search	Quando definido como verdadeiro, os resultados da pesquisa de detecções incluem itens de configuração associados que estão no seu CMDB. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
A pontuação de risco no intervalo é realçada em verde, no formato 0 - 49 sn_si.risk.score.green	Na lista Incidentes de segurança, os incidentes de segurança com uma pontuação de risco entre 0 e 49 são marcados com um ponto verde.
A pontuação de risco no intervalo é realçada em laranja, no formato 50 a 79 sn_si.risk.score.orange	Na lista Incidentes de segurança, os incidentes de segurança com uma pontuação de risco entre 50 e 79 são marcados com um ponto laranja.
A pontuação de risco no intervalo é realçada em vermelho, no formato 80 a 100 sn_si.risk.score.red	Na lista Incidentes de segurança, os incidentes de segurança com uma pontuação de risco entre 80 e 100 são marcados com um ponto vermelho.
Este parâmetro ativa ou desativa as configurações de pesquisa de detecções que têm esse recurso implementado.	Quando definido como verdadeiro, as pesquisas de detecções podem ser realizadas em integrações ativadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_si.enable_sighting_search	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
O número de linhas de dados brutos é salvo quando for realizada uma pesquisa de detecções. Intervalo de 0 a 100 sn_si.sighting_search_raw_data_rows	Esta propriedade tem como padrão 50 linhas de dados brutos. Metade das linhas de resultados são relatadas a partir do início do intervalo de tempo de pesquisa e metade a partir do final do intervalo de tempo de pesquisa. Portanto, se você selecionar 50 linhas, 25 virão do início do intervalo de tempo de pesquisa e 25 do fim do intervalo de tempo de pesquisa.
Avançar automaticamente o Estado do Incidente para Conter quando uma Tarefa de Resposta avançar para Trabalho em Andamento sn_si.rollup_task_state	Ao usar fluxos ou fluxos de trabalho, considere definir esta propriedade como **falso**. Isso permite que você controle o Estado do incidente de dentro de fluxos ou fluxos de trabalho. Também ajuda a evitar possíveis conflitos durante a transição de um estado de incidente para outro. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Propriedades de atribuição do Security Incident Response	
Peso do local sn_si.location.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, o local for considerado para uma tarefa, o valor do peso do local será adicionado à classificação do analista de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Peso das Habilidades sn_si.skills.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, habilidades forem consideradas para uma tarefa, o valor do peso das habilidades será adicionado à classificação do analista de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
	• **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Definir o número máximo de analistas de segurança a serem processados pela atribuição automática de uma vez sn_si.max.agents.processed	O sistema tem um limite absoluto de 300 analistas de segurança. Se você especificar mais de 300, ele definirá o valor para esse nível. O sistema não pode expedir automaticamente uma tarefa para um grupo de expedição que contém mais analistas de segurança do que o valor configurado. • **Tipo**: inteiro • **Valor padrão**: 100 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Peso do Fuso horário sn_si.timezone.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, o fuso horário do analista de segurança for considerado para uma tarefa, o valor do peso do fuso horário será adicionado à classificação do analista de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Quantidade de tempo (em minutos) para adicionar entre o final de uma tarefa e o início da próxima viagem. sn_si.work.spacing	Um exemplo de valor de tempo válido é 10. • **Tipo**: inteiro • **Valor padrão**: 0 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Campos de diário especificados que contenham marcadores de `código` que renderizem o conteúdo como HTML. sn_si.journal_field.html_enabled	• **Tipo**: cadeia de caracteres • **Valor padrão**: work_notes, comentários • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Calcule os serviços afetados em segundo plano. sn_si.refresh_impacted.event	A lista relacionada de Serviços afetados/ ICs impactados é gerada por meio de eventos. Quando habilitada, a atualização é executada em segundo plano e os

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
	marcadores de segurança são adicionados ao incidente. Defina o valor como **verdadeiro** para executar a operação em segundo plano. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Recupere o serviço crítico a partir de dados pré-calculados. sn_si.critical_service.calculator.use_cache	Permite que a calculadora de serviço crítico use dados pré-calculados de itens de configuração. Defina o valor como **verdadeiro** para pesquisar a partir de dados pré-calculados • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de Incidente de segurança [sn_si.admin]	Controle total sobre todos os dados de Security Incident Response. Também gerencia territórios e habilidades, conforme necessário. **Nota:** No sistema de base, o administrador também tem acesso a sn_si.admin. Security Incident Response pode ser restringido pelo administrador, desde que pelo menos outro usuário tenha a função de administrador de segurança atribuída.	• assessment_admin • catalog_admin • decisão_tabela_admin • decision_table_reader • filter_admin • flow_designer • autor_pd • pd_content_author • operador_pd • skill_admin • skill_model_admin • sn_si.analyst • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
		• sn_si.special_access_read_manager • sn_si.special_access_write_manager • sn_ti.malicious_attachment_access • sn_ti.observável.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
Analista de incidentes de segurança [sn_si.analyst]	Gerenciar incidentes de segurança. Função subjacente para acesso de segurança básico. Usuários com esta função podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas a seus incidentes.	• operador_pd • snc_platform_rest_api_access • sn_msi.promoter • sn_msi.proposer • sn_si.basic • sn_ti.malicious_attachment_access
Incidente de segurança básico [sn_si.basic]	Função subjacente para acesso de segurança básico. Usuários com esta função podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas a seus incidentes.	• canvas_user • document_management_user • e-mail_composer • flow_operator • Inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • treemap_user

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
Diretor de segurança da informação (CISO) [sn_si.ciso]	Exibir e manipular o painel do CISO. Além disso, se o plug-in Resposta a vulnerabilidades estiver ativado, os usuários com esta função poderão adicionar mapas de árvore de definição de significância de vulnerabilidade ao painel. Você também pode fazer o mesmo com o plug-in Security Incident Response.	• pa_viewer • sn_si.basic • sn_si.read
Incidente de segurança externo [sn_si.external]	Exibir todos os incidentes de segurança que pertencem ao grupo específico. **Nota:** As duas regras a seguir são aplicáveis em ServiceNow independentemente do administrador com escopo ou do app do escopo. • Ao adicionar qualquer usuário a um grupo, você também está atribuindo funções a esse grupo. Da mesma forma, quando você remove um usuário de um grupo, as funções herdadas também são removidas. • Cada função é atribuível por alguma função de precedência mais alta.	service_fulfiller
Usuário de integração de incidente de segurança [sn_si.integration_user]	Ferramentas externas podem fornecer novos registros de incidentes de segurança e atualizar	import_transformer

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	registros de incidentes de segurança.	
Administrador de conhecimento de incidente de segurança [sn_si.knowledge_admin]	Gerencie, atualize e exclua as informações na base de conhecimento do Incidente de Segurança.	• knowledge_admin • sn_si.read
Gerenciador de Incidentes de segurança [sn_si.manager]	Mesmo acesso que os analistas de segurança.	• autor_pd • operador_pd • sn_si.basic
Leitura de incidente de segurança [sn_si.read]	Ler incidentes de segurança.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippet_r • sn_ti.observable.read • workspace_user
Gerenciador de acesso de restrição de segurança [sn_si.restriction_access_manager]	Permite que usuários ou grupos "imponham restrição" em incidentes de segurança. Isso é aplicável somente para mudança de campo.	N/D
Acesso especial a incidente de segurança sn_si.special_access	Fornece acesso a incidentes de segurança específicos para usuários fora da organização do Security Operations.	N/D
Habilitador de acesso especial de segurança [sn_si.special_access_enabler]	Fornece função de acesso especial a um usuário fora da organização das Operações de segurança para incidentes de segurança específicos.	N/D
Gerenciador de leitura de acesso especial a incidentes de segurança [sn_si.special_access_read_manager]	Gerencie a função Acesso especial a incidentes de segurança [sn_si.special_access]. Use esta função para modificar o campo **Acesso de leitura** no formulário de incidente de segurança. Esta função pode ser atribuída por sn_si.admin.	sn_si.special_access_enabler

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
Gerenciador do gravador de acesso especial a incidentes de segurança [sn_si.special_access_write_manager]	Gerencie a função Acesso especial a incidentes de segurança [sn_si.special_access]. Use esta função para modificar o campo **Acesso privilegiado** no formulário de incidente de segurança. Esta função pode ser atribuída por sn_si.admin.	sn_si.special_access_enabler

Trabalhos agendados instalados

Trabalho agendado	Descrição
Pesquisar observáveis de incidente de segurança	Executa uma pesquisa de observáveis em uma programação definida pelo usuário.

Tabelas instaladas

Tabela	Descrição
Configuração do Feed de Notícias [sn_si_feed_configuration]	Registros de configuração usados para definir o conteúdo exibido no feed de notícias de incidentes de segurança.
Regra de Atribuição de Análise Pós-incidente [sn_si_pir_condition]	Automatiza a seleção de participantes de uma pesquisa de revisão pós-incidente quando um incidente de segurança é encerrado.
Incidente de Segurança [sn_si_incident]	Armazena um incidente de segurança, as respostas ao incidente, todas as tarefas vinculadas, mudanças, problemas e incidentes relacionados a este incidente de segurança.
Vetores de Ataque do Incidente de Segurança [sn_si_attack_vector]	Opções de vetor de ataque.
Log de Auditoria de Incidentes de Segurança [sn_si_audit_log]	Armazena logs de auditoria de aprimoramento de incidentes de segurança.
Calculadora de Incidentes de Segurança [sn_si_calculator]	Uma calculadora para definir determinados campos de incidente de segurança quando certas condições são atendidas.
Grupo de Calculadoras de Incidentes de Segurança	Um agrupamento de calculadoras de incidente de segurança. A ordem do grupo de calculadoras determina qual grupo é

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_si_calculator_group]	avaliado primeiro e, em cada grupo, uma calculadora é usada no máximo.
Firewall de aprimoramento de incidente de segurança [sn_si_enrichment_firewall]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos do Firewall da Palo Alto Networks.
Resultados de malware de aprimoramento de incidente de segurança [sn_si_enrichment_malware]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos do malware.
Estatísticas de Rede de Aprimoramento de Incidente de Segurança [sn_si_enrichment_network_statistics]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos das estatísticas de rede.
Processos em execução de Aprimoramento de Incidente de Segurança [sn_si_enrichment_running _processes]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos para processos em execução.
Serviços de Execução de Aprimoramento de Incidente de Segurança [sn_si_enrichment_running_service]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos para serviços em execução.
Pesquisa de E-mail de Incidente de Segurança [sn_si_m2m_incident_email_search]	Mapeia registros de pesquisa de e-mail para incidentes de segurança.
Importação de incidentes de segurança [sn_si_incident_import]	Tabela de importação para incidentes de segurança. Usado para criar incidentes de segurança a partir de sistemas externos.
Definição do Processo de Incidentes de Segurança [sn_si_process_definition]	Armazena a configuração dos fluxos do processo de incidente de segurança.
Seletor de Definição do Processo de Incidentes de Segurança [sn_si_process_definition_selector]	Armazena a definição do processo de incidente de segurança a ser usada para incidentes de segurança.
Caso do Atendimento ao cliente relacionado ao incidente de segurança [sn_si_m2m_incident_customerservice_case]	Mapeia casos de atendimento ao cliente e incidentes de segurança
Dados de aprimoramento relacionados ao Incidente de Segurança [sn_si_m2m_incident_enrichment]	Mapeia incidentes de segurança e registros de dados de aprimoramento relacionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Tarefa Security Incident Response [sn_si_task]	Gerencia subtarefas relacionadas à manipulação de um incidente de segurança. Essas tarefas podem ser atribuídas ao pessoal de segurança ou a pessoas em outros departamentos, para gerenciar a comunicação entre departamentos e o acompanhamento de tarefas.
Modelo de tarefas Security Incident Response [sn_si_task_template]	Usado para criar uma tarefa Security Incident Response. Esses modelos geralmente são usados em entradas do catálogo para criar automaticamente um conjunto de subtarefas apropriadas para um tipo específico de incidente de segurança.
Documento de runbook de incidente de segurança [sn_si_runbook_document]	Associa condições ou filtros de incidente de segurança a um artigo de conhecimento. Usado para especificar procedimentos de runbook para correção de incidente de segurança.
Modelo de Incidente de Segurança [sn_si_incident_template]	Usado para criar um incidente de segurança. Esses modelos geralmente são usados em entradas do catálogo para criar um incidente de segurança pré-criado.
Requisição de Segurança [sn_si_request]	Uma solicitação relacionada à segurança para a equipe de segurança.
Solicitação de Verificação de Segurança [sn_si_scan_request]	Uma solicitação de pesquisa de ameaças.
Calculadora de Gravidade sn_si_severity_calculator	Define os valores de severidade, impacto, risco e criticalidade de um incidente de segurança.
Usuário Afetado pela Tarefa [sn_si_m2m_task_affected_user]	Uma tabela muitos para muitos que associa incidentes de segurança aos usuários afetados.
Avaliador de Resultado de Atividade de Fluxo de Trabalho de Modelo [sn_si_wf_activity_outcome_evaluator]	Mapeia um recurso com um script de avaliação. Um novo subfluxo pode ser adicionado a um fluxo de trabalho de modelo para definir um resultado de tarefa de resposta em vez de ter um analista para defini-lo manualmente.

Outras tarefas de configuração Security Incident Response adicionais

Se você for um administrador no domínio global, configure como Security Incident Response lida com as operações diárias.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Essas opções são padrão para muitas aplicações de gestão de serviços e, como tal, usam a terminologia de gestão de serviços. Por exemplo, Solicitação é usada para a tarefa principal (ou seja, o incidente de segurança) e Tarefa é usada para subtarefas ou Tarefas de resposta.

Se você for um administrador em um domínio inferior ao domínio global, poderá exibir a tela Configurações, mas não poderá modificar as configurações.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração** > **Configuração**.
   As opções para configurar as aplicações são organizadas nestas guias:
   - A guia **Processo de negócios** contém opções para configurar o ciclo de vida da solicitação, criar catálogos e solicitações e configurar notificações.
   - A guia **Atribuição** contém opções para configurar a atribuição manual e automática.
   - A guia **Complementos** contém opções para habilitar a base de conhecimento, documentos gerenciados e atividades de tarefa.
2. Preencha os campos na guia **Processo de negócios**.

Tela de configuração — Guia Processo de negócios

Campo	Descrição
Ciclo de vida	
As Anotações de trabalho são necessárias para fechar ou cancelar uma solicitação ou tarefa	Habilite esta opção para exigir que o usuário insira anotações de trabalho antes que um incidente de segurança ou tarefa de resposta possa ser encerrado ou cancelado.
Copiar anotações de trabalho da tarefa para solicitação	Habilite esta opção para sincronizar as anotações de trabalho da tarefa de resposta com as anotações de trabalho no incidente de segurança. Portanto, quando anotações de trabalho na tarefa são adicionadas, as mesmas anotações de trabalho aparecem no incidente de segurança primário.
Criação de Solicitação e Catálogo	
Criar ou atualizar solicitações por e-mail de entrada	Habilite esta opção para criar ou atualizar incidentes de segurança a partir de e-mails de entrada.
As solicitações são criadas usando	Selecione **catálogo ou formulário regular** para ativar o catálogo e habilitar a publicação automática de modelos de incidente de segurança no catálogo. Selecione **o formulário regular somente** para desativar o catálogo e desabilitar a publicação automática de modelos de incidente de segurança no catálogo.
Os modelos criam um item do catálogo dedicado	Habilite esta opção para ativar a publicação automática de itens do catálogo para a aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Notificações	
Para uma solicitação ou tarefa, quando o campo selecionado mudar, envie uma notificação aos destinatários	Você pode configurar notificações a serem enviadas a destinatários específicos quando os campos selecionados em incidentes de segurança e tarefas de resposta forem alterados. **a.** Em **Tabela**, selecione **Solicitação (incidente de segurança** ou **Tarefa (tarefa de resposta)**. **b.** Em **Campo**, selecione o campo a ser usado para gerar notificações. Quando uma mudança é feita no campo selecionado, uma notificação é enviada aos destinatários identificados. **c.** Em **Destinatários**, selecione um ou mais destinatários. **d.** Se você selecionar **um usuário** ou **grupo específico**, será solicitado a selecionar um usuário ou grupo. **e.** Para definir mais notificações usando outros campos ou destinatários, repita as etapas anteriores para o próximo conjunto de configurações de notificação. **f.** Para remover uma notificação, clique no ícone do ⊖ à direita da notificação.

3. Clique na guia **Atribuição** e preencha os campos.

Tela de configuração — Guia Atribuição

Campo	Descrição
Método de atribuição para solicitações	Selecione o método para atribuir incidentes de segurança: ◦ **usando atribuição automática**: os incidentes de segurança são atribuídos automaticamente. ◦ **usando um fluxo de trabalho**: os incidentes de segurança são atribuídos pelo fluxo de trabalho selecionado. ◦ **manualmente**: os incidentes de segurança são atribuídos manualmente.
Use este fluxo de trabalho para atribuir solicitações	Selecione o fluxo de trabalho para expedir incidentes de segurança. Este campo aparece quando **o uso de um fluxo de trabalho** é selecionado na lista **Método de atribuição para solicitações**.
Método de atribuição para tarefas	Selecione o método para atribuir tarefas de resposta: ◦ **usando atribuição automática: as**tarefas de resposta são atribuídas automaticamente. ◦ **usando um fluxo de trabalho**: as tarefas de resposta são atribuídas pelo fluxo de trabalho selecionado. ◦ **manualmente**: as tarefas de resposta são atribuídas manualmente.
Use este fluxo de trabalho para atribuir tarefas	Selecione o fluxo de trabalho para atribuir tarefas de resposta. Este campo aparece quando **o uso de um fluxo de**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	trabalho é selecionado na lista **Método de atribuição para tarefas**.
Atribuir solicitações ou tarefas com base nas áreas cobertas do grupo de atribuições	Habilite esta opção para limitar a atribuição de incidentes de segurança e tarefas de resposta a grupos que cobrem o local da tarefa.
Programação	
A seleção automática de agentes considera o fuso horário para as tarefas	Habilite esta opção para considerar o fuso horário do agente ao atribuir uma tarefa. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
Fatores adicionais	
A seleção automática de agentes considera a localização dos agentes	Habilite esta opção para dar preferência aos agentes que estão mais próximos do local da tarefa ao atribuir tarefas. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
A seleção automática de agentes requer tarefas que eles estejam aptos a realizar	Selecione o grau em que as habilidades do agente devem corresponder a uma tarefa ao determinar a atribuição automática. ◦ Selecione **tudo** para exigir que um agente atribuído tenha todas as habilidades para executar a tarefa. Um agente que não tiver pelo menos uma habilidade será eliminado. ◦ Selecione **algumas** se quiser agentes que tenham a maioria das habilidades necessárias para executar a tarefa. ◦ Selecione **nenhum** se quiser atribuir agentes automaticamente sem levar em conta as habilidades. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
Tentativa de seleção automática de atribuir o mesmo agente a todas as tarefas em uma solicitação	Habilite esta opção para atribuir automaticamente todas as tarefas de resposta de um incidente de segurança ao mesmo agente.

4. Clique na guia **Complementos** e preencha os campos.

Tela de configuração — Guia Complementos

Campo	Descrição
Documentação	
Habilitar uma base de conhecimento dedicada	Habilite esta opção para ativar a base de conhecimento para Security Incident Response.
Habilitar documentos gerenciados	Habilite esta opção para adicionar uma lista relacionada a documentos gerenciados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Habilitar atividades da tarefa	Habilite esta opção para registrar interações e comunicações de tarefas, como chamadas telefônicas e mensagens de e-mail.

5. Clique em **Salvar**.

Bloquear administração de segurança

Para proteger as investigações e manter os incidentes de segurança privados, você pode restringir o acesso Security Incident Response a funções e ACLs específicas de segurança. Os administradores que não são de segurança podem ter acesso restrito, a menos que você permita expressamente a entrada.

Antes de Iniciar

Quando a aplicação Security Incident Response é ativada, o usuário Administrador do sistema recebe a função sn_si.admin por padrão. O Administrador do sistema é o único administrador que pode configurar grupos e usuários de segurança.

Uma função de segurança é necessária para ter acesso a Security Incident Response recursos e registros.

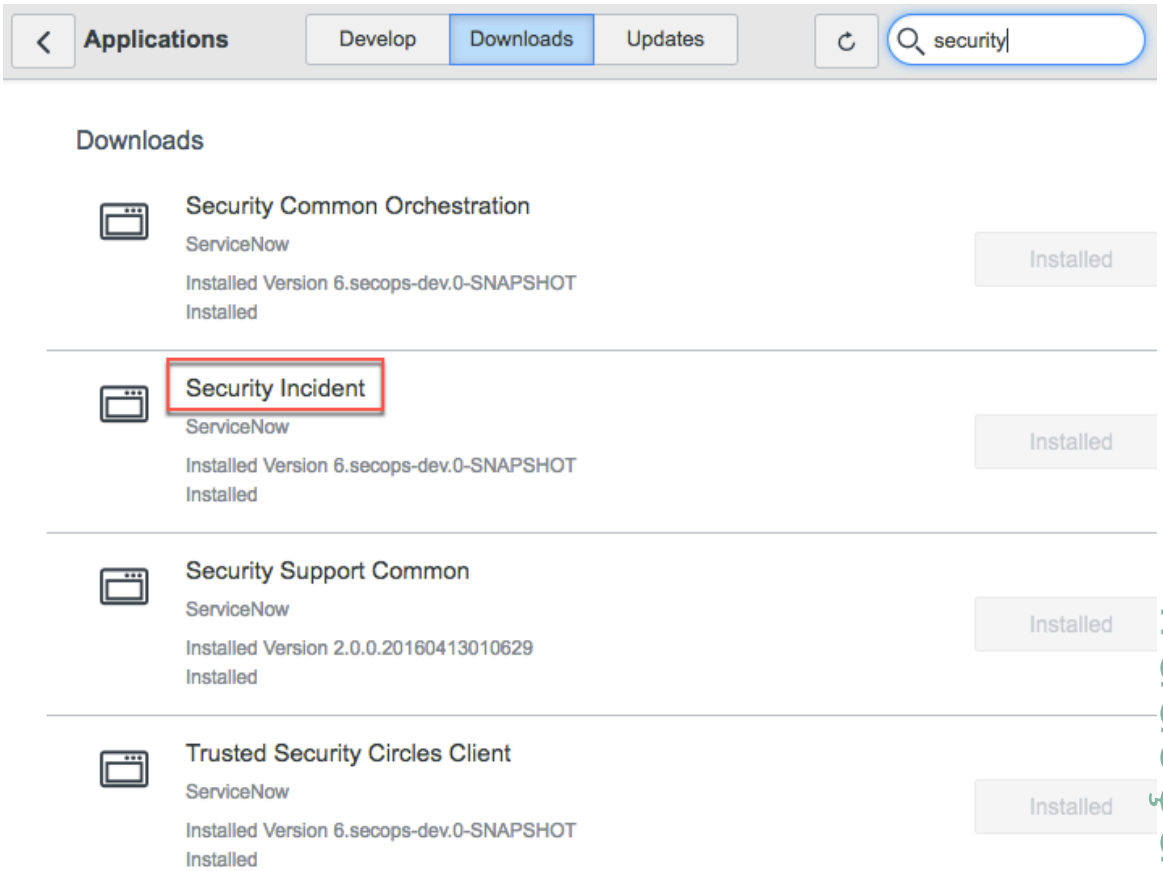
Função necessária: sn_si.admin

Procedimento

1. Depois que o plug-in Security Incident Response é ativado, um usuário com a função de administrador atribui a função de administrador com escopo (sn_si.admin) a pelo menos um usuário.
2. O usuário com a função de administrador muda para o escopo do Incidente de segurança.
3. Navegar até **Aplicações do sistema** > **Aplicações**.
4. Clique **em Downloads**.
5. Digite **segurança** no campo **Pesquisar aplicações**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique **em Incidente de segurança**.
7. Role para baixo até **Links relacionados** e clique em **Remover da função contida por administrador**.
8. Saia e faça login novamente.
   O usuário administrador não pode acessar a aplicação Security Incident Response.

Informações relacionadas

Administração de aplicação

Gerenciar acesso de chamador restrito

O recurso Acesso de chamador restrito (RCA) permite que um administrador defina o acesso entre escopos a uma aplicação ou recurso de aplicação e permita ou negue solicitações de acesso. Este recurso está habilitado em Security Incident Response por padrão para que os analistas de segurança possam proteger informações confidenciais relacionadas à segurança.

Um campo chamado **Acesso** do solicitante foi adicionado a todas as tabelas e inclusões de script em Security Incident Response, e o padrão do campo é **Acompanhamento de chamadas**. Essa configuração significa que os escopos da aplicação têm permissão para acessar Security Incident Response tabelas e inclusões de script. No entanto, um registro de acompanhamento é criado para cada registro e armazenado na tabela Privilégio de acesso de solicitante restrito [sys_restricted_caller_access].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Tenha cuidado ao mudar os registros de **Acompanhamento** de **chamadas para Restrito**a chamadores . Registros com este status não podem ser acessados até que um administrador permita manualmente o acesso a eles. O administrador deve navegar até **Aplicações do sistema** > **Acesso de chamador restrito a aplicação**, localize a tabela ou inclusão de script para a qual o acesso foi solicitado e altere o campo **Status** de **Solicitado** para **Permitido**.

Informações relacionadas

Configurações de privilégio de acesso de chamador restrito

Definir o escopo da aplicação, o recurso da aplicação e o acesso a eventos

Executar testes de início rápido para Security Incident Response

Valide se Security Incident Response ainda funciona depois que você faz mudanças de configuração, como aplicar um upgrade ou desenvolver uma aplicação. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

Os testes de início rápido Security Incident Response exigem a ativação do plug-in Resposta a incidentes de segurança (com.snc.security_incident) e o carregamento dos dados de demonstração.

Testes Security Incident Response

Teste	Descrição	Versão de lançamento
SIR: criar incidente de segurança	Determine se um usuário pode criar um incidente de segurança com êxito a partir do formulário de incidente de segurança.	Xanadu
SIR: criar incidente de segurança por meio do catálogo de incidentes de segurança	Determine se um usuário pode criar um incidente de segurança com êxito a partir do formulário de incidente de segurança.	Xanadu
SIR: ciclo de vida do incidente de segurança	Valide as tarefas de resposta do fluxo de trabalho de violação de política.	Xanadu
SIR: pesquisa de ameaças	Valida a funcionalidade de pesquisa de ameaças.	Xanadu
SIR: configuração OOTB das avaliações de PIR	Use este teste para validar avaliações de PIR e configurações de sistema de base.	Xanadu
SIR: configuração condicional das avaliações de PIR	Verifique se incidentes de segurança correspondentes à regra condicional obrigatória não são encerrados sem a conclusão da avaliação pós-incidente.	Xanadu

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Security Incident Response

Teste	Descrição	Versão de lançamento
	Verifique se os incidentes de segurança correspondentes à regra condicional opcional podem ser encerrados sem a conclusão da avaliação pós-incidente. Verifique se as avaliações não são geradas para os incidentes de segurança que não correspondem a nenhuma regra.	
SIR: verificação do tempo de execução do PIR	Verifique se os relatórios PIR estão configurados e anexados aos incidentes de segurança de acordo com o novo design.	Xanadu
SIR: verificação de configuração do tempo de design do PIR	Verifique se o incidente de segurança está mapeado com o modelo de relatório baseado na configuração do administrador.	Xanadu
SIR: Vincular o incidente de segurança a um importante incidente de segurança existente	Vincule um Incidente de Segurança a um Incidente de Segurança Importante existente e valide os dados do Incidente de Segurança implementados no Incidente de Segurança Importante.	Xanadu
SIR: promover o incidente de segurança como um incidente de segurança importante	Promova um Incidente de Segurança como um Incidente de Segurança Importante e valide os dados do Incidente de Segurança implementados no Incidente de Segurança Importante.	Xanadu
SIR: propor Incidente de Segurança como Incidente de Segurança Importante	Proponha um Incidente de Segurança como Incidente de Segurança Importante e valide os dados de Incidente de Segurança implementados no Incidente de Segurança Importante.	Xanadu
Verifique se somente Membros permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ATIVADA	Verifique se somente membros permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ativada.	Xanadu

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Security Incident Response

Teste	Descrição	Versão de lançamento
Verifique se somente Grupos permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ATIVADA	Verifique se somente grupos permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ativada.	Xanadu
Validar acesso de leitura	Valide o acesso de exibição.	Xanadu
Validar acesso de gravação	Valide o acesso de edição.	Xanadu

Informações relacionadas

Testes de início rápido

Referência do Assistente de configuração

O Assistente de configuração orienta você nas etapas que você precisa executar para configurar o sistema de base Security Incident Response. Esta seção fornece informações adicionais sobre as etapas complicadas para as quais você pode precisar de mais explicações.

Criar uma Security Incident Response definição de processo

Você pode criar uma definição de processo para definir a forma como os incidentes de segurança fazem a transição de um estado para o próximo. As definições de processo ajudam as centrais de serviços e os usuários finais a rastrear o problema durante todo o ciclo de vida.

Antes de Iniciar

Função necessária: sn.si_admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração** > **Definição de Processo**.
2. Clique em **Nova**.
3. Preencha os campos, se for o caso.

Como criar definições de processo

Campo	Descrição
Nome	Nome do registro que descreve o processo codificado no arquivo de inclusão de script. O nome é exibido como uma opção na lista **Seletor de definição de processo**.
Inclusão de script	O nome (incluindo o prefixo `sn_si`.) da inclusão de script que contém a definição do processo. O script deve estar no escopo da aplicação Incidente de segurança (`sn_si`). Para obter mais informações, consulte Criar uma inclusão de script de definição de processo personalizada Security Incident Response. Se este campo não contiver um nome de inclusão de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	script válido, a definição padrão de ProcessDefinition_NIST_Stateful será usada.
Descrição	Informações úteis sobre a inclusão de script.
Ordem	Determina a posição na lista de definição de processo.
Ativo	Quando marcada, torna esta definição de processo selecionável na página **Seletor de definição** de processo.

4. Clique em **Enviar**.

Informações relacionadas

Seleção do processo do Security Incident Response

Noções básicas sobre a definição do processo do Security Incident Response

Noções básicas sobre a definição do processo do Security Incident Response

Security Incident Response Definição de Processo O substitui os fluxos de estado e fornece aos usuários finais e às centrais de serviços o status de um problema. Uma definição de processo ajuda a rastrear o problema durante seu ciclo de vida. Security Incident Response é uma aplicação de Gestão de serviços (SM), que tem seu próprio conjunto de estados. Estados inválidos são relatados como parte de Seleção de processo.

Definição do processo do Security Incident Response

A definição de processo padrão (NIST Stateful) define os seguintes estados de incidente:

Nota: Os estados disponíveis variam de acordo com o estado atual do incidente.

Estados da definição do processo de incidente de segurança

Estado	Descrição
Rascunho	O iniciador da solicitação adiciona informações sobre o incidente de segurança, mas ainda não está pronto para ser trabalhado.
Análise	O incidente foi atribuído e o problema está sendo analisado.
Contém	O problema foi identificado e a equipe de segurança está trabalhando para contê-lo e executar o controle de danos. Essas ações podem incluir colocar servidores off-line, desconectar equipamentos da internet e verificar se existem backups.
Erradicar	O problema foi contido e a equipe de segurança está tomando medidas para corrigi-lo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da definição do processo de incidente de segurança

Estado	Descrição
Recuperar	O problema foi resolvido e a prontidão operacional dos sistemas afetados está sendo verificada.
Revisão	O incidente de segurança foi concluído e todos os sistemas estão de volta à função normal. No entanto, uma revisão pós-incidente ainda é necessária.
Encerrado	O incidente está concluído, mas antes que um incidente de segurança possa ser encerrado, você deve preencher as informações na guia **Informações de fechamento**.

Definições do processo da tarefa de incidente de segurança

As seguintes definições de processo são usadas para tarefas de incidente de segurança.

Estados da definição do processo da tarefa

Estado	Descrição
Pronto	A tarefa está pronta para ser trabalhada depois de ser atribuída a um agente.
Atribuído em	A tarefa está atribuída a um agente.
Trabalho em andamento	O agente atribuído está trabalhando na tarefa.
Concluir	A tarefa está concluída.
Cancelado	A tarefa foi cancelada.

O NIST é compatível com os dois modelos a seguir:

- **NIST com estado**

  Esta definição de processo permite que os analistas passem de um estado para outro em uma ordem sequencial sem ignorar nenhuma etapa. Por exemplo, se o Analista começar com o estado **Rascunho**, a ordem sequencial desta definição de processo será **Rascunho**>**Análise**>**Conter**>**Eliminar**>**Recuperar**. Portanto, a definição do processo com monitoramento de estados do NIST é unidirecional e permite que os analistas avancem somente para os estados avançados.

  Aqui está outro exemplo, se o Analista começar com o estado Análise, a ordem sequencial desta definição de processo será **Análise**>**Conter**>**Eliminar**>**Recuperar**.

- **NIST aberto**

  Esta definição de processo permite que os analistas passem de um estado para outro, seja para frente ou para trás. Por exemplo, se o Analista começar com o estado **Análise**, a ordem da definição do processo poderá ser **Análise**>**Conter**>**Eliminar**>**Recuperar** ou **Análise**>**Rascunho**. Portanto, a definição do processo aberto do NIST é bidirecional e permite que os analistas avancem ou retrocedam, dependendo dos requisitos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seleção do processo do Security Incident Response

Security Incident Response A seleção de processo lista os processos com estados inválidos para incidentes de segurança e tarefas de resposta.

Um administrador pode corrigir o incidente ou a tarefa para estados válidos manualmente ou usando um script. Uma lista relacionada vazia (sem incidentes, sem tarefas) indica que todas as tarefas ativas estão em um estado válido. Os estados disponíveis variam de acordo com o estado atual do incidente. Para obter mais informações, consulte Corrija um incidente de segurança ou estado de tarefa inválido com a definição de processo.

Selecione uma Security Incident Response definição de processo

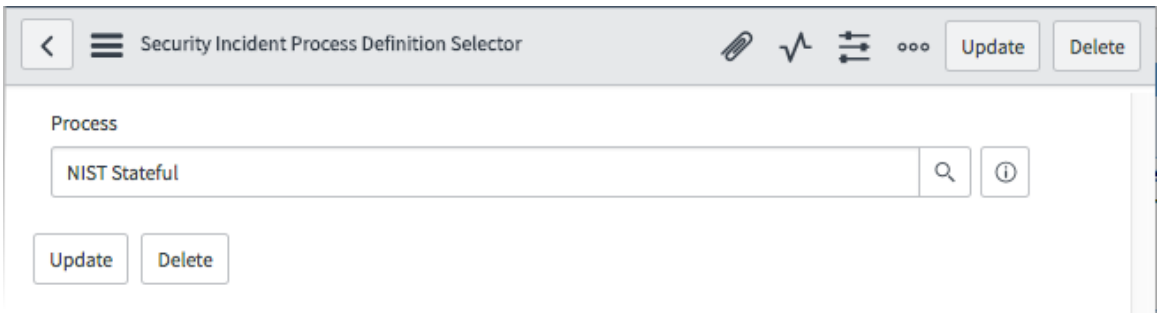
Você pode selecionar a definição de processo a ser usada para os estados apropriados para as tarefas de resposta e incidentes de segurança da sua empresa.

Antes de Iniciar
Função necessária: admin e sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Todos** > **Resposta a incidentes de segurança** > **Administração** > **Seleção de processo**.
2. Clique no ícone de pesquisa para listar as definições de processo disponíveis.



3. Selecione uma definição de processo.
4. Clique em **Atualizar**.

Criar uma inclusão de script de definição de processo personalizada Security Incident Response

Crie um script de definição de processo personalizado para os estados apropriados dos incidentes de segurança e tarefas de resposta da sua empresa.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
O script principal sn_si.ProcessDefinition inclui controles e definições de processo. **A definição de processo** determina qual definição está em uso (usando **Seleção de processo**). Ele chama o arquivo de inclusão de script apropriado para determinar os estados iniciais e as transições para incidentes de segurança e tarefas de resposta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

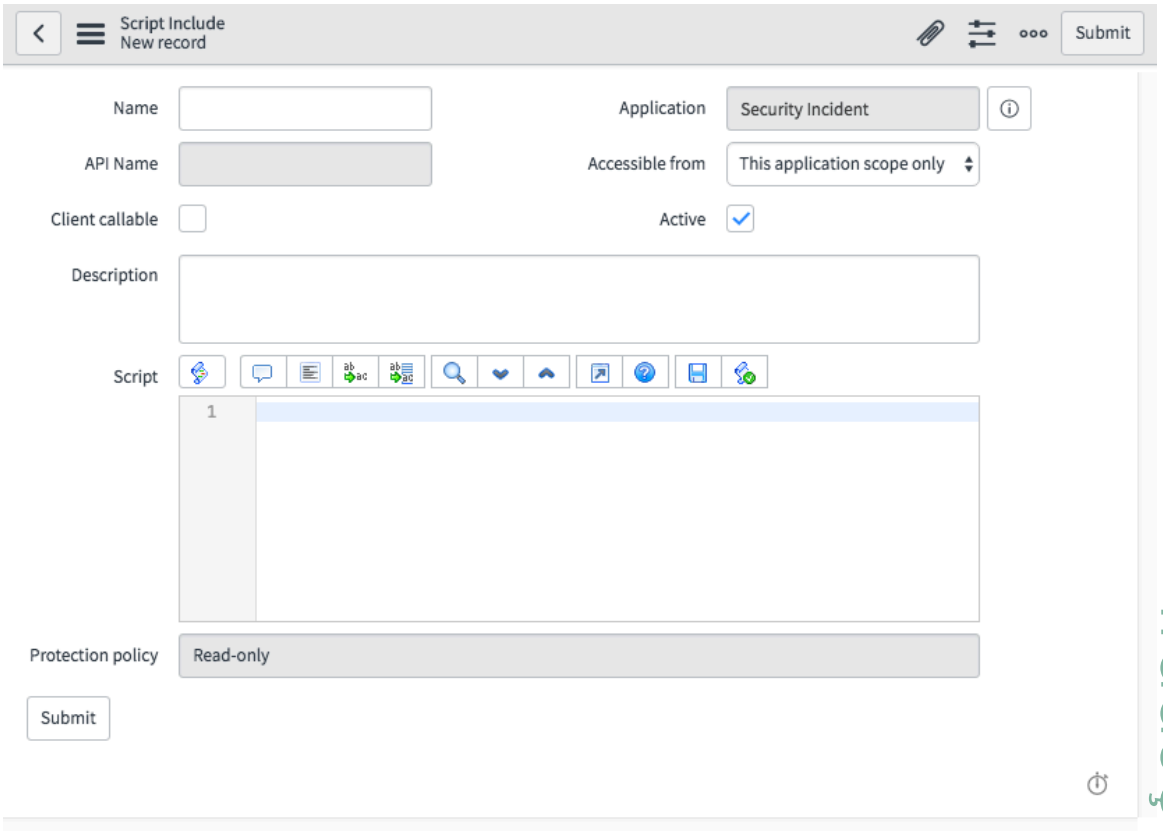
1. Navegar até **Todos** > **Definição do Sistema** > **Inclusões de script**.
2. Clique em **Novo.**
3. Preencha os campos, se for o caso.

Como criar definições de processo

Campo	Descrição
Nome	Nome desta inclusão de script.
Nome da API	Criado com base no nome da inclusão de script.
Cliente chamável	Torna a inclusão de script disponível para client scripts, filtros de lista e relatório, qualificadores de referência ou, se especificado, como parte do URL.
Aplicação	Incidente de segurança
Acessível de	Escolha **Somente este escopo da aplicação** .
Ativo	Quando marcada, torna esta inclusão de script selecionável na página **Definição de processo**.
Descrição	Informações úteis sobre a inclusão de script.
Script	Define o script do lado do servidor a ser executado quando chamado de outros scripts. O script deve definir uma única classe JavaScript ou uma função global. O nome da classe ou função deve corresponder ao campo Nome. Para obter informações sobre o conteúdo do script, consulte Inclusão de script de definição de processo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Enviar**.

Informações relacionadas

Inclusão de script de definição de processo

Inclusão de script de definição de processo

A inclusão de script Definição de processo fornece métodos para definir uma definição de processo.

Implemente as constantes, atributos, matrizes e chamadas de método descritas aqui para personalizar uma inclusão de script de definição de processo.

Onde usar

Use esta inclusão de script para criar uma definição de processo.

Corpo da inclusão de script

O corpo da inclusão de script é composto por três seções:

- Constantes: definições de estado inicial
- Tarefa de resposta e incidente de segurança: matrizes de definição de processo
- Chamadas de método: recuperando informações

Constantes

As constantes são usadas para definir os estados iniciais de incidentes de segurança e tarefas de resposta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O uso de constantes é opcional, mas incentivado para facilitar a leitura. Por exemplo:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Que são usados posteriormente pelos seguintes métodos:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

O próximo conjunto de constantes define os estados dos incidentes de segurança e das tarefas de resposta.

Cada matriz também contém a definição de quais estados estão disponíveis quando o incidente ou a tarefa está em um estado específico.

Por exemplo:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

O exemplo é uma matriz de objetos. Cada objeto define um estado e possíveis estados de transição.

A ordem do objeto do estado determina a ordem desejada para o fluxo.

Quando a tarefa está no estado "Rascunho" (valor 1), os estados possíveis são: 1 (Rascunho, que é nenhuma mudança) e 10 (Pronto, a próxima etapa do processo).

Não há limite para o número de transições de um estado. Os estados "Fechamento concluído" e "Cancelado" são estados finais e, portanto, não têm transições de estado possíveis.

A ordem dos atributos no objeto não é importante. Se isso tornar a definição mais clara, coloque o rótulo primeiro.

Atributos

Os atributos obrigatórios em um objeto de definição de estado são:

- estado: valor numérico do estado
- rótulo: texto legível associado ao estado
- opção: uma matriz de valores de estado para a qual o estado pode fazer a transição (determina o conteúdo da lista suspensa de estado)

Os atributos opcionais são:

- obrigatório: lista de IDs de campo que se tornam obrigatórios neste estado
- somente leitura: lista de IDs de campo que se tornam somente leitura neste estado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- visível: lista de IDs de campo que se tornam visíveis neste estado
- notmandatory: lista de IDs de campo que se tornam não obrigatórios neste estado
- notvisible: lista de IDs de campo que não estariam mais visíveis neste estado

Nota:

Se atributos opcionais forem usados, é responsabilidade do autor garantir que os campos sejam tornados visíveis/invisíveis, obrigatórios/não obrigatórios, visíveis/ocultos ou somente leitura adequadamente entre os estados.

Por exemplo, ocultar um campo em um estado não o torna visível em outro estado posteriormente, a menos que o atributo "visível" seja usado.

Matrizes de definição de fluxo de processo

Para definir as informações exibidas no formatador de fluxo de processo (a barra na parte superior dos formulários de tarefa de resposta e incidente de segurança), o sistema requer informações sobre o que exibir para cada estado.

Por exemplo:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ",
 description:"<p>Security Incident Response Task is in draft</p>"},
 {label:"Ready", condition:"state=10^EQ", description:"<p>Security
 Incident Response Task is ready to be assigned</p>"},
 {label:"Assigned", condition:"state=16^EQ", description:"<p>Security
 Incident Response Task is assigned</p>"},
 {label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work
 has started on this Security Incident Response Task</p>"},
 {label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ",
 description:"<p>Security Incident Response Task is complete</p>"},
],
```

A matriz TASK_PF é uma coleção de rótulos, condições e descrições usadas para determinar o texto exibido na barra do formatador de processos (incluindo ordem e atividade).

No exemplo, o texto "Pronto" é o segundo item exibido. É realçado quando a tarefa atende à condição 'state=10^EQ'.

Quando o ponteiro do mouse passa sobre o texto, a descrição "A tarefa do Security Incident Response está pronta para ser atribuída" é exibida.

Nota:

Os estados podem ser combinados para um único estado do formatador.

No exemplo, os estados "Fechado concluído" e "Cancelado" são exibidos como "Fechado" na barra superior.

Chamadas de método

Os métodos a seguir devem estar presentes na inclusão de script, pois são usados por sn_si.ProcessDefinition:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de retorno	Resumo do método	Descrição
Cadeia de caracteres	getInitialIncidentState: função ()	retornar o valor numérico do estado do incidente inicial
Cadeia de caracteres	getInitialTaskState: função():	retornar o valor numérico do estado da tarefa inicial
Matriz de cadeia de caracteres	getIncidentStates: função ()::	retornar a matriz do estado do incidente
Matriz de cadeia de caracteres	getTaskStates: função ()::	retornar a matriz do estado da tarefa
Matriz de objetos	getIncidentProcessFlows: função ()::	retornar a matriz de definição de fluxo do processo de incidente
Matriz de objetos	getTaskProcessFlows: função():	retornar a matriz de definição de fluxo do processo de tarefa

O próximo conjunto de métodos é chamado sempre que um incidente ou uma tarefa é atualizado e permite que ações sejam executadas em transições de mudança específicas.

Tipo de retorno	Resumo do método	Descrição
vazio	performIncidentStateChange: função (atual, anterior)	Nos exemplos, este método é usado para definir valores relacionados ao SM e garantir que um incidente avance para fora de "Rascunho" quando alguém for atribuído a ele.
vazio	performTaskStateChange: função (atual, anterior)	No exemplo, este método é usado para atualizar carimbos de data/hora (na atribuição e no fechamento) e avançar a tarefa de "Pronto" para "Atribuído" quando o campo assigned_to estiver preenchido.

As mesmas ações executadas por esses dois métodos podem ser realizadas usando uma regra de negócio. Ao defini-los na inclusão de script, a alternância das definições de processo é facilitada.

Corrija um incidente de segurança ou estado de tarefa inválido com a definição de processo

Um administrador pode corrigir o incidente de segurança ou a tarefa para estados válidos, manualmente ou usando um script. Os estados disponíveis variam de acordo com o estado atual do incidente.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Depois de alternar as definições de processo, a nova definição pode não oferecer suporte a alguns dos estados antigos. Para corrigir os estados de incidentes ou tarefas órfãos, você pode alterar a definição do processo, editar a inclusão de scriptou abrir manualmente cada incidente ou tarefa para atualizar o estado. Geralmente, atualizar o estado (o que pode ser feito em massa) é a solução mais fácil.

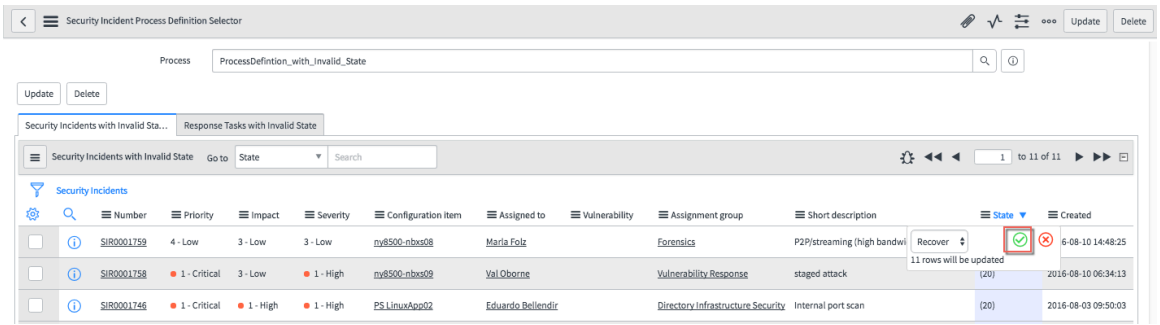
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para mudar os estados em massa, faça o seguinte:

Procedimento

1. Navegar até **Todos** > **Seleção de processo**.
2. Realce o campo **Estado** para os incidentes ou tarefas que você deseja mudar.
3. Clique duas vezes emno campo **Estado** no primeiro registro, selecione o novo **Estado** e clique na marca de seleção ( ) para concluir a mudança.



4. Clique em **Atualizar**.

Criar um grupo de incidentes de segurança

Configure um grupo de incidentes de segurança e atribua as funções e usuários apropriados ao grupo.

Antes de Iniciar

Funções necessárias:

- Se você tiver a função user_admin, poderá criar grupos de atribuição de incidentes de segurança.
- Se você tiver a função sn_si.admin, poderá criar e editar grupos de atribuição de incidentes de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Os usuários de um grupo herdam as funções do grupo, portanto, você não precisa atribuir funções a cada usuário separadamente.
É uma prática recomendada criar quantos grupos forem necessários em sua organização. Também é uma prática recomendada criar um grupo para administradores e atribuir a função de administrador somente a este grupo.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos** ou **Incidente de segurança** > **Configuração** > **Grupos**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Nota:

Para obter mais informações, consulte Criar um grupo de usuários .

4. Certifique-se de selecionar o tipo de **incidente de segurança** para este grupo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Se o campo **Tipo** não estiver visível, configure o formulário para adicioná-lo.

b. Clique no ícone de cadeado ao lado do campo **Tipo**.

c. Clique no ícone de pesquisa de referência ( )

d. Pesquise e selecione o tipo de **incidente de segurança**.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
6. Na lista relacionada **Funções**, adicione as funções que cada membro deste grupo recebe.
   Por exemplo, se você estiver criando um grupo para membros da equipe Security Incident Response, adicione sn_si.analyst. Se você estiver criando um grupo para administradores Security Incident Response, adicione sn_si.admin.
7. Na lista relacionada **Membros do grupo**, adicione usuários a este grupo.
8. Clique em **Atualizar**.

Criar um grupo de calculadoras de incidentes de segurança

Grupos de calculadoras de incidentes de segurança são usados para agrupar calculadoras.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **Grupos de calculadoras de incidentes de segurança**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da calculadora de incidentes de segurança.
Aplicação	A aplicação que contém este registro.
Ordem	A ordem na qual a calculadora de incidentes de segurança é executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Descrição	Uma descrição deste grupo de calculadoras.
Criado(a) por	Insira o nome do usuário que criou

4. Clique em **Enviar**.

Criar uma calculadora de incidente de segurança

As calculadoras de incidente de segurança permitem calcular a gravidade de um incidente de segurança com base em fórmulas predefinidas. Você pode definir suas próprias calculadoras de incidentes de segurança, conforme necessário.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **Grupos de calculadoras de incidentes de segurança**.
2. Clique no nome do grupo para o qual você deseja criar uma calculadora ou crie um grupo de calculadoras.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da calculadora de incidentes de segurança.
Grupo de Calculadoras	Nome do grupo ao qual esta calculadora pertence. **Nota:** Criar ou alterar o grupo de calculadoras se torna disponível depois que você insere um **Nome** e uma **Tabela**.
Tabela	Selecione a tabela a ser usada para esta calculadora. Ao adicionar calculadoras a tabelas diferentes de Vulnerabilidade [sn_vul_vulnerability] e Item vulnerável [sn_vul_vulnerable_item], você deve adicionar regras de negócio e Ações de IU a essas tabelas. Para ver exemplos: ◦ Navegar até **Definição do Sistema** > **Regras de negócio**e localize a regra de negócio **Calcular gravidade** na tabela Item vulnerável [sn_vul_vulnerable_item]. ◦ Navegar até **IU do Sistema** > **Ações de IU**e localize a ação de IU **Calcular gravidade** na tabela Item vulnerável [sn_vul_vulnerable_item]. Além disso, a função de administrador de vulnerabilidades deve receber capacidades totais de leitura, gravação (ou save_as_template) em qualquer tabela usada por uma calculadora para ver corretamente os valores a serem aplicados ao modelo.
Aplicação	A aplicação com escopo à qual a calculadora pertence.
Ordem	A ordem na qual a calculadora de incidentes de segurança é executada. Uma calculadora com uma entrada de pedido de 100 é executada antes de uma calculadora com uma entrada de pedido de 200.
Ativo	Ligue ou desligue a calculadora.
Descrição	Uma descrição desta calculadora.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
As guias **Condições** e **Valores a serem** aplicados são exibidas.
6. Preencha os campos na guia **Condições**, conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou criar um novo grupo de filtros para definir os critérios da calculadora.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir uma calculadora. Este campo aparecerá somente se você marcar a caixa de seleção **Usar grupos de filtros**.
Usar a condição avançada	Marque esta caixa de seleção para indicar que uma condição de script é usada para determinar quando esta calculadora é aplicada. Quando você marca a caixa de seleção, um campo de script **de condição avançada** é exibido. Se você marcou a caixa de seleção **Usar grupo de filtros**, este campo ficará oculto. **Nota:** Antes de definir condições avançadas e escrever scripts para determinar quando as calculadoras de incidentes de segurança são aplicadas, retorne à lista Calculadoras de incidentes de segurança. Explore os registros da calculadora enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora é usada. Se você marcou as caixas de seleção **Usar grupo de filtros** ou **Usar condições avançadas**, este campo ficará oculto.

7. Clique na guia **Valores a serem aplicados** e preencha os campos no formulário, conforme apropriado.
   Você tem a opção de criar um script para definir os valores a serem aplicados ao cálculo ou definir um modelo com base nos campos da tabela selecionada.

Campo	Descrição
Usar valores de script	Marque esta caixa de seleção para definir valores de campo com um script.
Valores de Script	Define a quais valores os cálculos serão aplicados. Este campo aparecerá somente se você marcar a caixa de seleção **Usar valores de script**.
Modelo	Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**. Selecione os campos e valores que você deseja usar para a calculadora.

8. Quando tiver concluído todas as entradas, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre calculadoras de incidentes de segurança

Calculadoras de incidentes de segurança são usadas para atualizar valores de registro quando condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

O sistema base Security Incident Response inclui os seguintes grupos de calculadoras de incidentes de segurança e calculadoras. A primeira calculadora que corresponde às condições é executada em cada grupo.

Calculadoras de incidentes de segurança no sistema de base

Nome do grupo da calculadora de incidente de segurança	Calculadoras incluídas no grupo	Descrição
Impacto nos negócios	Agregar de calculadoras de gravidade	Esta calculadora delega para a Calculadora de Criticidade de Segurança que determina a criticalidade ponderando os valores de outros campos.
Gravidade	Negócios impactados	Esta calculadora de gravidade define seus critérios de seleção usando um construtor de condições simples.
	Serviço crítico afetado	Esta calculadora de gravidade define seus critérios de seleção usando uma condição avançada. Se o item de configuração no incidente de segurança estiver associado a um serviço de negócios altamente crítico, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** serão elevados conforme definido pela calculadora.
	Mudanças em serviço crítico	Esta calculadora de gravidade define seus critérios de seleção usando uma condição avançada. Se o incidente de segurança atender às condições, um script será executado para definir os níveis para os quais os campos serão elevados. Se o item de configuração no incidente de segurança estiver associado a um serviço de negócios mais crítico ou um pouco crítico, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** serão elevados conforme definido pela calculadora.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do grupo da calculadora de incidente de segurança	Calculadoras incluídas no grupo	Descrição
	Vetores de ataque múltiplo	Esta calculadora de gravidade define seus critérios de seleção usando um construtor de condições simples. Se o item de configuração no incidente de segurança estiver associado a vetores de ataque da Web, e-mail e representação, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** serão elevados conforme definido pela calculadora.
	Definir prioridade com categoria e serviços	Esta calculadora de gravidade define seus critérios de seleção usando um construtor de condições avançado. A prioridade do incidente de segurança é definida como **1 - Crítica** quando as seguintes condições são atendidas: • O incidente de segurança tem serviços afetados associados e um deles é crítico. • A categoria de incidente de segurança é uma das seguintes: ◦ Negação de serviço ◦ Spear Phishing ◦ Atividade de código malicioso **Nota:** Esta calculadora está disponível no sistema de base quando você tem o tipo de preço de Operação de segurança inicial.
	Definir prioridade com observáveis	Esta calculadora de gravidade define seus critérios de seleção usando um construtor de condições avançado. A prioridade do incidente de segurança é definida como **1 - Crítica** quando as seguintes condições são atendidas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do grupo da calculadora de incidente de segurança	Calculadoras incluídas no grupo	Descrição
		• O incidente de segurança tem serviços afetados associados e um deles é crítico. • A categoria de incidente de segurança é uma das seguintes: ◦ Negação de serviço ◦ Spear Phishing ◦ Atividade de código malicioso • Um dos observáveis ou indicadores associados tem uma contagem de detecções que excede duas detecções com indicadores ativos (ou seja, os observáveis ou indicadores são confirmados como incorretos por várias origens). **Nota:** Esta calculadora está disponível no sistema de base quando você tem o tipo de preço de Operação de segurança avançada e ativa o plug-in Feeds de ameaças.
Criticidade do usuário	Obter criticidade do usuário	Esta calculadora de gravidade define seus critérios de seleção usando um construtor de condições simples. Esta calculadora de gravidade faz com que a criticalidade dos negócios do usuário mude para **1 - Crítica** quando o campo **Departamento** é alterado para **Finanças**.
	Obter criticidade do grupo de usuários	Esta calculadora de gravidade define seus critérios de seleção usando um construtor de condições avançado. Esta calculadora de gravidade fornece o exemplo de uma calculadora que é executada com dados em uma lista relacionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de gravidade

Quando você cria um incidente de segurança, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** contêm valores padrão. Quando você salva o incidente, uma regra de negócio valida automaticamente as informações no incidente de segurança em relação às condições definidas em cada uma das calculadoras de gravidade ativas. Eles são validados uma calculadora de segurança de cada vez, na ordem definida pelo campo **Pedido** em cada calculadora. Se as informações no incidente de segurança corresponderem às condições definidas em uma das calculadoras, os valores do campo de gravidade serão atualizados de acordo com as regras configuradas na calculadora.

Por exemplo, suponha que você crie um incidente de segurança para um IC afetado e o IC seja altamente crítico. Quando o incidente de segurança é salvo, as informações do IC são comparadas com as condições definidas nas calculadoras de gravidade. Quando o incidente de segurança é validado em relação à calculadora de gravidade **afetada do serviço crítico**, os campos de gravidade são atualizados automaticamente e uma mensagem semelhante à seguinte aparece na parte superior do incidente de segurança.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

Você pode usar essas calculadoras de gravidade como estão ou editá-las para atender melhor às necessidades do seu negócio. Por exemplo, se você quiser identificar ameaças da Web e de e-mail específicas da unidade de negócios Finanças, poderá alterar as condições da calculadora de **vetores de ataque múltiplo** :

- [Vetor de ataque] [contém] [Web]
- [Vetor de ataque] [contém] [E-mail]
- [Unidade de negócios] [contém] [Finanças]

Você também pode atualizar os valores de gravidade em um incidente de segurança existente a qualquer momento, abrindo o registro e clicando no link relacionado **Calcular gravidade**.

Calculadoras de pontuação de risco de incidente de segurança

As calculadoras **Definir prioridade com categoria e serviços** e **Definir prioridade com observáveis** são usadas para calcular uma pontuação de risco para um incidente de segurança.

Calculadoras de criticalidade do usuário

As duas calculadoras no grupo **de criticalidade do usuário** (**Obter criticalidade do usuário** e **Obter criticalidade do grupo de usuários**) fornecem exemplos de como você pode direcionar a criticalidade com base em critérios definidos em um registro de usuário ou com base no grupo ao qual um usuário pertence.

Eles podem ser editados conforme necessário ou novas calculadoras de criticalidade do usuário podem ser criadas.

A calculadora **Obter criticalidade do** usuário faz com que a criticalidade dos negócios do usuário mude para **1 - Crítica** quando o campo **Departamento** é alterado para **Finanças**.

A calculadora **Obter criticidade do grupo de** usuários faz com que a criticalidade dos negócios do usuário mude para **1 - Crítica** quando o usuário é adicionado ao grupo Banco de **dados**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: **Obter criticidade do grupo de usuários** é um exemplo de uma calculadora que é executada com dados em uma lista relacionada. Se você quiser adicionar mais grupos para iniciar uma mudança de criticalidade, adicione uma lista separada por vírgulas de sys_ids de grupo na primeira linha do script. Exemplo: `var CRITical_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id]`.

Cálculos de pontuação de risco de incidente de segurança

A pontuação de risco é calculada como uma média aritmética que representa o risco com base na prioridade de um incidente de segurança, no tipo de incidente de segurança (negação de serviço, Spear Phishing ou atividade de código malicioso) e no número de origens que acionaram uma falha pontuação de reputação em um indicador.

A pontuação de risco ajuda a priorizar o trabalho de incidente de segurança para os analistas.

Importante: Se você quiser usar a nova Calculadora de pontuação de risco, consulte Definir as novas regras da calculadora de pontuação de risco.

As calculadoras**Definir prioridade com categoria e serviços** e **Definir prioridade com observáveis** são usadas para calcular uma pontuação de risco para um incidente de segurança. Além disso, as seguintes regras de negócio acionam o cálculo automático de pontuações de risco:

- Calcular Gravidade
- Atualizar pontuação de risco
- Atualizar pontuação de risco de SI

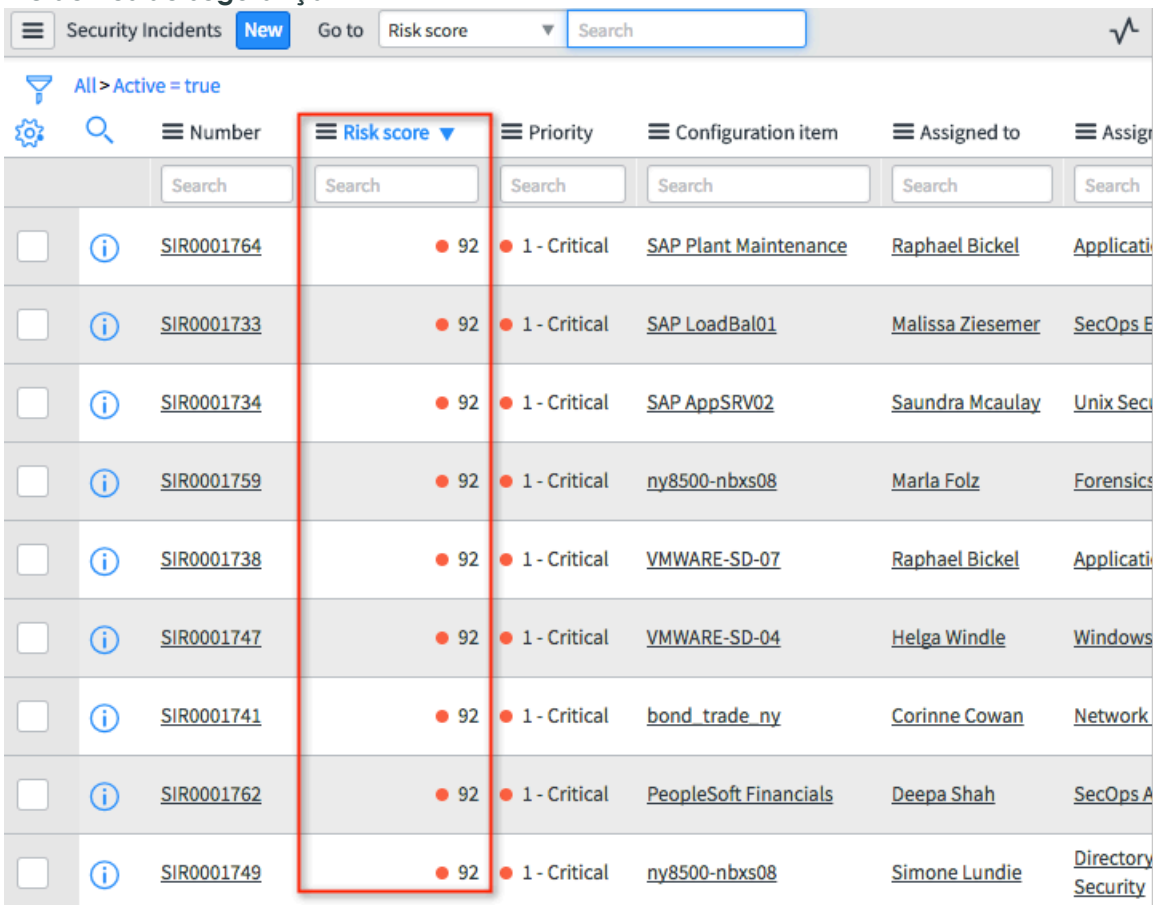
Nota: A calculadora de risco disponível no sistema de base depende do seu tipo de preço das Operações de segurança.

Ao observar uma lista de incidentes de segurança no sistema de base, observe a coluna **Pontuação de risco**.

Tradução automática

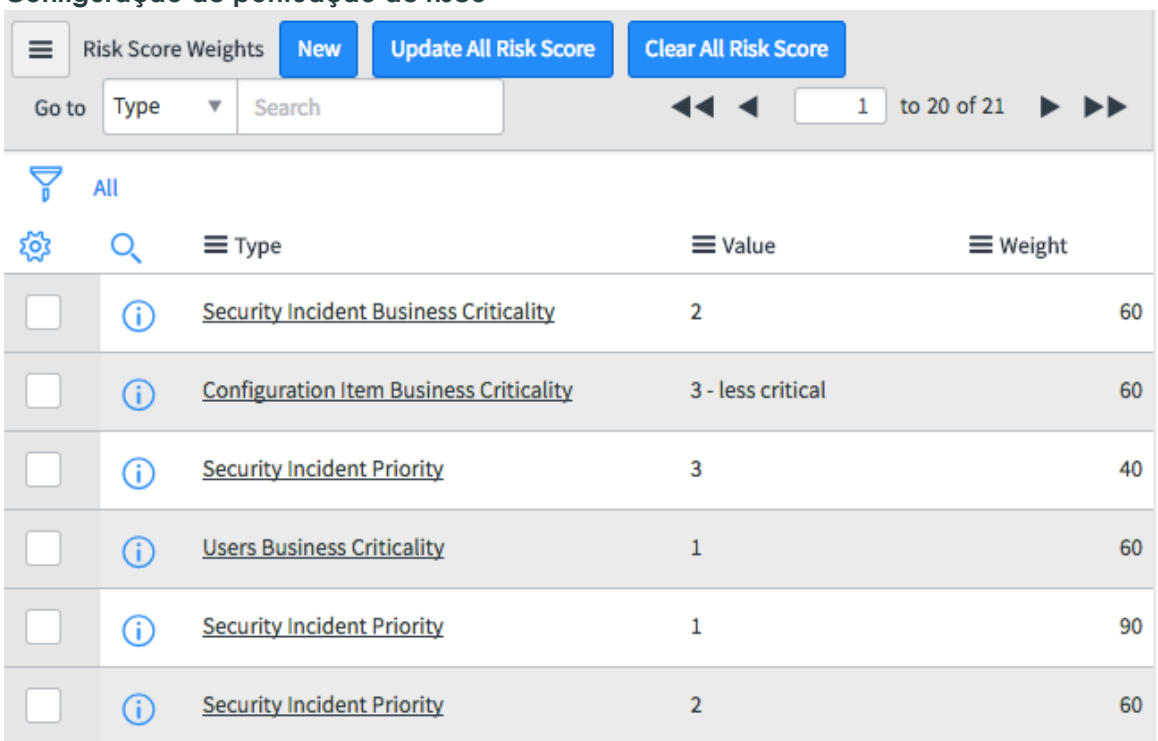
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidentes de segurança



A pontuação de risco é calculada usando pesos definidos na **configuração de pontuação de risco**.

Configuração de pontuação de risco



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, se um incidente de segurança tiver um **Impacto nos negócios** definido como **2-Alto** e uma **Prioridade** definida como **3-Moderado**, os respectivos pesos na tabela Ponderações de pontuação de risco serão pesquisados e calculados da seguinte forma:

Impacto do incidente de segurança nos negócios com um valor de 2 = um peso de 60.

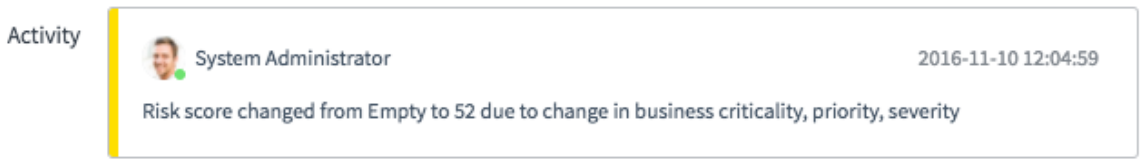
Prioridade de incidente de segurança com um valor de 3 = um peso de 40.

(60 + 40)/2 = uma pontuação de risco de 50.

A posição do incidente de segurança na lista de incidentes de segurança é reordenada com base em sua pontuação de risco atualizada.

Se, no exemplo acima, o **Impacto nos negócios** ou a **Prioridade** do incidente de segurança forem alterados, a pontuação de risco será recalculada e as mudanças serão refletidas nas anotações de trabalho.

Anotações de trabalho



As anotações de trabalho são atualizadas quando os seguintes campos são alterados (fazendo com que a pontuação de risco seja atualizada):

- **Impacto nos negócios** no formulário de Incidente de segurança
- **Prioridade** no formulário de Incidente de segurança
- **Gravidade** no formulário de Incidente de segurança (oculta por padrão)
- **Impacto nos negócios** na lista relacionada de **Usuários afetados**
- **Impacto nos negócios** na lista relacionada de **serviços afetados**
- **Impacto nos negócios** nas vulnerabilidades na lista relacionada de **itens vulneráveis**

Além disso, as anotações de trabalho são atualizadas nas seguintes situações:

- Quando uma associação entre usuários afetados e um incidente de segurança é criada ou modificada
- Quando uma associação entre serviços afetados e um incidente de segurança é criada ou modificada
- Quando uma associação entre itens vulneráveis e um incidente de segurança é criada ou modificada

As anotações de trabalho também são atualizadas sempre que **Atualizar todas as pontuações de risco** e **Limpar todas as pontuações de risco** no formulário Ponderações de pontuação de risco são clicados.

Manter pesos de pontuação de risco

Os pesos de pontuação de risco usados para calcular as pontuações de risco em incidentes de segurança podem ser removidos ou atualizados individualmente. Eles também podem ser removidos ou atualizados para todos os incidentes de segurança. A capacidade de removê-los de incidentes de segurança é útil ao alterar valores de peso.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Usuários com a função sn_si.read podem exibir a configuração de pontuação de risco em Security Incident Response.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **Configuração de pontuação de risco**.

   Nota: Usuários com a função sn_si.read podem exibir a configuração de pontuação de risco navegando até **Incidente de segurança** > **Alertas e eventos** > **Configuração de pontuação de risco**.

2. Para adicionar um novo peso de pontuação de risco, clique em **Novo** e insira as informações nos campos.

Campo	Descrição
Tipo	Selecione o tipo de pontuação de risco que você está definindo.
Valor	Especifique o valor associado ao tipo selecionado. Se vários valores estiverem disponíveis para o tipo, convém definir vários registros de ponderação de pontuação de risco. Exemplo: prioridade de incidente de segurança com um valor de 1, prioridade de incidente de segurança com um valor de 2 e assim por diante.
Ponderação	O peso associado ao par de tipo/valor selecionado. As entradas válidas estão entre 0 e 100, sendo 0 o menor peso e 100 o maior.

3. Clique em **Enviar**.
4. Execute qualquer uma dessas etapas, conforme necessário.
   - Para limpar um registro de ponderação de pontuação de risco, abra-o na lista e clique em **Excluir**.
   - Para limpar todos os registros de ponderação de pontuação de risco, clique em **Limpar todas as pontuações de risco**.
   - Para atualizar todos os registros de ponderação de pontuação de risco, clique em **Atualizar todas as pontuações de risco**.

Criar um Security Incident Response ANS

Você pode definir um Acordo de nível de serviço (ANS) para Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **ANS**.
2. Clique em **Nova**.
   Para obter descrições de campo e instruções detalhadas, consulte Criação de uma definição do ANS .

Reparar ANS de incidente de segurança

Você pode reparar registros de ANS para garantir que as informações de tempo e duração do ANS sejam precisas.

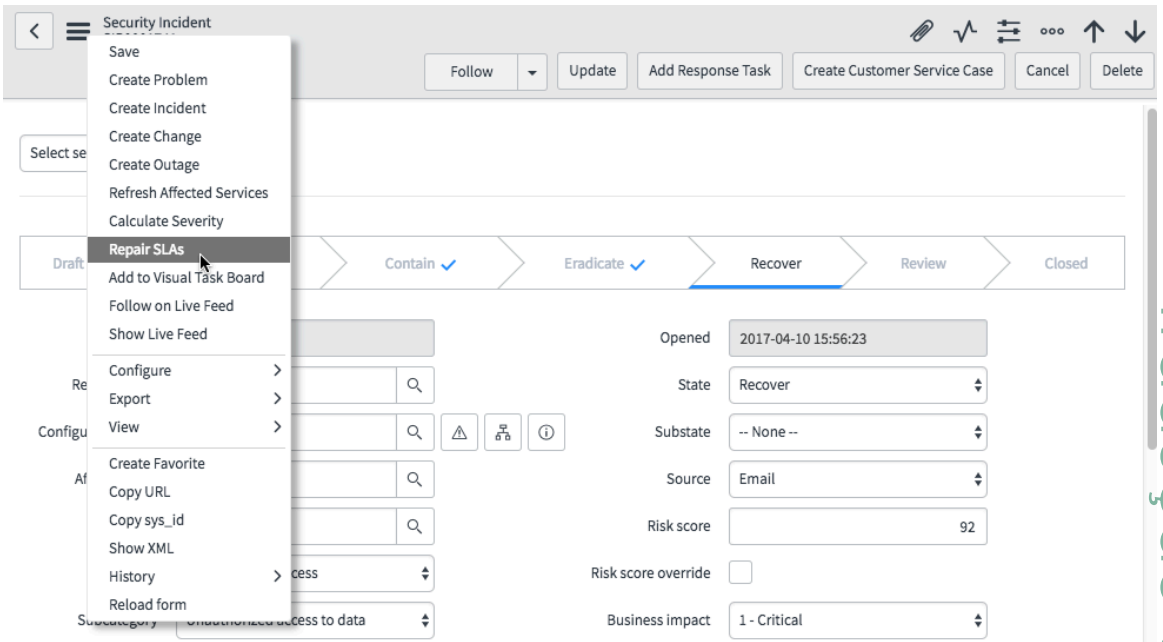
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja reparar SLAs.
2. Clique no menu de contexto do cabeçalho do formulário e selecione **Reparar ANS**:



3. Clique em **OK** na caixa de confirmação Aviso.
   Para obter mais informações, consulte ANS de reparo .

Criar um runbook do Security Incident Response

Um runbook é uma associação entre um artigo de conhecimento publicado e uma tarefa específica. Enquanto você executa a tarefa, um artigo de conhecimento no runbook é aberto automaticamente, fornecendo informações pertinentes à tarefa.

Antes de Iniciar
Deve haver artigos de conhecimento existentes na Security Incident Response base de conhecimento do Runbook. Ao criar um artigo de conhecimento sobre incidentes de segurança, certifique-se de selecionar **o Runbook do Security Incident Response** no campo **Base de conhecimento**. Depois de publicar o artigo, você pode clicar no botão **Criar runbook**.

Função necessária: sn.si.knowledge_admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode usar runbooks durante os processos de criação de tarefas de resposta ou incidentes de segurança ou pode associar os artigos da base de conhecimento em um runbook a tarefas no playbook.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Runbook manual** > **Criar novo runbook**.
2. Preencha os campos, se for o caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Artigo de conhecimento	Selecione um artigo de conhecimento para incluir no runbook.
Ativo	Marque a caixa para disponibilizar o runbook no **Navegador**de filtros.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou criar um novo grupo de filtros para definir os critérios do runbook.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir um runbook. Este campo aparecerá somente se a caixa de seleção **Usar grupos de filtros** estiver marcada.
Tabela	Selecione Incidente de segurança [sn_si_incident] ou Security Incident Response Tarefa [sn_si_task]. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, este campo será padronizado para a tabela associada ao grupo de filtros selecionado.
Condição	Defina as condições que conectam este runbook ao incidente ou à tarefa. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, os campos **Condição** não serão exibidos.

3. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A guia Detalhes do artigo de conhecimento e uma série de botões são exibidos.
4. Para exibir os detalhes do runbook, clique na guia **Detalhes da base de conhecimento**.
5. Para ver o artigo de conhecimento como ele aparecerá para o usuário, clique em **Exibir artigo**.
6. Para Para editar os detalhes do artigo de conhecimento , clique em **Editar artigo**.

Criar regras para validar ataques de phishing relatados por usuários

Quando seus funcionários recebem e-mails que parecem ser ataques de phishing, eles podem denunciá-los a você usando um endereço de e-mail de phishing. O e-mail suspeito é validado usando regras definidas pela sua organização.

Antes de Iniciar

Antes que as regras de correspondência de e-mail possam ser usadas para identificar possíveis ataques de phishing, defina um endereço de e-mail para o qual os e-mails encaminhados de seus funcionários seriam enviados para processamento. Você tem as

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

seguintes opções para definir este endereço de e-mail (assumindo que o domínio de e-mail da sua empresa seja acme.com):

- Defina um endereço de e-mail como **acme+phishing@service-now.com**. O marcador **+phishing** é compatível com SMTP para habilitar a filtragem e sua instância pode receber e-mails enviados para ela.
- Defina um endereço de e-mail, como **phishing@acme.com** (sua caixa de correio do Exchange), que por sua vez o encaminha para **acme+phishing@service-now.com** (sua caixa de correio da instância definida por meio de uma regra de encaminhamento de e-mail).

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Quando um funcionário encontra um e-mail suspeito, ele deve encaminhá-lo como um anexo para o seu endereço de e-mail de phishing. Se o e-mail anexado corresponder a uma regra que define uma ameaça, um incidente de segurança será criado.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Processamento de E-mails** > **Phishing relatado pelo usuário**.
2. Clique em **Nova**.
3. Preencha os campos conforme necessário.

Formulário Regras de correspondência de e-mail

Campo	Descrição
Nome	Nome desta regra de correspondência de e-mail. Por exemplo, Phishing relatado pelo usuário.
Condições	Use o Construtor de condições para validar se um e-mail enviado para o endereço de e-mail de phishing da sua empresa é um ataque de phishing. Veja o exemplo a seguir.

4. Clique em **Enviar**.

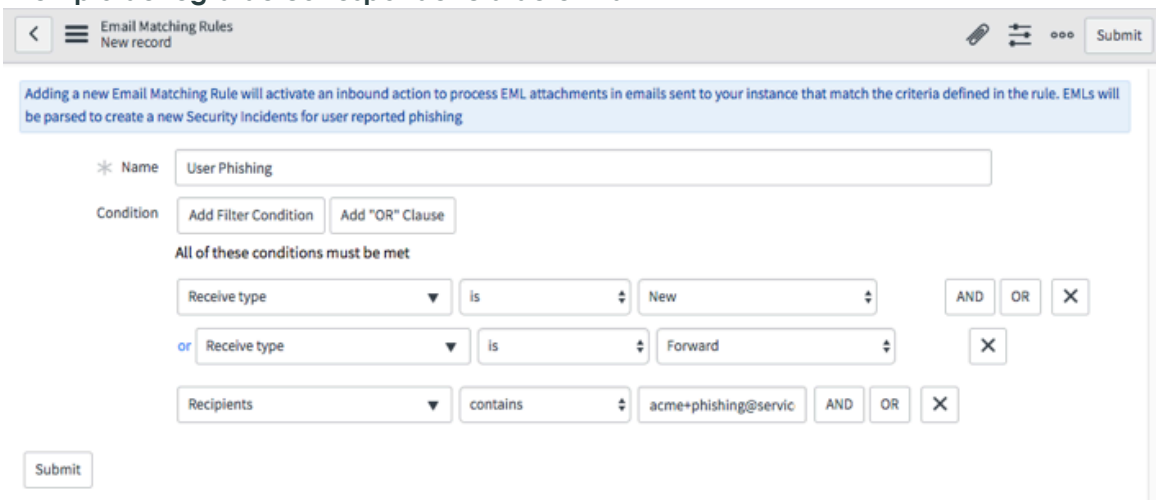
Example:

Este exemplo mostra uma regra de correspondência para lidar com phishing relatado pelo usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de regra de correspondência de e-mail



Configure o Espaço do analista de segurança

Configure a interface do usuário do registro de Incidente no Espaço do analista de segurança para especificar os campos que você deseja exibir.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Especifique os campos a serem exibidos no registro de Incidente e a ordem em que os campos devem aparecer no formulário de Incidente de segurança e no formulário de Tarefa de resposta. Você também pode definir um limite para o número de campos que deseja exibir.

Nota: Você pode criar regras para determinar qual exibição deve ser usada para um formulário específico. Várias exibições estão incluídas no sistema de base, incluindo as exibições de IU Padrão e SIR Nova. Várias regras de exibição também são enviadas com o sistema de base, incluindo a regra de Tarefa de Resposta Todos os Outros. Esta regra impõe a exibição Padrão no formulário de Tarefa de resposta quando a condição especificada na regra de exibição é atendida. O Espaço do analista de segurança usa a exibição de nova IU SIR. Se os campos de formulário exibidos em Espaço do analista de segurança não corresponderem aos campos de formulário no ambiente clássico, uma regra de exibição provavelmente será aplicada. Para usar a exibição de **nova IU SIR** para o formulário, você deve desabilitar a regra de exibição. Consulte Controle quando o sistema exibir uma exibição para obter detalhes.

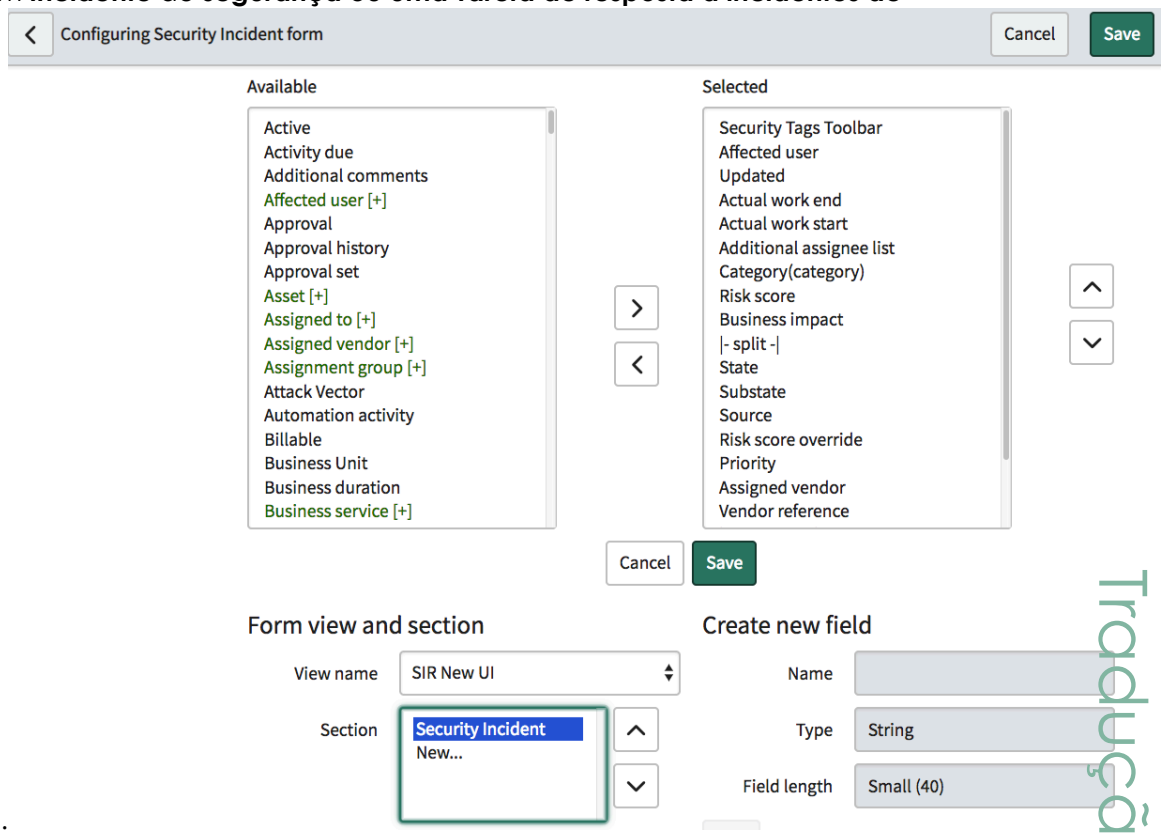
Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**).
2. Para abrir o registro de incidente de segurança, clique no link de um incidente de segurança.
3. Para navegar até a página do formulário Configuração de Incidente de segurança, clique no ícone do menu Menu de e selecione **Configurar** > **Layout do formulário**.
4. Na lista **Exibir nome**, selecione **SIR Nova IU**.
5. No campo **Seção**, selecione a seção apropriada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pode ser um **Incidente** de **segurança ou uma Tarefa de resposta a incidentes de segurança**.



6. Selecione os campos e a ordem em que você deseja que eles apareçam na faixa de Incidente na nova IU.
7. Clique em **Salvar**.

Nota:

- Certos campos estão ocultos por padrão nas faixas de Incidente e Tarefa de resposta. Altere os campos que estão ocultos ou exibidos modificando as propriedades `sn_app_secops_ui.form.excluded_fields.incident` e `sn_app_secops_ui.form.excluded_fields.response_task` conforme descrito em Propriedades do Espaço do analista de segurança.
- Especifique o número de campos que podem ser exibidos nas faixas de Incidente e Tarefa de resposta e na primeira linha da faixa de Incidente definindo estas propriedades:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

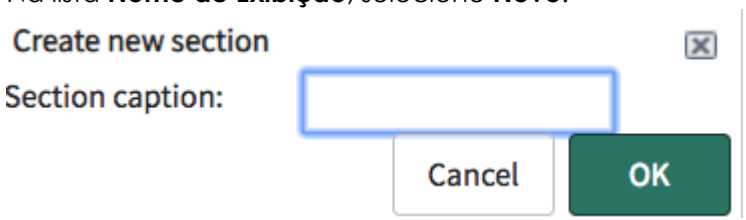
8. Para configurar os estilos dos círculos pontilhados que aparecem ao lado de um valor de campo no registro de Incidente, por exemplo, navegue até **IU do Sistema** > **Estilos de Campo** e modifique ou crie um novo registro de estilo para a tabela específica e o nome do campo.
   A propriedade cor de fundo no campo Estilo do registro de estilo determina a cor do círculo pontilhado.
9. Para exibir a faixa de incidente atualizada, clique em **Incidentes de segurança** > **Incidentes (Nova IU)** para navegar até o registro de Incidente no Espaço do analista de segurança e atualizar a página para exibir a faixa de Incidente atualizada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Para configurar a faixa de Tarefa de resposta no registro de Incidente, navegue até **Incidentes de segurança** > **Tarefas de Resposta** > **Mostrar todas as tarefas** e repita as etapas.
11. Se você estiver criando uma nova tabela de tarefas que se estende a partir da tabela de tarefas base do Security Incident Response, também deverá adicionar a nova exibição de IU do SIR à tabela.

    a. Na lista **Nome de Exibição**, selecione **Novo**.



    b. Insira **SIR New UI** (diferencia maiúsculas de minúsculas) na janela Criar nova exibição e clique em **OK**.

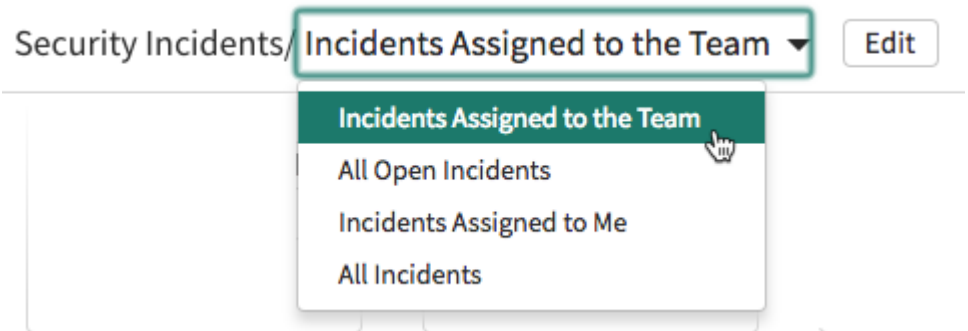
Resultados
As faixas de tarefa de resposta e incidente de segurança são atualizadas no Espaço do analista de segurança (Gerenciar ameaças à segurança usando o Espaço do analista de segurança).

Configurar filtros primários e secundários para Espaço do analista de segurança

O sistema base Espaço do analista de segurança inclui um conjunto de filtros primários para restringir a lista de incidentes de segurança para análise (para incidentes de segurança atribuídos a você, todos os incidentes abertos e assim por diante) e um conjunto de filtros rápidos (ou secundários) para restringir a lista ainda mais (por novos incidentes, incidentes abertos, somente incidentes críticos e assim por diante).

Antes de Iniciar
Você pode usar o ambiente Clássico para definir filtros primários e secundários adicionais.

Ao definir os filtros a serem usados no Espaço do analista de segurança, você pode atribuir marcadores para indicar se eles podem ser usados como filtros primários ou secundários. Os filtros primários são mostrados na parte superior da lista de incidentes de segurança.



Clique em **Editar** ao lado da opção Filtros rápidos para selecionar filtros secundários (ou rápidos).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: administrador ou sn_sec_cmn.write

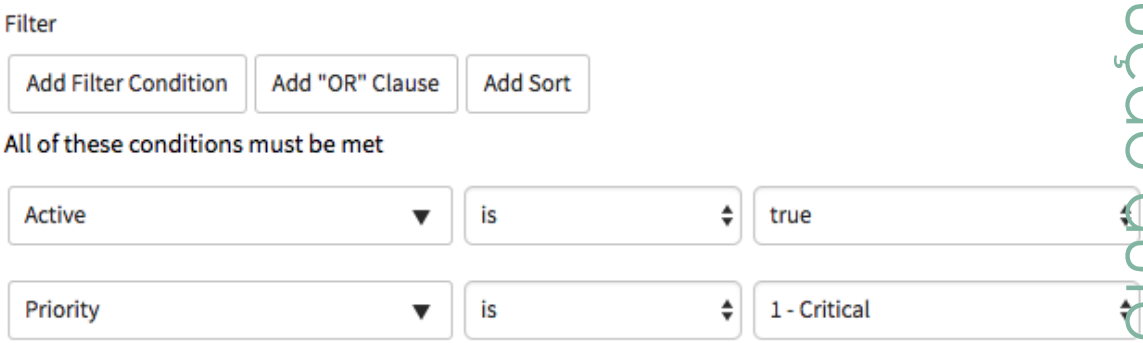
Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Filtros**.
2. Clique em **Novo** e conclua as etapas a seguir.

   a. Insira um **Título**.

   b. Selecione **Incidente de segurança [sn_si_incident]** na lista de seleção **Tabela**.

   c. Adicione suas condições de filtro.
   Por exemplo, o filtro **Incidentes em aberto com Prioridade = Crítica** usa essas condições.



   d. Clique em **Enviar**.

3. Se a coluna **Marcadores** não estiver visível na lista de filtros, clique no ícone de engrenagem e personalize a exibição para adicioná-la.
4. Localize o filtro que você criou e adicione um dos seguintes marcadores para indicar como o filtro deve aparecer no Espaço do analista de segurança.
   - **SN_SI_Primary**: se este marcador for selecionado, o filtro poderá ser selecionado no slushbucket de filtro primário no Espaço do analista de segurança.
   - **SN_SI_Primary_OOB**: se este marcador for selecionado, o filtro aparecerá no lado **selecionado** do slushbucket de filtro primário por padrão.
   - **SN_SI_Secondary**: se este marcador for selecionado, o filtro poderá ser selecionado no slushbucket de filtro secundário (rápido).
   - **SN_SI_Secondary_OOB**: se este marcador for selecionado, o filtro aparecerá no lado **selecionado** do slushbucket de filtro primário por padrão.

Informações relacionadas

Criar e editar filtros

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Essas propriedades do sistema são usadas para configurar o Espaço do analista de segurança.

Existem dois tipos de propriedades:

- Propriedades que normalmente não são modificadas, como sys_ids e chaves de produto.
- Propriedades que são modificadas conforme necessário, como longos intervalos de pesquisa e configurações de interface do usuário.

Nota: As propriedades do Espaço do analista de segurança estão localizadas neste local: **Incidente de segurança** > **Configuração do espaço do analista** > **Propriedades do espaço do analista**.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
Campos que estão ocultos por padrão na faixa de tarefa de resposta. sn_app_secops_ui.form.excluded_fields.response_task	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ número ◦ descrição resumida ◦ comentários ◦ work_notes ◦ comments_and_work_notes ◦ lista_anotações_trabalho ◦ automação_atividade
Campos que estão ocultos por padrão na faixa de incidentes. sn_app_secops_ui.form.excluded_fields.incident	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ número ◦ descrição resumida ◦ comentários ◦ work_notes ◦ comments_and_work_notes ◦ lista_anotações_trabalho ◦ automação_atividade ◦ marcadores_de_segurança
O estilo de cor de fundo é aplicado aos campos listados aqui. sn_app_secops_ui.form.color_coded_fields	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ criticalidade dos negócios ◦ impacto ◦ prioridade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
	◦ risk_score ◦ severidade
Se verdadeiro, as tabelas estendidas da tabela de tarefas de resposta base sn_si_task também terão acesso aos modelos de e-mail criados para a tabela de tarefas de resposta base. sn_app_secops_ui.extend.base.response_task.email_templates	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
Define a largura de cada campo de resumo em cada faixa de tarefa de resposta. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Tipo**: inteiro • **Valor padrão**: 10
Define a largura de cada campo de resumo em cada faixa de incidente. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Tipo**: inteiro • **Valor padrão**: 15
Define um limite para o número de campos de resumo permitidos na faixa de incidentes. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Tipo**: inteiro • **Valor padrão**: 12
Define um limite para o número de campos de resumo permitidos na faixa de tarefa de resposta. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Tipo**: inteiro • **Valor padrão**: 12
Define um limite para o número de campos de resumo permitidos na primeira linha da faixa de incidente. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Tipo**: inteiro • **Valor padrão**: 3
Lista separada por vírgulas de campos que podem ter fotos do usuário. sn_app_secops_ui.form.user_fields	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ afetado_usuário ◦ Solicitante ◦ sys_updated_by ◦ sys_created_by

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
	◦ opened_by ◦ closed_by ◦ enviado_por
Define a largura de cada campo de resumo em cada exibição de inspeção de incidente. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Tipo**: inteiro • **Valor padrão**: 13,5
Lista separada por vírgulas de campos que exibem a hora. sn_app_secops_ui.form.time_fields	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ opened_at ◦ sys_created_on ◦ sys_updated_on
Controla a frequência (em milissegundos) com que os resultados da pesquisa de detecções são atualizados. sn_app_secops_ui.poller_interval.search_action	• **Tipo**: inteiro • **Valor padrão**: 30000 **Mínimo**: 15.000
Controla a frequência (em milissegundos) na qual os dados de contagem ou consulta são atualizados. sn_app_secops_ui.poller_interval.related_list	• **Tipo**: inteiro • **Valor padrão**: 30000 **Mínimo**: 15.000
Controla a frequência (em milissegundos) com que os dados de resultado são atualizados (para o playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Tipo**: inteiro • **Valor padrão**: 30000 **Mínimo**: 15.000
ID do fluxo de trabalho Integração com Operações de segurança - Isolar host. sn_app_secops_ui.workflow.id.isolate_host	• **Tipo**: cadeia de caracteres • **Valor padrão**: d72041f1ff203200c68c84648e94fa5e
ID do fluxo de trabalho Integração de Operações de segurança - Lista de observação. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Tipo**: cadeia de caracteres • **Valor padrão**: 35800c0eff343200c68c84648e94fa85

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID do fluxo de trabalho Integração com Operações de segurança - Solicitação de bloqueio. sn_app_secops_ui.workflow.id.block_request	• **Tipo**: cadeia de caracteres • **Valor padrão**: 11a6a5270b9032008f9108e3c5673a24
ID da função do usuário sn_si_analyst. sn_app_secops_ui.roles.id.sn_si.write	• **Tipo**: cadeia de caracteres • **Valor padrão**: 66878663ff123100158bfffffffff8d
ID da função do usuário sn_si_read. sn_app_secops_ui.roles.id.sn_si.read	• **Tipo**: cadeia de caracteres • **Valor padrão**: ae878663ff123100158bfffffffff8e
ID da função de usuário sn_si_admin. sn_app_secops_ui.roles.id.sn_si.admin	• **Tipo**: cadeia de caracteres • **Valor padrão**: 22878663ff123100158bfffffffff8d
ID do fluxo de trabalho do Microsoft Exchange - Executar pesquisa e exclusão de e-mail. sn_app_secops_ui.email.phishing.manual.fluxo de trabalho	• **Tipo**: cadeia de caracteres • **Valor padrão**: ed9f289cc310220031fbdccdf3d3aeb4
ID da ação personalizada Adicionar à lista de proibições na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Tipo**: cadeia de caracteres • **Valor padrão**: DENY_e9bd0ac50b632200263a089b37673a0b
ID da ação personalizada Adicionar à lista de permissões na guia Explorar do Espaço do analista de segurança sn_app_secops_ui.explore.action.direct.id.allow_list	• **Tipo**: cadeia de caracteres • **Valor padrão**: ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
ID da ação de IU Executar pesquisa de ameaças. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Tipo**: cadeia de caracteres • **Valor padrão**: da5ff4420b540300263a089b37673ae7

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID da capacidade de integração de pesquisa de ameaças. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Tipo**: cadeia de caracteres • **Valor padrão**: 39344d4f0b273200263a089b37673ab1
ID da ação personalizada de aprimoramento de observável na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.id.observable_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão**: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e
ID da capacidade de integração Aprimorar observável. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão**: 9ad183640b1003009f66e94685673af4
ID da Ação de IU Publicar na Lista de Observação. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Tipo**: cadeia de caracteres • **Valor padrão**: 8ee94002ff743200c68c84648e94faf9
ID da ação de IU de solicitação de bloqueio. sn_app_secops_ui.explore.action.id.block_request	• **Tipo**: cadeia de caracteres • **Valor padrão**: 7158f6e40b2032008f9108e3c5673adf
ID da ação de IU Executar pesquisa de detecções. sn_app_secops_ui.explore.action.id.sightings_search	• **Tipo**: cadeia de caracteres • **Valor padrão**: 43f91a6f0b032200b97c67d985673a2c
ID da ação de IU Criar incidente de segurança secundário. sn_app_secops_ui.explore.action.id.create_child_incident	• **Tipo**: cadeia de caracteres • **Valor padrão**: 5a6882645363530099d5ddeeff7b1272
ID da ação de IU Adicionar anotação de segurança. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Tipo**: cadeia de caracteres • **Valor padrão**: 1e3a3e723b5332005a9149a4d2efc4eb
ID da ação personalizada de aprimoramento de IC na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão**: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID da ação de IU Isolar host. sn_app_secops_ui.explore.action.id.isolate_host	• **Tipo**: cadeia de caracteres • **Valor padrão**: d6244e0aff203200c68c84648e94fad3
ID da ação de IU Adicionar vários observáveis. sn_app_secops_ui.explore.action.id.multiple_observable	• **Tipo**: cadeia de caracteres • **Valor padrão**: 138de478d78322007a6de294de6103aa
Chave do produto para ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Tipo**: cadeia de caracteres • **Valor padrão**: ServiceNow_ServiceNow_5Devs2_August_2018__MTUzMzE2

Configuração adicional do Espaço do analista de segurança

Configure o Espaço do analista de segurança e defina filtros, ações de IU e listas relacionadas.

- Configuração de filtro da página principal
- Habilitar ações de IU
- Ações de IU do formulário
- Configuração da Lista relacionada
- Ações de IU da Lista relacionada
- Propriedades do sistema de configuração de formulário
- Habilitar playbooks para seleção de analista

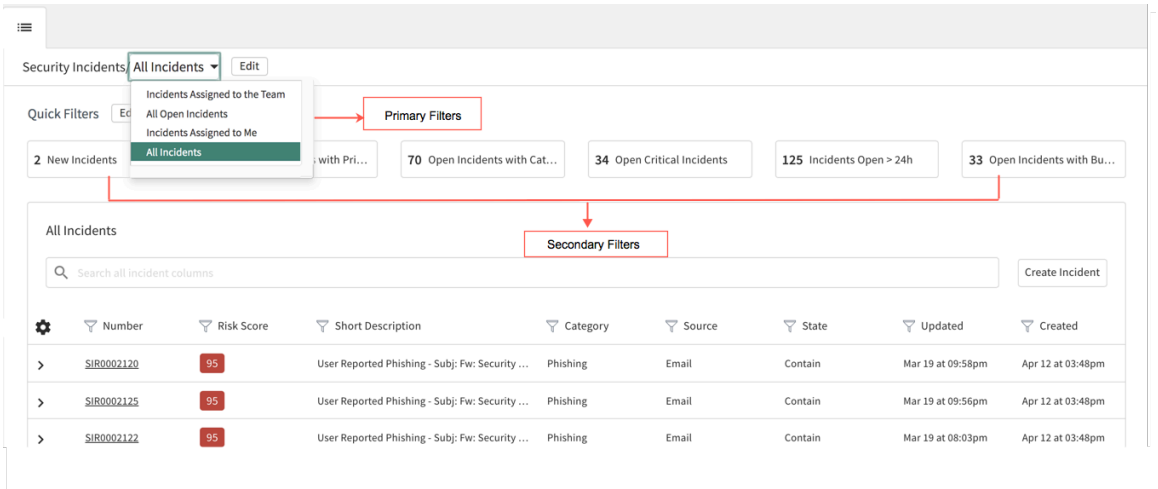
Configuração de filtro da página principal

Você pode adicionar novos filtros ou modificar os filtros existentes que aparecem no Espaço do analista de segurança.

O Espaço do analista de segurança tem filtros primários e secundários que permitem filtrar a lista de incidentes de segurança para que você possa encontrar rapidamente os incidentes de segurança que deseja analisar. Para obter mais informações, consulte Gerenciar ameaças à segurança usando o Espaço do analista de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar um novo filtro

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Configuração de filtro da página principal**.
2. Clique em **Nova**.
3. Insira um título para o filtro, especifique a condição do filtro e clique em **Enviar** para retornar à página anterior.

   Você verá o filtro recém-adicionado listado na página.
4. Adicione um marcador para este filtro para indicar se este é um filtro primário ou secundário. Os seguintes marcadores estão disponíveis:
   - SN_SI_Primário
   - SN_SI_Secondary

Editar filtros existentes

Você também pode fazer o seguinte:

- Modificar filtros existentes: clique no título de um filtro existente. Modifique o título e a condição do filtro e clique em **Atualizar**.
- Modificar marcadores: selecione um filtro e clique na coluna Marcador na Configuração de filtro da página principal. Você pode excluir o marcador existente ou adicionar um novo marcador ao filtro.

Habilitar ações de IU

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança.

Nota: Para modificar as ações de IU, faça login como um usuário com as seguintes funções:

- iu_action_admin
- ui_page_admin
- web_service_admin

Existem dois tipos de ações de IU que podem ser configurados para o Espaço do analista de segurança:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ação de IU baseada em diálogo
- Ação de IU do lado do servidor

Ação de IU baseada em diálogo

Para habilitar ações de IU baseadas em diálogo no Espaço do analista de segurança, faça as seguintes mudanças nas páginas de IU associadas às respectivas Ações de IU padrão.

1. **Seção HTML**: modifique a seção HTML para incluir o marcador de entrada de *reação*. O valor do marcador de entrada de *reação* é usado na seção de client script para identificar se a Página de IU foi iniciada a partir de Espaço do analista de segurança. Um exemplo é mostrado abaixo:

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Script do cliente**: a lógica adicional precisa ser escrita no script do cliente quando o sinalizador de *reação* é verdadeiro. Isso é necessário para lidar com os eventos do botão **Enviar** e **Cancelar** mostrados como parte da janela de diálogo.
   a. O manipulador de eventos onCancel () precisa despachar o evento "SIR_WORKBENCH_POPUP_CANCEL" do Espaço do analista de segurança
   b. O manipulador de eventos onSubmit () precisa despachar o evento "SIR_WORKBENCH_POPUP_SUBMIT" do Espaço do analista de segurança
3. A execução do script de processamento é ignorada no contexto Espaço do analista de segurança, já que a ação "onSubmit" foi modificada para retornar falso quando o valor do marcador de entrada de *reação* for verdadeiro. A lógica do script de processamento precisa ser tratada por meio de um script de cliente chamável (invocado por meio da API GlideAjax) ou do endpoint de recurso REST.

Consulte as seguintes páginas de IU de amostra para obter mais detalhes:

- Exemplo de ação de IU da Lista relacionada: publicar na lista de observação (nome da página de IU: publicar_to_watchlist)
- Exemplo de ação de IU de formulário: criar problema (nome da página de IU: create_prb_change_inc)

Ação de IU do lado do servidor

Para habilitar ações de IU do lado do servidor, você deve fazer o seguinte:

A lógica do script de ação de IU padrão deve ser tratada como parte de um recurso REST com script.

Consulte os seguintes exemplos de ações de IU de formulário para obter mais detalhes:

- Criar indisponibilidade
- Cancelar

Ações de IU do formulário

Você pode configurar as ações de IU que são exibidas no Espaço do analista de segurança.

Pré-requisitos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.

Para configurar uma ação de IU de formulário para Espaço do analista de segurança, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Ações de IU de Formulário**.
2. Insira os seguintes detalhes:

Nome do Campo	Descrição
Ação	Selecione uma ação de IU na lista de seleção.
Tipo	Selecione o tipo de ação. Pode ser: ◦ Ação baseada em diálogo: este tipo de ação é usado quando a interação ou as entradas do usuário são necessárias para executar a lógica de negócios específica. ◦ Ação do lado do servidor: esta ação executa a lógica de negócios necessária sem nenhuma entrada adicional do usuário. **Nota:** Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.
Aplicação	O nome do escopo da aplicação (IU de resposta a incidentes de segurança) ao qual a ação de IU está sendo adicionada é exibido aqui.
Ação baseada em diálogo Se você selecionar Ação baseada em diálogo no campo Tipo, insira os seguintes detalhes:	
Página da interface do usuário	Selecione a página de IU associada à ação.
Título da Caixa de Diálogo	Insira um título para a ação de diálogo.
Largura e altura da caixa de diálogo	Insira a altura e a largura da caixa de diálogo em pixels.
Script	Para a Página de IU selecionada, você pode especificar parâmetros de consulta adicionais aqui. O modelo fornecido com o sistema de base constrói e retorna somente o parâmetro `sysparm_sys_id`. Você pode substituir isso especificando parâmetros diferentes aqui.
Ação do lado do servidor Se você selecionar Ação do lado do servidor no campo Tipo, insira os seguintes detalhes:	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

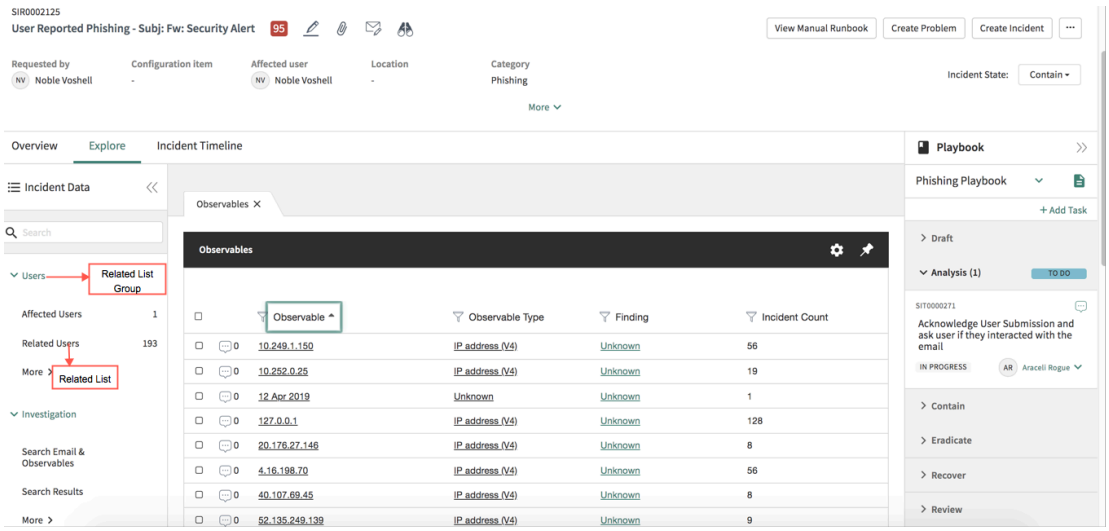
Nome do Campo	Descrição
Recurso Rest de Script	Selecione o Recurso de REST com script que define a ação. **Nota:** A ACL **SIR UI ANALYST** deve ser adicionada ao recurso REST.

3. Clique em **Enviar**.
4. Navegar até **Incidentes de segurança** > **Incidentes (Nova IU)** página.
5. Clique no número de um incidente de segurança para exibir o registro do incidente de segurança. Você pode ver a nova ação de IU na parte superior da página.

Para modificar uma ação de IU de formulário existente, clique no Nome da ação para navegar até a página Ações de IU de formulário. Você pode modificar o Nome da ação, o Tipo e o restante dos campos com base no tipo selecionado.

Configuração da Lista relacionada

Você pode adicionar novas listas relacionadas ou novos grupos de listas relacionadas e modificar grupos existentes ou listas relacionadas que aparecem no Espaço do analista de segurança.



Adicionar um grupo de lista relacionada

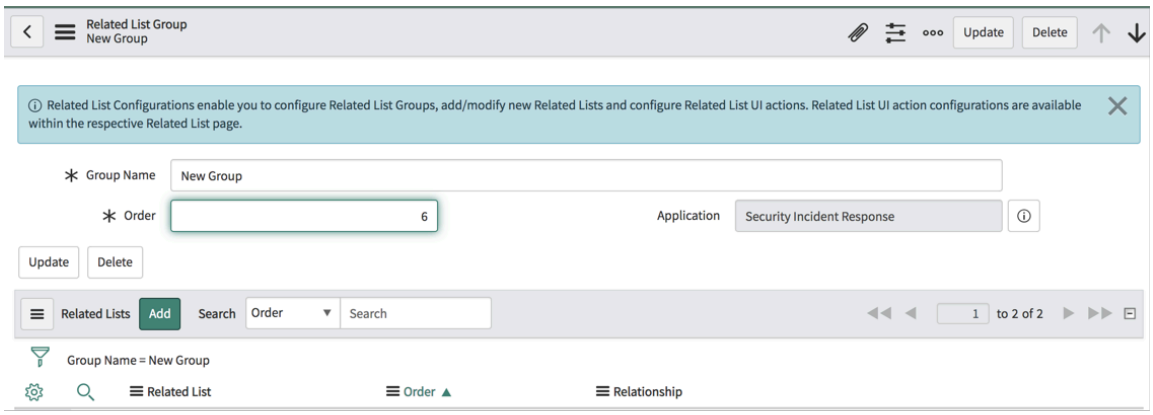
Para adicionar um grupo de lista relacionada, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Configurações de Lista relacionada**.
2. Clique em **Novo** para adicionar um novo Grupo de lista relacionada. Insira o Nome do grupo e a Ordem em que ele deve aparecer na página Incidentes (Nova IU).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Enviar**. O grupo recém-adicionado aparece na página Grupos da lista relacionada.



Adicionar uma lista relacionada

Para adicionar uma nova Lista relacionada, siga estas etapas:

1. Clique em um link de Grupo de lista relacionada.
2. Na seção Listas relacionadas, clique em **Adicionar** para adicionar uma nova lista relacionada.

   Se você não vir o botão **Adicionar**, verifique se você está no mesmo escopo da aplicação que o Grupo da Lista relacionada.

3. Selecione a Lista relacionada a ser incluída no grupo.

   Nota: Se você não vir uma lista relacionada específica, faça o seguinte:

   a. Navegar até **IU do Sistema** > **Listas relacionadas** e pesquise Listas relacionadas presentes na tabela *sn_si_incident*.

   b. Clique na tabela *sn_si_incident* associada à **nova exibição de IU do SIR**.

   c. Na seção Entradas da lista relacionada, clique em **Novo** para adicionar a Lista relacionada à exibição de **IU do SIR Novo**.

4. Especifique a ordem em que ele deve aparecer e clique em **Enviar**.

   A Lista relacionada que você adicionou aparecerá em Espaço do analista de segurança.

Para modificar um grupo de lista relacionada existente, clique no nome do grupo para navegar até a página Grupo de lista relacionada. Você pode modificar o Nome do grupo, a Ordem e adicionar ou excluir Listas relacionadas do grupo.

Ações de IU da Lista relacionada

Você pode adicionar novas ações de IU às listas relacionadas que aparecem em Espaço do analista de segurança.

Pré-requisitos:

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para adicionar uma nova ação de IU de Lista relacionada, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Configurações de Lista relacionada**.
2. Clique no Nome do grupo. A página de configuração do Grupo de lista relacionada é exibida.
3. Clique na Lista relacionada à qual você deseja adicionar uma ação de IU.
4. Clique em **Adicionar** na seção Ações de IU da Lista relacionada.
5. Insira os seguintes detalhes:

Nome do Campo	Descrição
Ação	Selecione uma ação de IU na lista de seleção.
Tipo	Selecione o tipo de ação. Pode ser: ◦ Ação baseada em diálogo: este tipo de ação é usado quando a interação ou as entradas do usuário são necessárias para executar a lógica de negócios específica. ◦ Ação do lado do servidor: esta ação executa a lógica de negócios necessária sem nenhuma entrada adicional do usuário. **Nota:** Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que elas estejam disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para obter detalhes.
Aplicação	O nome do escopo da aplicação (IU de resposta a incidentes de segurança) ao qual a ação de IU está sendo adicionada é exibido aqui.
Ação baseada em diálogo Se você selecionar Ação baseada em diálogo no campo Tipo, insira os seguintes detalhes:	
Página da interface do usuário	Selecione a página de IU associada à ação.
Título da Caixa de Diálogo	Insira um título para a ação de diálogo.
Largura e altura da caixa de diálogo	Insira a altura e a largura da caixa de diálogo em pixels.
Script	Para a Página de IU selecionada, você pode especificar parâmetros de consulta adicionais aqui. O modelo fornecido com o sistema de base constrói e retorna somente os parâmetros `sysparm_incident_id`, `sysparm_record_table`e `sysparm_related_sys_ids`. Você pode substituí-los especificando diferentes parâmetros aqui.
Ação do lado do servidor Se você selecionar Ação do lado do servidor no campo Tipo, especifique o seguinte:	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
Recurso Rest de Script	Selecione o Recurso de REST com script que define a ação. **Nota:** A ACL **SIR UI ANALYST** deve ser adicionada ao recurso REST.

6. Clique em **Enviar**.
7. Navegar até **Incidentes de segurança** > **Incidentes (Nova IU)** página.
8. Clique no número de um incidente de segurança para exibir o registro do incidente de segurança. Inicie a respectiva Lista relacionada para exibir a nova ação de IU.

Propriedades do sistema de configuração de formulário

Essas propriedades do sistema definem os intervalos de atualização do formulário para as tarefas do playbook.

Para configurar essas propriedades, navegue até **Configuração do espaço de analista (nova IU)** > **Propriedades do espaço do analista**.

Propriedade	Valor padrão	Descrição
sn_app_secops_ui.poller_interval.playbook_tasks	10.000 ms	O tempo de intervalo usado pelo componente do playbook para atualizar suas tarefas de resposta para cada tempo de intervalo configurado.
sn_app_secops_ui.poller_interval.event.playbook_limit	9 vezes	O número de vezes que o componente do playbook pesquisa tarefas de resposta.
sn_app_secops_ui.poller_interval.related_list	30.000 ms	Este tempo de intervalo é usado pelo componente Explorar para atualizar suas contagens de Lista relacionada para cada tempo de intervalo configurado.

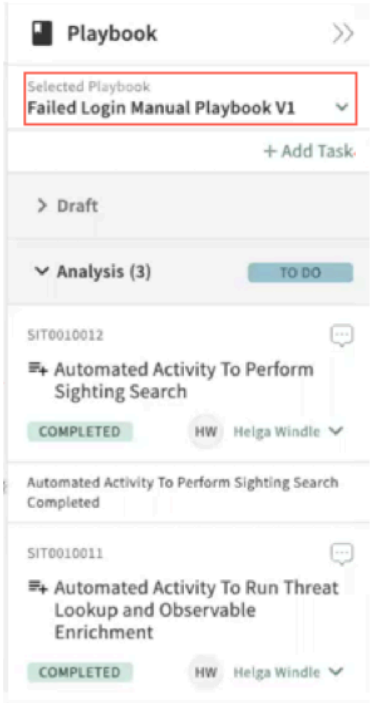
Habilitar playbooks para seleção de analista

Adicione novos playbooks à lista de seleção de playbooks.

Você pode selecionar um playbook apropriado para investigar incidentes de segurança no Espaço do analista de segurança (Gerenciar ameaças à segurança usando o Espaço do analista de segurança). A opção de seleção de playbook é compatível somente com os playbooks projetados usando o Flow Designer.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois de criar um playbook usando o Flow Designer, siga estas etapas para incluí-lo na lista de seleção Playbook selecionado:

1. Navegue até a tabela *sys_hub_flow*.
2. Pesquise o novo playbook que você criou usando o Flow Designer.
3. Adicione o marcador **sir_playbook** aos playbooks que você deseja incluir na lista de seleção Playbook selecionado.

Nota: Se você tiver playbooks antigos que não foram migrados de fluxos de trabalho para o Flow Designer, eles não serão exibidos na lista. Mas, se um playbook criado usando fluxos de trabalho for atribuído a um incidente de segurança por uma condição de gatilho ou por seleção manual (usando a opção **Executar Orquestração** no ambiente clássico), esse playbook será iniciado quando você abrir o incidente de segurança no Espaço do analista de segurança.

Solução de problemas do Security Incident Response

Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas ao Security Incident Response.

Problemas com as regras de controle de acesso

As regras de controle de acesso permitirão o acesso ao recurso especificado se todas as três condições a seguir forem atendidas:

- O usuário tem uma das funções especificadas na lista **Função** ou a lista está vazia.
- As condições no campo **Condição** são avaliadas como verdadeiras ou as condições estão vazias.
- O script no campo **Script** (avançado) é avaliado como verdadeiro, define a variável **resposta** como verdadeira ou está vazio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre Regras de controle de acesso, consulte Como explorar listas de controle de acesso

Importante: Se a opção de **Substituições de administrador** estiver desmarcada para uma tabela de incidentes de segurança e se o administrador puder acessar a tabela de incidentes de segurança, consulte o artigo KB1444673

Security Incident Response Soluções Análise da plataforma e relatórios

As Soluções Análise da plataforma e relatórios contêm painéis pré-configurados. Os painéis apresentam métricas importantes para analisar seu processo Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto.

Análise da plataforma visualizações de dados usam dados do indicador Performance Analytics para mostrar dados ao longo do tempo, ajudando você a analisar seus processos de negócio e identificar áreas de melhoria. Com o Soluções Análise da plataforma e relatórios, você pode obter valor do Performance Analytics para seu aplicativo com o mínimo de configuração. Você sempre pode criar seus próprios objetos.

Importante: Configure e teste Soluções Análise da plataforma e relatórios em uma instância de não produção antes de habilitá-los na produção.

A solução Security Incident Response Performance Analytics está disponível no ServiceNow Store. Para obter informações sobre como baixar e instalar esta aplicação, consulte Operações de segurança e ServiceNow Store.

Nota: Para avaliar a funcionalidade, você pode ativar as soluções de Performance Analytics e a análise no formulário em instâncias que não tenham o Performance Analytics licenciado. No entanto, você tem as seguintes limitações:

- Você não pode criar novos indicadores.
- Você não pode coletar dados com mais de 180 dias.

Para obter a funcionalidade completa, licencie o Performance Analytics. Para obter mais informações, consulte Ativar assinatura da Análise de desempenho .

Importante: Por padrão, o limite de coleta de dados para a propriedade *(com.snc.pa.dc.max_records)* no Performance Analytics é definido como 5.000 registros. Mas você pode aumentar esse limite de acordo com seus requisitos, como 50.000 registros. No entanto, o aumento desse limite pode afetar o desempenho durante a coleta de dados ou ao executar operações na tabela de snapshot. Para saber mais sobre as propriedades do Performance Analytics, consulte Propriedades Performance Analytics .

Informações relacionadas

Soluções Análise da plataforma e relatórios

Ative sua assinatura do Performance Analytics

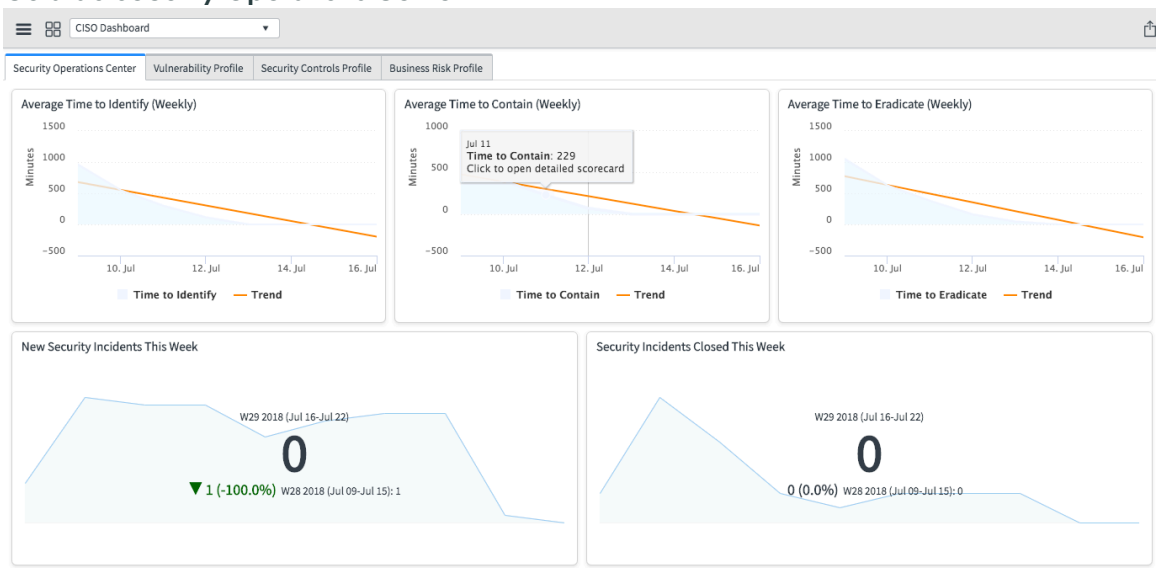
Painel do CISO

Este painel revela a postura geral de segurança da sua organização, incluindo vulnerabilidades e incidentes de segurança.

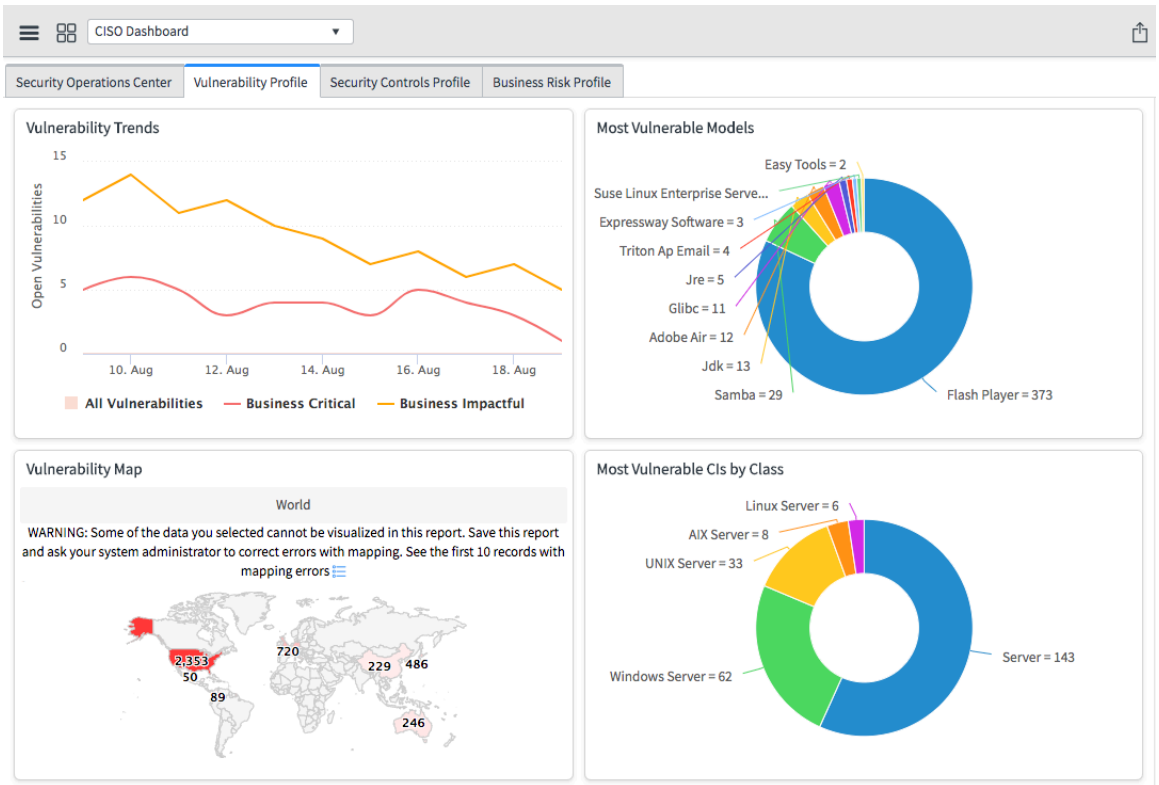
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia do Security Operations Center



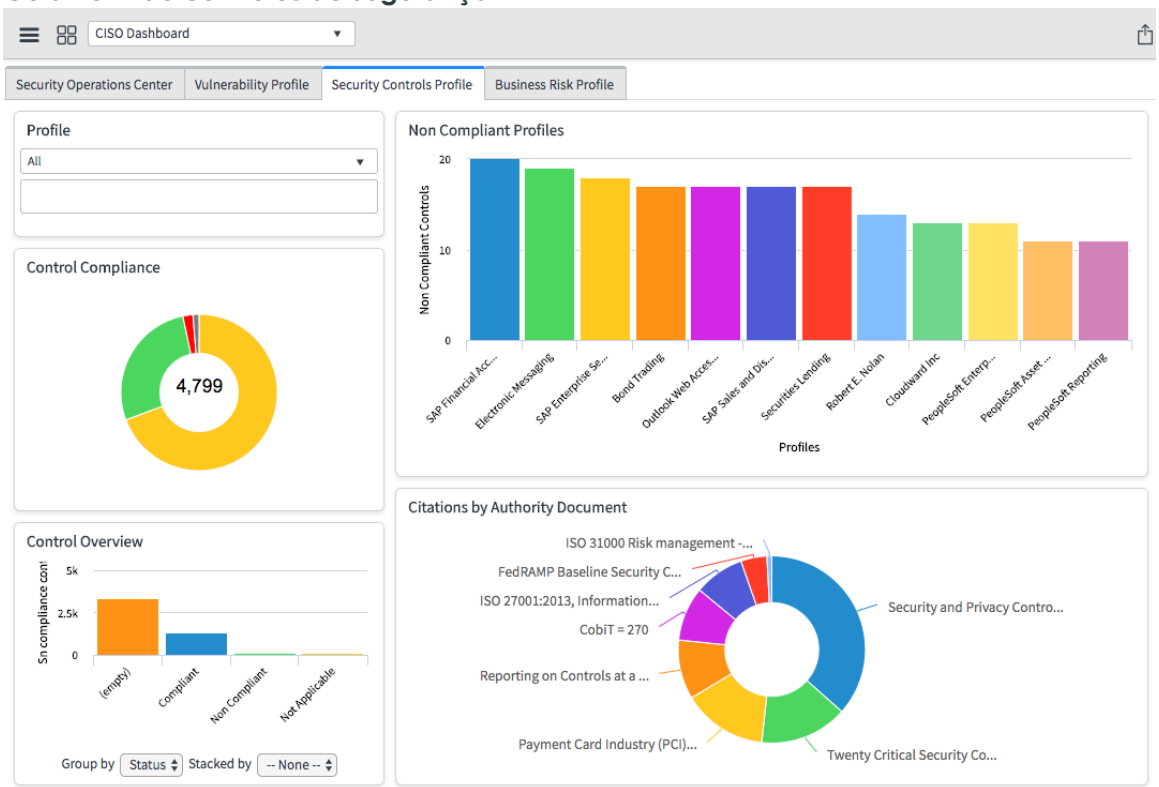
Guia Perfil de vulnerabilidade



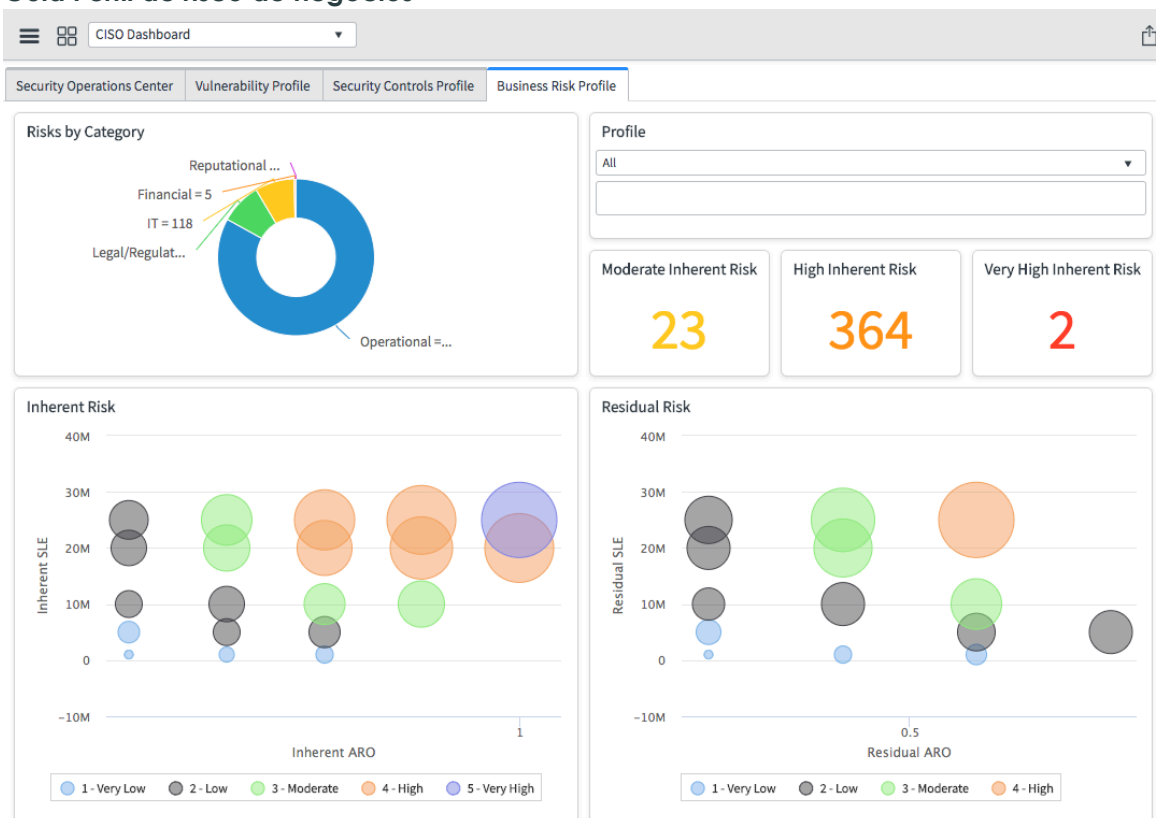
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Perfil de controles de segurança



Guia Perfil de risco de negócios



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções e usuário finais

Usuário final e objetivo	Função necessária
CISO: precisa de visibilidade clara sobre a postura de segurança atual da organização em geral	sn_si.ciso

Indicadores do painel do CISO

O painel do CISO apresenta os seguintes principais indicadores de desempenho:

Incidente de segurança: tempo médio de identificação

Uma média de 7 dias do tempo em minutos necessário para identificar um incidente de segurança, calculada diariamente.

Tempo médio de contenção

Uma média de 7 dias do tempo em minutos necessário para conter um incidente de segurança, calculada diariamente.

Tempo médio para eliminar

Uma média de 7 dias do tempo em minutos necessários para erradicar um incidente de segurança, calculada diariamente. O tempo médio de contenção e o tempo médio de eliminação são baseados no indicador Incidente de segurança: tempo médio de duração dividido por estado de incidente de segurança.

Novos Incidentes de segurança nesta semana

A soma semanal da pontuação do indicador diário de Número de novos incidentes de segurança.

Incidentes de segurança encerrados (semanalmente)

A soma de 7 dias consecutivos do indicador diário de Número de incidentes de segurança encerrados.

Novos incidentes de segurança por prioridade

Detalhamento diário do indicador Número de novos incidentes de segurança por Prioridade.

Volume de incidentes de segurança novos versus encerrados (semanalmente)

A série temporal de soma de 7 dias do indicador Número de novos incidentes mapeada em relação à série temporal de soma de 7 dias do indicador Número de incidentes encerrados.

Mapa térmico de incidente de segurança

Um mapa global que mostra o número de incidentes de segurança em aberto em cada país.

Mapa de árvore de incidentes de segurança

Um mapa de árvore interativo em que você pode selecionar para ver:

- Incidentes de segurança por serviço de negócio, divididos por criticidade do negócio
- Incidentes de segurança divididos por categoria ou subcategoria de incidente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Incidentes de segurança por grupo de atribuição ou por designado
- "Estatísticas de vítima" de incidente de segurança por recurso afetado ou usuário afetado

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Criticalidade dos negócios
- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Código de fechamento de incidentes de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança
- SI - Serviço de negócios
- Vulnerabilidade

Visualizações de dados

O painel inclui as seguintes visualizações:

Título	Tipo	Descrição
Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado	Mapa térmico	Exibe modelos com os itens mais vulneráveis.
Risco por categoria	Rosca	Lista a idade dos itens vulneráveis reabertos.
Citações por documento de autoridade	Rosca	Número de vulnerabilidades ativas
Incidentes de segurança com atribuído que não está ativo	Mapa térmico	Exibe o número de itens vulneráveis em aberto associados a vulnerabilidades (registros de Enumeração de vulnerabilidade comum (CVE), do maior para o menor).
Incidentes de segurança não atualizados por mais de 30 dias por grupo de atribuição e estado	Mapa térmico	Exibe os fornecedores com os itens mais vulneráveis.
Mapa de vulnerabilidade	Mapa	Um mapa-múndi mostrando vulnerabilidades por local
Modelos mais vulneráveis	Rosca	As aplicações que contêm mais vulnerabilidades
ICs mais vulneráveis por classe	Rosca	ICs por tipo de servidor

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
Serviços com vulnerabilidades críticas significativas	Lista	
Perfis fora de conformidade	Barra de barra	Controles fora de conformidade por perfil
Visão geral de controle	Barra de barra	Número de controles conformes e não conformes
Exceções às políticas	Lista	Exceções às políticas com prioridade, proprietário e descrição resumida
Risco por categoria	Rosca	O número de riscos em cada categoria de risco
Risco inerente	Bolha de bolha	SLE Inerente versus ARO Inerente
Risco residual	Bolha de bolha	SLE residual vs. ARO residual
Riscos moderados, altos e muito altos	Pontuações	O número de riscos moderados, altos e muito altos, respectivamente
Risco por perfil	Barra	Contagem de risco em que você pode selecionar o que agrupar e o que empilhar

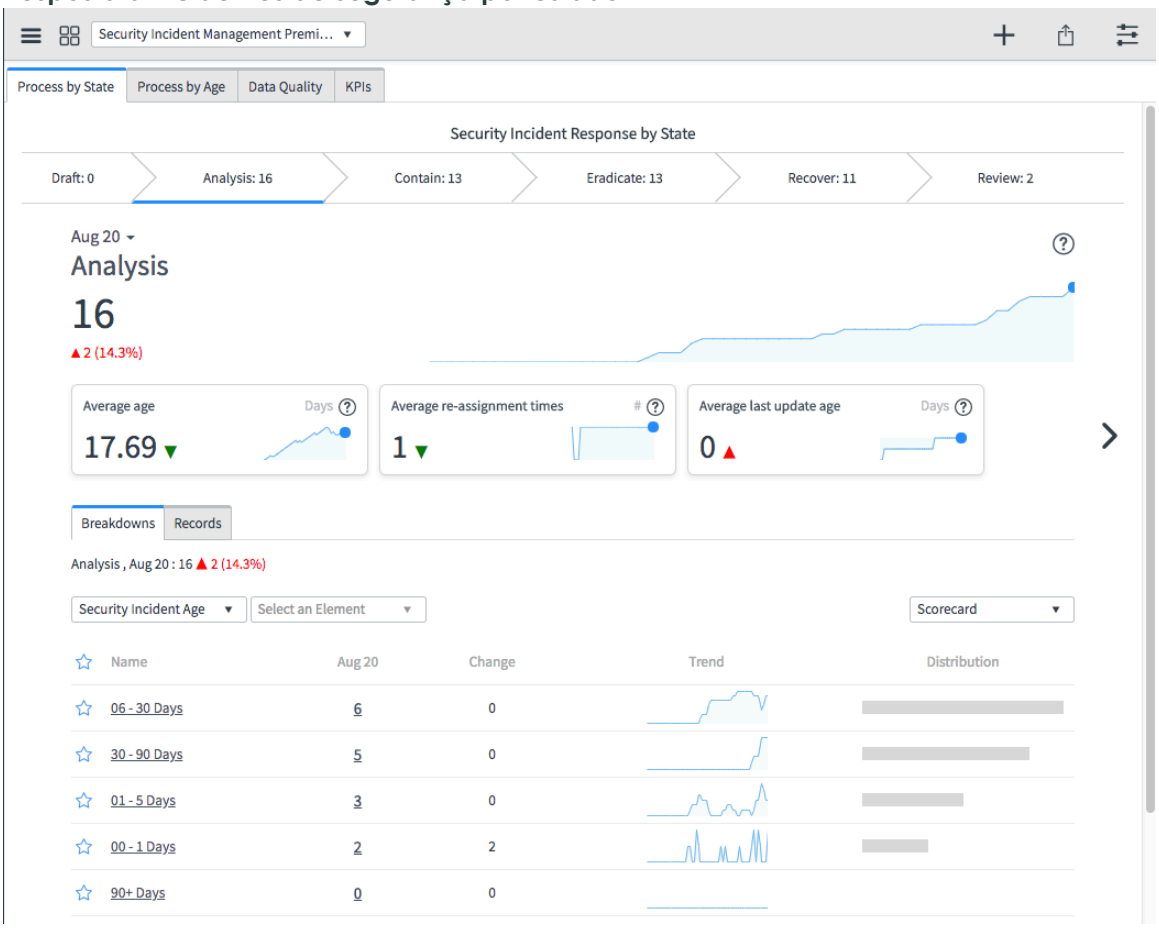
Painel do Security Incident Management Premium

Este painel usa visualizações Análise da plataforma avançadas para ajudar os gerentes de segurança a rastrear o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação. A versão licenciada de Performance Analytics é, portanto, necessária.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

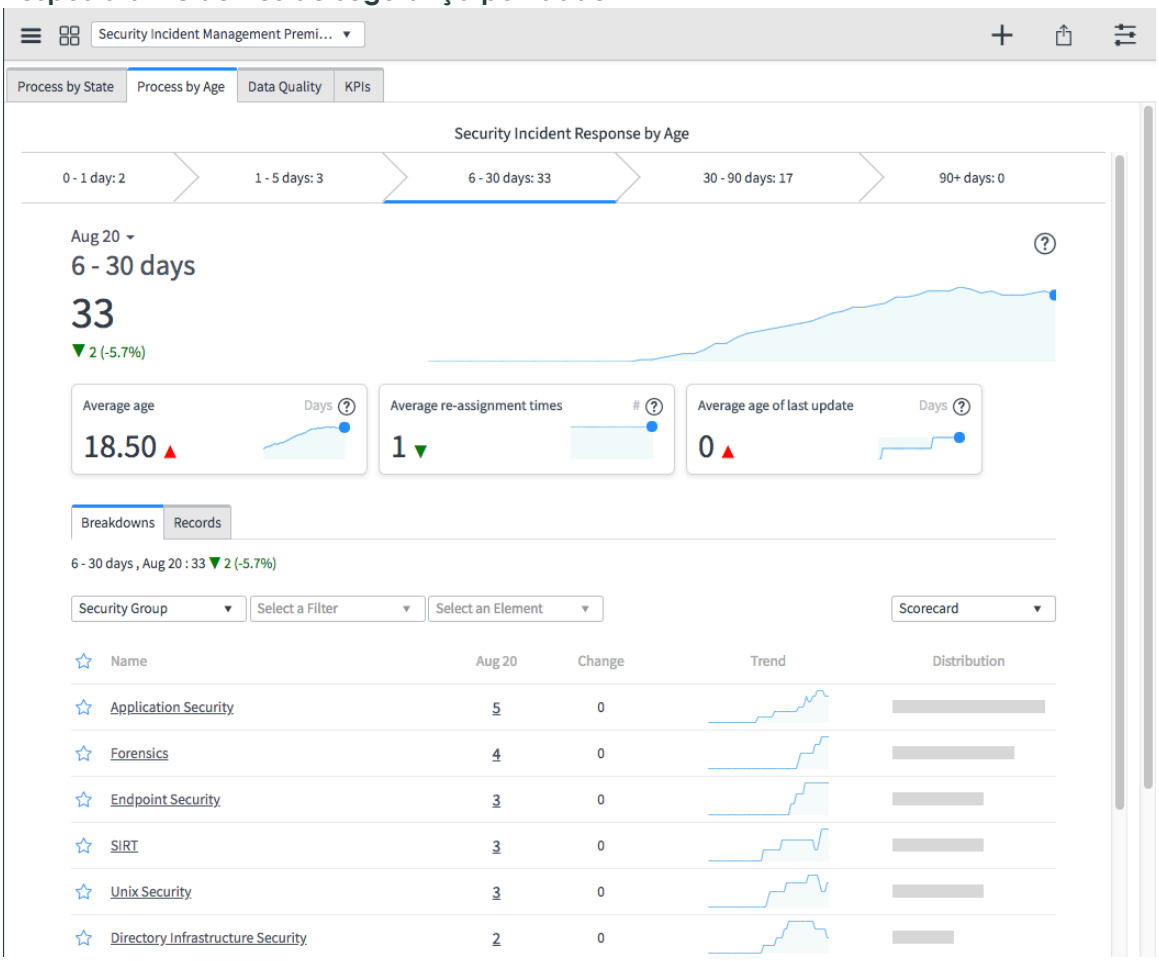
Resposta a incidentes de segurança por estado



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resposta a incidentes de segurança por idade



Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Gerenciador de resposta de segurança: precisa de visibilidade clara sobre o estado geral e o volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador do Security Response: precisa identificar áreas de preocupação rapidamente e ter controle total sobre todos os dados do Security Incident Response enquanto administra territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam tratados primeiro.
Analistas de resposta de segurança: precisam priorizar rapidamente em	sn_si.analyst	Os analistas de segurança de níveis 1 e 2 trabalham em incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário final e objetivo	Função necessária	Benefícios
quais vulnerabilidades se concentrar com base na criticidade para a organização.		Eles podem criar e atualizar incidentes, solicitações e tarefas de segurança, bem como problemas, mudanças e indisponibilidades relacionadas aos incidentes.

Indicadores do Security Incident Management Premium

As guias Processar por estado e Processar por idade contêm widgets de workbench com os seguintes indicadores:

Idade média

O indicador Idade média dos incidentes de segurança em aberto usa a fórmula `[[Soma da idade dos incidentes de segurança em aberto]] / [[Número de incidentes de segurança em aberto]] / 24` para fornecer um resultado em dias.

Tempos médios de reatribuição

O indicador Reatribuição média de incidentes de segurança em aberto usa a fórmula `Soma de reatribuições de incidentes de segurança em aberto / Número de incidentes de segurança em aberto`.

Idade média do último upgrade

O indicador Idade média da última atualização de incidentes de segurança em aberto usa a fórmula `Soma da idade da última atualização de incidentes de segurança em aberto/Número de incidentes de segurança em aberto/24` para fornecer um resultado em dias.

% não atualizada em 5 dias

O indicador % de incidentes de segurança em aberto não atualizados nos últimos 5 dias usa a fórmula `([[Número de incidentes de segurança em aberto não atualizados nos últimos 5 dias]] / [[Número de incidentes de segurança em aberto]]) * 100`.

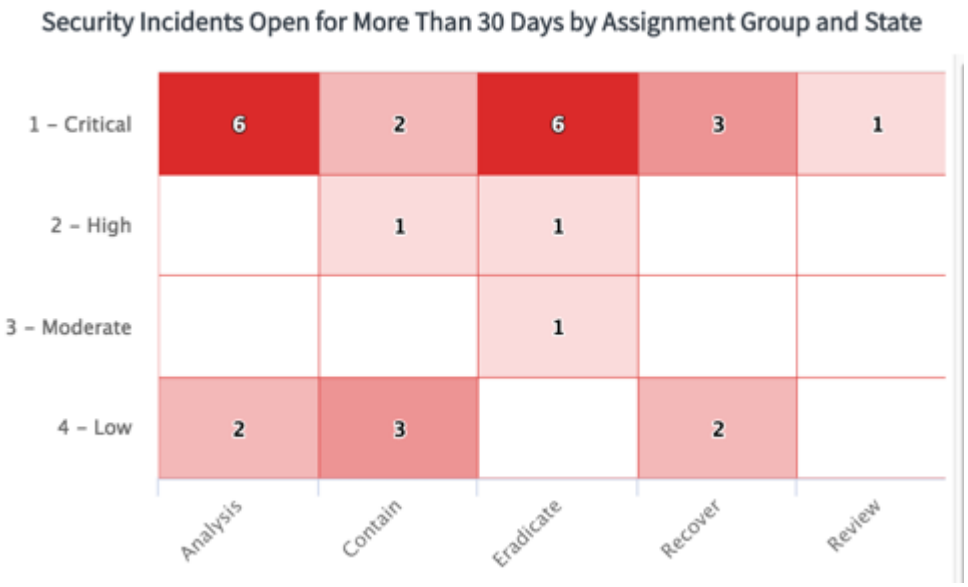
A guia Qualidade de dados tem filtros interativos para a categoria do incidente de segurança e os níveis de risco, prioridade e gravidade. Esses filtros são aplicados simultaneamente aos seguintes indicadores:

Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado

O número de incidentes de segurança em aberto filtrados por 30 dias e divididos por grupo de atribuição e estado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Incidentes de segurança com atribuído que não está ativo

O número de incidentes de segurança em aberto sem designado ou um designado que não está ativo.

Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado

O indicador Número de incidentes de segurança em aberto não atualizados nos últimos 30 dias dividido por Grupo de atribuição e Estado.

A guia KPI tem os seguintes indicadores adicionais:

- Percentual de novos incidentes de segurança críticos
- Idade média dos incidentes de segurança em aberto
- Tempo médio de encerramento de incidentes de segurança
- Percentual de incidentes de segurança que foram reatribuídos
- Percentual de incidentes de segurança encerrados na primeira atribuição
- Percentual de incidentes de segurança encerrados por autoatendimento
- Percentual de incidentes de segurança não resolvidos
- Tempo médio de encerramento das tarefas de incidente de segurança

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança

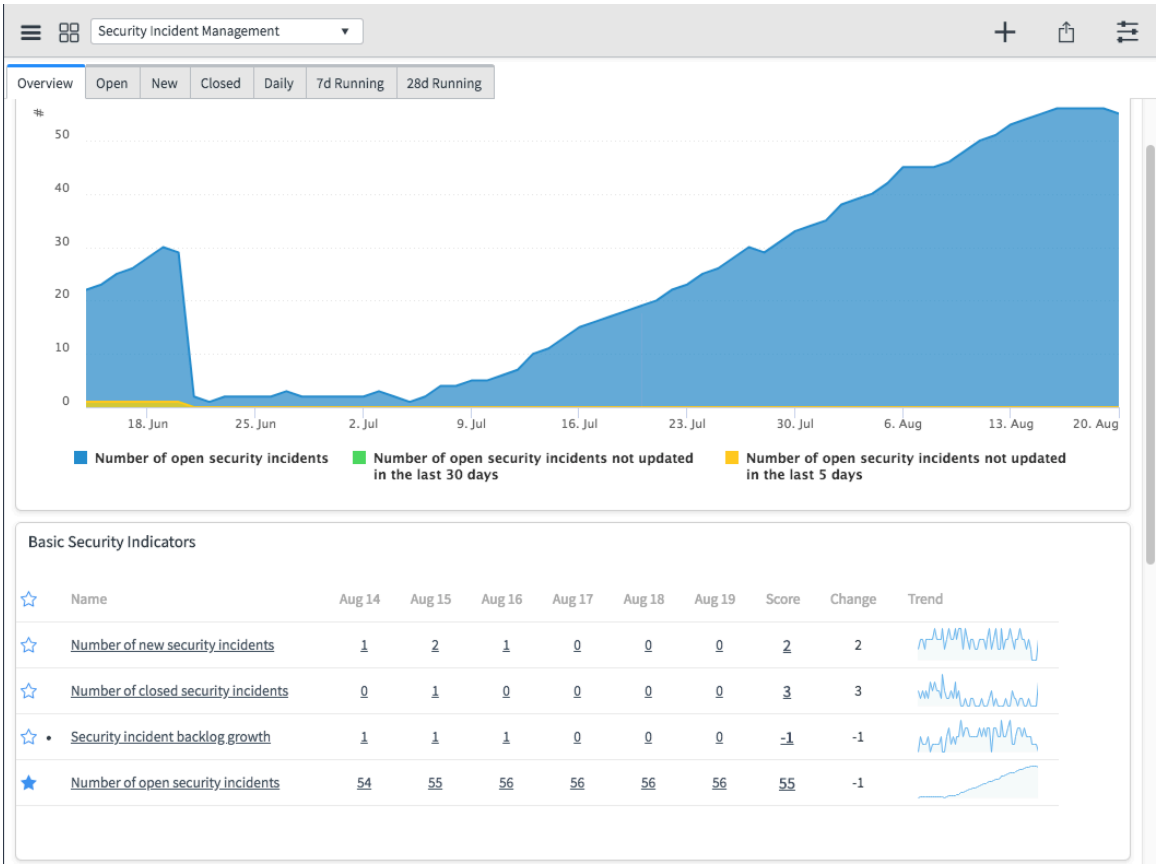
Painel do Gestão de incidentes de segurança

Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

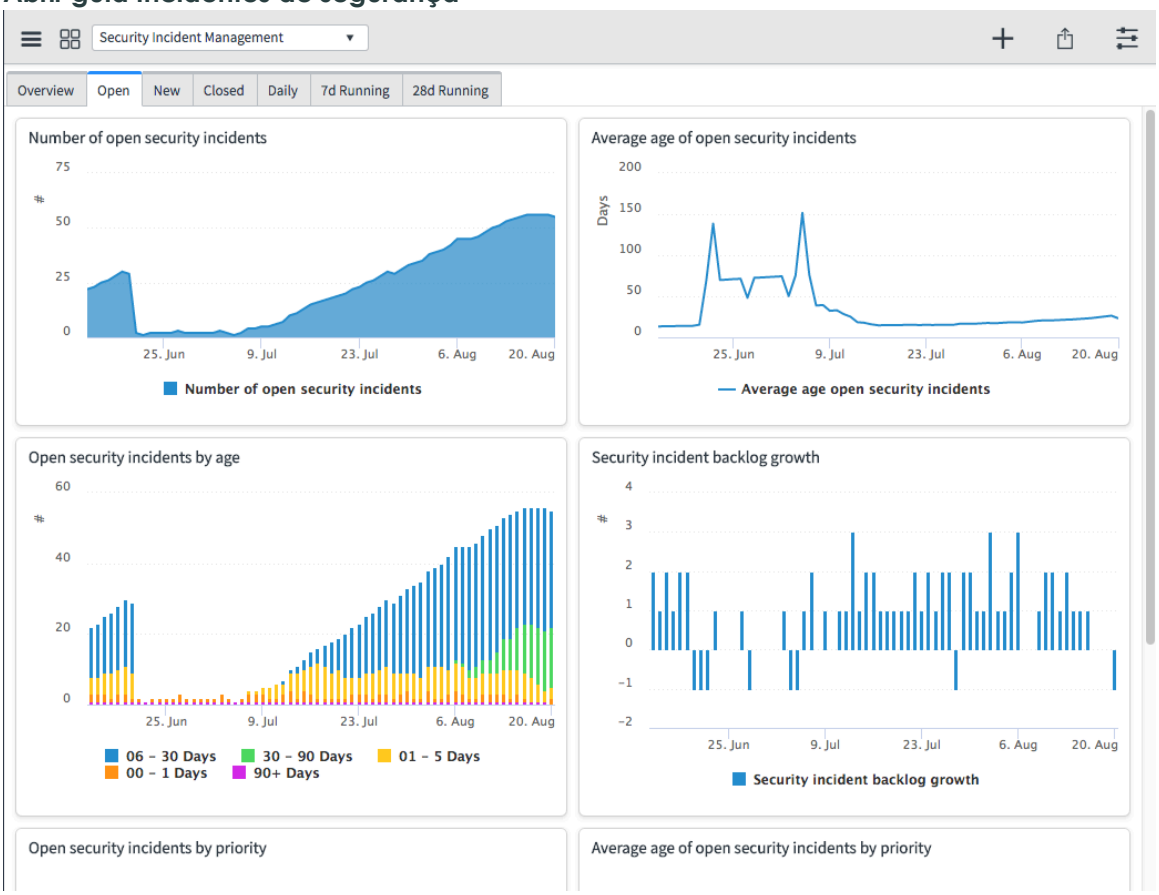
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão Geral



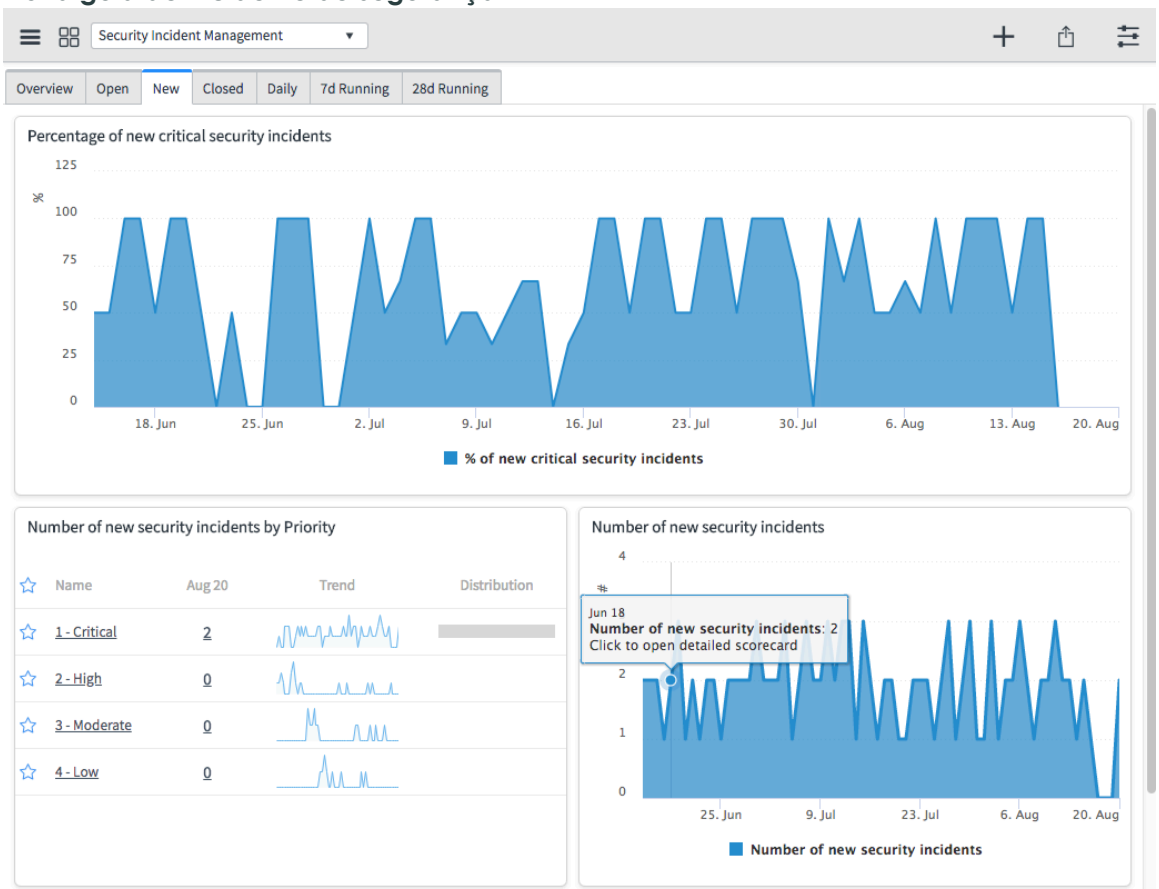
Abrir guia Incidentes de segurança



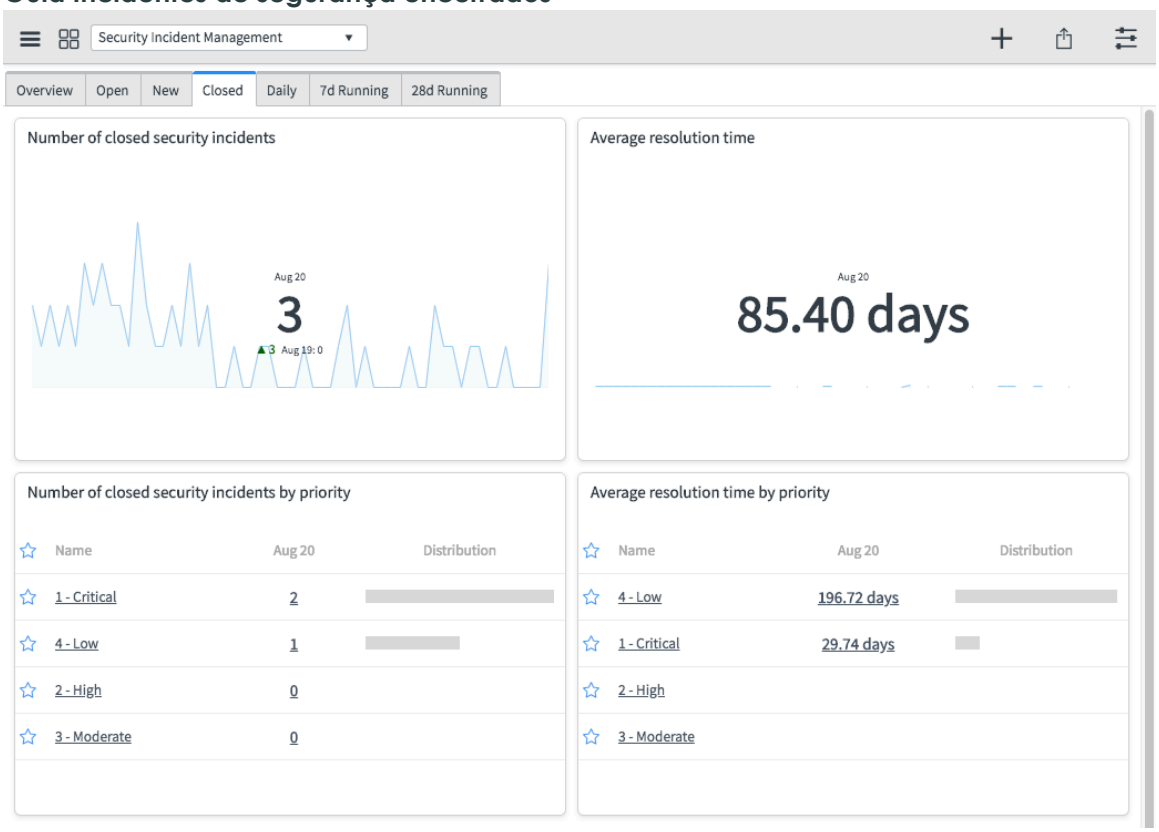
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nova guia de incidente de segurança



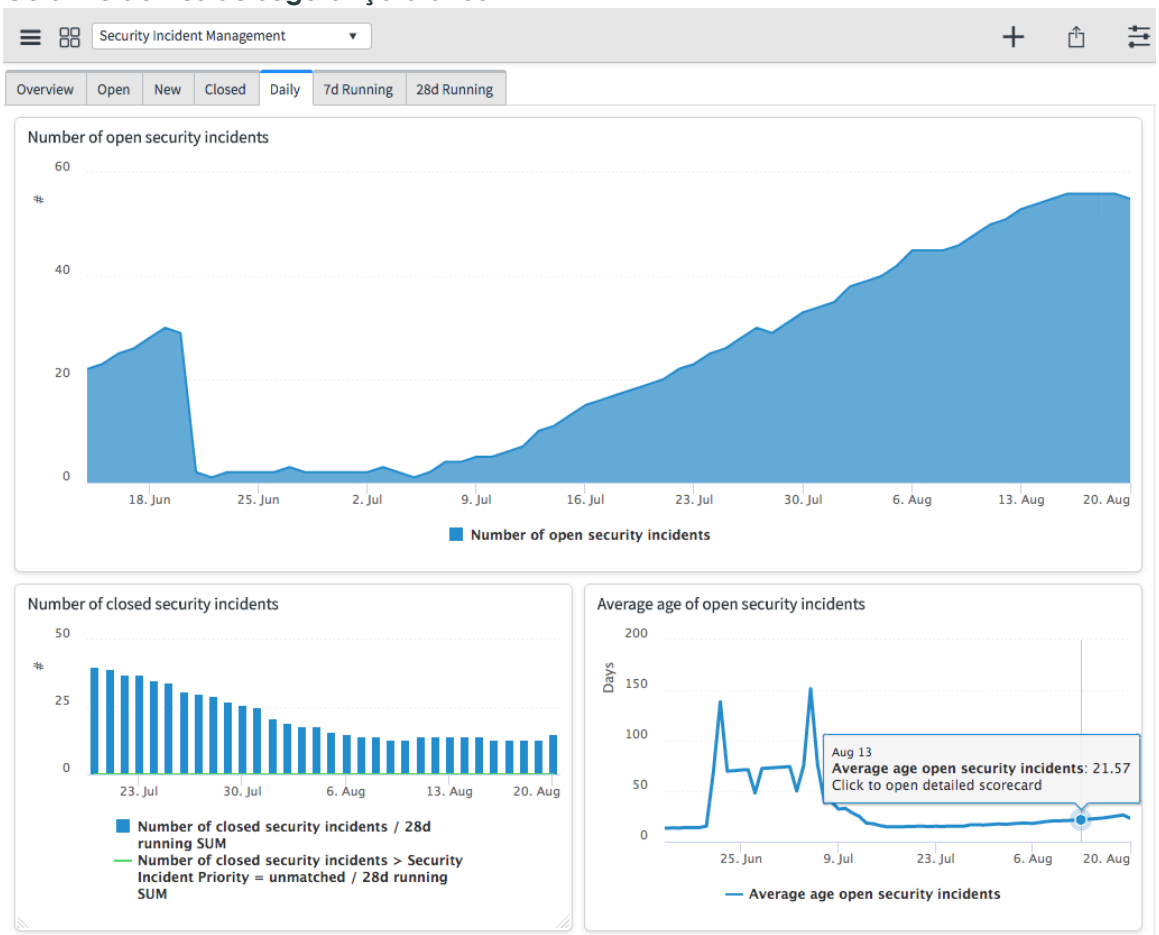
Guia Incidentes de segurança encerrados



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Incidentes de segurança diários



As guias **Execução** de 7 dias e **Execução** de 28 dias seguem o formato da guia **Diariamente**.

Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Gerenciador de resposta de segurança: precisa de visibilidade clara sobre o estado geral e o volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador do Security Response: precisa identificar áreas de preocupação rapidamente e ter controle total sobre todos os dados do Security Incident Response enquanto administra territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam tratados primeiro.
Analistas de resposta de segurança: precisam	sn_si.analyst	Os analistas de segurança de níveis 1 e 2 trabalham em

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário final e objetivo	Função necessária	Benefícios
priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.		incidentes de segurança. Eles podem criar e atualizar incidentes, solicitações e tarefas de segurança, bem como problemas, mudanças e indisponibilidades relacionadas aos incidentes.

Indicadores de Gestão de incidentes de segurança

O painel do Gestão de incidentes de segurança apresenta os seguintes indicadores principais de desempenho:

Novos incidentes de segurança

Um gráfico do número de novos incidentes de segurança.

Incidentes de segurança em aberto

Um gráfico em que você pode comparar o número de incidentes de segurança em aberto, o número de incidentes de segurança em aberto não atualizados nos últimos 30 dias e o número de incidentes de segurança em aberto não atualizados nos últimos 5 dias.

Indicadores básicos de segurança

Os últimos 6 dias de pontuações do número de novos incidentes de segurança, o número de incidentes de segurança encerrados, o crescimento do backlog de incidentes de segurança e os indicadores de Número de incidentes de segurança em aberto.

Novos incidentes de segurança por prioridade

O número de novos incidentes de segurança divididos por prioridade.

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança

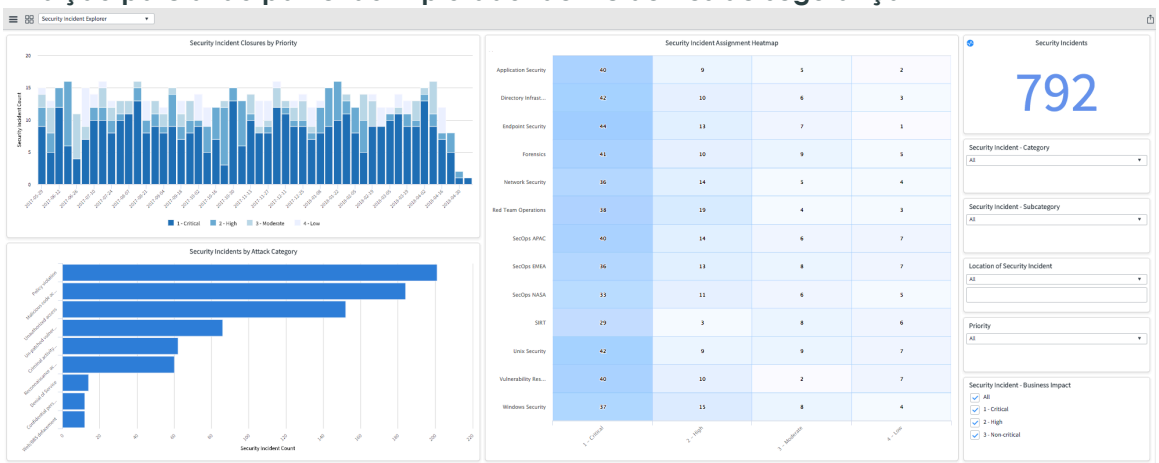
Painel do Explorador de incidentes de segurança

Com este painel, os gerentes de segurança podem exibir incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios. Essas exibições permitem que os gerentes obtenham informações rapidamente sobre a frequência com que os ataques estão ocorrendo e quais serviços de negócio são afetados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição parcial do painel do Explorador de incidentes de segurança



Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Gerenciador de resposta de segurança: precisa de visibilidade clara sobre o estado geral e o volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador do Security Response: precisa identificar áreas de preocupação rapidamente e ter controle total sobre todos os dados do Security Incident Response enquanto administra territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam tratados primeiro.
Analista de resposta de segurança: precisa priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de níveis 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes, solicitações e tarefas de segurança, bem como problemas, mudanças e indisponibilidades relacionadas aos incidentes.

Indicadores do Explorador de incidentes de segurança

O painel do Explorador de incidentes de segurança apresenta os seguintes indicadores principais de desempenho:

Incidentes de segurança

O volume total de incidentes de segurança abertos e pendentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Encerramentos de incidente de segurança por prioridade

O número de incidentes de segurança encerrados divididos por Prioridade.

Incidentes de segurança por categoria de ataque

O número de incidentes de segurança em aberto dividido por categoria.

Mapa térmico de atribuição de incidente de segurança

Um detalhamento em dois níveis do número de incidentes de segurança em aberto por grupo de atribuição e prioridade.

Mapa térmico de incidente de segurança

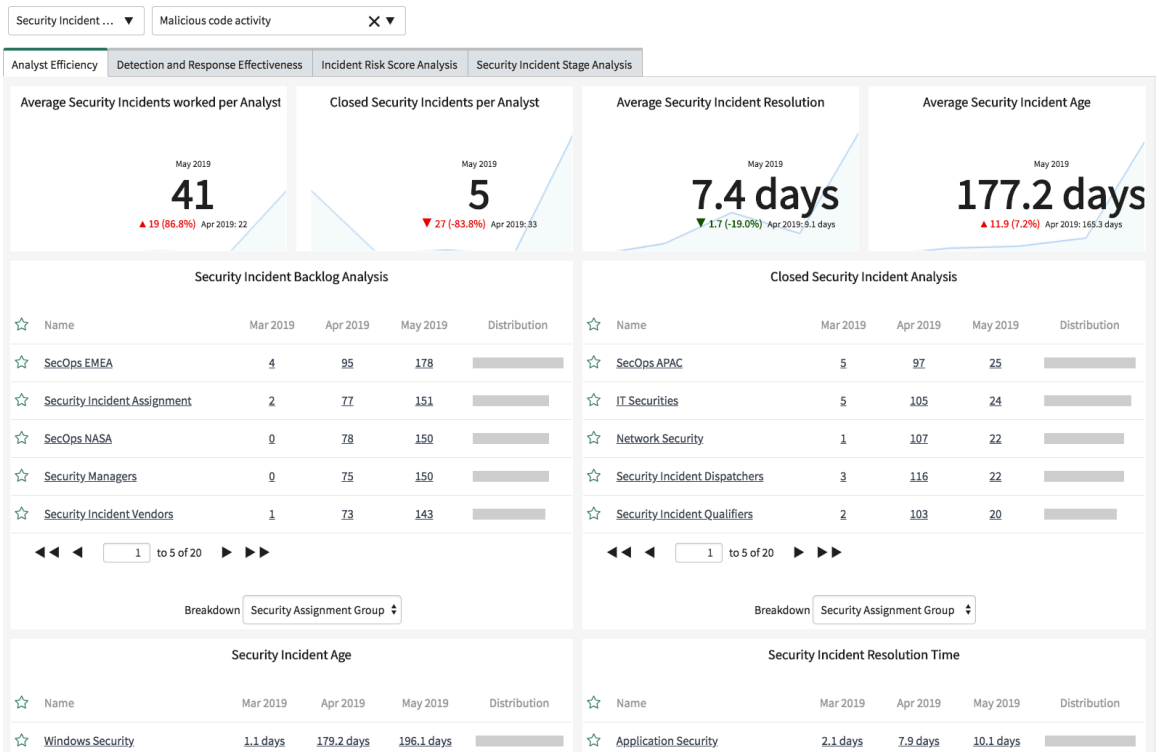
Um mapa global que mostra o número de incidentes de segurança em aberto em cada país.

Painel Eficiência das Operações de segurança

Os gerentes do centro de operações de segurança (SOC) podem visualizar as métricas gerais de eficiência e medir o desempenho individual dos membros da equipe de SOC na organização.

O gerente do SOC pode usar o painel do Performance Analytics para melhorar a eficiência e desenvolver uma imagem de como o SOC está se saindo em áreas gerais e específicas ao longo do tempo.

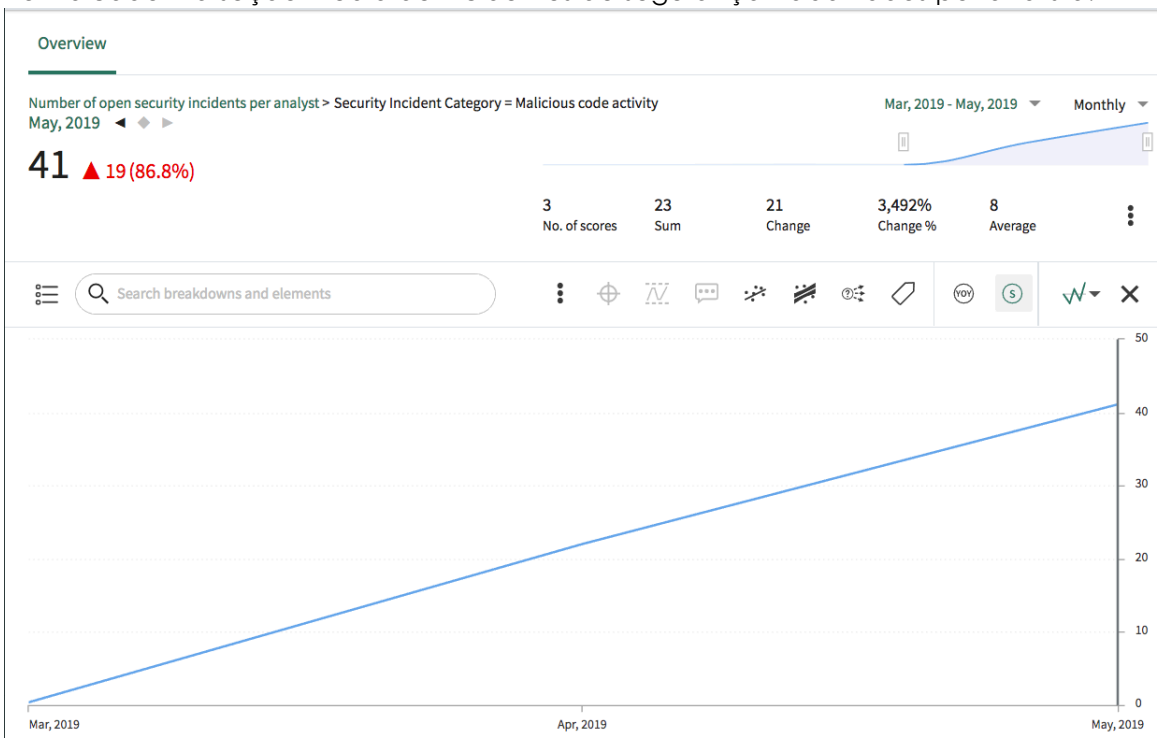
Guia Eficiência do analista



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clique em qualquer um dos indicadores para obter mais detalhes. Por exemplo, clique no indicador na seção Média de incidentes de segurança trabalhados por analista.



O gráfico mostra que o número de incidentes de segurança em aberto aumentou de 0 em março para mais de 40 em maio. Observe os dados exibidos no cabeçalho:

- Indicador de tendências: mostra a mudança no número de incidentes em aberto no último período em que os dados foram coletados. Este gráfico mostra dados do período de março de 2019 a maio de 2019 e o número de incidentes em aberto aumentou em 19 no mês de maio. A eficiência do analista é melhor se o número de incidentes abertos tiver diminuído ao longo de um período de tempo.
- Número de pontuações: o período para o qual os dados foram coletados (março a maio de 2019).
- Soma: o número de novos incidentes em aberto no período entre março e maio.
- Mudança: o número de novos incidentes em aberto entre março e abril.
- Média: o número médio de incidentes em aberto por analista no período selecionado.

Guia Eficiência do analista

Indicador	Descrição
Média de incidentes de segurança trabalhados por analista	Número médio de incidentes de segurança em aberto por analista no período especificado. A fórmula usada é `[[Número de incidentes de segurança em aberto / Por mês MÉDIA +]]/ [[Número de agentes de segurança]]`
Incidentes de segurança encerrados por analista	O número total de incidentes encerrados por cada analista na categoria selecionada no período especificado. A fórmula usada é `[Número de incidentes de segurança encerrados > Categoria do incidente de segurança =`<category_name> / SOMA por mês +]]/[[Número de agentes de segurança / Por mês MÉDIA +]]

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

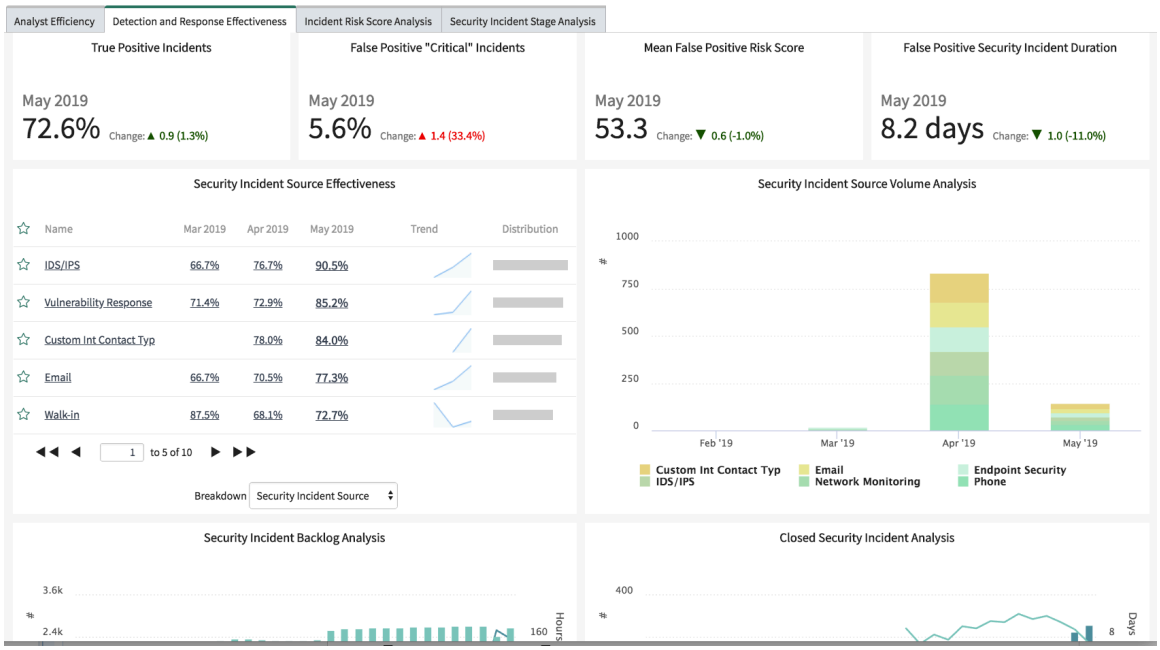
Guia Eficiência do analista

Indicador	Descrição
Resolução média de incidentes de segurança	O tempo médio gasto por cada analista para fechar incidentes de segurança no período especificado. A fórmula usada para mostrar o resultado em dias é `([[Soma da duração de incidentes de segurança encerrados > Categoria de incidente de segurança =`<category_name> / MÉDIA por mês +]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança = / MÉDIA por mês +]]) / 24
Idade média do incidente de segurança	O número médio de dias pelos quais os incidentes de segurança permanecem abertos para cada analista. A fórmula usada para mostrar o resultado em dias é `([[Soma da idade dos incidentes de segurança em aberto > Categoria do incidente de segurança =`<category_name> / MÉDIA por mês +]]/ [[Número de incidentes de segurança em aberto > Categoria de incidente de segurança = / MÉDIA por mês +]]) / 24
Análise de backlog de incidentes de segurança	O número total de incidentes de segurança em aberto no período especificado. Selecione uma opção na lista Detalhamento para exibir o backlog de cada analista, grupo de segurança, prioridade e assim por diante. Você também pode comparar o número de incidentes de segurança em aberto entre dois meses selecionados.
Análise de incidente de segurança encerrado	O número total de incidentes de segurança encerrados no período especificado. Selecione uma opção na lista Detalhamento para exibir a contagem de cada analista, grupo de segurança, prioridade e assim por diante. Você também pode comparar o número de incidentes de segurança que foram encerrados entre dois meses selecionados.
Idade do incidente de segurança	O número médio de dias que os incidentes de segurança permanecem em aberto no período especificado. Selecione uma opção na lista Detalhamento para exibir a idade do incidente de segurança para cada analista, grupo de segurança, prioridade e assim por diante. A fórmula usada para mostrar o resultado em dias é `([[Soma da idade dos incidentes de segurança em aberto > Categoria do incidente de segurança =`<category_name> > Grupo de atribuição de segurança =<group_name> / MÉDIA por mês +]]/ [[Número de incidentes de segurança em aberto > Categoria de incidente de segurança = > Grupo de atribuição de segurança = / MÉDIA por mês +]]) / 24
Tempo de resolução do incidente de segurança	O número médio de dias necessários para resolver incidentes de segurança durante o período especificado. Selecione uma opção na lista Detalhamento para exibir o tempo de resolução do incidente de segurança para cada analista, grupo de segurança, prioridade e assim por diante. A fórmula usada para mostrar o resultado em dias é `([[Soma da duração de incidentes de segurança encerrados > Categoria do incidente de segurança = Atividade de código malicioso > Segurança atribuída a = John Ashby / Por mês MÉDIA +]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = John Ashby / Por mês MÉDIA +]]) / 24`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Eficácia de detecção e resposta



Guia Eficácia de detecção e resposta

Indicador	Descrição
Incidentes verdadeiros positivos	Porcentagem de incidentes de segurança positivos verdadeiros na categoria selecionada para o período especificado. A fórmula usada é `(1-([[Número de incidentes de segurança falso-positivos > Categoria de incidente de segurança = Atividade de código malicioso / Por mês SOMA +]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso / Por mês SOMA +]])) * 100`
Incidentes críticos falso-positivos	Percentual de incidentes de segurança críticos falso-positivos na categoria selecionada para o período especificado. A fórmula usada é `([[Número de incidentes de segurança falso-positivos > Pontuação de risco do incidente de segurança = Risco crítico > Categoria do incidente de segurança = Atividade de código malicioso/Por mês SOMA +]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = Mal-intencionado atividade de código / Por mês SOMA +]]) * 100`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicador	Descrição
	Nota: Qualquer incidente de segurança em que o `Código fechado = Vulnerabilidade inválida ou Falso-positivo` é tratado como um incidente falso-positivo
Pontuação média de risco falso-positivo	Pontuação de risco média mensal de incidentes de segurança encerrados que foram identificados como incidentes falso-positivos. Uma pontuação de risco mais baixa indica que os analistas de segurança gastaram menos tempo analisando incidentes falso-positivos. A fórmula usada é `([[Número de incidentes de segurança falso-positivos > Pontuação de risco do incidente de segurança = Risco crítico > Categoria do incidente de segurança = Atividade de código malicioso/Por mês SOMA +]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = Mal-intencionado atividade de código / Por mês SOMA +]]) * 100`
Duração do incidente de segurança falso-positivo	Número médio de dias que os analistas de segurança gastaram na investigação de incidentes falso-positivos. A fórmula usada é `([[Soma da duração de incidentes de segurança falso-positivos]] / [[Número de incidentes de segurança falso-positivos]]) / 24`
Eficácia da origem do incidente de segurança	Percentual de incidentes de segurança verdadeiros positivos identificados por uma origem específica para o período especificado. A origem pode ser e-mail, atividade de rede,suporte ao cliente e assim por diante. Esses dados ajudam a medir a eficácia da origem do incidente de segurança. A fórmula usada é `(1-([[Número de incidentes de segurança falso-positivos > Categoria do incidente de segurança = Atividade de código malicioso > Origem do incidente de segurança = IDS/IPS / SOMA por mês +]] / [[Número de incidentes de segurança encerrados > Incidente de segurança Categoria = Atividade de código malicioso > Origem do incidente de segurança = IDS/IPS / Por mês SOMA +]])) * 100`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

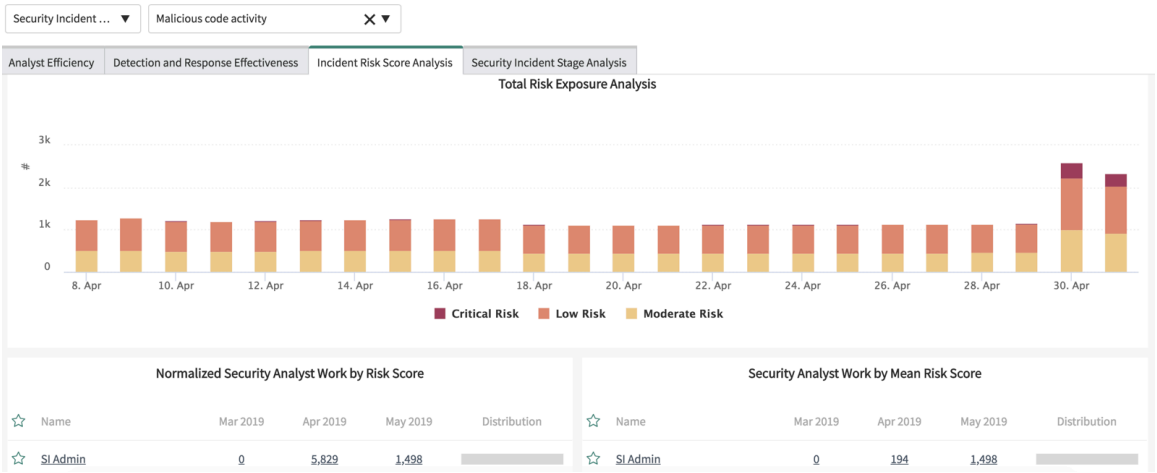
Guia Eficácia de detecção e resposta

Indicador	Descrição
Análise de volume de origem do incidente de segurança	Número de incidentes de segurança encerrados no mês atual para cada origem de incidente de segurança. Você também pode comparar o número de incidentes de segurança para cada tipo de origem entre dois meses selecionados.
Análise de backlog de incidentes de segurança	O número total de incidentes de segurança em aberto no período especificado e o número médio de dias pelos quais os incidentes permanecem abertos. Você também pode comparar o número de incidentes de segurança em aberto entre dois meses selecionados. A fórmula usada para calcular o período médio do backlog é `([[Soma da idade dos incidentes de segurança em aberto > Categoria do incidente de segurança = Atividade de código malicioso]]/[[Número de incidentes de segurança em aberto > Categoria do incidente de segurança = Atividade de código malicioso]]) / 24`
Análise de incidente de segurança encerrado	O número total de incidentes de segurança encerrados no período especificado e o tempo médio de resolução desses incidentes. A fórmula usada para calcular o tempo médio de resolução é `([[Soma da duração de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso]]) / 24`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Análise de pontuação de risco do incidente



Guia Análise de pontuação de risco do incidente

Indicador	Descrição
Análise de exposição total ao risco	Número total de incidentes em aberto em cada categoria de risco (baixo, moderado e crítico) no período especificado. Você também pode comparar o número de incidentes nas diferentes categorias de risco entre dois meses.
Trabalho de analista de segurança normalizado por pontuação de risco	A pontuação de risco total para cada analista de segurança no período especificado. Isso é calculado com base no número de incidentes de segurança positivos verdadeiros que o analista de segurança fechou. A fórmula usada é `[[Soma da pontuação de risco de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = Administrador de SI / Por mês SOMA +]] - [[Soma da pontuação de risco de incidentes de segurança falso-positivos > Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = Administrador de SI / Por mês SOMA +]]`
Trabalho do analista de segurança por pontuação de risco média	A pontuação de risco médio de cada analista de segurança no período especificado. A fórmula usada é `[[Soma da pontuação de risco de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = Administrador de SI / Por mês MÉDIA`

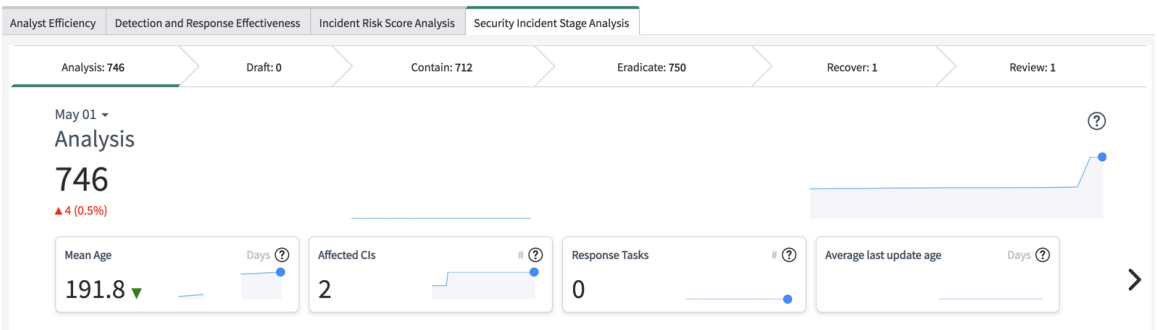
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Análise de pontuação de risco do incidente

Indicador	Descrição
	+]] - [[Soma da pontuação de risco de incidentes de segurança falso-positivos > Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = Administrador de SI / Por mês MÉDIA +]]

Guia Análise de fases do incidente de segurança



Você pode ver o número de incidentes em aberto em um dia específico e o status (análise, rascunho, contenção, erradicação, recuperação ou revisão) desses incidentes. Em cada fase, você pode exibir a idade média, ICs afetados, tarefas de resposta e assim por diante. Clique em um link para exibir detalhes adicionais ou o detalhamento desses incidentes.

Espaço de resposta a incidentes de segurança

O ServiceNow® Espaço de resposta a incidentes de segurança é uma interface recriada que fornece uma experiência de usuário de última geração para os analistas de segurança e gerentes de SOC. Os analistas de segurança podem usar isso para gerenciar o ciclo de vida dos incidentes de segurança, desde uma análise inicial até a contenção, erradicação e recuperação.

Para começar com Espaço SIR

Selecione um bloco para começar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar espaço

Saiba mais sobre conceitos e recursos do Espaço SIR

Administradores que usam o espaço

Configurar espaço e recursos de SIR

Analistas usando o espaço

Saiba como os analistas usam o espaço SIR

Exibir Painéis SIR

Exibir painéis do espaço de SIR

Tradução automática

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

- A instalação da versão Security Incident Response 13.4.5 ou posterior a partir de ServiceNow Store instalará automaticamente a versão Espaço de resposta a incidentes de segurança (sn_si_aw) 1.5.1 ou posterior por padrão. Para obter mais informações sobre as aplicações dependentes, consulte a seção Espaço SIR plug-ins e funções.
- Observe que as versões 1.5.1 e superiores do Espaço de resposta a incidentes de segurança só podem ser instaladas/atualizadas por meio de uma instalação/atualização do Security Incident Response e não podem ser instaladas independentemente.

Mais recursos

Visite o Security Incident Response fórum no ServiceNow Community.

Exploração do Espaço SIR

Explore Espaço de resposta a incidentes de segurança para entender como os analistas e gerentes de segurança executam suas operações diárias com uma experiência do usuário aprimorada, fazem uma investigação de incidentes completa e obtêm uma visão geral dos incidentes de segurança, tarefas de resposta e ANS atribuídos ao analista de segurança e equipe.

Esta seção descreve o seguinte:

- Espaço SIR plug-ins e funções necessárias.
- Recursos de chave Espaço SIR.

Espaço SIR plug-ins e funções

A seguir estão as aplicações necessárias para trabalhar com o plug-in Espaço de resposta a incidentes de segurança (sn_si_aw).

Aplicações

A instalação da versão 13.4.5 ou posterior da aplicação [Security Incident Response instala automaticamente a Espaço de resposta a incidentes de segurança e as seguintes aplicações.

- Componentes comuns do PAD de gestão de casos de segurança empresarial [sn_escm_pad_cmn]
- Espaço comum de Operações de segurança [sn_escm_ws_cmn]
- Componente do cartão de IU de incidente de segurança [sn_sirw_evam]
- Spoke das Operações de segurança [sn_sec_spoke]

Importante:

- A instalação da versão Security Incident Response 13.4.5 ou posterior a partir de ServiceNow Store instalará automaticamente a versão Espaço de resposta a incidentes de segurança (sn_si_aw) 1.5.1 ou posterior por padrão. Para obter mais informações sobre as aplicações dependentes, consulte a seção Espaço SIR plug-ins e funções.
- Observe que as versões 1.5.1 e superiores do Espaço de resposta a incidentes de segurança só podem ser instaladas/atualizadas por meio de uma instalação/atualização do Security Incident Response e não podem ser instaladas independentemente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enterprise Security Case Management PAD Commons requer o plug-in Playbook Experience [playbook_experience].

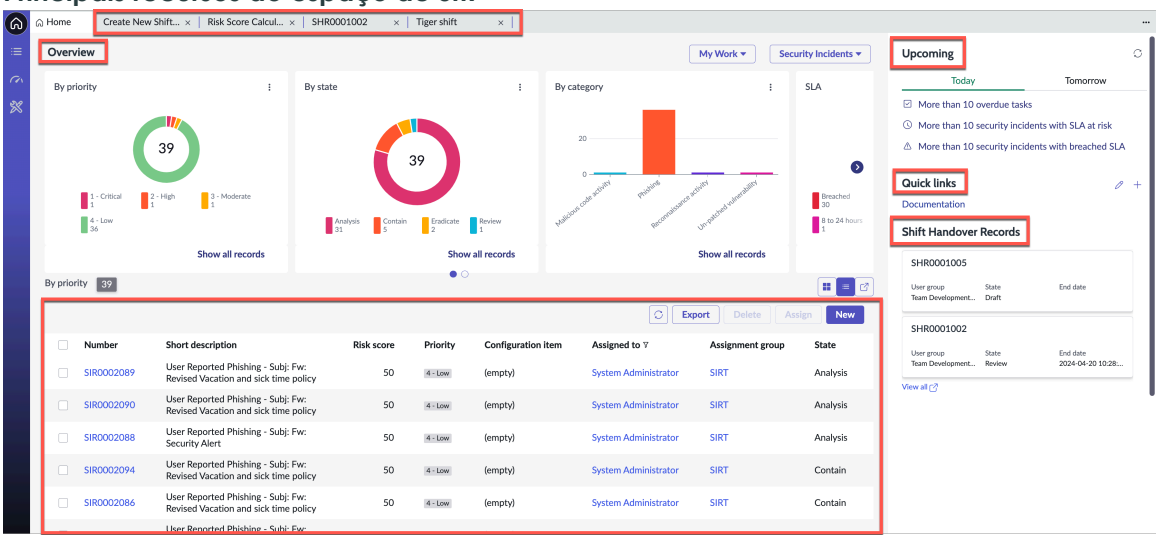
Para obter informações sobre Security Incident Response funções, tabelas, propriedades e trabalhos agendados, consulte Componentes instalados com Security Incident Response

Recursos do espaço SIR

O Espaço de resposta a incidentes de segurança consiste nos seguintes recursos principais.

- Seção de Visão geral
- Seção A seguir
- Seção Links rápidos
- Seção Registros de transferência de turno
- Exibição em lista
- Interface com várias guias que oferece suporte à abertura de vários incidentes de segurança

Principais recursos do espaço de SIR



Espaço SIR visão geral da interface

A página Espaço SIR Visão geral consiste nos detalhes dos Incidentes de segurança e Tarefas de resposta que estão sob os analistas de segurança e sua equipe.

Existem vários widgets presentes em cada filtro agrupado por prioridade, categoria, estado e ANS, que estão nas filas dos analistas de segurança e da equipe de analistas de segurança.

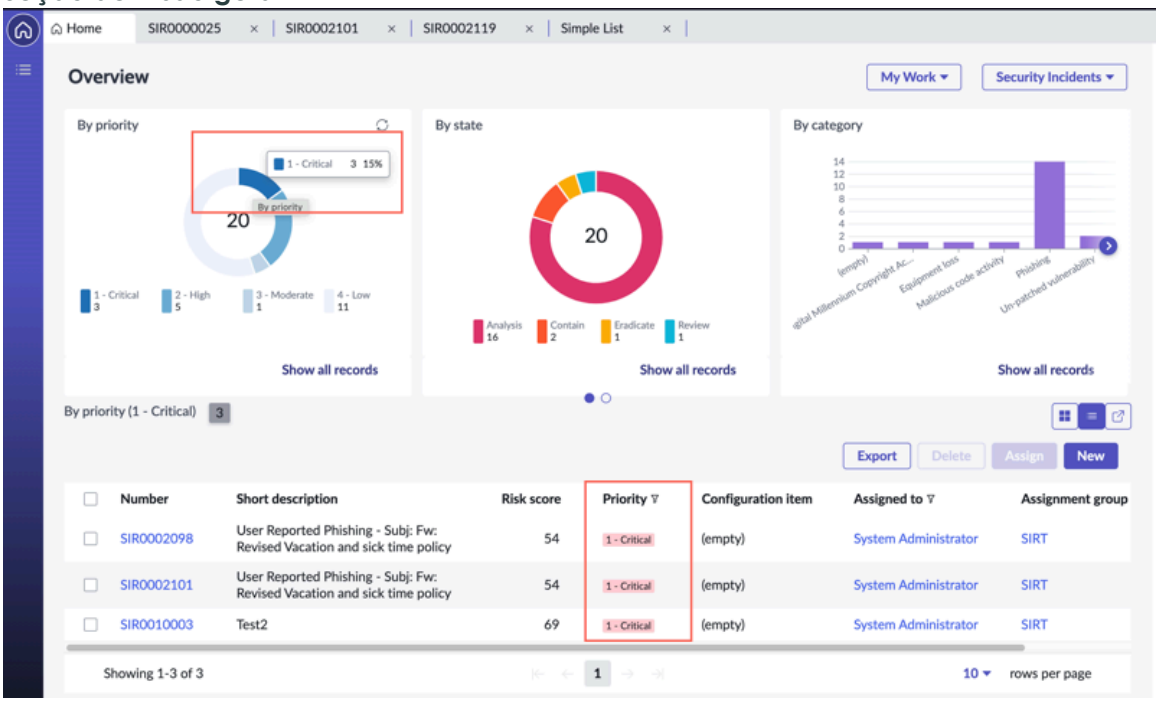
Quando os filtros são aplicados nos widgets, a metade inferior da página de visão geral é preenchida com os incidentes de segurança correspondentes ou tarefas de resposta apresentadas como cartões ou itens de lista. O analista pode alternar entre a exibição do cartão ou a exibição de lista, conforme desejado.

Por exemplo, no widget **Prioridade**, se você quiser selecionar todos os incidentes críticos ou tarefas de resposta, clique no segmento **Crítico** (exemplo de captura de tela abaixo) do widget e os incidentes ou tarefas de resposta que são críticos serão exibidos na lista ou no cartão exibição.

Tradução automática

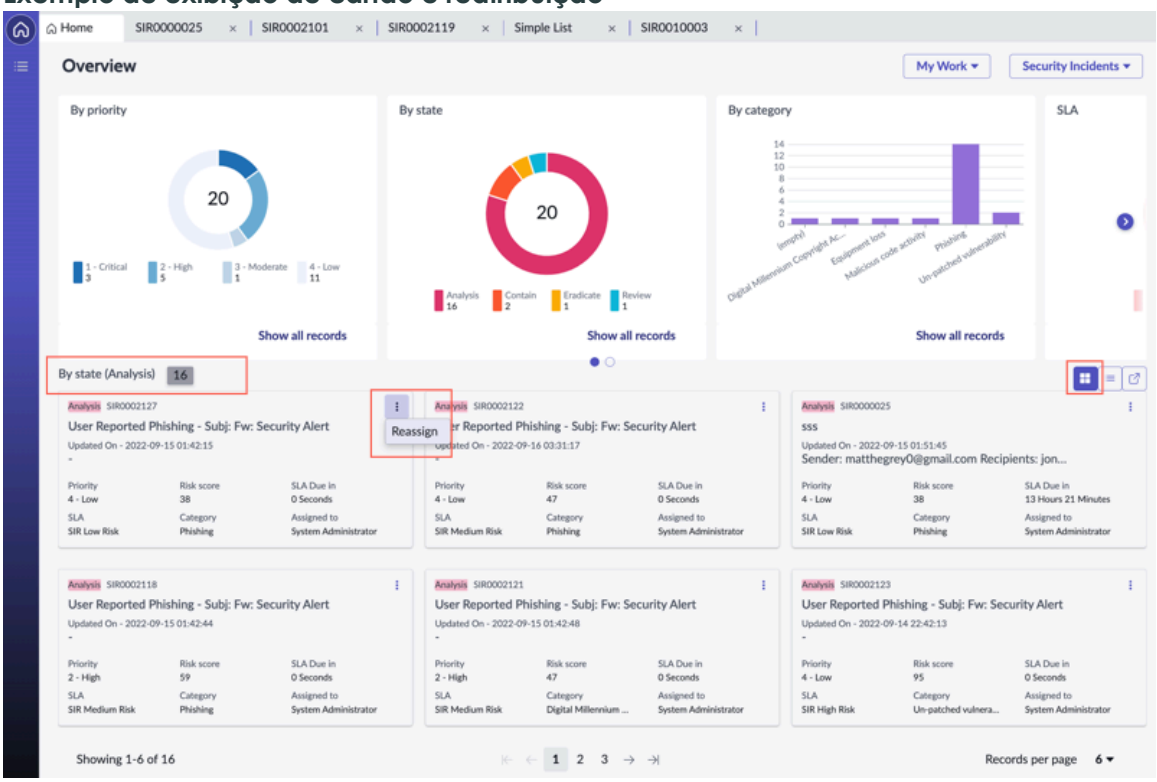
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção de Visão geral



Você pode atribuir ou reatribuir os incidentes de segurança ou tarefas de resposta diretamente nesta exibição, clicando no ícone de elipse e selecionando **Atribuir** (opção na exibição de cartão) ou diretamente o botão **Atribuir** (opção na exibição de lista) de acordo para atribuir um incidente.

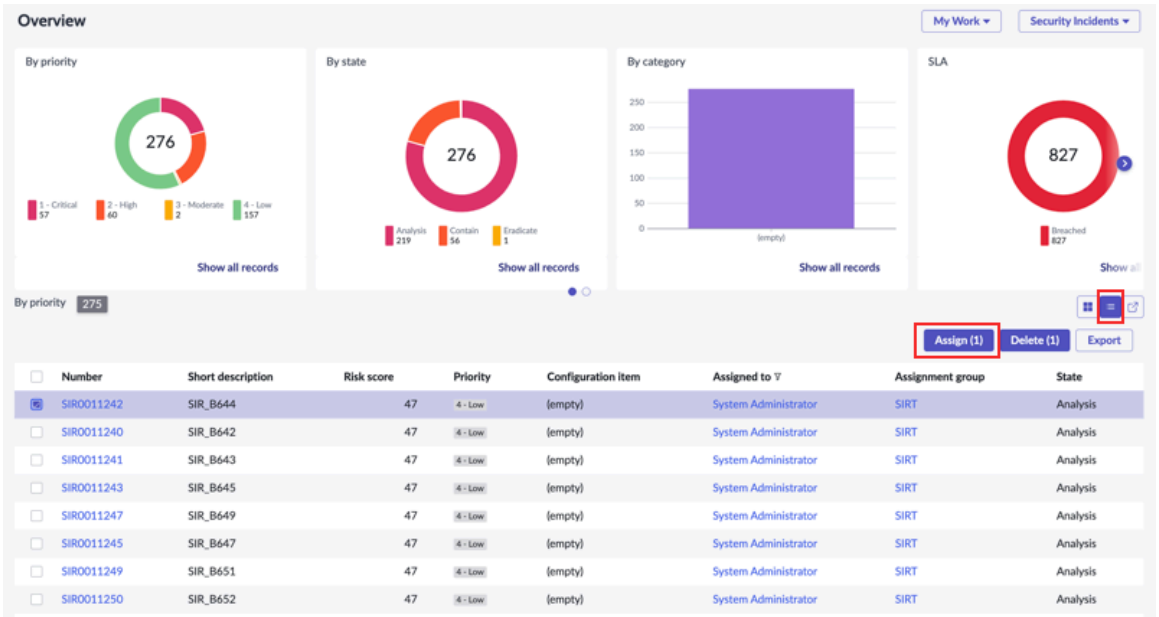
Exemplo de exibição de cartão e reatribuição



Tradução automática

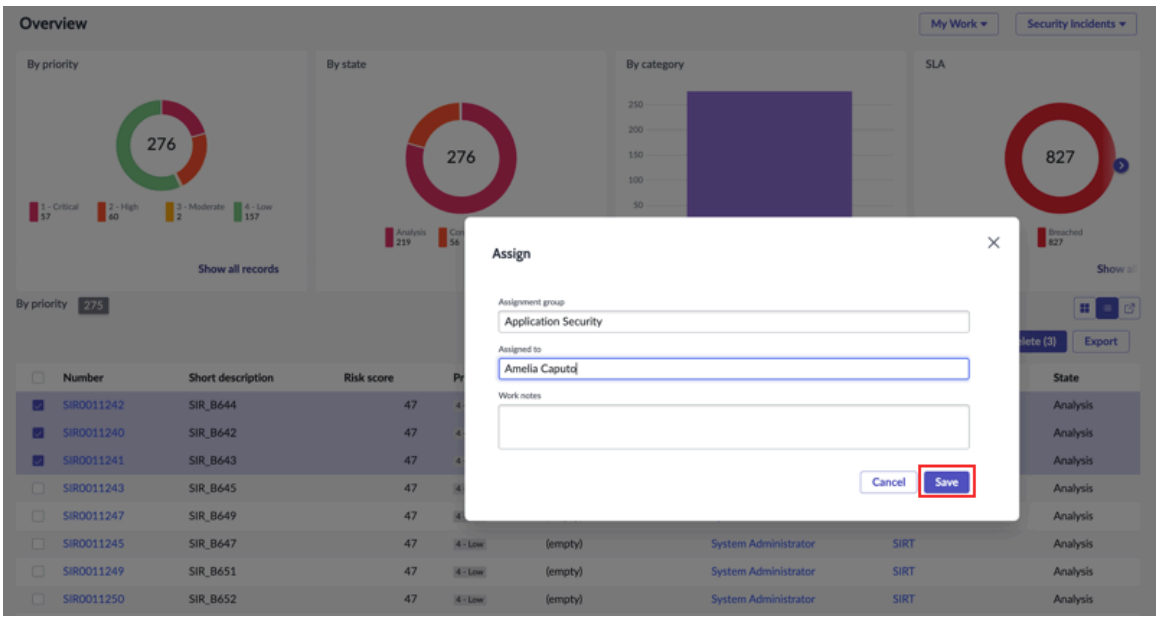
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuir incidente



Aqui está um exemplo da exibição de lista. O usuário também pode atribuir incidentes na exibição de lista.

Atribuir incidente



Adicione ou modifique os detalhes do atribuído, como Grupo de atribuição e Atribuído a, adicione anotações de trabalho, se necessário.

Nota: Você pode atribuir um ou mais incidentes de segurança ou tarefas de resposta aos grupos de atribuição. O número selecionado é exibido no botão **Atribuir**.

O usuário pode excluir incidentes de segurança nesta exibição. Clique no botão **Excluir** para excluir o incidente de segurança. O registro será excluído da exibição de lista.

O usuário também pode exportar o conteúdo da lista. Clique no botão **Exportar** para exportar a lista no formato desejado.

Tradução automática

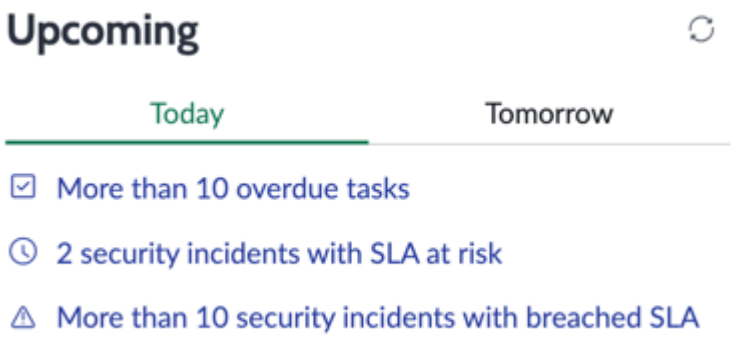
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção A seguir

Esta seção exibe as tarefas futuras, como os incidentes de segurança e as tarefas de resposta que vencem no mesmo dia e no dia seguinte.

A lista de incidentes de segurança e tarefas de resposta exibida é baseada no campo de data de vencimento e na definição do ANS definida para esses registros.

Se esta seção contiver mais de um incidente de segurança ou tarefa de resposta, o incidente ou os registros abrirão todos esses registros em uma nova guia.



Exibir tarefas futuras

O analista de segurança pode exibir as próximas tarefas relacionadas aos incidentes de segurança e tarefas de resposta que estão vencidas, atrasadas ou violaram o ANS definido.

Antes de Iniciar

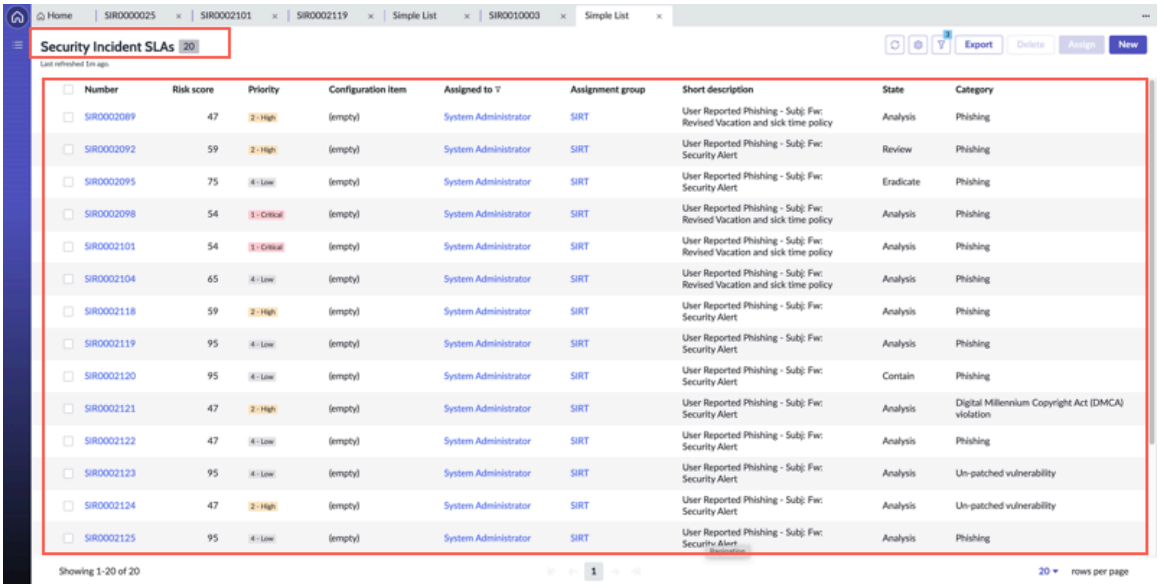
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Futuro**.
2. Clique na guia **Hoje** para exibir as tarefas que vencem no mesmo dia.
3. Selecione a guia **Amanhã** para exibir as tarefas que estão atrasadas para o dia seguinte.
   A próxima seção lista os incidentes de segurança ou tarefas de resposta que estão atrasados com base na data de vencimento e que violaram a definição do ANS.
4. Clique no ícone **Atualizar** para atualizar a lista de seções futuras.
   Por exemplo, se você clicar no link **Mais de 10 incidentes de segurança com ANS violado**, a lista de incidentes de ANS violados será exibida em uma nova guia no espaço.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você pode executar as operações Novo, Atribuir, Exportar e Excluir em qualquer exibição de lista.

Seção de links rápidos

Links rápidos funcionam como links de favoritos. Você pode adicionar URLs externos e acessá-los rapidamente de dentro do espaço.

Como trabalhar com links rápidos

Adicione links rápidos para facilitar a referência.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

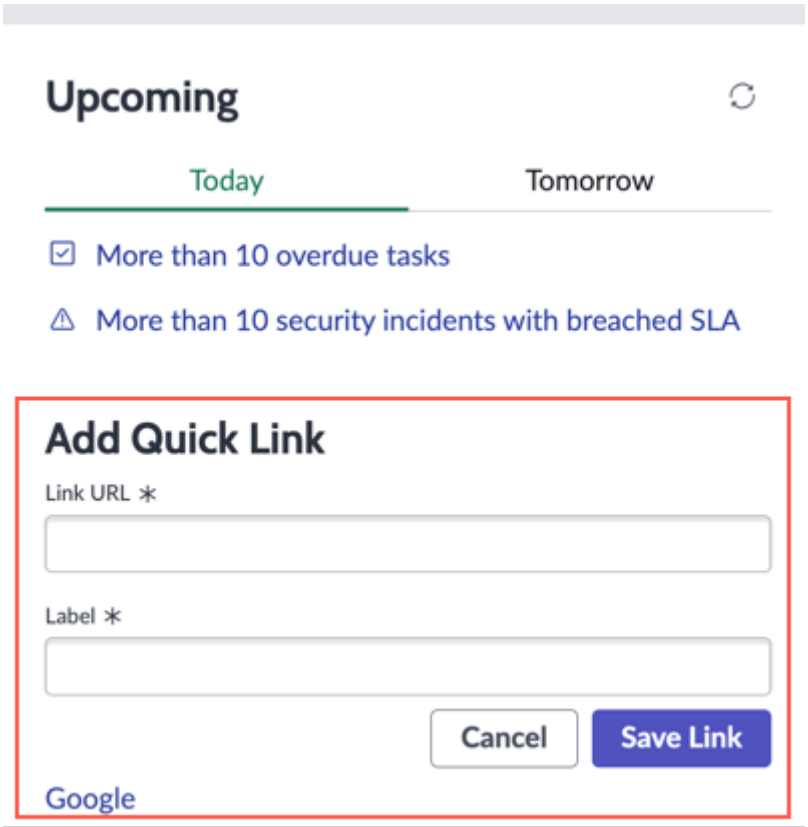
Você pode adicionar e modificar links rápidos úteis e marcar como favoritos esses links que ajudam na resolução do incidente.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Links rápidos**.
2. Clique no ícone **Adicionar link rápido** para adicionar os links.
3. Insira o link para a URL e o rótulo.
4. Clique **em Salvar link**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O novo link é adicionado abaixo da seção de links rápidos.

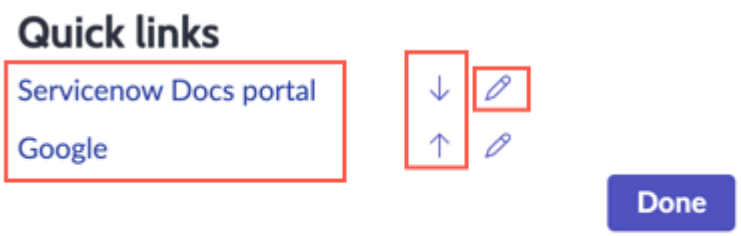
5. **Para modificar ou excluir os links:**

   a. Clique no ícone **Editar link**.

   b. Modifique o link desejado ou o texto de exibição que é o rótulo do URL.

   c. Clique em **Salvar**.

   d. Clique em **Concluído**.



   e. Use as setas para cima e para baixo para mover a posição dos links.

   f. Clique em **Excluir** para excluir os links marcados como favoritos durante a edição.

Seção Registros de transferência de turno

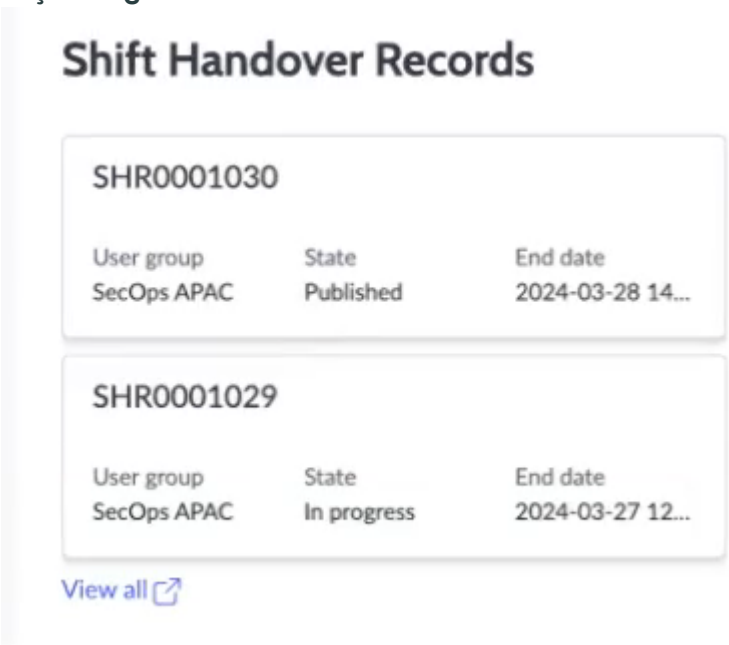
A seção exibe a lista de registros de transferência de turno no espaço do Security Incident Response Workspace.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seção Registros de transferência de turno no Espaço de resposta a incidentes de segurança exibe os dois últimos registros de transferência de turno com base nos campos Data de término, Estado e Grupo de usuários definidos para esses registros. Para exibir todos os registros de transferência de turno, selecione **Exibir tudo**.

Seção Registros de transferência de turno



Exibição de lista em Espaço SIR

A exibição de lista consiste em incidentes de segurança, tarefas de resposta, e-mails de phishing e avaliações.

A exibição de lista tem filtros pré-aplicados, como Atribuído a mim, Atribuído à equipe, Não atribuído, Todos em aberto, Todos e assim por diante.

Usando essas categorias de lista e listas filtradas, os analistas podem encontrar rapidamente os registros necessários de Incidentes de segurança e Tarefas de resposta nos quais precisam trabalhar.

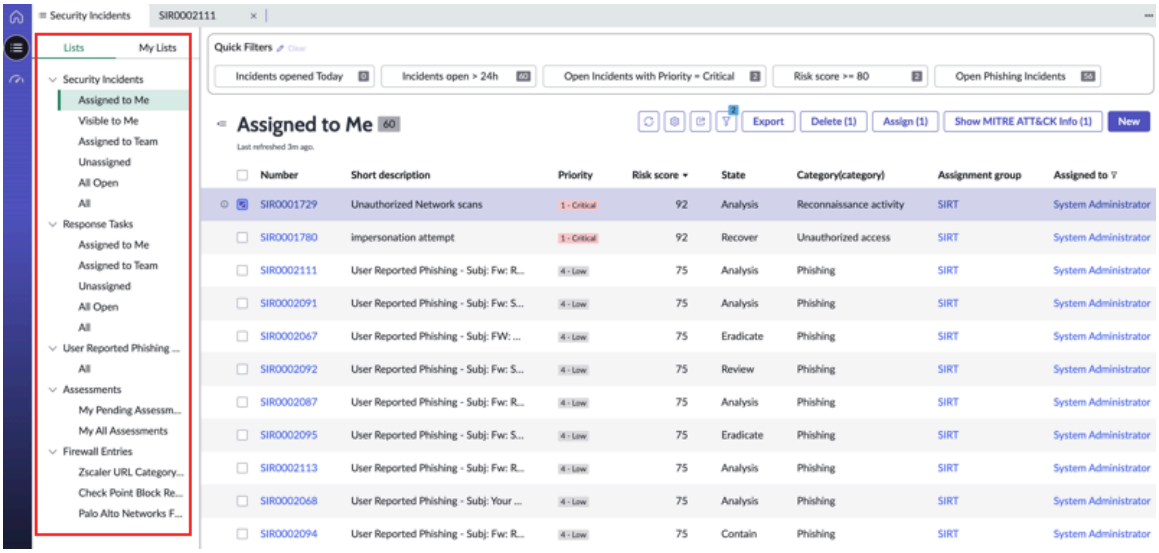
Para acessar a exibição de lista, clique no ícone de lista (de lista). Quando você clica em um registro em uma exibição de lista, o registro é aberto em uma nova guia.

Tipos de listas

Veja a seguir um exemplo de exibição das listas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O painel de lista contém as seguintes seções:

Listas

Item de lista	Descrição	Capacidade
Incidentes de segurança	Exiba a lista de incidentes de segurança e navegue até o incidente desejado para começar a trabalhar neles. As seguintes listas estão disponíveis: • **Visível para mim**: incidentes de segurança que estão visíveis para o usuário conectado. • **Atribuído a mim**: incidentes de segurança atribuídos ao analista. • **Atribuído à equipe**: incidentes de segurança atribuídos a todas as equipes às quais os analistas pertencem. • **Não atribuídos**: lista de incidentes de segurança não atribuídos. • **Todos em aberto**: lista de todos os incidentes de segurança em aberto. • **Todos**: lista de todos os incidentes de segurança.	• Na exibição de lista, o analista pode configurar a lista de colunas clicando no ícone de engrenagem que está disponível acima das colunas de incidentes. • O analista pode selecionar um ou mais incidentes de segurança e atribuir esses incidentes a outros usuários. • O analista pode excluir os incidentes de segurança. • O analista pode criar um novo incidente de segurança. • O analista pode aplicar os filtros rápidos. Aplique os filtros clicando na opção **Filtros rápidos** em vez de usar a opção **Filtro** avançado. Usando os filtros rápidos, você pode filtrar rapidamente a lista de incidentes de segurança que precisam de atenção imediata. Para obter mais informações, consulte Como trabalhar com filtros rápidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
		• Os analistas podem atualizar a lista de incidentes. • O analista pode exportar a exibição de lista para os formatos Excel, CSV, JSON e PDF.
Registros de transferência de turno	Exibir a lista de registros de transferência de turno. As seguintes listas estão disponíveis: • **Atribuído à equipe**: registros de transferência de turno atribuídos a todas as equipes/grupos de usuários aos quais os analistas pertencem. • **Todos**: lista de todos os incidentes de segurança.	A transferência de turno é compatível com as três funções a seguir: • Administrador: função de proprietário do turno • Analista de segurança: função de analista de turno • Gerenciador de segurança: a função de proprietário do turno, mas não tem acesso ao grupo de usuários ao qual o registro de transferência de turno está atribuído. • Os usuários com a função de Proprietário/Analista de turno que fazem parte do grupo de usuários no turno ativo podem adicionar ou modificar o conteúdo nos registros de transferência de turno no estado de rascunho. • Os usuários que não têm a função de Proprietário/ analista de turno ou que não fazem parte do grupo de usuários no turno ativo só podem exibir o conteúdo nos registros de Transferência de turno.
Tarefas de Resposta	Exiba a lista de tarefas de resposta e navegue até a tarefa de resposta desejada para começar a trabalhar nelas. A exibição de lista contém:	• Na exibição de lista, o analista pode configurar a lista de colunas clicando no ícone de engrenagem que está disponível acima das colunas de incidentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
	• **Atribuído a mim**: tarefas de resposta atribuídas ao analista. • **Atribuído à equipe**: tarefas de resposta atribuídas às equipes às quais os analistas pertencem. • **Não atribuídos**: lista de tarefas de resposta não atribuídas. • **Todas em aberto**: lista de todas as tarefas de resposta em aberto. • **Todos**: lista de todas as tarefas de resposta.	• O analista pode selecionar uma ou mais tarefas de resposta e atribuir essas tarefas a outros usuários. • O analista pode criar uma nova tarefa de resposta. • O analista pode aplicar os filtros rápidos. Aplique os filtros clicando na opção **Filtros rápidos** em vez de usar a opção **Filtro** avançado. Usando os filtros rápidos, você pode filtrar rapidamente a lista de tarefas de resposta que precisam de atenção imediata. • Os analistas podem atualizar a lista de tarefas de resposta. • O analista pode exportar a exibição de lista para os formatos Excel, CSV, JSON e PDF. Para obter mais informações, consulte Exportar incidentes de segurança ou tarefas de resposta.
E-mails de Phishing	Exibir a lista de todos os e-mails de phishing. A exibição de lista será classificada com base na última atualização.	• Denunciar e-mail de phishing. Para obter mais informações, consulte Relatar E-mail de Phishing sobre como denunciar um e-mail de phishing. • Excluir e-mails de phishing. • Exporte a exibição de lista de e-mails de phishing para os formatos Excel, CSV, JSON e PDF.
Avaliações	Exiba a lista de avaliações necessárias para executar a análise pós-incidente.	Fazer avaliações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
	• **Minhas avaliações pendentes**: lista de avaliações pendentes. • **Minhas todas as avaliações**: lista de todas as avaliações.	

Personalizar uma lista

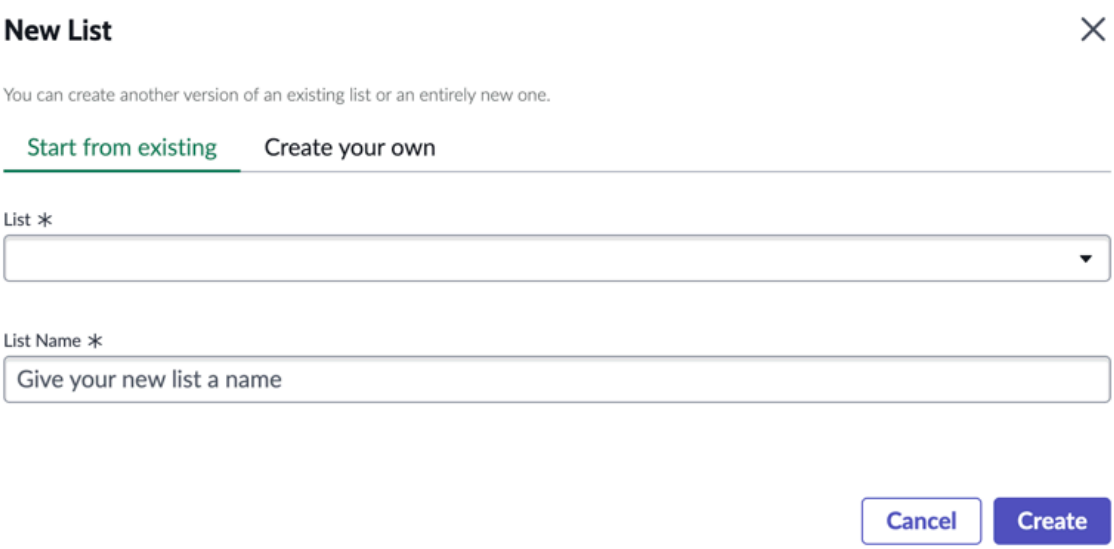
Os analistas ou gerentes de segurança podem personalizar os incidentes de segurança ou tarefas de resposta ou exibição de lista personalizada de e-mails de phishing com base em suas preferências individuais.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique **em Exibição de lista**.
3. Clicar **Minhas listas**.
4. Clique em **Adicionar nova lista**, disponível na parte inferior da exibição **Minhas listas**.



Os analistas de segurança podem criar outra versão de uma lista existente ou uma lista personalizada totalmente nova.

5. **Para criar a partir de uma exibição de lista existente:**

   a. Clique no link **Iniciar a partir de um existente**.

   b. Selecione a **Lista** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

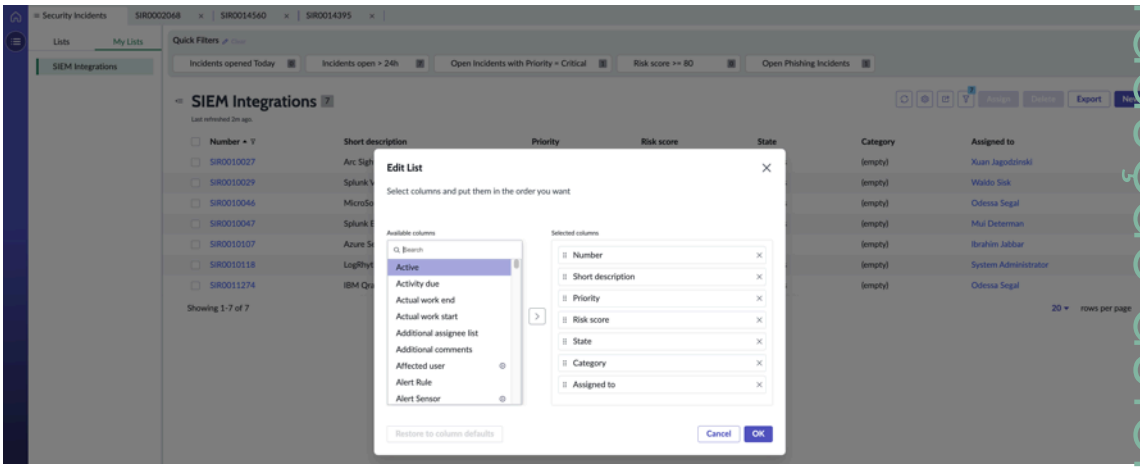
Nota: Qualquer que seja a lista selecionada na lista suspensa, o nome da lista será a cópia da lista principal. Por exemplo, se você selecionar **Atribuído a mim** na seção de incidentes de segurança, o nome da lista será **Atribuído a mim Cópia** da seção de incidentes de segurança.

c. Selecione as colunas a serem personalizadas e adicione filtros.
Crie um filtro adicionando condições que contenham um campo, operador e valor(es).

d. Clique em **Criar**.

Nota: Para personalizar sua própria exibição de lista, você pode adicionar colunas personalizadas, filtros, definir condições e classificar pela ordem conforme necessário.

e. Depois que uma exibição de lista personalizada for criada, clique no ícone de engrenagem e personalize as colunas da lista escolhendo a opção **Editar colunas** para editar as colunas e colocá-las na ordem que você preferir.



Você também pode:

- **Renomeie** a exibição de lista personalizada.
- **Exclua** a exibição de lista personalizada.
- Salve a exibição de lista personalizada conforme desejado usando a opção **Salvar como**.
- **Redefina a largura** da exibição de lista.

Nota: Você também pode executar diretamente essas operações usando os outros botões Ações da lista, como atribuir, excluir e exportar a exibição de lista que são fornecidos.

6. Para criar sua própria lista:

a. Clique em **Criar seu próprio** link.

b. Forneça um **Nome de lista**.

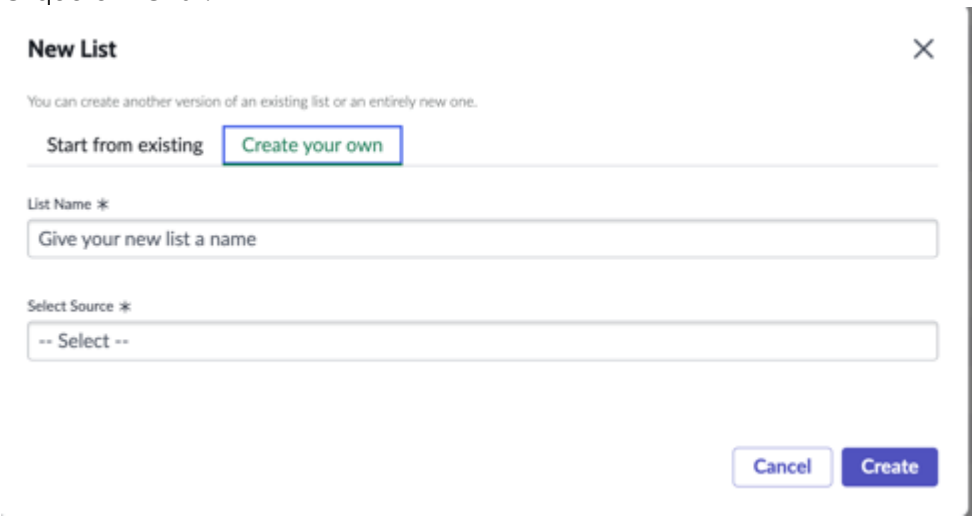
c. Selecione a **Origem** e as **Colunas**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Adicionar filtros.
Crie um filtro adicionando condições e forneça a ordem em que a lista deve aparecer.

e. Clique em **Criar**.



Uma nova lista é criada conforme definido e personalizado por você abaixo da seção **Minhas listas**.

Nota: você pode **reordenar** sua exibição personalizada movendo suas posições.

Atribuir incidentes de segurança

Atribuir incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

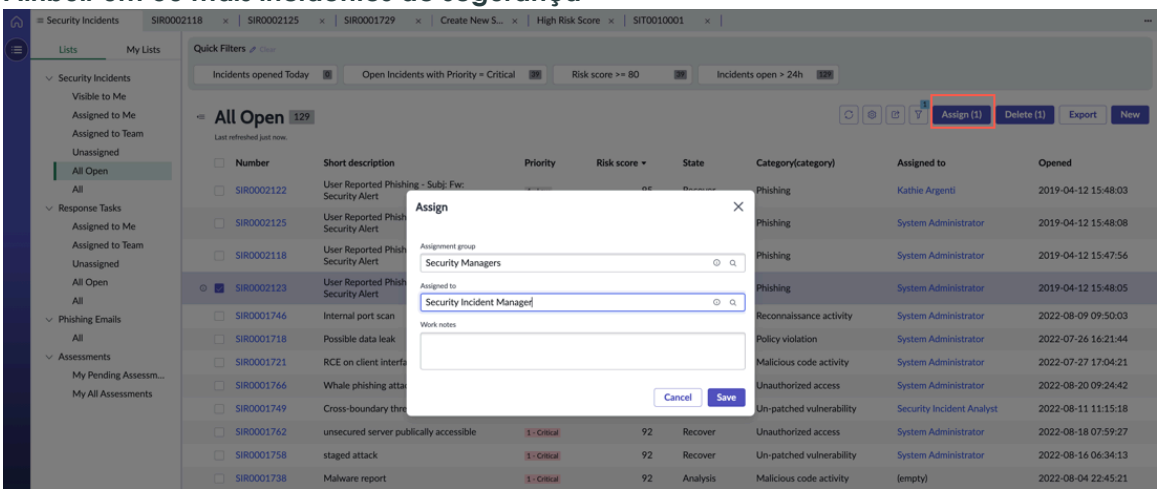
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Clique **em Listas**.
4. Por exemplo, vá para **Incidentes de segurança** > **Todos em Aberto**.
5. Selecione um ou mais incidentes de segurança.
6. Clique **em Atribuir**.
7. Preencha os detalhes, como Grupo de atribuição, Atribuído a, e adicione Anotações de trabalho, se necessário.
   O incidente será atribuído ao usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Salvar**.

Atribuir um ou mais incidentes de segurança



Atribuir tarefas de resposta

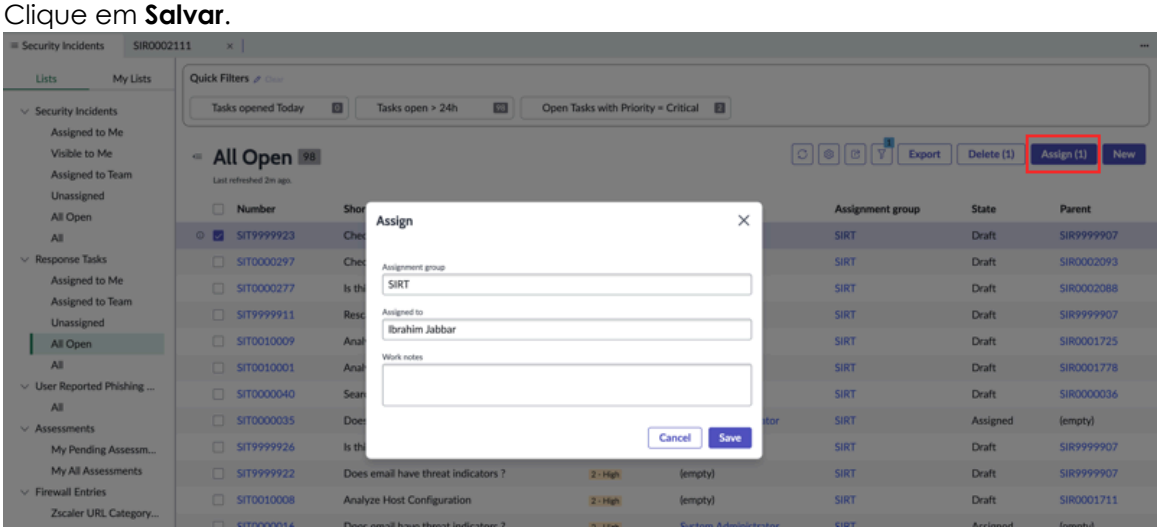
Atribuir tarefas de resposta para um problema de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Clique **em Listas**.
   Por exemplo, vá para **Tarefas de Resposta** > **Todos em Aberto**.
4. Selecione uma ou mais tarefas de resposta.
5. Clique **em Atribuir**.
6. Preencha os detalhes, como Grupo de atribuição, Atribuído a, e adicione Anotações de trabalho, se necessário.
   O incidente será atribuído ao usuário.
7. Clique em **Salvar**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatar E-mail de Phishing

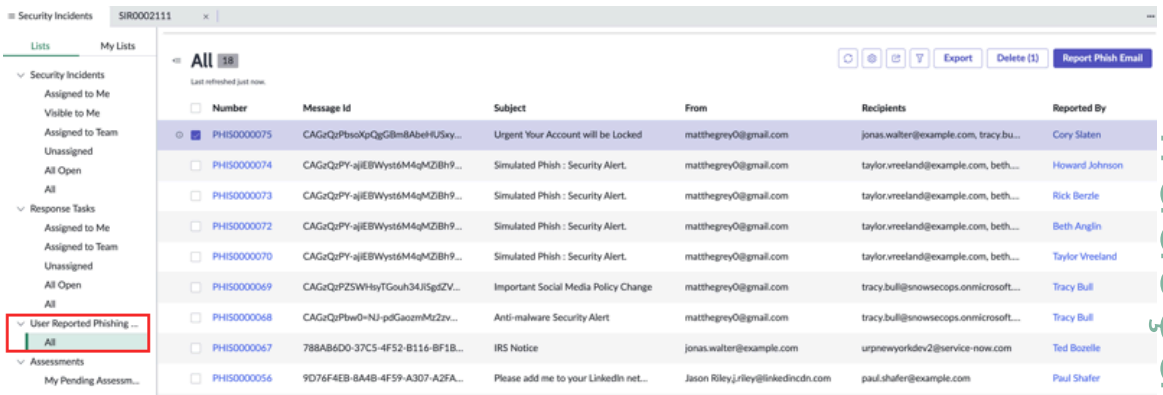
Relate e-mails de phishing na exibição de listas.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Ir para **E-mails de phishing relatados por usuário** > **Todos**.
   A lista de e-mails de phishing relatados pelo usuário é exibida.



4. Clique no botão **Denunciar e-mail de phishing**.
   Relate um e-mail de phishing carregando-o.
5. Clique em **Adicionar arquivo** para adicionar anexos.
6. Clique em **Carregar**.

> **Nota:** Relate um e-mail de phishing carregando os anexos. Você pode carregar apenas um e-mail de phishing por vez e deve estar no formato .eml.

7. Clique em **Enviar**.
   O e-mail de phishing para registrar um incidente de segurança foi criado.

Como trabalhar com filtros rápidos

Filtros rápidos são filtros de fácil acesso que estão disponíveis em, incidentes de segurança e listas de tarefas de resposta.

Antes de Iniciar

Função necessária: sn_si.admin

O Espaço SIR fornece o recurso de filtros rápidos que permite filtrar a lista de incidentes de segurança ou tarefas de resposta com facilidade.

Você pode usar filtros rápidos para configurar novos filtros ou modificar os filtros existentes que aparecem nessas listas. O sistema de base fornece os seguintes filtros rápidos para cada incidente de segurança:

- **Incidentes abertos hoje**
- **Incidentes em aberto > 24 horas**
- **Incidentes em aberto com Prioridade= Crítica**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Risco >= 80**
- **Incidentes de phishing abertos**

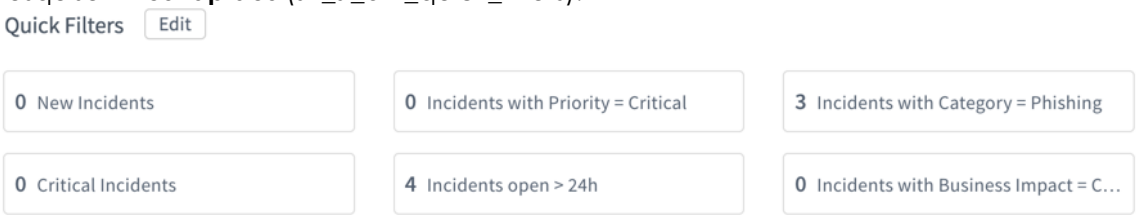
O sistema de base fornece os seguintes filtros rápidos para cada tarefa de resposta:

- **Tarefas em aberto > 24h**
- **Tarefas em aberto com Prioridade = Crítica**

Nota: Um administrador pode configurar a lista necessária de filtros rápidos de acordo com a necessidade da organização.

Procedimento

1. Navegar até **Definição do Sistema** > **Tabelas**.
2. Pesquise **filtros rápidos** (sn_si_aw_quick_filters).



3. Ir para **Links relacionados** > **Mostrar lista** seção.
   A página da lista de **Filtros rápidos** é exibida. OOTB, a seguir está a lista de filtros rápidos enviados com a aplicação.

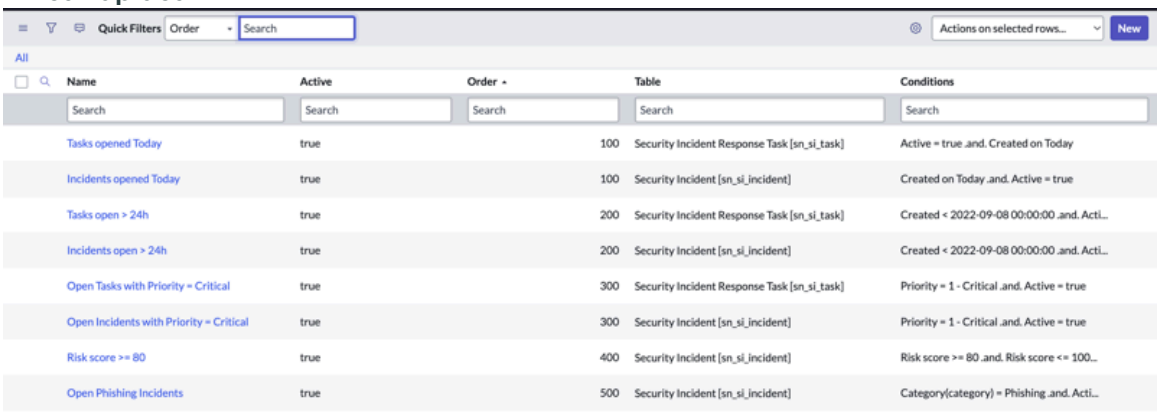
Nome	Tabela	Valor
Tarefas abertas hoje	Tarefa de incidente de segurança [sn_si_task]	Verdadeiro
Incidentes abertos hoje	Incidente de segurança [sn_si_incident]	Verdadeiro
Tarefas em aberto > 24h	Tarefa do Security Incident Response [sn_si_task]	Verdadeiro
Incidentes em aberto > 24h	Incidente de segurança [sn_si_incident]	Verdadeiro
Tarefas em aberto com Prioridade = Crítica	Tarefa do Security Incident Response [sn_si_incident]	Verdadeiro
Incidentes em Aberto com Prioridade = Crítica	Incidente de segurança [sn_si_incident]	Verdadeiro
Pontuação de risco >= 80	Incidente de segurança [sn_si_incident]	Verdadeiro
Incidentes de phishing abertos	Incidente de segurança [sn_si_incident]	Verdadeiro

Nota: O administrador de segurança pode prosseguir e configurar esses filtros rápidos. De acordo com a necessidade do negócio, o administrador pode modificar o valor existente para falso e criar um novo filtro rápido.

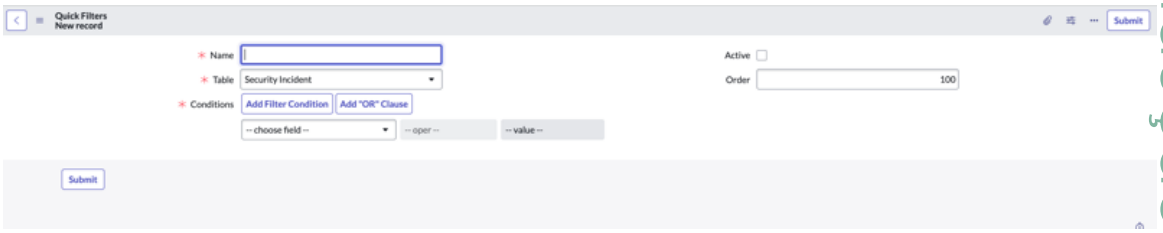
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtros Rápidos



4. Clique em **Novo** para criar um novo filtro.
5. Insira um nome para o filtro, selecione a Tabela e especifique a condição do filtro.
6. Clique em **Enviar** para retornar à página da lista anterior.
   Você verá o filtro recém-adicionado listado na página.

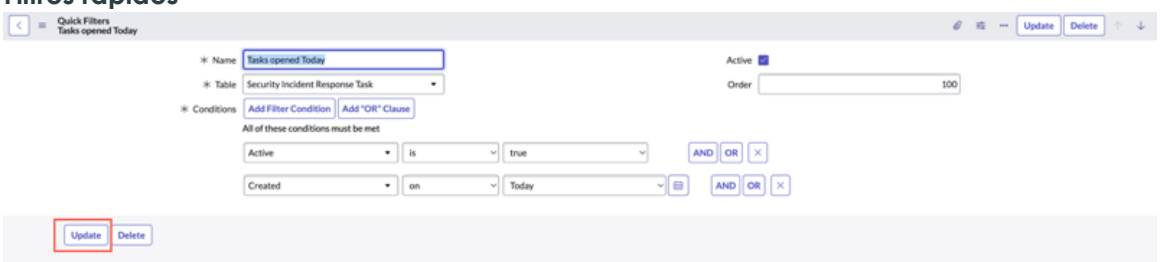


Nota:

- O filtro rápido será aplicável somente se a caixa de seleção **Ativo** estiver marcada.
- No espaço, qualquer usuário conectado pode personalizar os filtros rápidos ativos que estão disponíveis na aplicação. Os usuários podem ocultar ou reexibir os filtros rápidos recém-criados. Este recurso se baseia na preferência do usuário.
- Se um usuário tiver modificado as preferências de filtros rápidos e um novo filtro rápido for criado depois disso, se o filtro rápido estiver definido como ativo, ele não será aplicado à preferência do usuário. O usuário precisa alterar manualmente as preferências na exibição personalizada.

7. Selecione qualquer registro de filtro existente para modificar os filtros rápidos existentes.
8. Modifique o nome e a condição do filtro.
9. Clique em **Atualizar**.

Filtros rápidos



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar ou modificar filtros rápidos

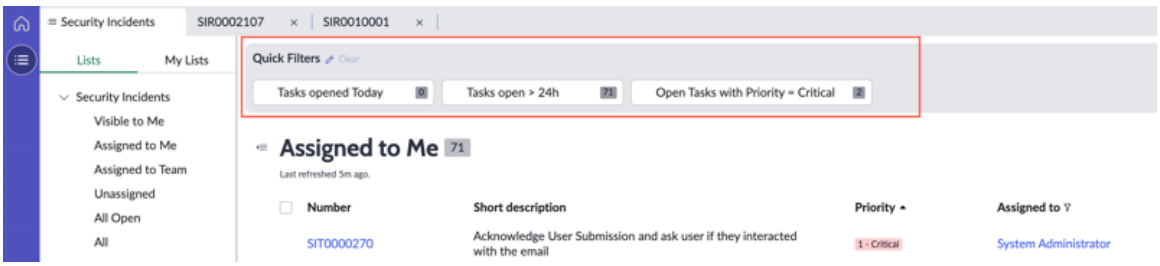
Adicione ou modifique filtros rápidos para incidentes de segurança ou tarefas de resposta na exibição de lista.

Antes de Iniciar

Função necessária: sn_si.basic

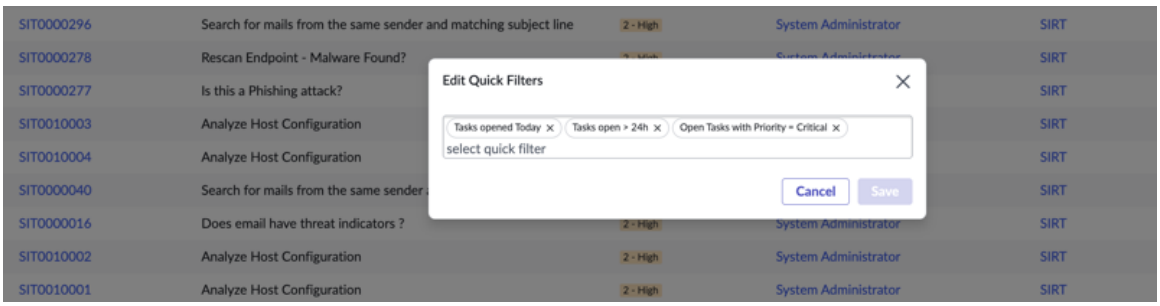
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Por exemplo, vá para **Listas** > **Incidentes de segurança** > **Filtros Rápidos** seção.



4. Clique no ícone **Editar** para fazer as mudanças.

> **Nota:** A mudança que você fizer será mantida e, quando o usuário retornar a esta página na próxima vez, a preferência persistente será exibida.



5. Clique em **Salvar**.

Exportar incidentes de segurança ou tarefas de resposta

Exporte os incidentes de segurança ou as tarefas de resposta da exibição de lista.

Antes de Iniciar

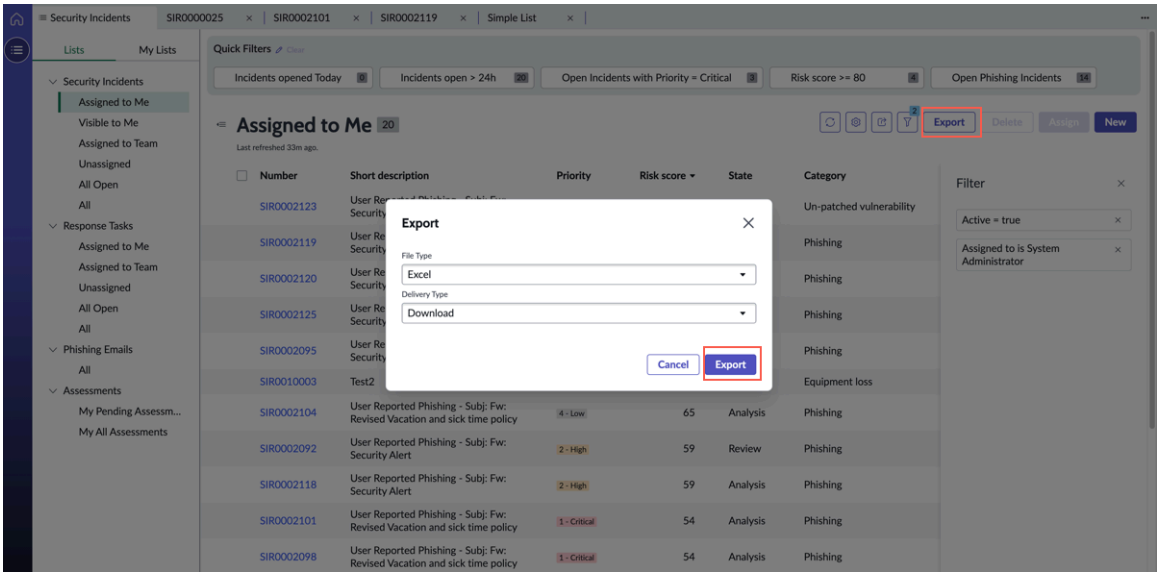
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de lista .
3. Clique **em Listas**.
4. Ir para **Incidentes de segurança ou tarefas de resposta** > **Todos em Aberto**.
5. Exiba a lista e clique em **Exportar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione o Tipo de **arquivo e o Tipo** de **entrega**.
   Por exemplo, **Excel** e **Baixar** ou Enviar e- **mail** da lista.
7. Clique em **Exportar**.
   O arquivo será baixado ou enviado por e-mail de acordo com a opção escolhida.

Gerenciar registros de transferência de turno

Use a exibição de lista de registros de transferência de turno para criar, editar, copiar ou excluir registros de transferência de turno. Cada registro de transferência de turno está associado a um modelo de relatório de transferência de turno.

Antes de Iniciar

Função necessária:

- sn_escm_sh.shift_analyst: requisito mínimo para acessar os registros de transferência de turno.
- sn_escm_sh.shift_owner: crie, edite e exclua registros de log de transferência nos grupos de usuários dos quais o proprietário do turno faz parte. Esta função herda a função sn_escm_sh.shift_analyst.
- sn_escm_sh.shift_analyst: exibe todos os registros de log de transferência de turno, mas só pode contribuir para registros de transferência de turno em andamento atribuídos ao grupo do analista de turno.
- sn_si.analyst - herda a função sn_escm_sh.shift_analyst.
- sn_si.admin - herda a função sn_escm_sh.shift_admin.
- sn_escm_sh.shift_admin — Herda a função sn_escm_sh.shift_owner

Importante: Para saber como configurar o modelo de transferência de turno como um administrador, consulte Configurar modelos de transferência de turno.

Por Que e Quando Desempenhar Esta Tarefa

O proprietário do turno e a respectiva equipe ou grupo de usuários criam os registros de log de transferência de turno. O proprietário do turno deve escolher o modelo de transferência de turno e o grupo de usuários que trabalharão no relatório de transferência de turno. Depois que o relatório de transferência de turno for concluído, ele será compartilhado com o próximo proprietário de turno ativo e a equipe.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontos-chave do modelo de transferência de turno:

- Se algum outro analista da equipe do turno ativo já tiver atualizado o relatório antes de você e se as mudanças estiverem sendo processadas, você poderá ver uma mensagem de erro informando que há atualizações de conteúdo pendentes. Você deve aguardar 30 segundos e selecionar **Mudar para o estado "Revisão"** novamente. Você pode ver o relatório consolidado no painel direito sendo atualizado com o conteúdo atualizado de outros analistas.
- Se o proprietário do turno tiver modificado o conteúdo de uma seção no estado Revisão, o mesmo conteúdo será refletido para o analista quando o registro voltar para o estado Em andamento.
- O proprietário do turno deve estar atento ao editar o conteúdo no estado Revisão e executar ações como mesclar duas linhas, mesclar duas seções, remover uma seção, pois isso afetará o relatório de transferência de turno dos outros analistas.
- Depois de publicar o relatório de transferência de turno, o proprietário do turno pode modificar o conteúdo, mas não pode mudar o estado do registro.
- Quando alguém estiver modificando o conteúdo e, durante esse tempo, se o estado do registro for alterado de Em andamento para Revisão, as mudanças de conteúdo não salvas serão descartadas.
- O administrador de turno terá acesso de gravação a todos os registros de log de transferência de turno, independentemente dos grupos de usuários.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione o Lista de incidentes de segurança.
3. Na guia **Listas**, selecione **Registros de transferência de turno**.
4. Selecione **Todos os registros** para exibir a lista de todos os registros de transferência de turno.
5. Selecione **Atribuído à equipe** para exibir a lista de registros de transferência de turno atribuídos a todas as equipes/grupos de usuários aos quais os analistas pertencem.
6. Para criar um novo registro de transferência de turno, selecione **Novo**.
7. No formulário, preencha os campos.

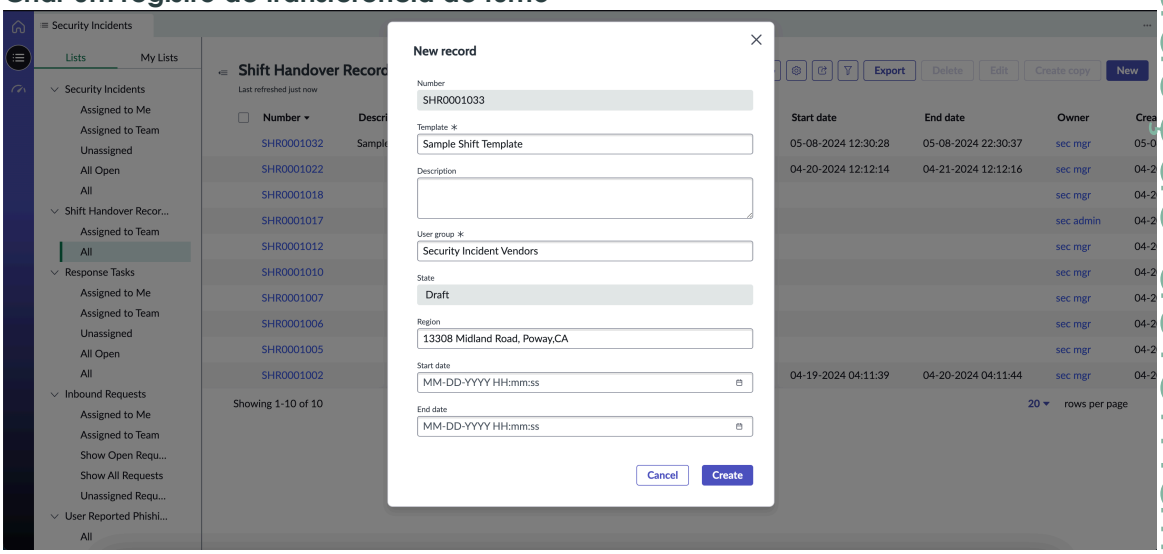
Campo	Descrição
Número	Número exclusivo que é gerado automaticamente para um registro de transferência de turno.
Modelo	Selecione o modelo de transferência de turno a ser usado. Por exemplo, Modelo de turno de amostra.
Descrição	Descrição do registro de transferência de turno.
Grupo de usuários	Selecione o Grupo de usuários/Equipe ao qual o registro de transferência de turno será atribuído. Por exemplo, Desenvolvimento da equipe Revisores de código.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	O estado atual do registro de transferência de turno. Por padrão, o estado inicial é Rascunho **Nota:** O estado não pode ser alterado durante a criação de um registro. .
Região	Selecione a região para a qual o registro de transferência de turno será atribuído. Por exemplo, APAC.
Data de início	Selecione a data de início do registro de transferência de turno.
Data de término	Selecione a data de término do registro de transferência de turno.

Criar um registro de transferência de turno



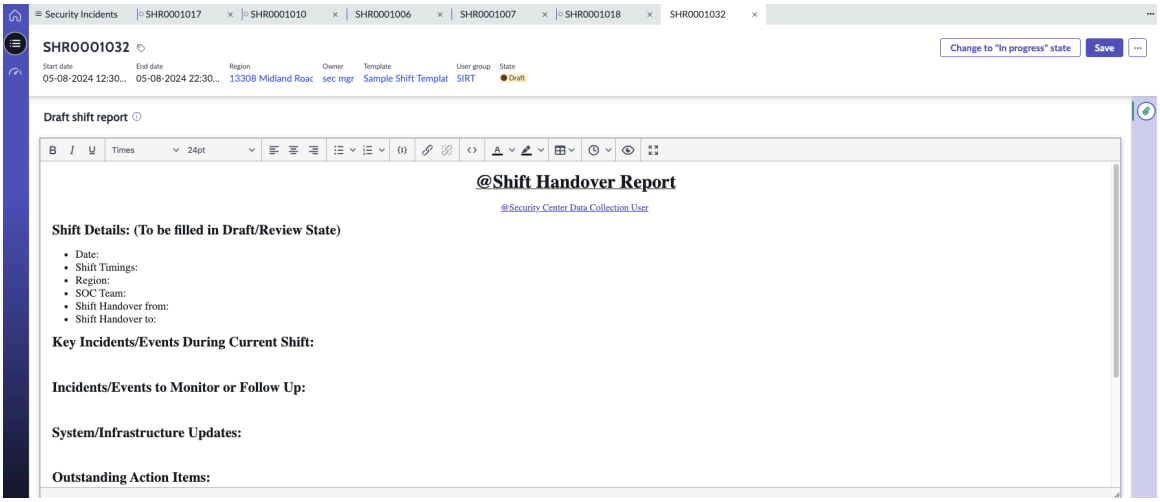
8. Selecione **Criar**.
   Um novo registro de Transferência de turno é criado com base no modelo que você selecionou e adicionou à exibição de lista.
9. Abra o novo registro de transferência de turno para atualizar o status e os detalhes dos incidentes de segurança no relatório de transferência de turno.
   Por padrão, o registro de Transferência de turno está no estado **Rascunho**.

Nota: Somente o proprietário do turno pode modificar o conteúdo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conteúdo do relatório de transferência de turno



10. No editor de relatório de turno de rascunho, use as seções de modelo de relatório de transferência de turno para atualizar os detalhes dos incidentes de segurança e dos usuários.

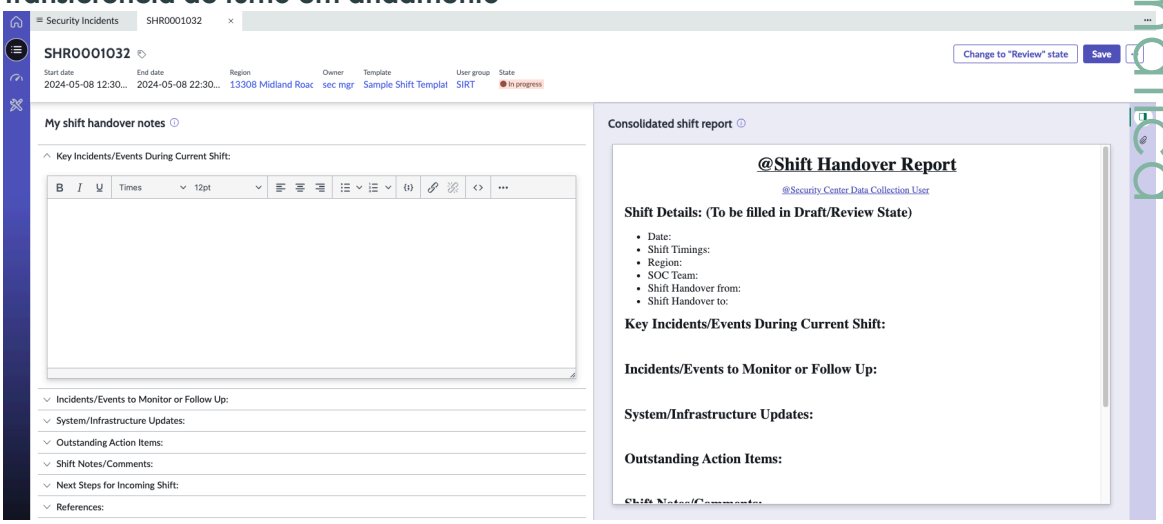
Você pode formatar seu relatório com todas as opções no editor, como fontes, cores, marcadores, links e anexos.

Nota: O proprietário do turno e o analista do turno podem modificar o conteúdo.

a. Depois de fazer as mudanças necessárias no relatório de transferência de turno, selecione **Salvar**.

b. Selecione a ação **Mudar para o estado "Em andamento"** para mover o registro de Transferência de turno para o estado Em andamento.

Transferência de turno em andamento



11. No editor de anotações de transferência do meu turno, atualize os detalhes necessários para todas as seções, como incidente de segurança e detalhes do usuário.

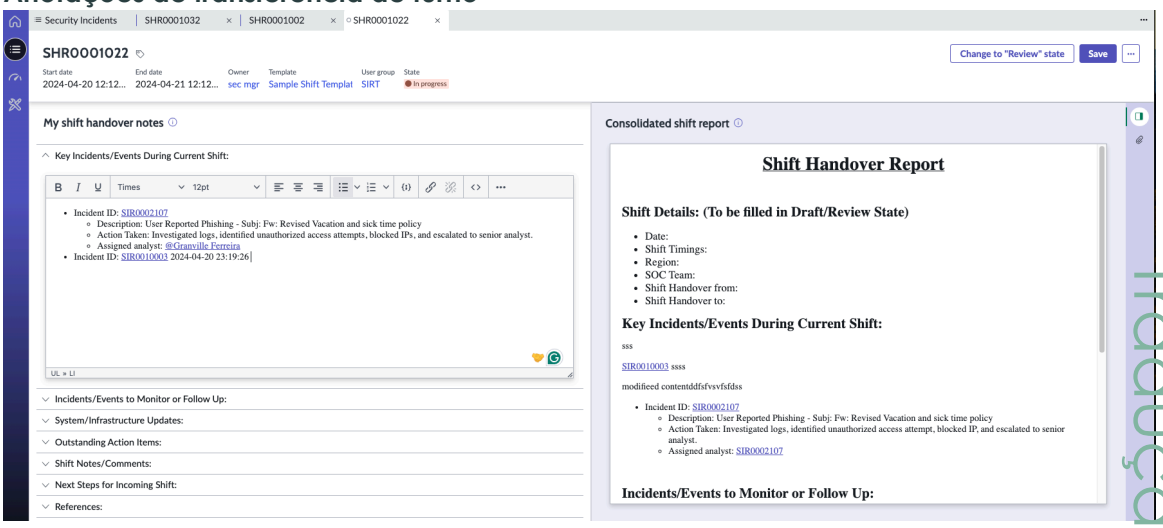
Nota: O proprietário do turno e o analista do turno podem modificar o conteúdo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para mencionar um registro específico no editor, use **/** e escolha **Selecionar um registro**e selecione um registro na lista de tabelas pop-up.
Por exemplo, se você selecionar o registro **de Incidentes de segurança**, uma lista de incidentes de segurança será exibida. Selecione um incidente de segurança (**SIR0010025**) na lista e atualize os detalhes de transferência de turno necessários.
Você também pode mencionar os campos associados ao incidente de segurança, como descrição resumida, observe o desejo usando **/** após o número do incidente de segurança.

Anotações de transferência de turno



b. Para mencionar um usuário específico no editor, use **/** e escolha **Selecionar um usuário**e selecione um usuário na lista pop-up.

c. Você pode formatar seu relatório com todas as opções no editor, como fontes, cores, marcadores, links e anexos.

d. Depois de fazer as mudanças necessárias nas anotações de transferência de turno, selecione **Salvar**.

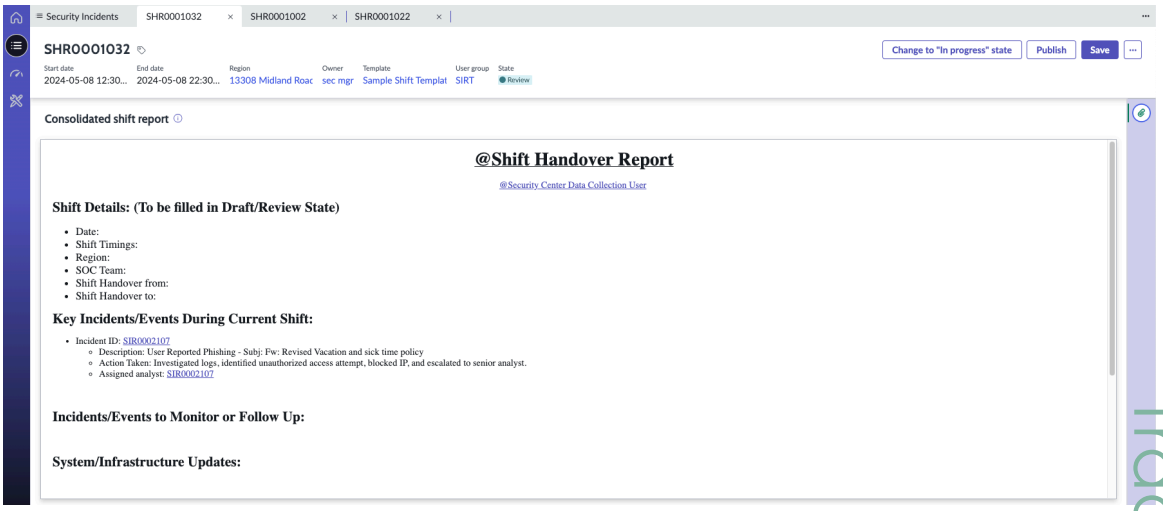
e. Selecione a ação de **estado Mudar para "Revisar"** para mover o registro de Transferência de turno para o estado Revisar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se algum outro analista da equipe do turno ativo já tiver atualizado o relatório antes de você e se as mudanças estiverem sendo processadas, uma mensagem de erro poderá ser exibida. Aguarde alguns segundos e selecione **Mudar para o estado "Revisão"** novamente.

Revisão de transferência de turno



12. No relatório de turno consolidado, revise o relatório de transferência de turno e faça as mudanças necessárias.

Nota: Somente o proprietário do turno pode modificar o conteúdo.

a. Depois de fazer as mudanças necessárias nas anotações de transferência de turno, selecione **Salvar**.

b. Se o relatório de transferência de turno exigir mais atualizações dos analistas, você poderá selecionar **Mudar para o estado "Em andamento"**.

c. Selecione **Publicar** ação para publicar o relatório de transferência de turno.

Publicação de transferência de turno

13. Selecione **Salvar** para salvar o relatório de transferência de turno.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de salvar, você pode ver uma visualização do relatório de transferência de turno com suas atualizações mais recentes no painel Visualização.

Nota: Embora você possa visualizar as atualizações feitas no relatório de transferência de turno imediatamente, os outros analistas podem levar alguns segundos para ver as mudanças.

14. Como proprietário de turno, você também pode executar as seguintes ações na exibição de lista de transferência de turno.

    a. Para editar um registro de Transferência de turno existente, selecione o registro e selecione a ação **Editar**.
    Você pode modificar somente a Hora de início, a Hora de término, a Descrição e a Região.

    b. Para criar uma cópia de um registro de transferência de turno, selecione o registro e clique em **Criar ação de cópia**.

    c. Para excluir um registro de Transferência de turno existente, selecione o registro e selecione a ação **Excluir**.

Configuração da Espaço SIR

Esta seção descreve as configurações necessárias para trabalhar com o Espaço de resposta a incidentes de segurança.

Configurar exibição de registros SIR

Esta seção descreve como as listas relacionadas são agrupadas e apresentadas na guia Registros relacionados SIR para facilitar a navegação.

Os usuários do espaço também podem pesquisar facilmente a lista relacionada por nome.

Configurar investigação de tempo de design de SI

Use esta seção para configurar a página de investigação do tempo de design do incidente de segurança para adicionar vários pontos de entrada e seus registros associados no Espaço de resposta a incidentes de segurança.

Função necessária: sn_si.admin.

A seguir detalhamos as etapas envolvidas na configuração da página de investigação no Espaço de resposta a incidentes de segurança.

- Criando exibição para tabelas de informações associadas
- Como adicionar uma lista de ponto de entrada
- Exibição de mapeamento das informações associadas à lista de ponto de entrada
- Configure cada lista associada da exibição para lidar com a renderização de dados em tempo de execução

Informações relacionadas

Explorar tela de investigação

Criando exibição para tabelas de informações associadas

A tela de investigação aproveita as exibições de lista relacionadas criadas no incidente de segurança para configurar as listas associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

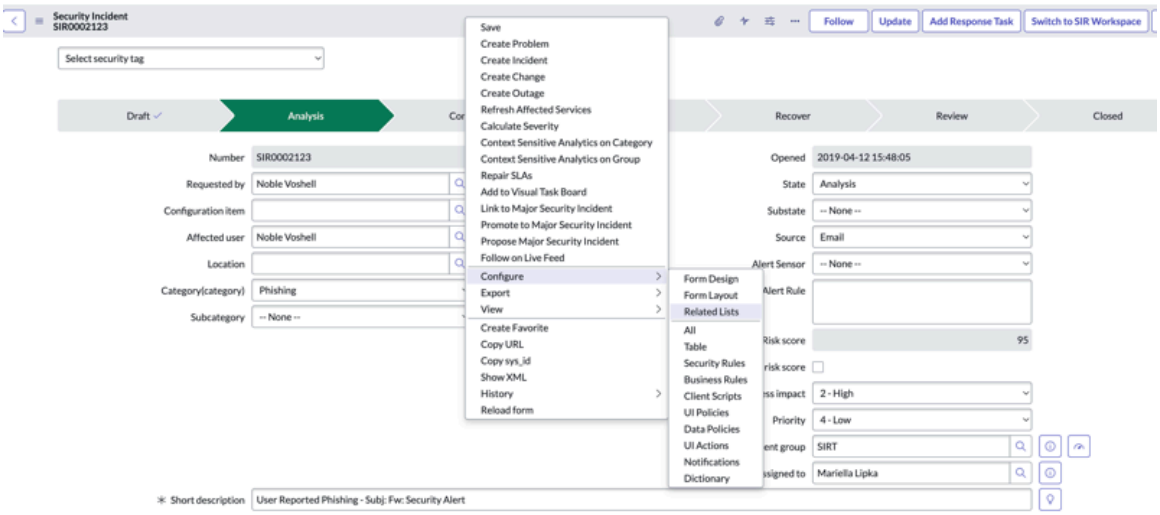
Antes de Iniciar

Função necessária: sn_si.admin

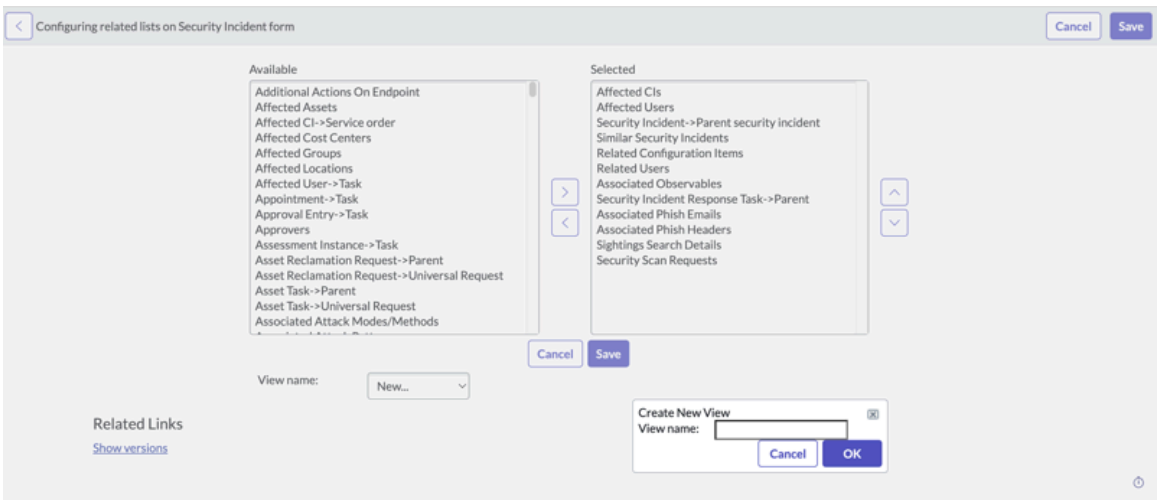
A seguir está um procedimento para criar uma exibição e adicionar listas relacionadas a ela.

Procedimento

1. Navegue até a Lista de **incidentes de segurança**.
2. Abra qualquer incidente de segurança na IU clássica.
3. No menu de contexto do formulário, navegue até **Configurar** > **Listas relacionadas**.
   A janela de bucket de slush é exibida.



4. Acesse a lista suspensa **Exibir nome** e clique em **Novo** para criar uma nova exibição.
   Você deve adicionar um nome à exibição.



5. Adicione as listas relacionadas desejadas ao bucket direito na exibição recém-criada e salve a exibição.
   Esta exibição será usada para renderizar as informações associadas na guia Investigação.

Como adicionar uma lista de ponto de entrada

Configure a nova lista de ponto de entrada para adicioná-la à página de investigação.

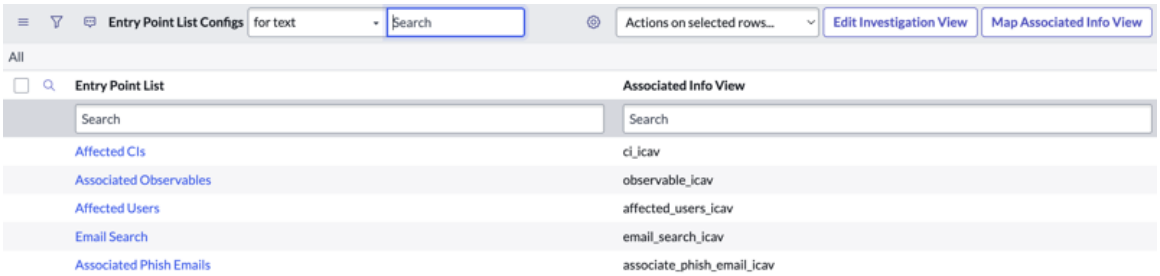
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

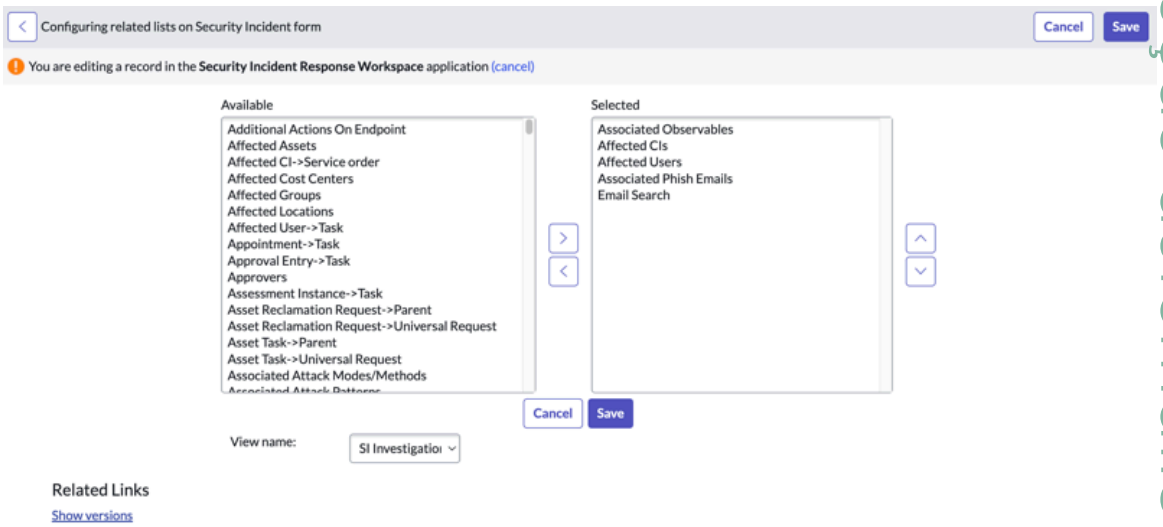
Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **sn_si_aw_entry_point_config.list**.
   A página **Configurações de listas de ponto de entrada** é exibida.



2. Clique no botão **Editar exibição de investigação** para adicionar uma lista de pontos de entrada à tela de investigação.
   O **formulário Configurando listas relacionadas no incidente de segurança** é exibido.



3. Adicione ou remova a lista de ponto de entrada da exibição de slush bucket.
4. Clique em **Salvar**.

> **Nota:** A exibição correspondente à tela Investigação que contém as listas de ponto de entrada é chamada **Exibição de investigação de SI** e, por padrão, é selecionada quando você navega para a página **Editar exibição de investigação**.
>
> A ordem na qual as listas de ponto de entrada são exibidas na tela de investigação é determinada pela ordem na exibição selecionada do slush bucket.

Exibição de mapeamento das informações associadas à lista de ponto de entrada

Mapeie a exibição de informações associada à lista de ponto de entrada recém-adicionada usando a ação Mapear Exibição de Informações Associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

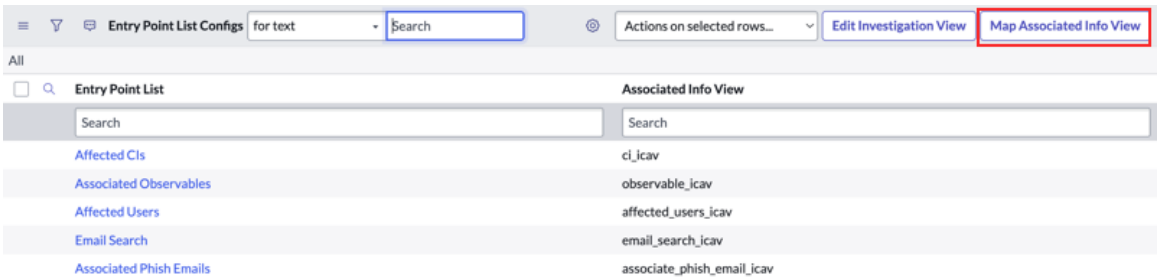
Antes de Iniciar

Nota: Esta etapa é necessária para que a lista de pontos de entrada fique visível na página Investigação. Mesmo que você não queira que nenhuma lista de informações associada seja mostrada em um ponto de entrada, você ainda precisará criar uma exibição fictícia e mapeá-la.

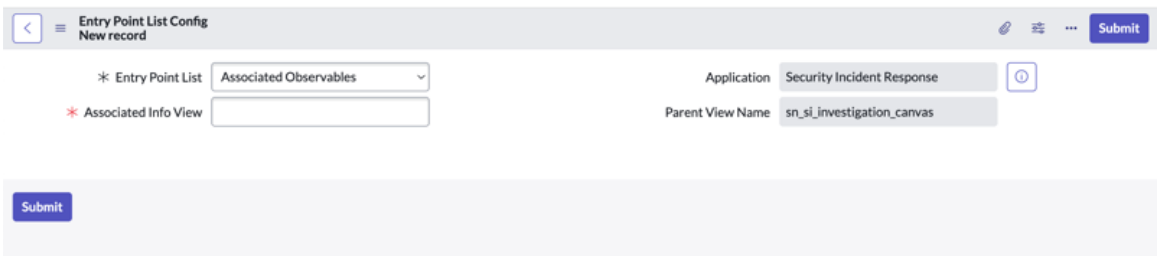
Função necessária: administrador

Procedimento

1. Clique no botão **Mapear exibição de informações associadas** na página **Configurações de ponto de entrada**.



2. Selecione a lista de pontos de entrada recém-adicionados na lista suspensa **Lista** de pontos de entrada.
3. Insira o nome da exibição que contém as listas relacionadas às informações associadas no campo **Exibição** de informações associadas.
   Para obter informações sobre como criar uma exibição para as listas relacionadas a informações associadas, consulte Criando exibição para tabelas de informações associadas.



4. **Salve** o formulário.
5. Além disso, se necessário, você pode adicionar ou remover mais listas associadas usando a **Exibição Editar informações associadas**.
   Você também pode configurar o layout da lista de ponto de entrada usando a ação **Editar** layout da lista de ponto de entrada. Adicione ou remova colunas do bucket de slush conforme desejado e salve o formulário.

Configure cada lista associada da exibição para lidar com a renderização de dados em tempo de execução

Configure cada lista associada da exibição para lidar com a renderização de dados em tempo de execução.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

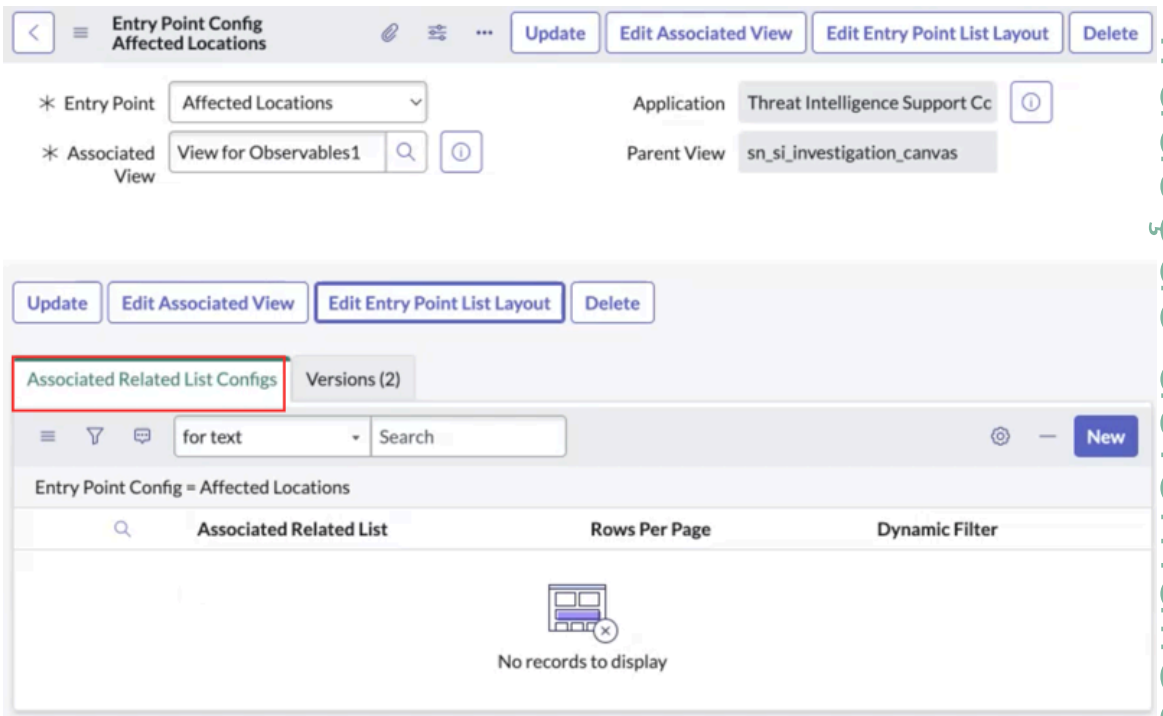
Nota: Esta etapa é obrigatória para cada lista associada configurada na exibição de informações associadas. Caso contrário, a lista associada não estará disponível na página de investigação.

Cada lista associada adicionada (ao mapear uma exibição de informações associada a uma lista de ponto de entrada) Exibição de mapeamento das informações associadas à lista de ponto de entrada (ou diretamente da exibição) precisa de uma configuração adicional para filtrar os dados em relação à seleção de registro de tempo de execução e seleção de filtros.

Função necessária: administrador

Procedimento

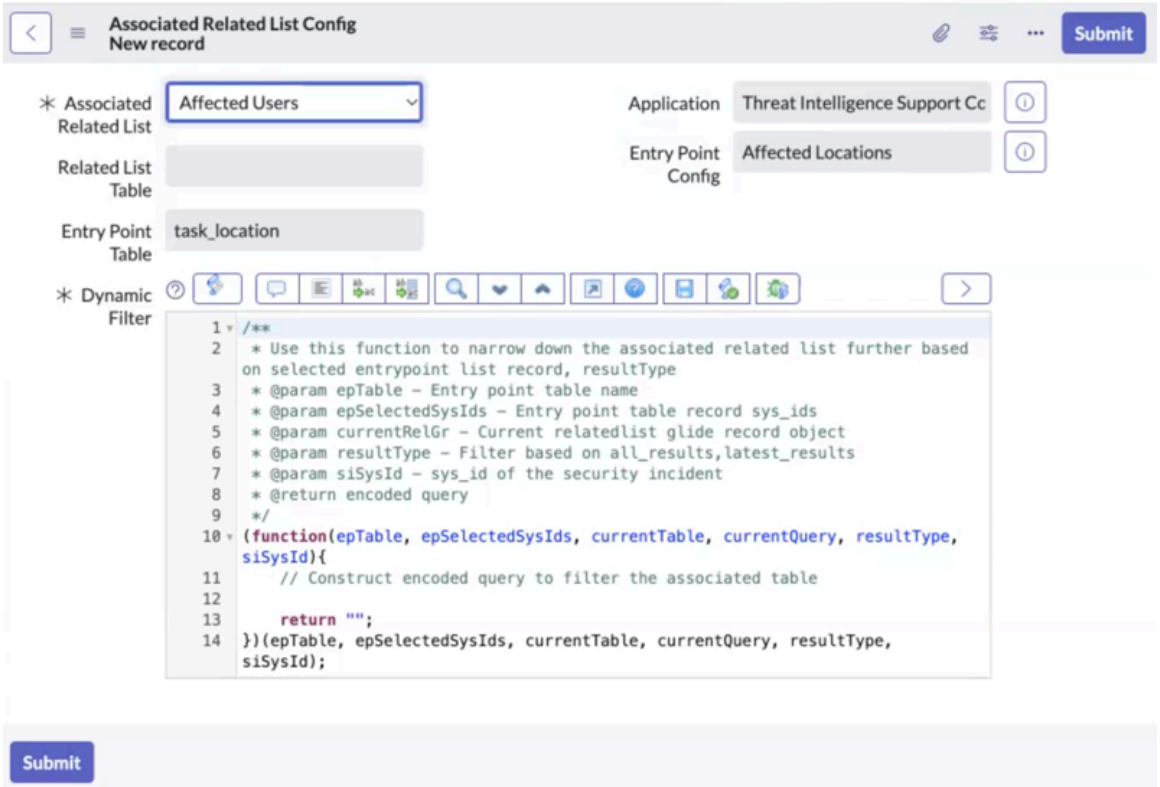
1. Clique em **Novo** em Configurações da **lista associada**.



2. Selecione o valor do campo **Lista associada**.
3. Use a coluna **Filtro dinâmico** para filtrar ainda mais a lista associada com base nos registros da lista de ponto de entrada selecionados e no tipo de resultado (últimos resultados de cada implementação do fornecedor, todos os resultados). Consulte os exemplos existentes que são enviados com o produto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Além disso, você pode configurar o layout de lista associado usando a ação **Editar Layout de Lista Associada**.
   Na janela de bucket de slush, adicione ou remova colunas conforme necessário.

Espaço SIR Registros relacionados

Esta seção consiste nos itens de listas relacionadas que são agrupados em seções, como observáveis associados e itens de configuração.

Os grupos de listas relacionadas a seguir que estão disponíveis como parte do sistema de base. Você pode modificar esses grupos ou criar grupos na aplicação e suas respectivas ações.

Você pode modificar esses grupos ou criar novos grupos. Para obter mais informações, consulte Configurar lista relacionada de incidentes de segurança sobre como configurar e agrupar a lista relacionada a incidentes de segurança e tarefas de resposta. Cada lista relacionada é totalmente funcional no Espaço SIR.

Lista relacionada	Item agrupado
Impacto nos negócios	• Itens de configuração • Usuários afetados • Itens de Configuração Relacionados • Usuários relacionados • Serviços afetados

Tradução automática

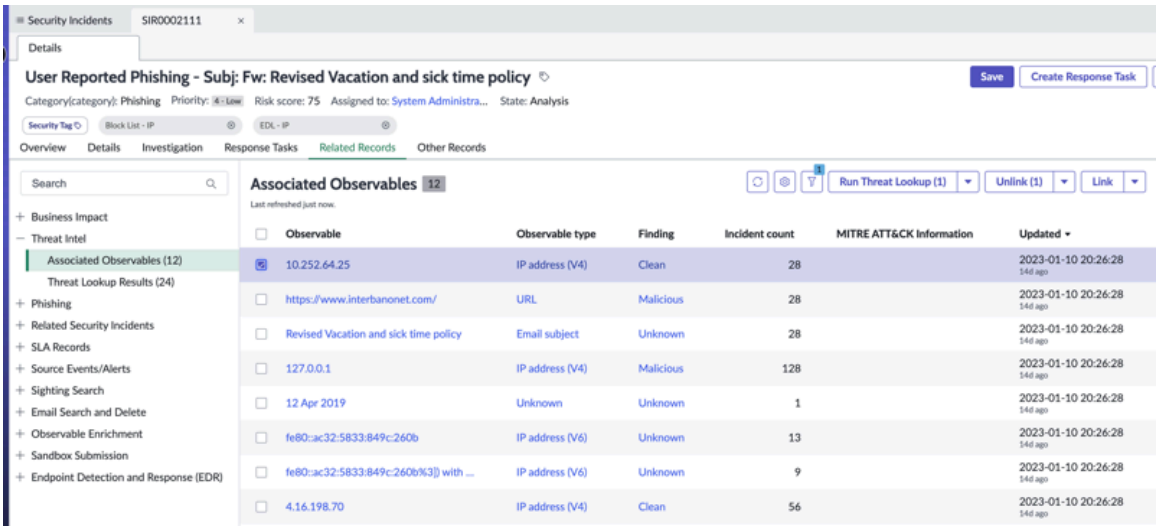
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Item agrupado
Inteligência sobre ameaça	• Observáveis Associados • Resultados da Pesquisa de ameaças
Phishing	• E-mails de Phishing Associados • Cabeçalhos de phishing associados
Incidentes de segurança relacionados	• Incidente primário de segurança • Incidente secundário de segurança • Incidente de segurança semelhante
Registro de ANS	ANS de tarefas
Eventos/alertas de origem	Eventos ou alertas de origem são a lista relacionada à integração de SIEM habilitada, como e-mail de origem, logs de detalhamento do LogRhythm, eventos do LogRhythm, infração agregada do IBM QRadar e assim por diante. **Nota:** Esta lista depende totalmente da integração que você tem em sua instância. Para exibir a lista relacionada à integração SIEM relevante, você deve instalar a versão mais recente.
Pesquisa de detecções	• Resultados da pesquisa de detecções • Detalhes de Pesquisa de detecções • Detecção
Aprimoramento de Observável	• Resultados de enriquecimento observável • Eventos de MISP associados • Resultados de enriquecimento de MISP
Detecção e resposta de endpoint (EDR)	• Detalhes do host • Processos em execução • Serviços em execução • Usuários Conectados • Estatísticas de Rede • Obter arquivo • Isolar Entradas de Host

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Item agrupado
	• Ações adicionais no endpoint • Detalhes do Microsoft Defender para máquinas relacionadas ao endpoint



Nota: Em geral, você pode criar novos registros, vincular ou desvincular registros existentes ou novos registros em relação ao grupo de listas relacionadas, conforme aplicável.

Informações relacionadas

Configurar lista relacionada de incidentes de segurança

Configurar lista relacionada de incidentes de segurança

Você pode adicionar novas listas relacionadas ou novos grupos de listas relacionadas e modificar grupos existentes ou listas relacionadas que aparecem no Espaço SIR.

Antes de Iniciar

A lista relacionada a incidentes de segurança é agrupada e exibida como itens de lista relacionada a grupo na guia **Registros relacionados** no espaço.

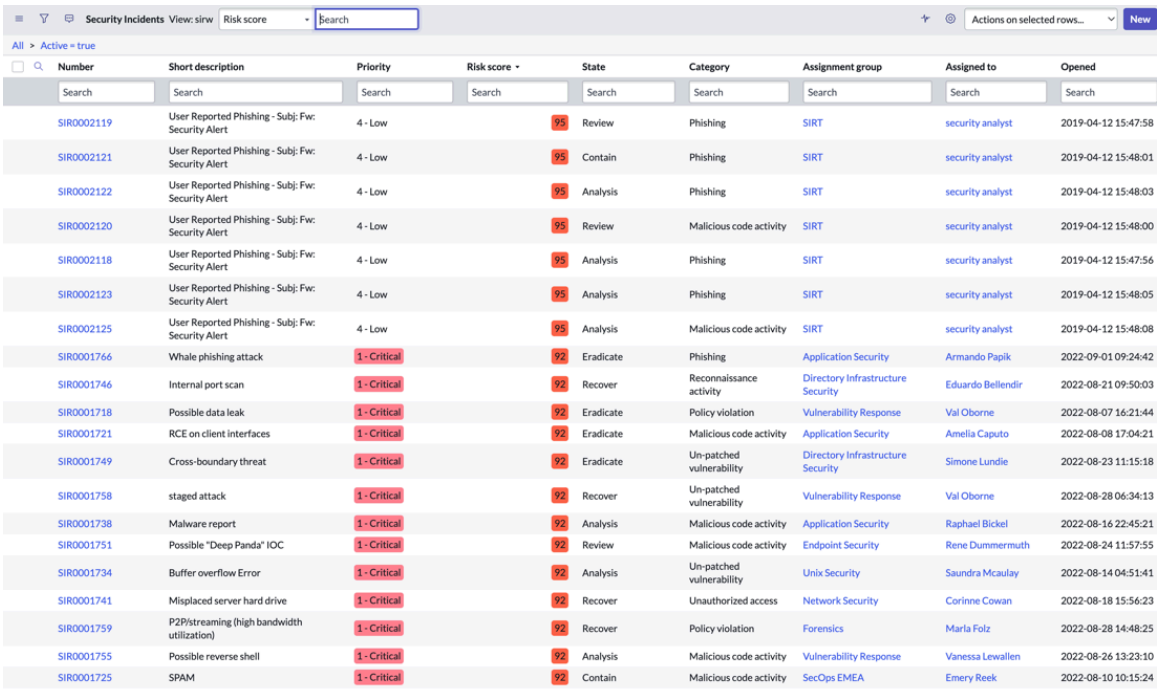
Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

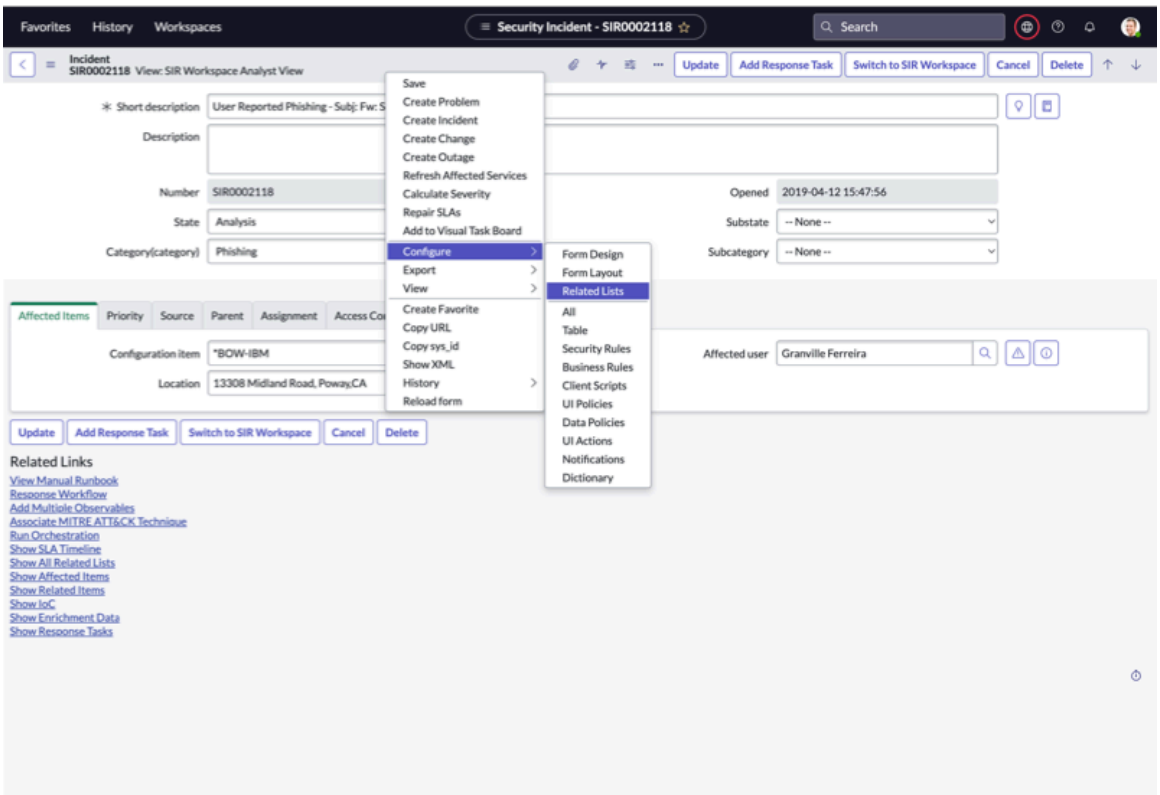
Procedimento

1. Na IU clássica, navegue até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.



Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Selecione qualquer registro de incidente.
3. Clique com o botão direito do mouse no menu de contexto do incidente.
4. Ir para **Configurar** > **Lista relacionada**.

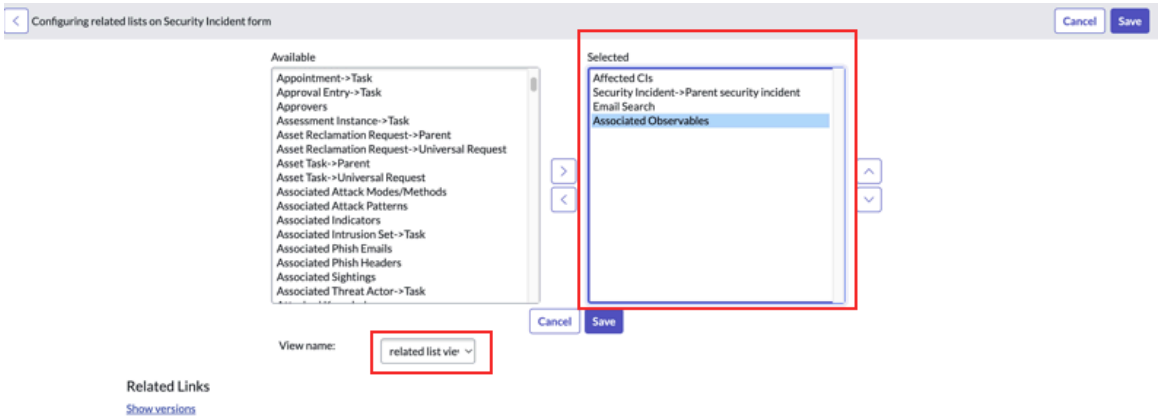


O **formulário Configurando listas relacionadas no incidente de segurança** é exibido.

Tradução automática

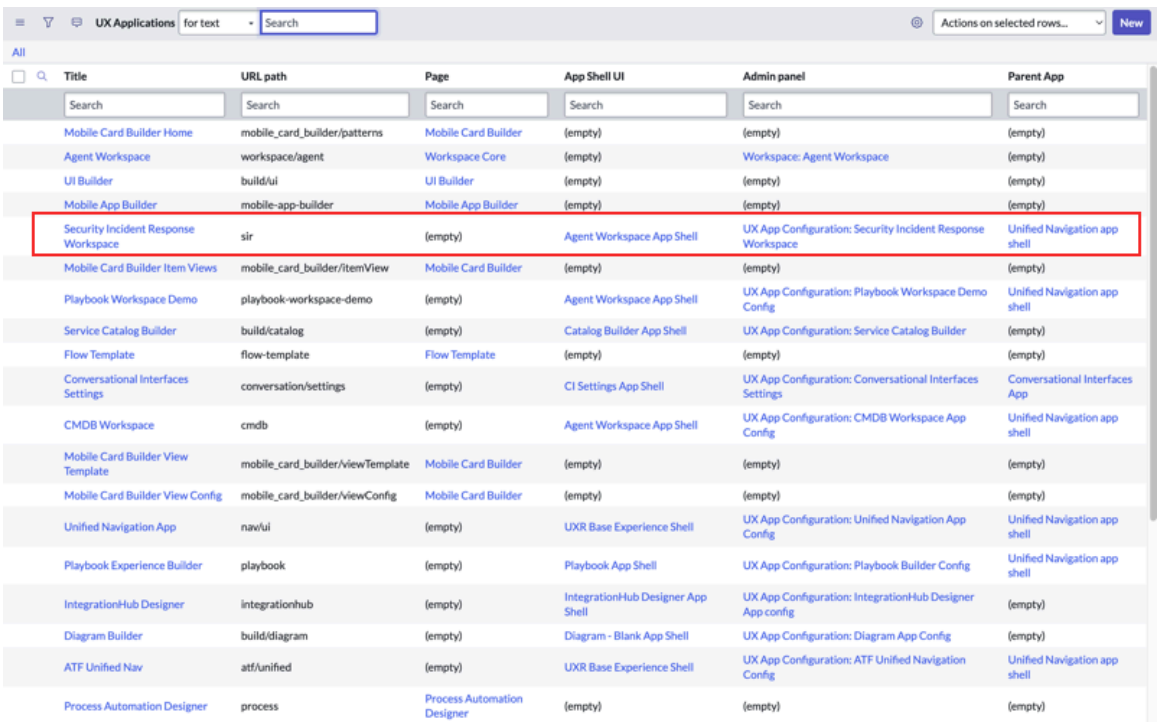
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Acesse **Exibir nome** e selecione **Novo**.
6. Insira um nome para a exibição.
7. Selecione a exibição recém-criada.
   Depois de selecionar a exibição, escolha os campos de lista relacionada necessários no bucket de slush.



Nota: Se você quiser modificar algo, selecione a exibição e remova ou adicione os itens.

8. Clique em **Salvar**.
9. Na navegação à esquerda, navegue até **Todos** > **Estrutura do Now Experience** > **Experiências**.
10. Selecione **Espaço do Security Incident Response**.

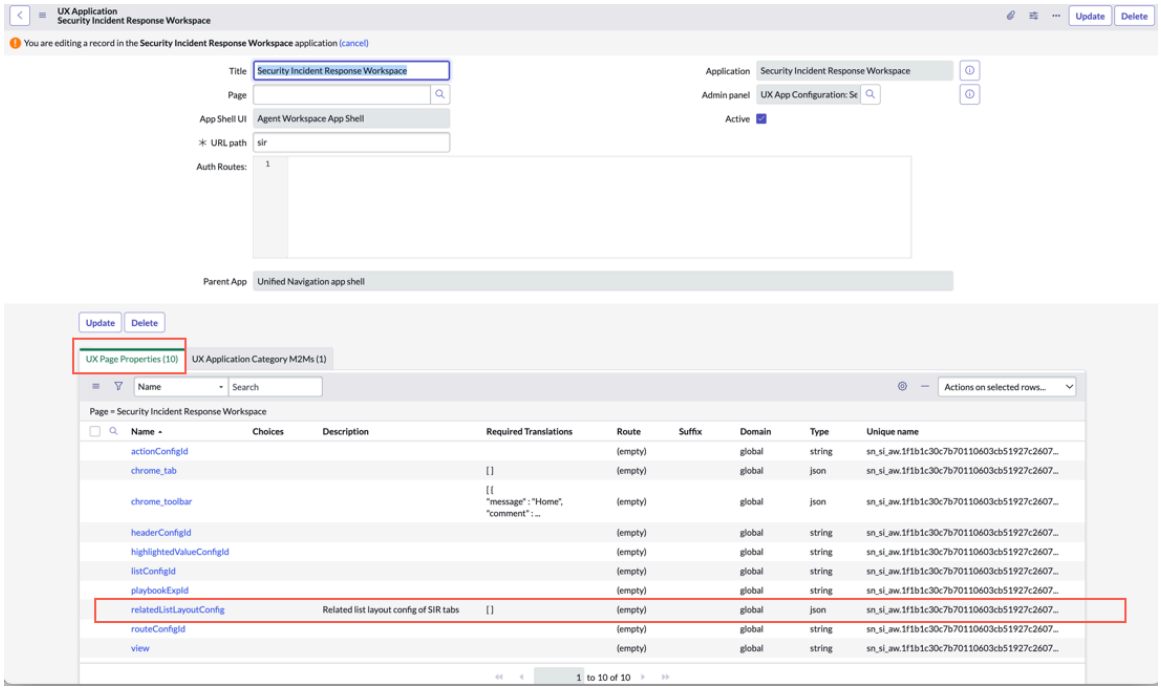


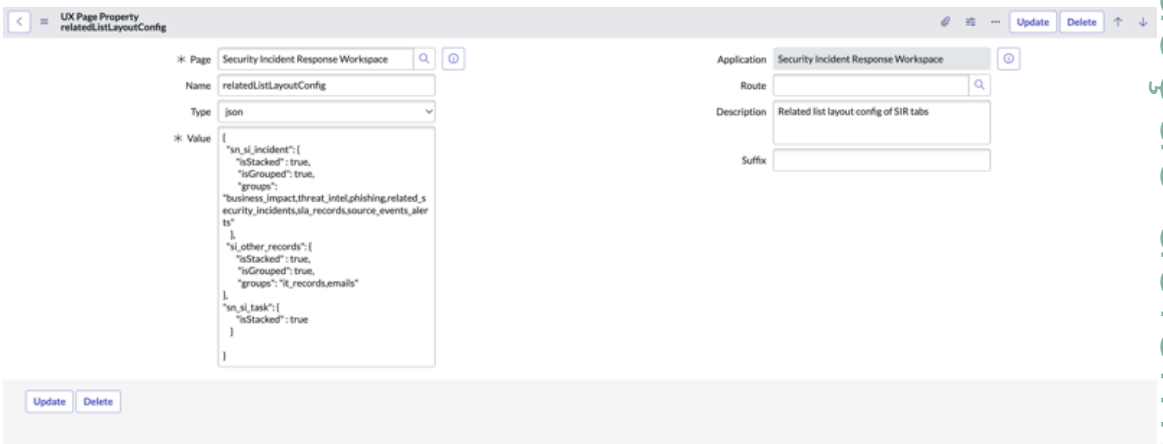
A página **Espaço de resposta a incidentes de segurança da aplicação UX** é exibida.

11. Vá para a guia **Propriedades da página de UX** e selecione a opção **relatedListLayoutConfig** na exibição de lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

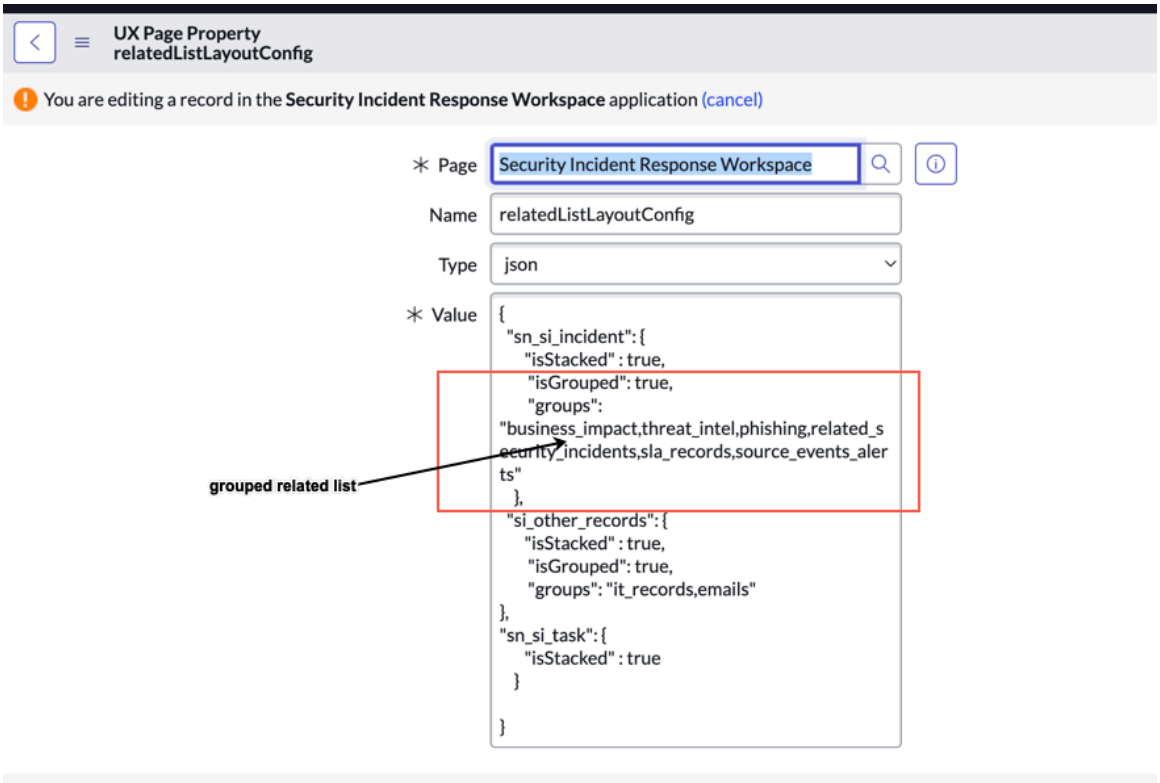




12. Adicione o nome de exibição recém-criado separado por uma vírgula a uma lista de valores já existente na caixa de texto **Valor** no campo **sn_si_incident.viewsUsedForGrouping**.
Por exemplo, se você tiver criado um novo nome de exibição como **Impacto nos negócios**, na caixa de texto **Valor**, deverá especificá-lo como **business_impact** (que é separado por sublinhado no nome da exibição e separado por uma vírgula após um valor existente) em sn_si_incident :campo de grupos.

Tradução automática

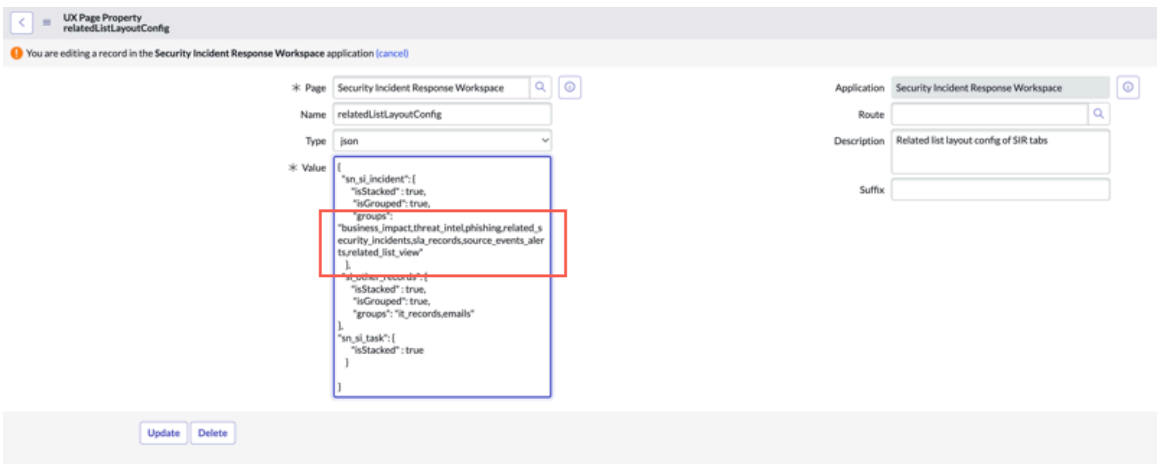
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Se você adicionar o novo nome de exibição no campo **sn_si_incident.viewsUsedForGrouping**, a entrada será criada na guia **Registros relacionados** do espaço.

Se você atualizar a entrada do nome de exibição em **si_other_records.viewsUsedForGrouping**, o grupo de listas relacionadas será adicionado à guia **Outros registros** do espaço.

Abaixo está uma exibição de exemplo que mostra as exibições recém-criadas adicionadas.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: **requiredRolesForGrouping** contém nomes de registros sys_user_role separados por vírgulas. O usuário do Espaço SIR deve ter pelo menos uma dessas funções para usar as listas relacionadas agrupadas. Quando um usuário não tiver nenhuma dessas funções, a exibição de listas relacionadas configurada para a função do usuário atual usando a configuração de regra de exibição será representada verticalmente sem agrupamento. Esta propriedade é ignorada quando a propriedade **isGrouped** está definida como falsa. Se esta propriedade estiver vazia, qualquer usuário poderá acessar as listas relacionadas agrupadas.

13. Clique em **Salvar**.
14. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
15. Selecione qualquer incidente de segurança específico.
16. Vá para a guia **Registros relacionados** do espaço.
    As listas relacionadas agrupadas são exibidas.

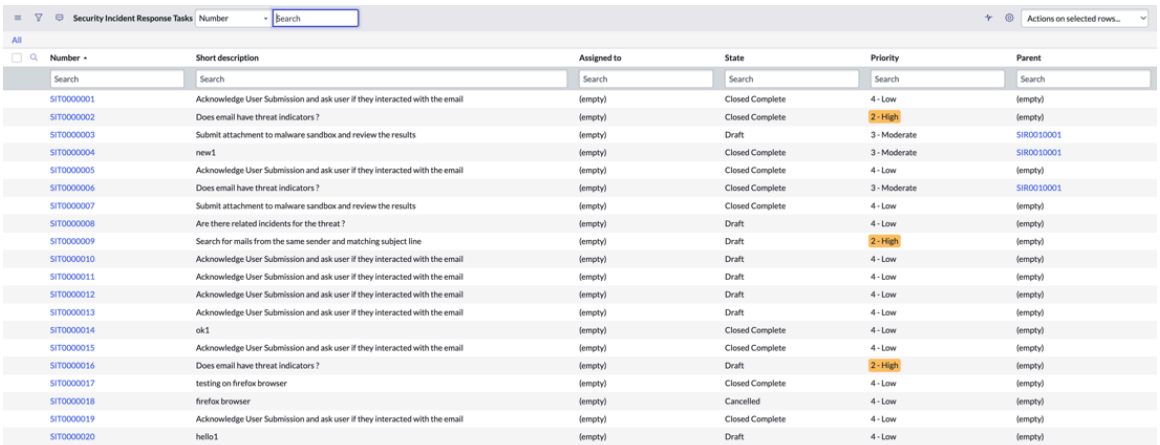
Configurar lista relacionada de tarefas de resposta

Use esta seção para configurar as novas listas relacionadas a tarefas de resposta que aparecem na aplicação Security Incident Response.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A lista relacionada de tarefas de resposta não é agrupada, mas exibida como itens de lista relacionados individuais, pois há algumas listas padrão. Exiba os itens relacionados às tarefas de **resposta na guia Tarefas** de resposta do registro de incidente de segurança do espaço.

Procedimento
1. Navegar até **Todos** > **Incidente de segurança** > **Tarefas de Resposta** > **Mostrar todas as tarefas**.

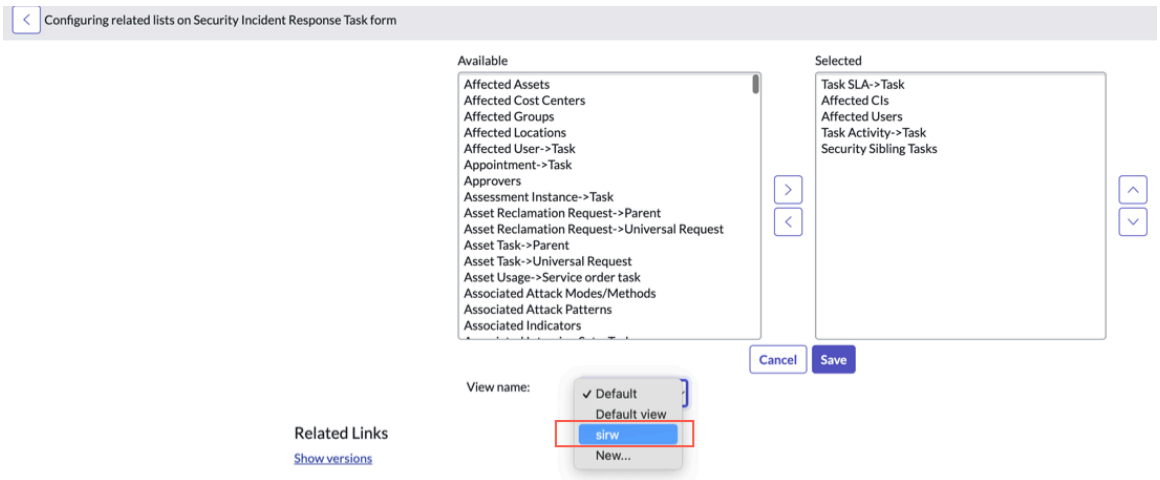


2. Selecione qualquer registro de tarefa de resposta.
3. Clique com o botão direito do mouse no menu de contexto da Tarefa do Security Incident Response.
4. Navegar até **Configurar** > **Lista relacionada**.
   O **formulário Configurando listas relacionadas na tarefa de resposta de segurança** é exibido.

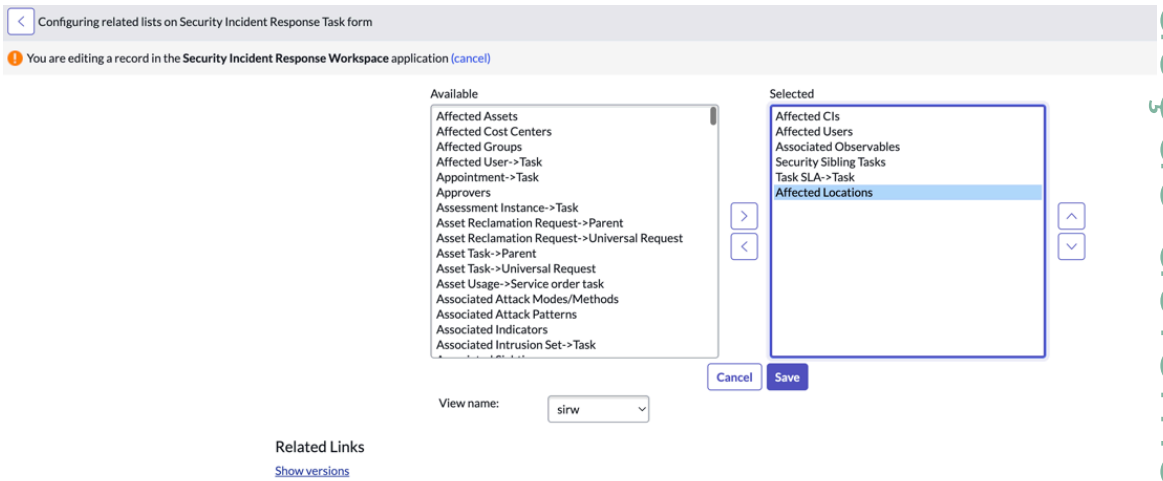
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Vá para **Exibir nome** e selecione Exibição de **sirw**.



6. Selecione os campos de lista relacionada desejados no bucket de slush.
   Por exemplo, Locais afetados.

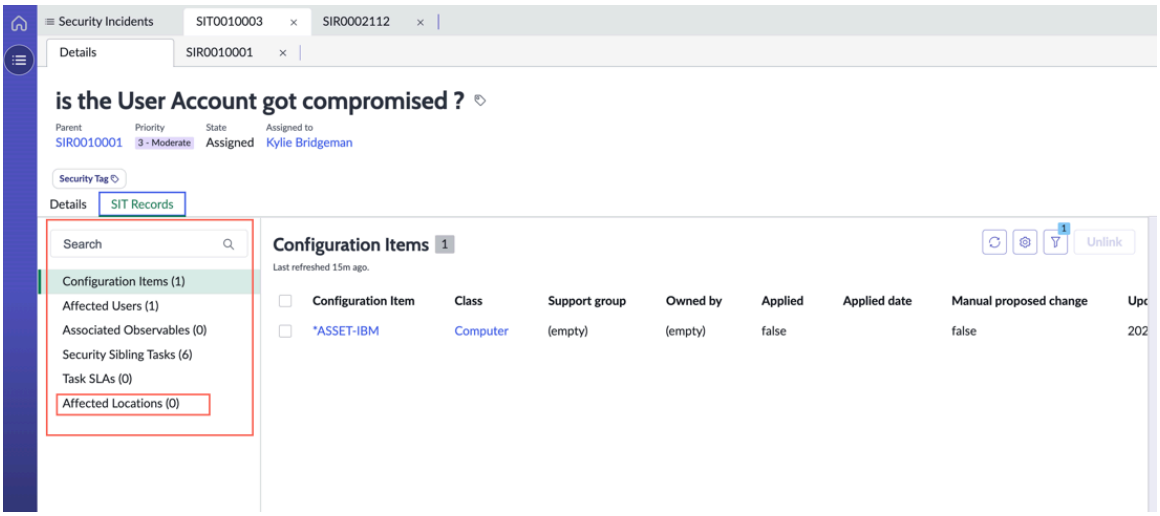


7. Clique em **Salvar**.
8. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Tarefas de Resposta** > **Registros de SIT**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas relacionadas configuradas (por exemplo, locais afetados conforme selecionado) são listadas na lista de registros SIT.



Definir as novas regras da calculadora de pontuação de risco

Use a nova Calculadora de pontuação de risco para definir e calcular a pontuação de risco de incidentes de segurança com base nos critérios definidos pelo usuário, que fornecem uma pontuação de inteligência transparente de incidentes de segurança. A pontuação de risco é calculada automaticamente para os registros de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.admin.

Ative a nova Calculadora de pontuação de risco definindo a propriedade do sistema `sn_si_aw.activate_new_risk_score_calculator` como verdadeira.

Por Que e Quando Desempenhar Esta Tarefa

Defina uma pontuação de risco para os registros de incidentes de segurança que são gerados com base nos parâmetros definidos pelo usuário. O sistema base é provisionado com uma regra de pontuação de risco, que pode ser personalizada e habilitada de acordo.

Nota:

- Por padrão, a nova Regra da Calculadora de Pontuação de Risco está inativa e você precisa habilitar a regra para ver a pontuação de risco dos incidentes de segurança.
- Para calcular a pontuação de risco de tabelas relacionadas adicionais além das disponíveis no sistema de base, consulte Calculadora de pontuação de risco para tabelas relacionadas adicionais.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Administração**.
2. Navegar até **Mecanismo de regras** > **Regra da calculadora de pontuação de risco**.
   A página Regra da calculadora de pontuação de risco é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Como parte do sistema de base, você recebe um modelo de regra de pontuação de risco predefinido para exibir, editar ou modificar a pontuação de risco. No entanto, você não pode criar ou excluir o modelo de regra de pontuação de risco predefinido.
- As mudanças feitas serão aplicadas a todos os novos incidentes de segurança ou atualizações dos existentes. Para redefinir pontuações históricas, use a ação **Recalcular pontuação**.

3. Selecione a regra da **Calculadora de pontuação de risco**.
4. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do valor da pontuação de risco. Por exemplo, Calculadora de pontuação de risco.
Ponderação geral (aplicável ao construtor de critérios)	Ponderação deste campo na regra de risco. Este campo não é editável e exibe a ponderação geral calculada pelo sistema com base na ponderação correspondente aos critérios habilitados. A ponderação geral deve ser sempre de 100%.
Descrição	Descrição do registro de pontuação de risco. Por exemplo, calcula a pontuação de risco com base na soma ponderada das pontuações de critérios predefinidos.
Critérios de pontuação	Indica os critérios de pontuação para um incidente de segurança. Você pode definir os **critérios de pontuação** de risco usando as seguintes opções: ◦ **Construtor de critérios**: Use esta opção para adicionar, editar ou remover e habilitar e desabilitar critérios que contribuem para o cálculo da pontuação de risco e verificar se a ponderação agregada total é de 100%. ◦ **Usar script (Avançado)**: o recurso de script é um recurso avançado para criar um script personalizado que deve retornar a pontuação de risco no intervalo de 0 a 100.

5. Para definir os **critérios de pontuação** usando o **Construtor de critérios**, execute as seguintes etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode editar ou modificar os critérios existentes ou adicionar novos critérios.

a. Para adicionar novos critérios, selecione a ação **+Novos critérios**.

b. Selecione a **Tabela** para a qual você deseja definir os critérios.

Nota:

- Se a tabela selecionada for um incidente de segurança, a condição será aplicada ao registro do incidente de segurança para o qual a pontuação de risco é calculada. Se a tabela selecionada não for um incidente de segurança, a condição será aplicada somente se os registros estiverem relacionados ao incidente de segurança para o qual a pontuação de risco é calculada.
- Um tipo Agregado adicional é adicionado para definir as pontuações com base no número de relações associadas aos incidentes de segurança.

c. Selecione os critérios de **tipo** para a tabela selecionada.
O valor de Tipo pode ser **Campo** ou **Agregado** com base na tabela escolhida.

d. Selecione os critérios de **campo** para a tabela selecionada.
Se você selecionou o valor de Tipo como **Campo**, os critérios de Campo exibirão os valores de campos relacionados à tabela. Se você selecionou o valor de Tipo como **Agregado**, os critérios de Campo exibirão os valores agregados relacionados à tabela.

Nota: O tipo Agregado é compatível somente com o valor de Contagem.

Por exemplo, se você selecionar os critérios de Tabela como **Incidente de segurança**, os critérios de Tipo exibirão somente a opção **Campo**. Os critérios de campo exibem todos os valores de campo relacionados à tabela, que podem ser Gravidade, Ativo e assim por diante. Da mesma forma, se você selecionar os critérios de tabela como **Usuários afetados**, os critérios de tipo exibirão as opções **Campo** e **Agregado**. Se você selecionar o Tipo como Agregado, os critérios de Campo exibirão os valores agregados relacionados à tabela, que é **Contagem**.

e. Insira a **ponderação** dos critérios entre 0 e 100.
A ponderação geral de todos os critérios deve ser de 100%.

f. Insira o nome e uma descrição resumida dos critérios.

g. Marque a caixa de seleção **Habilitar critérios de pontuação** para habilitar os critérios de pontuação.

h. Defina as **Condições** e defina a pontuação das condições.

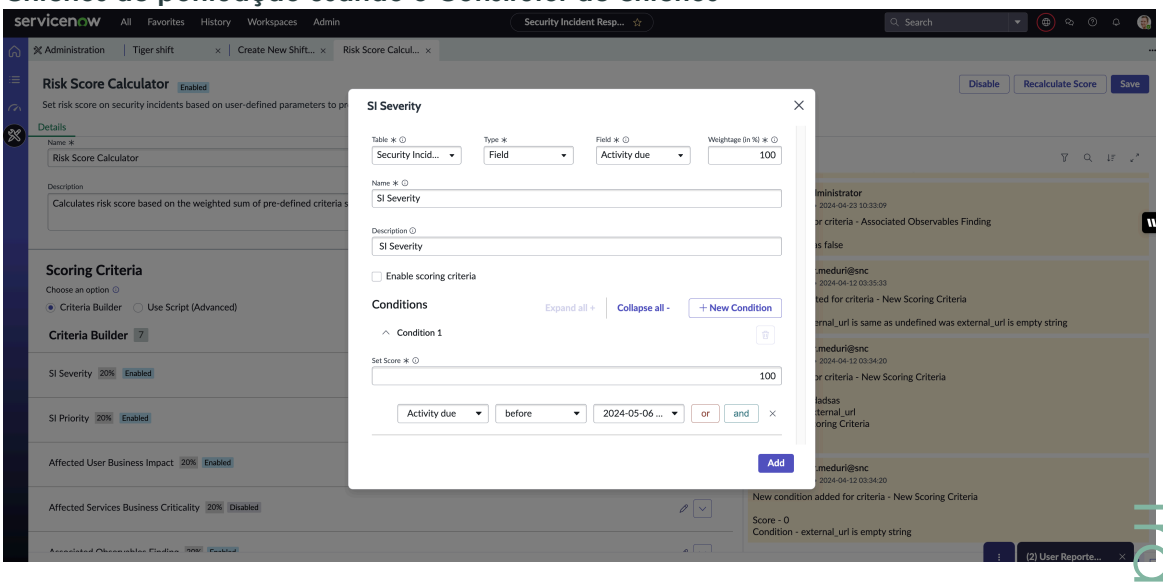
i. Você também pode adicionar novas condições usando a opção **Nova condição** e excluir as condições existentes usando o ícone **Excluir critérios**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

j. Selecione **Adicionar** para adicionar os critérios configurados.

Critérios de pontuação usando o Construtor de critérios



6. Selecione a opção **Recalcular pontuação** para recalcular a pontuação de risco.

Por exemplo, se houver mudanças na regra de pontuação de risco. Nesse caso, você deve reaplicar a regra de pontuação aos incidentes de segurança com a pontuação de risco já calculada no passado. Use a ação **Recalcular pontuação** para acionar o trabalho de recálculo.

7. Selecione **Confirmar**.

Nota: Depois que você acionar esta ação, o processo será executado em segundo plano e levará alguns minutos para ser concluído. Você não poderá fazer mudanças até que ele seja concluído.

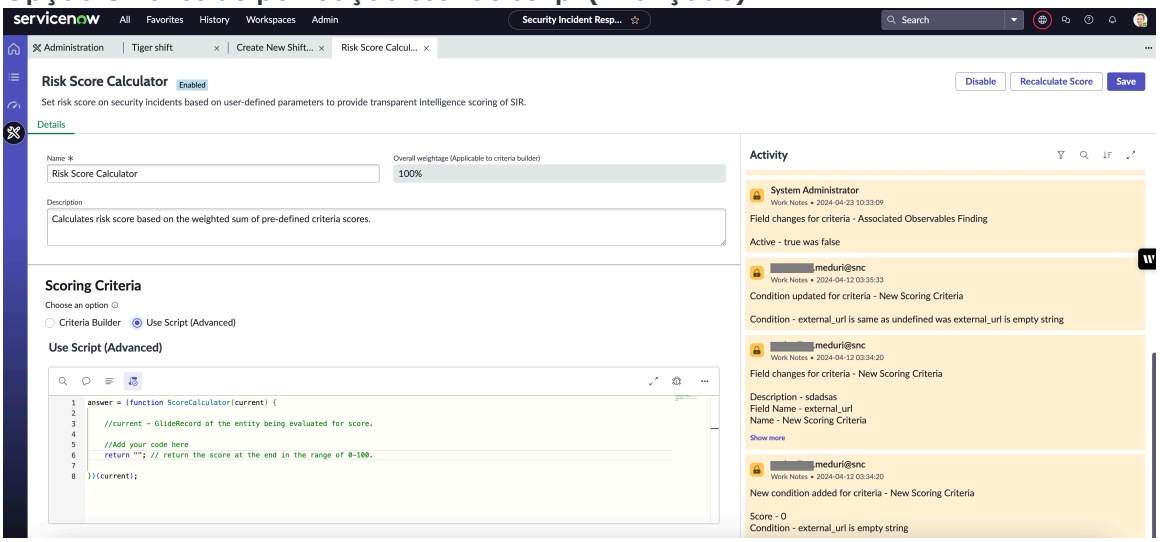
8. Para definir os **critérios de pontuação** usando a opção **Usar script (Avançado)**, execute as seguintes etapas:

a. Use este script predefinido para criar um script personalizado que deve retornar a pontuação de risco no intervalo de 0 a 100.
O campo de script avançado é preenchido automaticamente com uma função, que usa os parâmetros **atuais** e essa função deve retornar a pontuação de risco no intervalo de 0 a 100.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção Critérios de pontuação usando script (Avançado)



Aqui, o parâmetro atual é o objeto GlideRecord da entidade (incidente de segurança) para o qual a pontuação de risco está sendo calculada. Para os incidentes de segurança, corresponde ao GlideRecord da tabela sn_si_incident.

9. Para desabilitar a Calculadora de pontuação de risco, selecione **Desabilitar**.
10. Selecione **Salvar**.

Calculadora de pontuação de risco para tabelas relacionadas adicionais

A Calculadora de pontuação de risco é provisionada com uma regra de pontuação de risco como parte do sistema de base para calcular a pontuação de risco de incidentes de segurança com base em critérios definidos pelo usuário. No entanto, você pode personalizar e incluir tabelas relacionadas adicionais para calcular a pontuação de risco.

Antes de Iniciar

Função necessária: sn_si.admin.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**.
2. Selecione qualquer registro de incidente de segurança.
3. Selecione a opção **Ações adicionais** ao lado do número do incidente de segurança.
4. Ir para **Configurar** > **Listas relacionadas**.
5. Acesse o Nome de exibição e selecione **Calculadora de pontuação de risco**.
   Depois de selecionar a exibição, escolha a lista relacionada necessária que você deseja adicionar do bucket de slush. Por exemplo, Detecções associadas.
6. Selecione **Salvar**.
   Você adicionou com sucesso as novas listas ou tabelas relacionadas para as quais deseja calcular a pontuação de risco.

> **Importante:** Para calcular a pontuação de risco dos incidentes de segurança que têm novos critérios com as listas relacionadas recém-criadas, você precisa definir regras de negócio na tabela base da lista relacionada.

7. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócio**.

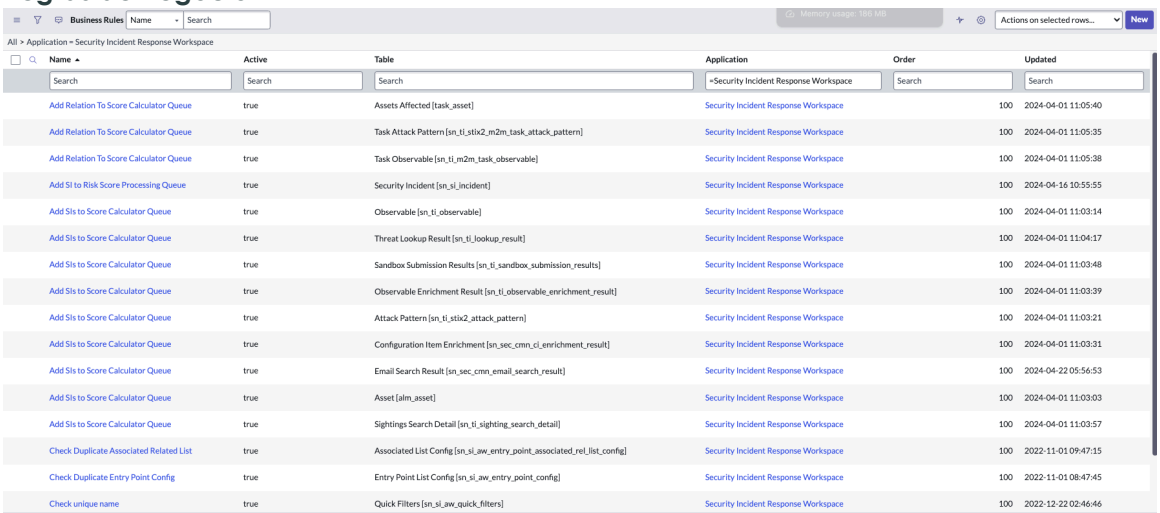
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar as duas regras de negócio a seguir como referência para criar suas próprias regras de negócio:

- Adicionar incidentes de segurança (SIs) à fila da calculadora de pontuação
- Adicionar relação à fila da calculadora de pontuação (aplicável a tabelas m2m)

Regras de negócio



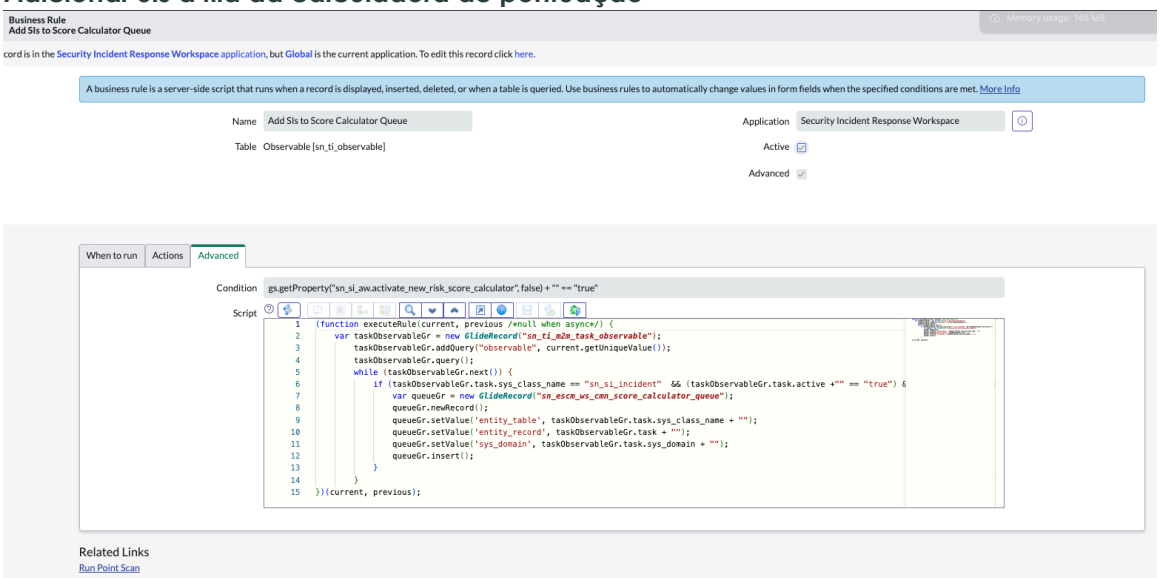
Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. Por exemplo, para que os critérios de observáveis associados funcionem, definimos duas regras de negócio.

   A primeira é a regra de negócio **Adicionar SIs à fila da calculadora de pontuação**.

   Por exemplo, um novo incidente de segurança é criado e associado a uma tabela de observáveis (`Observables[sn_ti_observable]`). Após a pesquisa de ameaças, o observável é considerado mal-intencionado. Em seguida, você precisa adicionar todos os incidentes de segurança associados a este observável mal-intencionado à Fila para recalcular a pontuação de risco dos incidentes de segurança.

Adicionar SIs à fila da calculadora de pontuação



   A segunda é a regra de negócio **Adicionar relação à fila da calculadora de pontuação**.

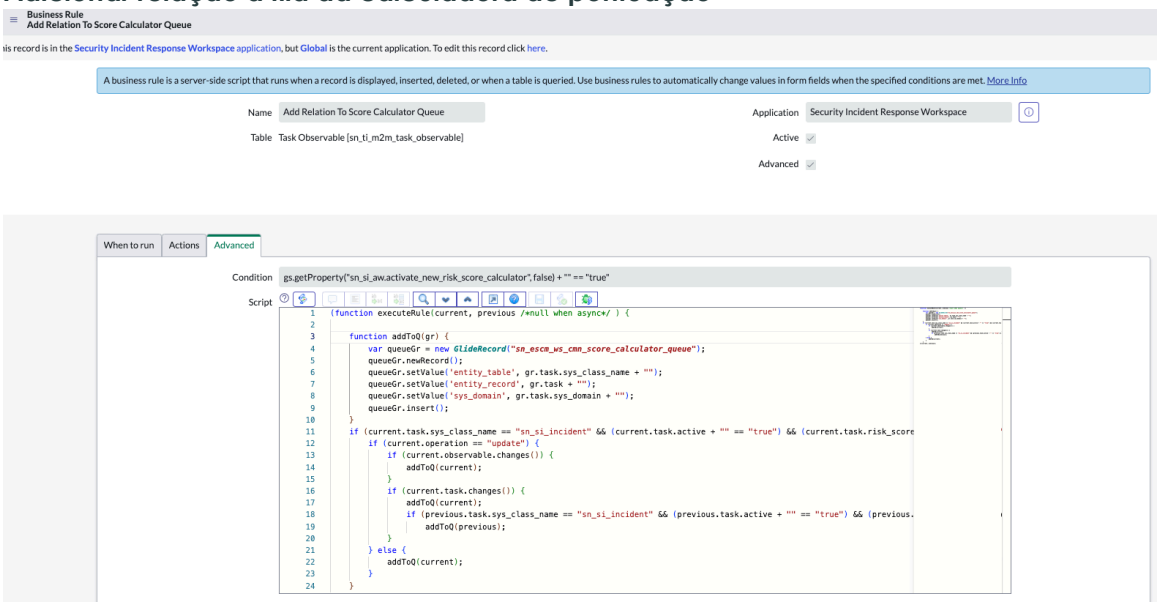
   Por exemplo, um novo incidente de segurança é criado ou excluído e associado a uma tabela de observáveis (`Task Observables[sn_ti_m2m_task_observable]`). Portanto,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

há uma mudança na associação do incidente de segurança. Em seguida, você precisa adicionar esse incidente de segurança à Fila para recalcular a pontuação de risco do incidente de segurança.

Adicionar relação à fila da calculadora de pontuação



Configurar modelos de transferência de turno

O administrador pode definir e configurar diferentes modelos de transferência de turno para o proprietário do turno criar registros de transferência de turno e entregá-los à equipe do próximo turno.

Antes de Iniciar

Função necessária:

- sn_escm_sh.shift_admin
- sn_si.admin herda a função sn_escm_sh.shift_admin

Por Que e Quando Desempenhar Esta Tarefa

Para configurar um modelo de transferência de turno, o administrador cria um novo modelo de transferência de turno ou abre um modelo existente no sistema de base com o nome **Modelo de turno** de amostra e modifica os detalhes e as seções de acordo com seus requisitos.

O proprietário do turno pode usar o modelo configurado para criar registros de log de transferência de turno e, em seguida, o relatório de transferência de turno é compartilhado com o próximo proprietário de turno ativo e a equipe.

Nota: Somente os modelos de transferência de turno ativos estão visíveis para o responsável pelo turno criar registros de log de transferência.

Procedimento

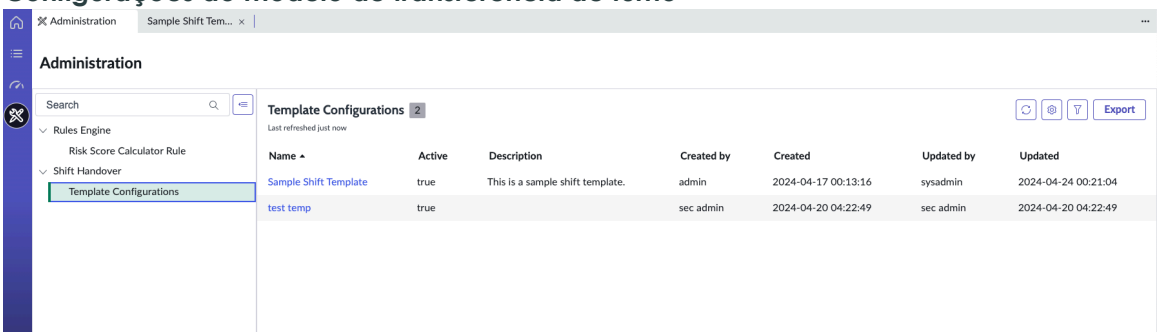
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Administração**.
2. Navegar até **Transferência de turno** > **Configurações do modelo**.
   A página Configurações do modelo é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Como parte do sistema de base, você recebe uma configuração predefinida de modelo de transferência de turno para exibir, editar ou modificar o modelo de transferência de turno. No entanto, você não pode criar ou excluir a configuração predefinida do modelo de transferência de turno.

Configurações do modelo de transferência de turno



3. Para criar um novo modelo de Transferência de turno, selecione **Novo**.
4. No formulário Detalhes, preencha os campos.

Criar um novo modelo de transferência de turno

Campo	Descrição
Nome	Nome do modelo de transferência de turno. Por exemplo, Modelo SIR.
Aplicação	Nome da aplicação para a qual você está criando o modelo de Transferência de turno. Por exemplo, Espaço de resposta a incidentes de segurança.
Ativo	Opção para indicar se o modelo de Transferência de turno está ativo. Habilite esta opção para ativar o modelo de Transferência de turno.
Descrição	Descrição do modelo de transferência de turno.
Configuração da menção de registro	Use este campo para configurar os detalhes de menção de registro do Editor de Rich Text (RTE). A entrada é uma matriz de objetos JSON com os seguintes campos: ◦ *sourceTable*: nome da tabela de origem. ◦ *label*: nome do rótulo a ser exibido. ◦ *filterCondition*: consulta codificada para filtragem ◦ *fields*: selecione os campos para consultar o padrão Configuração de exemplo que você pode copiar e colar no campo Configuração de menção de registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

	<pre>[
	    {
	        "sourceTable":
	 "incident",
	        "label": "Incidents",
	        "filterCondition":
	 "active=true",
	        "fields": [
	            "number"
	        ]
	    }
	]</pre>
	Para copiar a configuração de exemplo, use a ação **Copiar para a área de transferência** no painel Assistência contextual. Em seguida, você pode fazer modificações adicionais com base em seus requisitos.

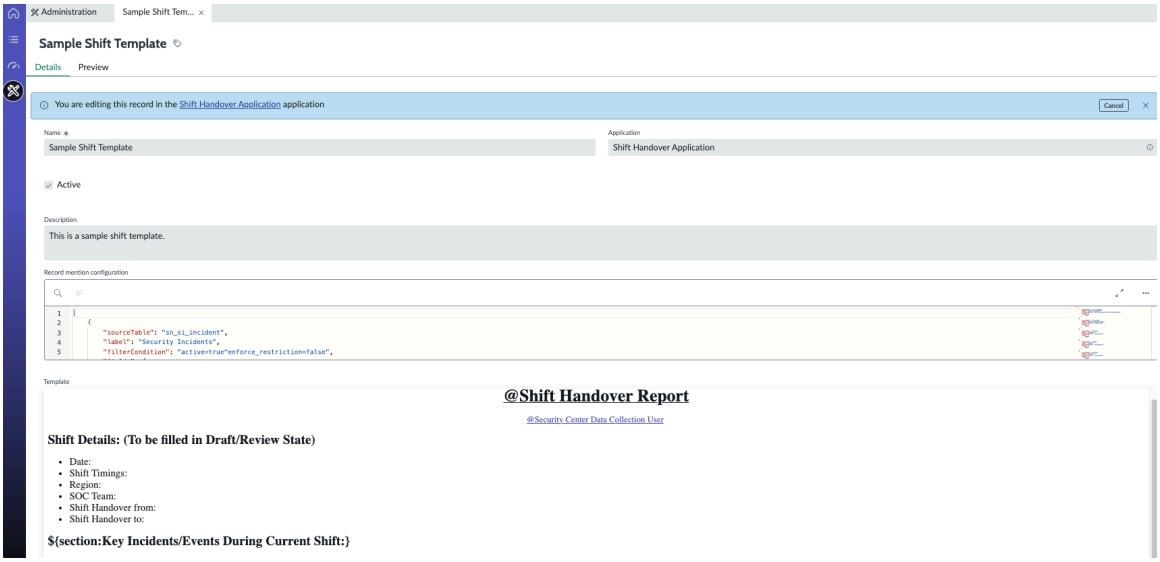
Modelo	Crie um modelo de transferência de turno usando seções. Certifique-se de que haja pelo menos uma seção para que os analistas possam contribuir para os registros de log de transferência de turno com base no modelo.
	
	O modelo pode ter texto estático, imagens e assim por diante, nas seções apropriadas. Você pode copiar e colar imagens diretamente no campo Modelo. Você pode criar seções no modelo usando o seguinte código:
	<pre>${section:Section Label}</pre>
	Exemplo:
	<pre>${section:Key Incidents/Events
	 During Current Shift}
	${section:Incidents/Events to
	 Monitor or Follow Up}
	${section:System/Infrastructure
	 Updates}
	${section:Next Steps for Incoming
	 Shift}
	${section:References}</pre>
	Nota: Para obter mais informações, consulte a **Assistência contextual** no painel direito.

5. Para usar e modificar um modelo de transferência de turno existente, selecione **Amostra de modelo de turno**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

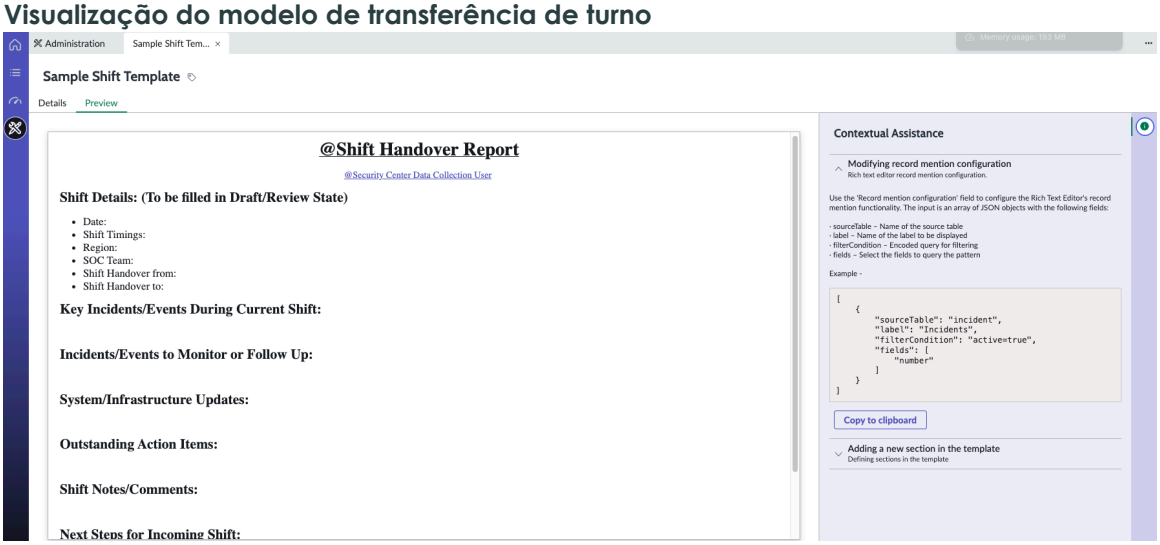
Modelo de transferência de turno



6. Atualize o modelo de Transferência de turno de acordo com seus requisitos.
7. Selecione **Visualizar** para exibir a visualização do tempo de execução do modelo de Transferência de turno.

   O relatório gera uma visualização com base na configuração do modelo de Transferência de turno.

Visualização do modelo de transferência de turno



8. Selecione **Salvar** para salvar o modelo de Transferência de turno.

O que Fazer Depois

Para saber como gerenciar registros de transferência de turno na exibição de lista e executar ações como criar, editar, copiar ou excluir registros de transferência de turno, consulte Gerenciar registros de transferência de turno.

Como usar o Espaço SIR

Analistas e gerentes de segurança usam Espaço SIR para executar operações diárias com uma experiência do usuário aprimorada, fazer a investigação completa de incidentes e obter uma visão geral.

Tradução automática

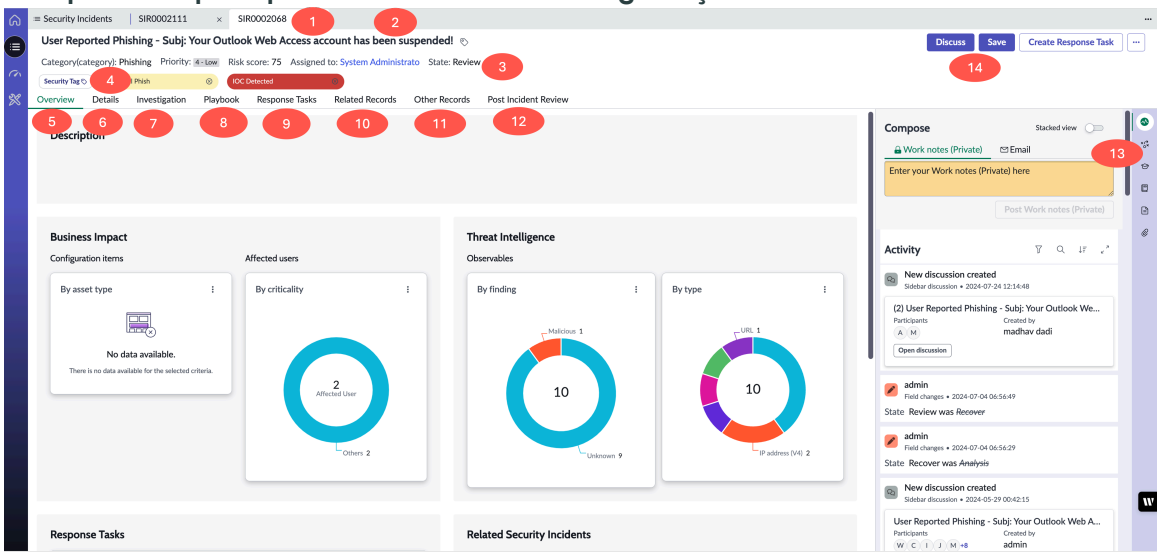
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como trabalhar com registros de incidentes de segurança

O registro de incidente de segurança consiste no seguinte.

Componentes principais disponíveis em um registro de incidente de segurança:

Componentes principais de um incidente de segurança



Número	Nome	Descrição
1	Número do incidente de segurança	O número do incidente de segurança está disponível em relação ao nome da guia.
2	Descrição resumida	Descrição resumida do incidente de segurança que é exibida acima da faixa do formulário.
3	Faixa de formulário	Esta é uma seção somente leitura que contém os campos-chave, como Categoria, Prioridade, Pontuação de risco, Estado e os detalhes de atribuição do incidente. **Nota:** Os marcadores de plataforma regulares também podem ser aplicados aqui.
4	Marcadores de segurança	Exibe os marcadores de segurança associados a um incidente de segurança.
5	Visão geral	Fornece uma visão geral do snapshot do incidente de segurança, como Descrição, Impacto nos negócios, composto por detalhes de ativos por tipo, usuários afetados por criticidade, Itens de inteligência contra ameaças, compostos por observáveis por descoberta e por tipo, Tarefas de resposta, Incidentes de segurança relacionados, compostos por incidentes de segurança secundários e incidentes de segurança semelhantes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número	Nome	Descrição
6	Detalhes	A guia de detalhes exibe o formulário de incidente de segurança.
7	Investigação	A guia Investigação exibe a experiência de investigação de incidentes.
8	Playbook	O playbook é acionado por meio do Designer de automação de processos (PAD). Se um processo for criado e uma condição de gatilho estiver definida para acionar o playbook para um incidente de segurança. Em seguida, um playbook é exibido.
9	Tarefas de Resposta	As Tarefas de resposta capturam todas as tarefas de resposta associadas a um incidente de segurança.
10	Registros relacionados	A guia Registros relacionados consiste em todas as listas relacionadas da IU clássica nesta seção. As listas relacionadas são agrupadas em várias seções, como impacto nos negócios, informações sobre ameaças e assim por diante, para facilitar a navegação.
11	Outros registros	A guia Outros registros consiste em registros de TI, como solicitações de mudanças, incidentes e e-mails agrupados e exibidos nesta seção.
12	Guia Análise pós-incidente	Conforme o incidente de segurança avança para o estado Revisão, a guia Revisão pós-incidente é exibida com as avaliações e relatórios pós-incidente na guia.
13	Menu contextual	Fornece acesso fácil às ações rápidas e está disponível em todas as guias para o analista acessar sempre que necessário. O menu contextual fornece navegação fácil para vários recursos, como: **1.** Fluxo de atividades **2.** Playbook **3.** Assistência de Analista **4.** Runbook **5.** Modelos **6.** Anexos
14	Ações de IU do formulário	As várias ações de IU do formulário de incidente de segurança são exibidas no canto superior direito do formulário de incidente. As ações de IU de formulário disponíveis são: • Discutir • Salvar • Criar Tarefa de Resposta

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número	Nome	Descrição
		• Compor E-mail • Adicionar Playbook • Abrir fluxo ou fluxos de trabalho associados • Incidente do Crete • Criar Problema • Criar solicitação de mudança • Criar indisponibilidade • Calcular Gravidade • Vincular a Incidente grave de segurança • Propor como Incidente grave de segurança • Promover a Incidente grave de segurança • Executar ações adicionais no endpoint • Associar técnica do MITRE ATT&CK • Alternar para a IU Clássica • Adicionar ao Caso de Segurança • Excluir Para obter mais informações, consulte Como trabalhar com ações de IU de formulário.

Seção Visão geral do incidente de segurança

A seção Visão geral no espaço apresenta as principais informações associadas ao incidente de segurança.

Os gráficos de rosca são habilitados para detalhamento, quando um analista seleciona qualquer um dos itens do gráfico, ele direciona você para o respectivo registro com uma exibição de lista filtrada de itens na guia correspondente. Por exemplo, se **Observáveis maliciosos** for selecionado, você será direcionado para os observáveis com uma exibição de lista filtrada de observáveis maliciosos na guia **Registros relacionados**.

A seção Visão geral exibe o seguinte:

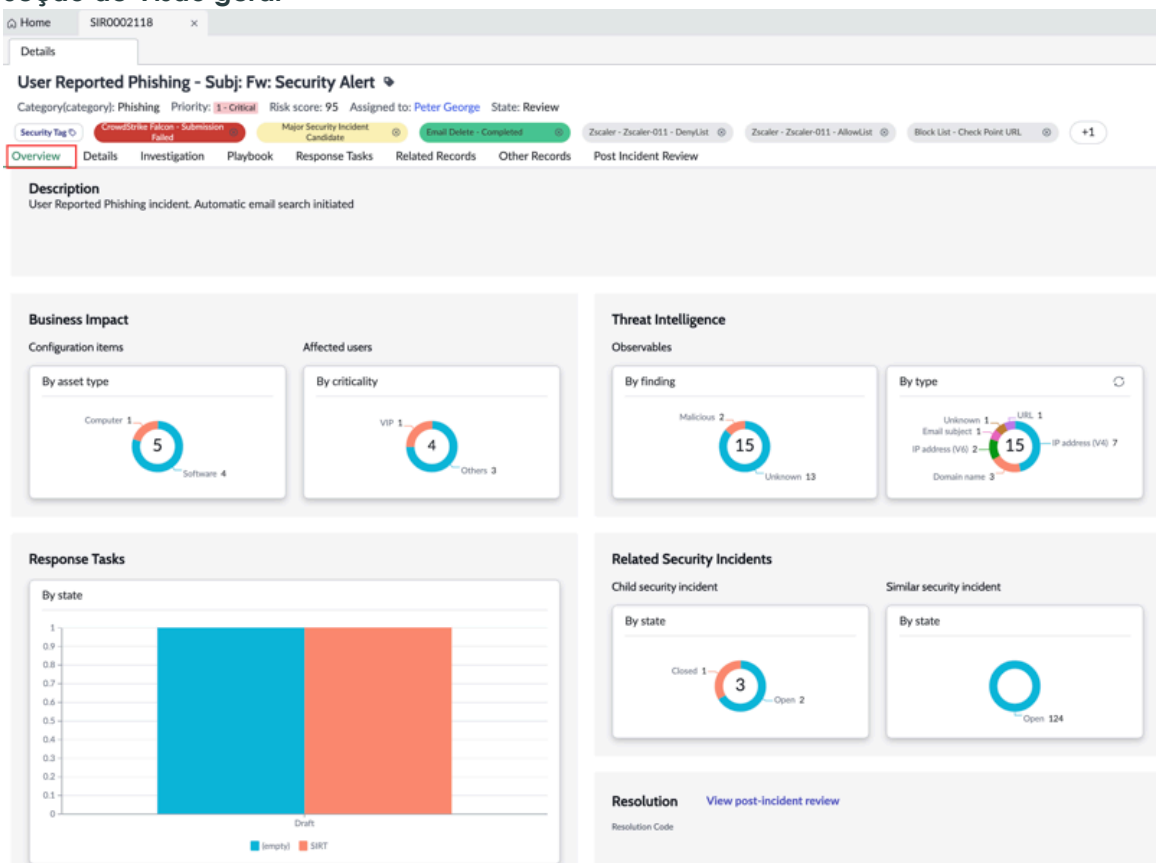
- Descrição do incidente de segurança.
- Detalhes do impacto nos negócios, como os itens de configuração por tipo de ativo e usuários afetados por criticidade - sejam usuários VIP ou outros usuários.
- Itens de inteligência contra ameaças, como observáveis, descobrindo se os observáveis são maliciosos ou desconhecidos e por tipo.
- Tarefas de resposta por estado e grupo de atribuição.
- Incidentes de segurança relacionados que compreendem incidentes de segurança secundários por estado - aberto ou fechado, e incidentes de segurança semelhantes por estado - aberto ou fechado.
- A seção Resolução é exibida quando um incidente passa para o estado Revisão e, em seguida, a seção de resolução é exibida na seção **Visão geral** com uma capacidade de exibir a revisão pós-incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Resolução - exibir análise pós-incidente: selecione o link para navegar até a página de **análise pós-incidente**.
- Depois que o incidente é encerrado, a seção Resolução exibe o código de resolução, as anotações de resolução e o resolvido por (usuário) junto com os detalhes da análise pós-incidente.

Seção de Visão geral



Incidente de segurança Seção de detalhes

Esta seção exibe os campos do formulário de incidente de segurança que são renderizados a partir da IU clássica de incidente de segurança.

A IU clássica tem uma exibição chamada Exibição de **SIRW** criada. Esta exibição é mapeada para a guia **Detalhes** no novo espaço. Todas as personalizações necessárias precisam ser implementadas nesta exibição.

Os campos de formulário são agrupados nas seguintes seções e exibidos na exibição de formulário da guia Detalhes. Clique em qualquer seção ou vá para a respectiva seção no formulário:

- Incidente de segurança
- Prioridade
- Origem
- Primário
- Atribuição
- Controles de acesso

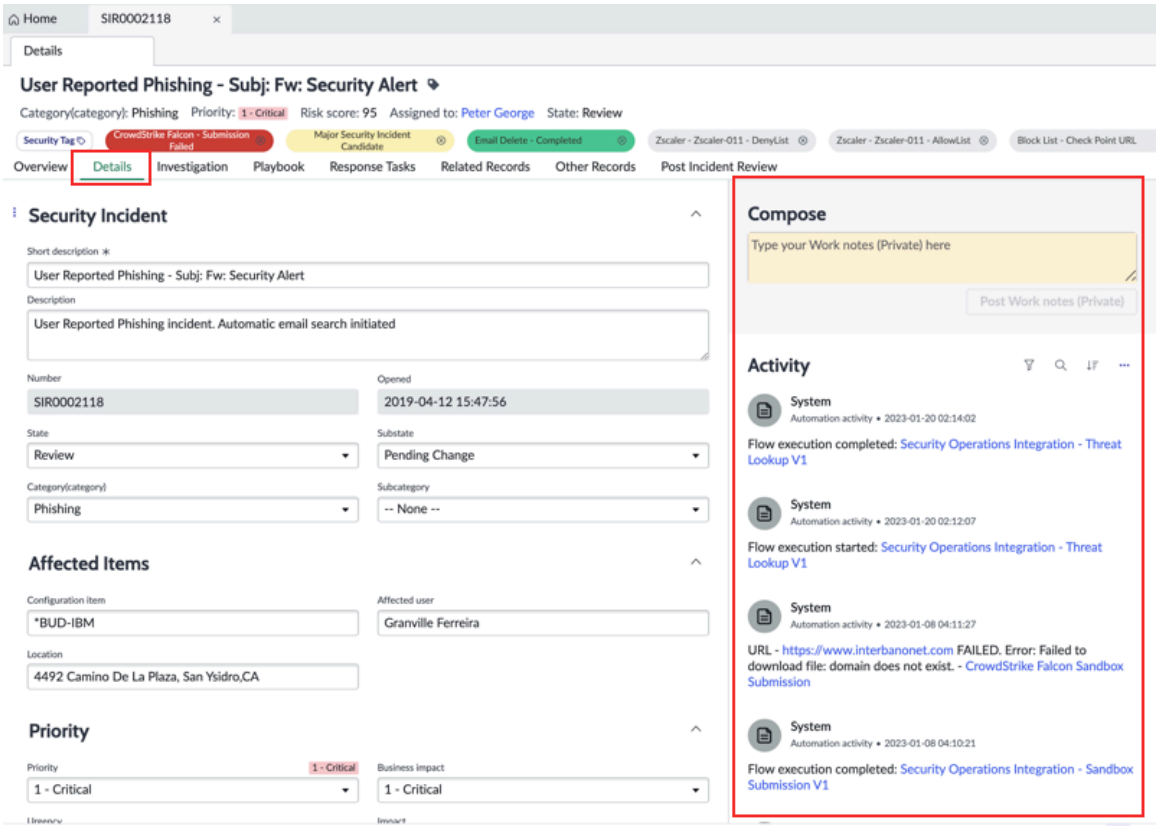
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Itens afetados
- Resolução

A guia **Detalhes** contém a seção Fluxo de **atividades** no próprio formulário de detalhes para um acesso rápido aos analistas de segurança para adicionar comentários e publicá-los.

Guia Detalhes e Fluxo de atividades



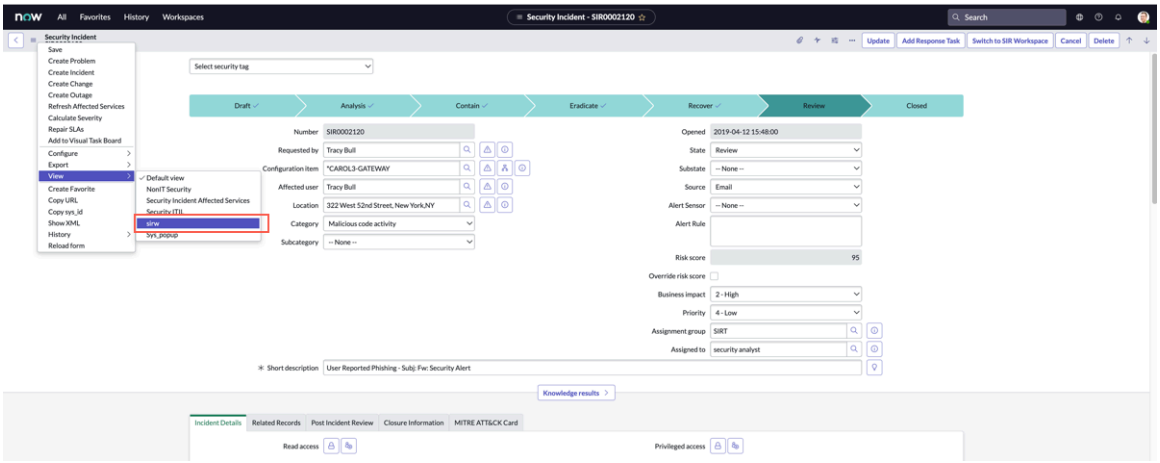
Veja a exibição do Espaço do analista de SIR:

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes abertos**.
2. Selecione qualquer registro de incidente de segurança.
3. Clique no menu de contexto e selecione **Exibição** > **SIRW**.

Nota: Você pode personalizar usando a exibição do espaço **sirw** no formulário de IU clássico.

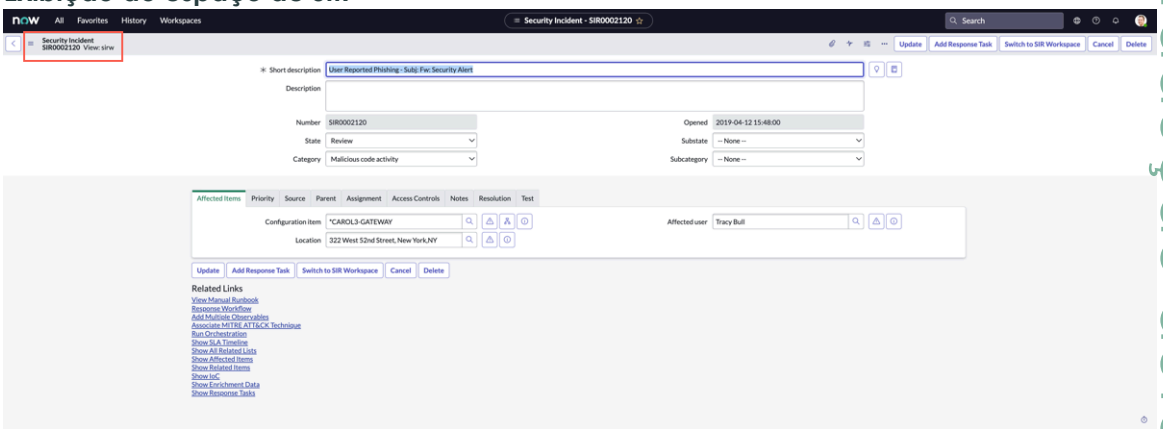
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



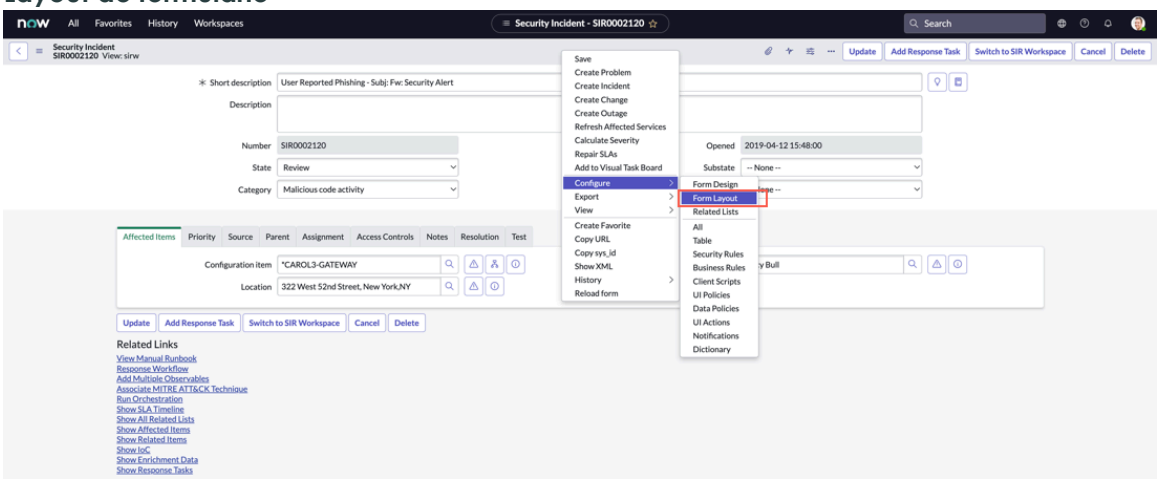
4. A exibição do espaço de incidente de segurança é renderizada conforme mostrado abaixo.

Exibição do espaço de SIR



5. No registro de Incidente de segurança, clique com o botão direito do mouse e vá para **Configurar** > **Layout do formulário**.

Layout do formulário

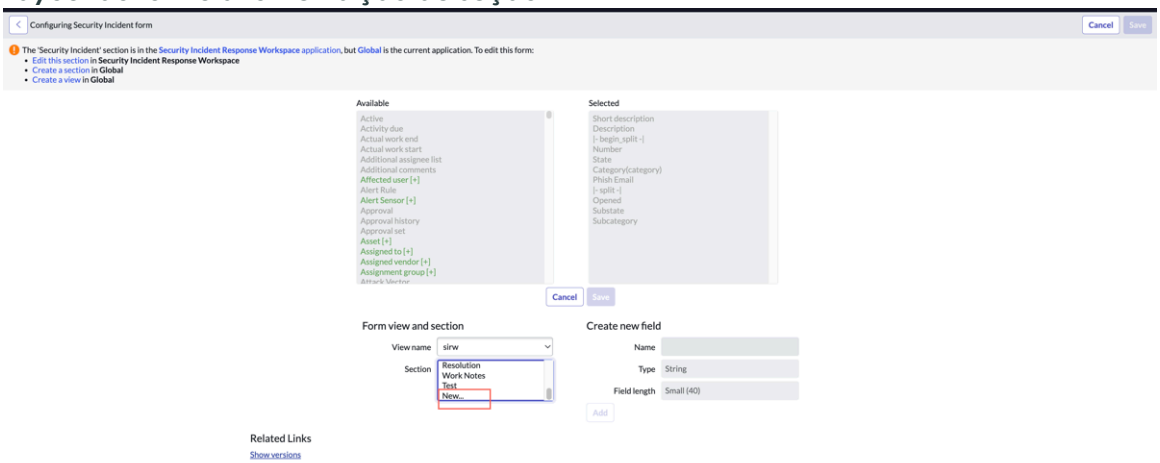


6. Faça um detalhamento ativo até a **exibição de formulário e a seção** e selecione **Novo** da **seção** para criar uma nova seção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

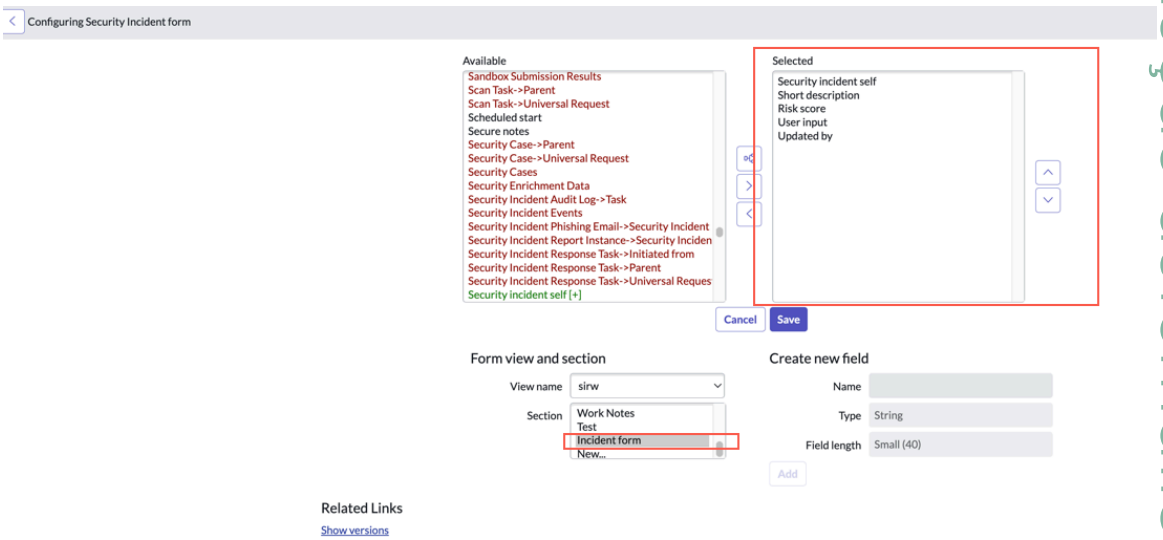
Layout do formulário - exibição de seção



7. Forneça o novo nome da seção e clique em **OK**.

Por exemplo, formulário Incidente.

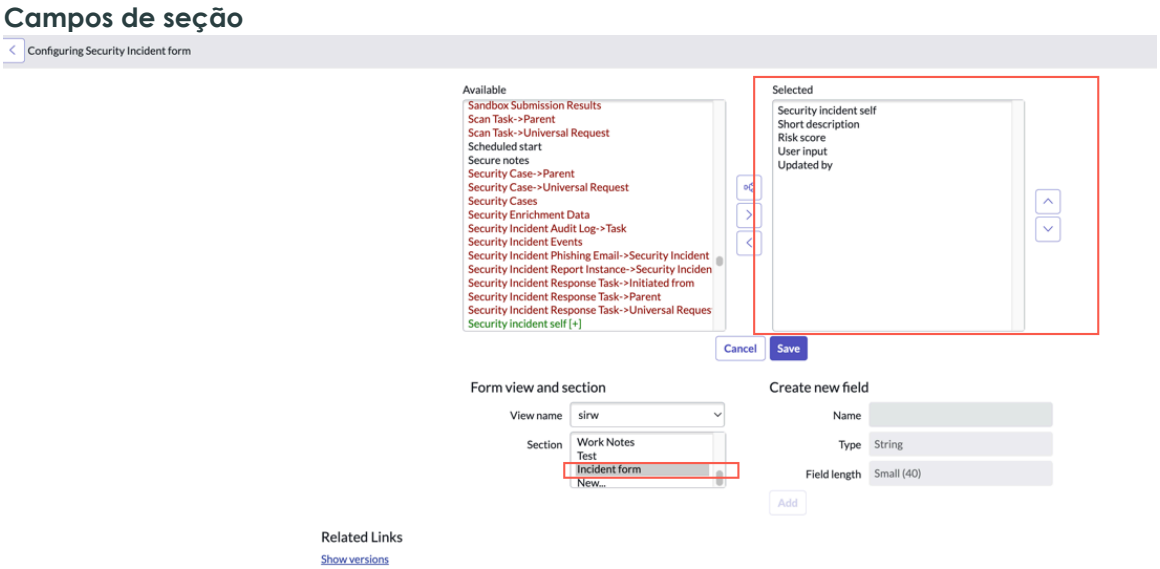
8. A nova seção é criada e adicionada à **Seção**.



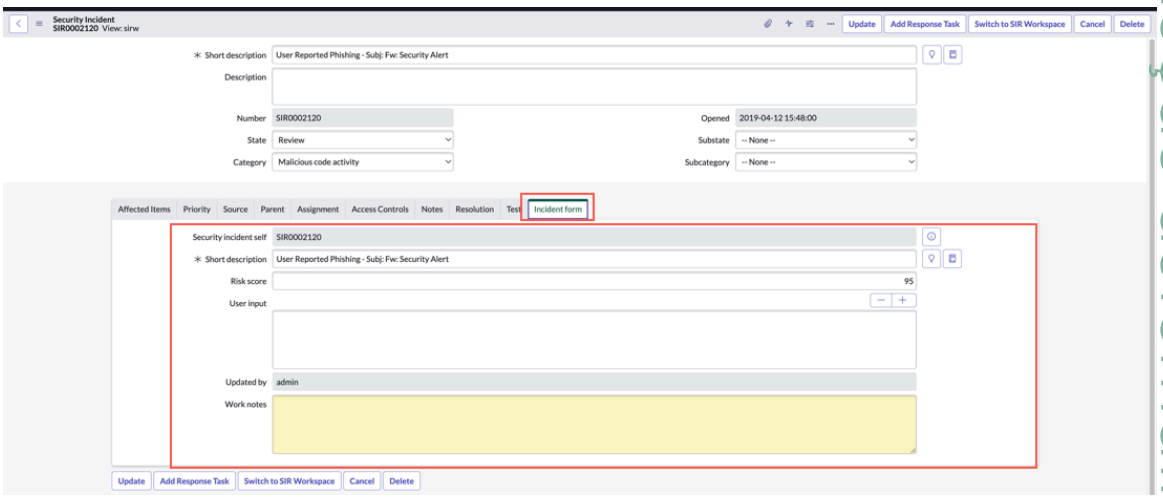
9. Selecione sua nova seção e adicione os campos de seção necessários ao slush bucket e clique em **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. A seção recém-adicionada é exibida junto com o layout da seção existente no formulário de incidente de segurança.



11. Agora, clique em **Alternar para o espaço SIR** para ir para o formulário de incidente de segurança e a seção personalizada na guia **Detalhes** do espaço.

Espaço SIR Orquestração

Espaço de resposta a incidentes de segurança As atividades de orquestração ajudarão os analistas de segurança a exibir a tela de investigação e executar várias ações aplicáveis.

Espaço SIR Tela de investigação

Espaço de resposta a incidentes de segurança permite que os analistas de segurança exibam as principais informações associadas ao incidente de segurança durante o processo de correção de incidentes. As informações principais também incluem as listas relacionadas, como Observáveis, Resultados de pesquisa de ameaças, Pesquisa de detecções, Aprimoramento de observável e assim por diante.

Na IU clássica, a maioria das ações de orquestração associadas às integrações prontas para uso está disponível nas listas relacionadas. Por exemplo, Executar pesquisa de ameaças, Executar aprimoramento de observável etc. estão presentes na lista relacionada

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de observáveis associados. Da mesma forma, Obter detalhes do host, Obter estatísticas de rede e assim por diante estão disponíveis na lista relacionada Itens de configuração.

Quando um analista de segurança executa essas ações, os resultados são preenchidos em uma lista relacionada diferente. Por exemplo, quando um usuário executa Executar pesquisa de ameaças, os resultados ficam disponíveis na tabela Resultados da pesquisa de ameaças. Às vezes, os resultados estão disponíveis em várias tabelas diferentes. Durante esse processo, os analistas de segurança têm uma experiência do usuário separada e desorganizada ao correlacionar as informações de vários locais.

No novo Espaço SIRredesenhado, a tela de **investigação** (guia) fornece todas as informações necessárias agrupadas logicamente em um local para o analista realizar a investigação.

Explorar tela de investigação

O objetivo primário da tela de investigação é apresentar os dados necessários do incidente de segurança em um local comum.

Dentro do Espaço SIR, a investigação de incidentes de segurança gira principalmente em torno de alguns pontos de entrada principais.

A seguir estão alguns pontos de entrada principais que são provisionados para os analistas de segurança no sistema de base:

- Observáveis Associados
- Itens de configuração
- Usuários afetados
- E-mails de Phishing Associados
- Pesquisa de E-mail

Você também pode configurar os pontos de entrada acima adicionando, modificando ou removendo os pontos de entrada conforme aplicável. Para obter mais informações, consulte Configurar investigação de tempo de design de SI.

Na guia **Investigação**, a tabela de ponto de entrada atua como a tabela primária. Todas as tabelas que contêm os resultados de uma ação de orquestração realizada na tabela primária são apresentadas como tabelas secundárias no ponto de entrada.

Por exemplo, para o ponto de entrada de **Observáveisassociados, a tabela Observáveis associados** é a tabela primária e outras tabelas, como Resultados de pesquisa de ameaças, resultados de envio da área restrita e assim por diante, são a tabela secundária.

O Analista de segurança pode executar todas as ações de orquestração na tabela Observáveis associados e poderá exibir todas as informações associadas na mesma página, sem a necessidade de navegar por vários locais.

Nota: Quando um usuário clica nos gráficos interativos na página **Visão geral**, como observáveis maliciosos, o usuário será direcionado para a exibição filtrada de observáveis maliciosos na tela de investigação. Como alternativa, o usuário pode iniciar diretamente a investigação navegando até a tela de investigação que terá todos os dados.

A lista de tabelas secundárias em um ponto de entrada também é configurável. Para obter mais informações, consulte Configurar investigação de tempo de design de SI.

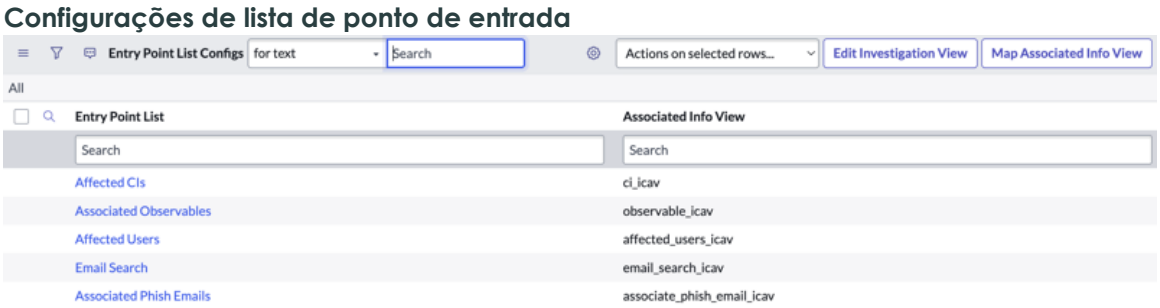
A seguir está um exemplo detalhado de um ponto de entrada (observável associado) que é configurado e provisionado no sistema de base:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecione o ponto de entrada **Observáveis associados** na lista suspensa.

   Aqui, a tabela primária também é **Observável associado**.



2. Selecione um ou mais observáveis da tabela primária.
3. Execute a capacidade desejada.

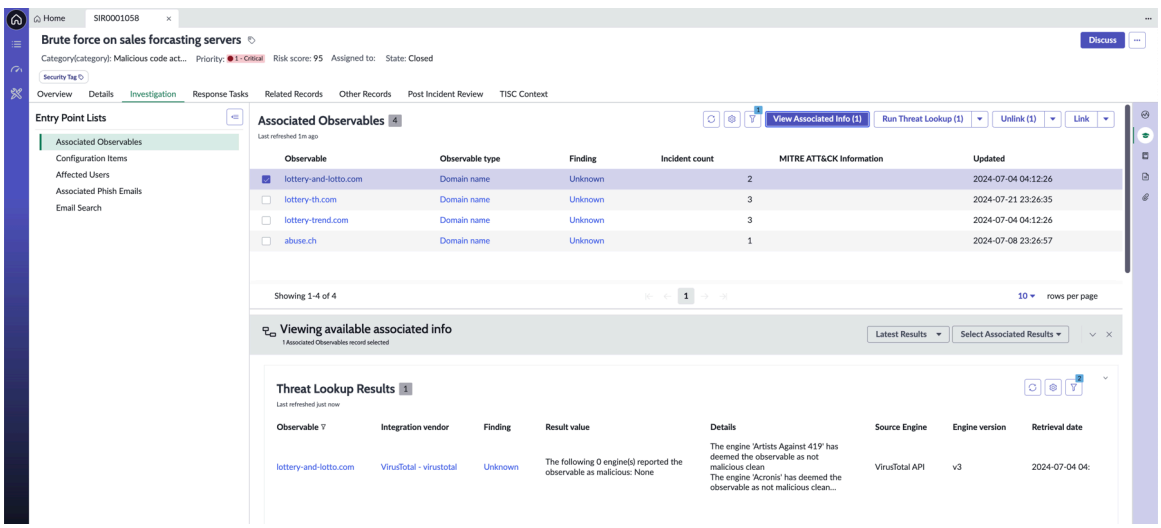
   Por exemplo, selecione **Executar pesquisa de ameaças** para buscar os resultados da pesquisa de ameaças para um observável selecionado.

   Nota: Quando uma ação de observável correspondente é executada, o processo é executado no back-end e os resultados são exibidos abaixo da lista de Observáveis.

4. Clique em **Exibir informações associadas** para exibir os resultados dos observáveis. Os resultados são exibidos na mesma página.

   Nota: Você pode exibir os resultados usando filtros por resultados, selecione **Todos os resultados** ou **Últimos resultados**, o que for a exibição desejada. Por padrão, os resultados mais recentes são exibidos. Se houver várias implementações (de integrações), os resultados mais recentes por implementação serão mostrados.

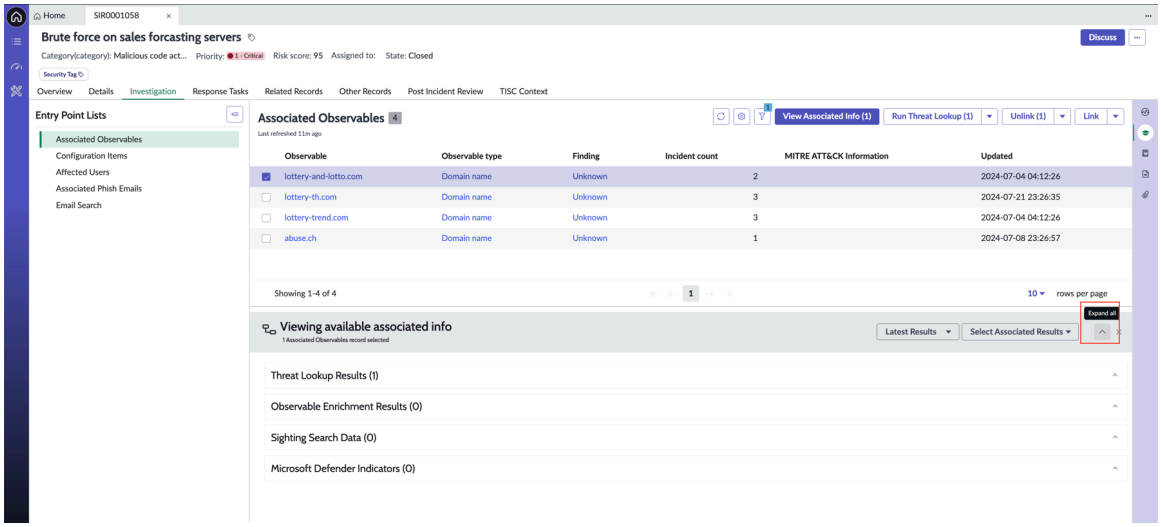
   Além disso, você pode filtrar os resultados **por listas relacionadas associadas**, que são os resultados da tabela secundária. Por padrão, todas as listas relacionadas à tabela secundária configurada são exibidas. Para obter mais informações, consulte Configurar investigação de tempo de design de SI. No entanto, você pode optar por selecionar somente as tabelas secundárias necessárias.



Tradução automática

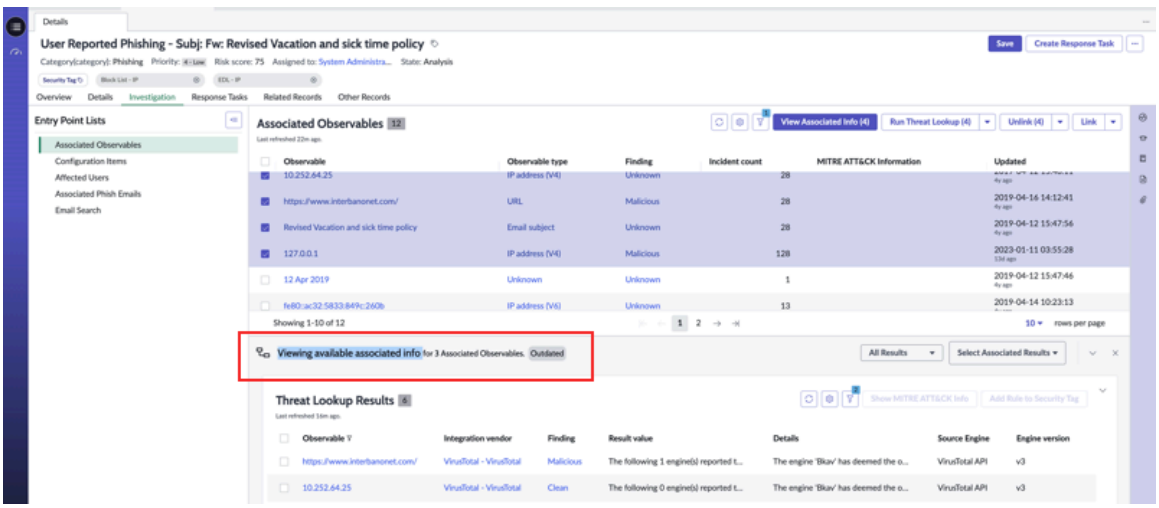
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Ao clicar em **Exibir informações associadas,** você pode exibir todos os dados da tabela secundária associada em um só lugar. No entanto, você pode fechar a exibição de listas relacionadas selecionando o botão **Fechar exibição**. Depois de fechar a exibição, você só poderá ver a tabela primária de observáveis como antes.
6. Clique no ícone **Expandir tudo** na direção ascendente na tabela **Exibição de resultados de informações associadas disponíveis** para expandir todos os dados da tabela secundária de listas relacionadas.



7. Clique no ícone de direção descendente de **Recolher tudo** para recolher todos os dados da tabela secundária de listas relacionadas.

> **Nota:** A faixa na parte superior da seção de informações associada que contém todos os dados da tabela secundária mostra quantas informações relacionadas ao observável estão sendo apresentadas ao usuário. Por exemplo, inicialmente, se você selecionar dois observáveis e clicar em **Exibir informações associadas**, a faixa mostrará **Exibição de informações associadas disponíveis para 2 observáveis associados.**. Se você selecionar, por exemplo, outro observável, a faixa informará que as informações estão desatualizadas (captura de tela abaixo). Você precisará clicar em **Exibir informações associadas** novamente para obter os dados mais recentes.



Além da exibição abrangente acima das informações associadas aos observáveis, se você quiser exibir mais informações sobre um registro na tabela primária, clique no observável e o formulário de registro da tabela primária será aberto em uma guia

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

diferente com uma exibição mais detalhada do registro selecionado. Todos os dados da tabela secundária associada desse registro selecionado específico também são apresentados na seção **Informações associadas**.

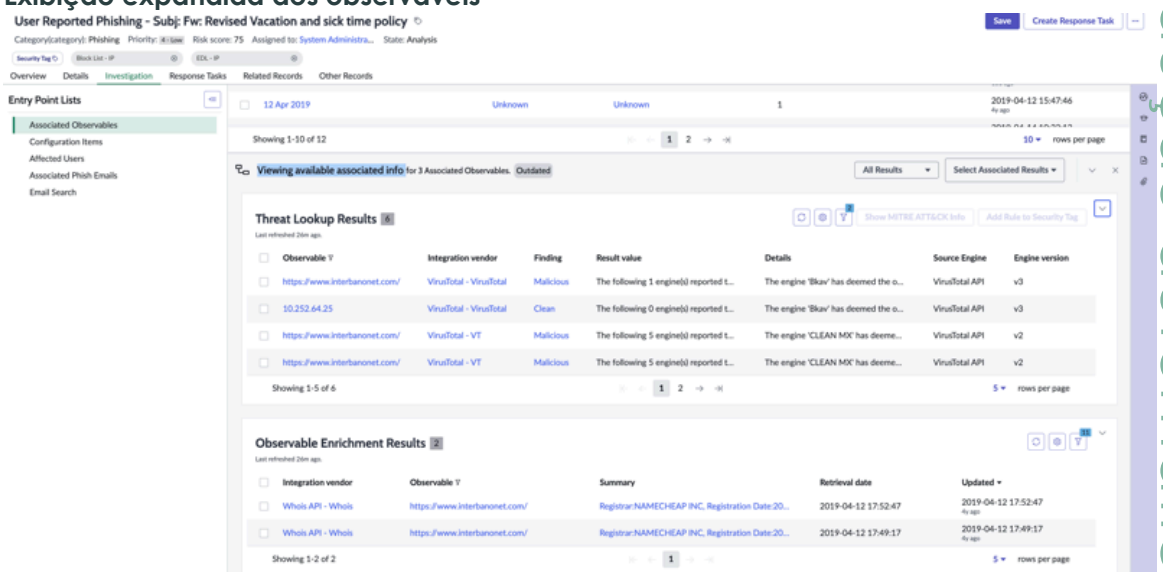
No entanto, a seção de informações associada exibe somente os resultados mais recentes da tabela secundária, conforme visto na tela de investigação, no modo somente leitura. Nenhuma ação é possível nesta exibição. A página de formulário da tabela secundária pode ser aberta em uma nova guia que renderizará a página totalmente funcional com todas as ações, se houver.

Você pode alternar entre as diferentes tabelas usando a lista suspensa. Você também pode expandir ou recolher cada formulário na seção de informações associada.

Na página do formulário **Observável** (página do formulário de registro da tabela primária), você pode executar determinadas ações conforme disponíveis. Sempre que executar uma ação, você pode clicar em Atualizar na faixa de informações associada para atualizar os dados.

8. Clique em **Expandir tudo** para expandir todas as tabelas secundárias de listas relacionadas. Por padrão, todos os secundários são expandidos.

Exibição expandida dos observáveis



Informações relacionadas

Configurar investigação de tempo de design de SI

Estrutura de experiência unificada para integrações fornecidas pelo Capability Framework

Na IU clássica, a experiência é separada ao executar atividades de orquestração, como executar pesquisa de ameaças, executar pesquisa de detecções e assim por diante. Cada capacidade tem sua própria experiência ao executá-la. No novo espaço, há uma experiência unificada em todas as capacidades.

A experiência unificada é aplicável somente para as integrações e atividades de orquestração que se enquadram na estrutura de capacidades. Pode haver ações específicas para integração, por exemplo, Criar indicadores no Microsoft Defender. Essas ações terão sua própria experiência conforme exigido pelo caso de uso.

A nova estrutura consiste em telas modais com três etapas, conforme explicado abaixo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. **Implementações**: a primeira etapa envolve a seleção de uma ou mais implementações que estão presentes em relação à capacidade selecionada.

   Por exemplo, quando o analista clicar em **Executar pesquisa de ameaças**, o analista poderá selecionar uma ou mais implementações que estão presentes para a **capacidade Executar pesquisa de ameaças**.

   Cada implementação terá os detalhes da origem da integração. Consulte a tabela abaixo. Informações adicionais também são apresentadas em relação a cada implementação.

   As informações adicionais podem incluir, por exemplo, informações sobre filtros, tipos de observáveis compatíveis etc. As informações adicionais podem ser configuradas conforme desejado. Para obter mais informações, consulte o procedimento de configuração técnica da estrutura de UX.

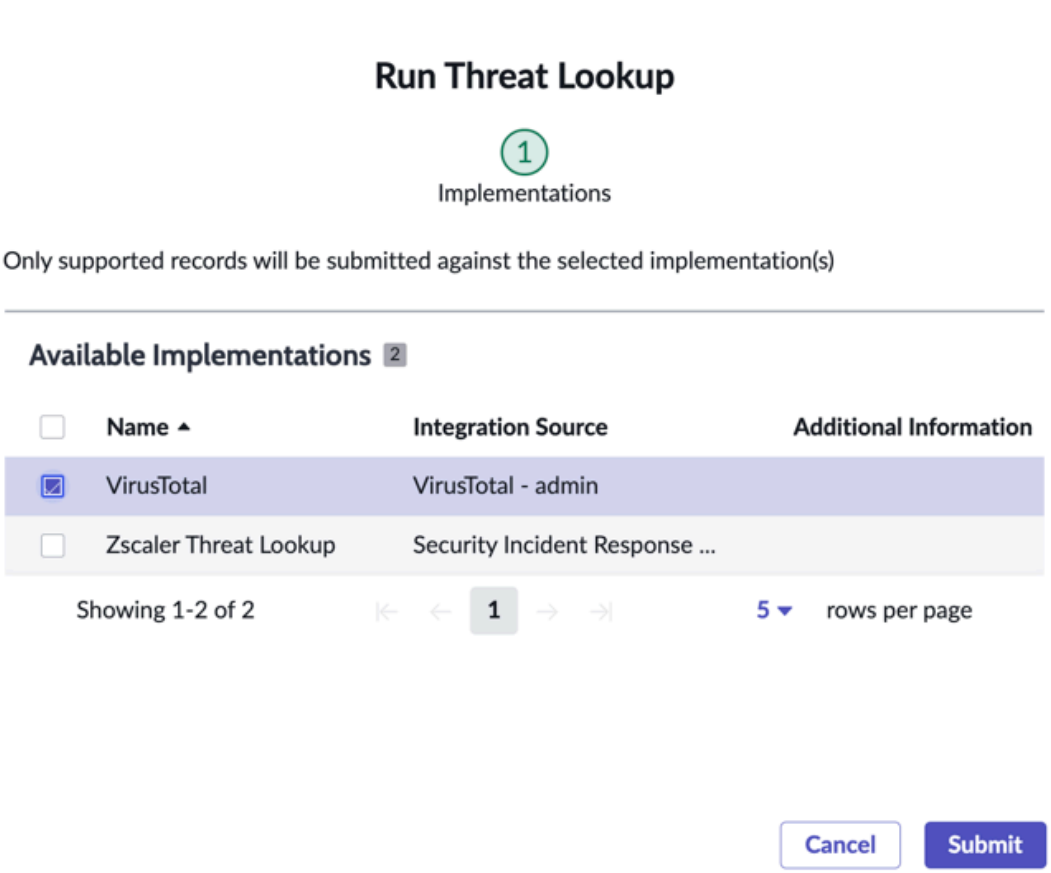
Modal da Estrutura de implementação unificada

Implementação	Descrição
Nome	Nome da implementação.
Origem da Integração	A origem da implementação, como a configuração que está sendo usada.
Informações adicionais	Esta coluna captura as informações estáticas que adicionam mais contexto ao analista de segurança em relação às implementações selecionadas para prosseguir com uma ação. Por exemplo, suporte ou informações filtradas. Além disso, se uma implementação oferecer suporte apenas a um determinado tipo de observáveis, como Domínio ou URL, você poderá adicionar essas informações adicionais aqui nesta coluna para fornecer o contexto ao usuário. **Nota:** A estrutura de IU basicamente permitiria a seleção de qualquer tipo de implementação e qualquer tipo de observável. Durante o envio, as integrações do sistema de base existentes que são enviadas cuidarão da filtragem no back-end e enviarão somente o tipo compatível de observáveis. O restante dos registros que não correspondem à capacidade de suporte será ignorado. Portanto, uma mensagem de informações de IU é exibida enquanto você seleciona a capacidade: **Somente registros compatíveis serão enviados em relação às implementações selecionadas.**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tela 1: Implementação(ões)

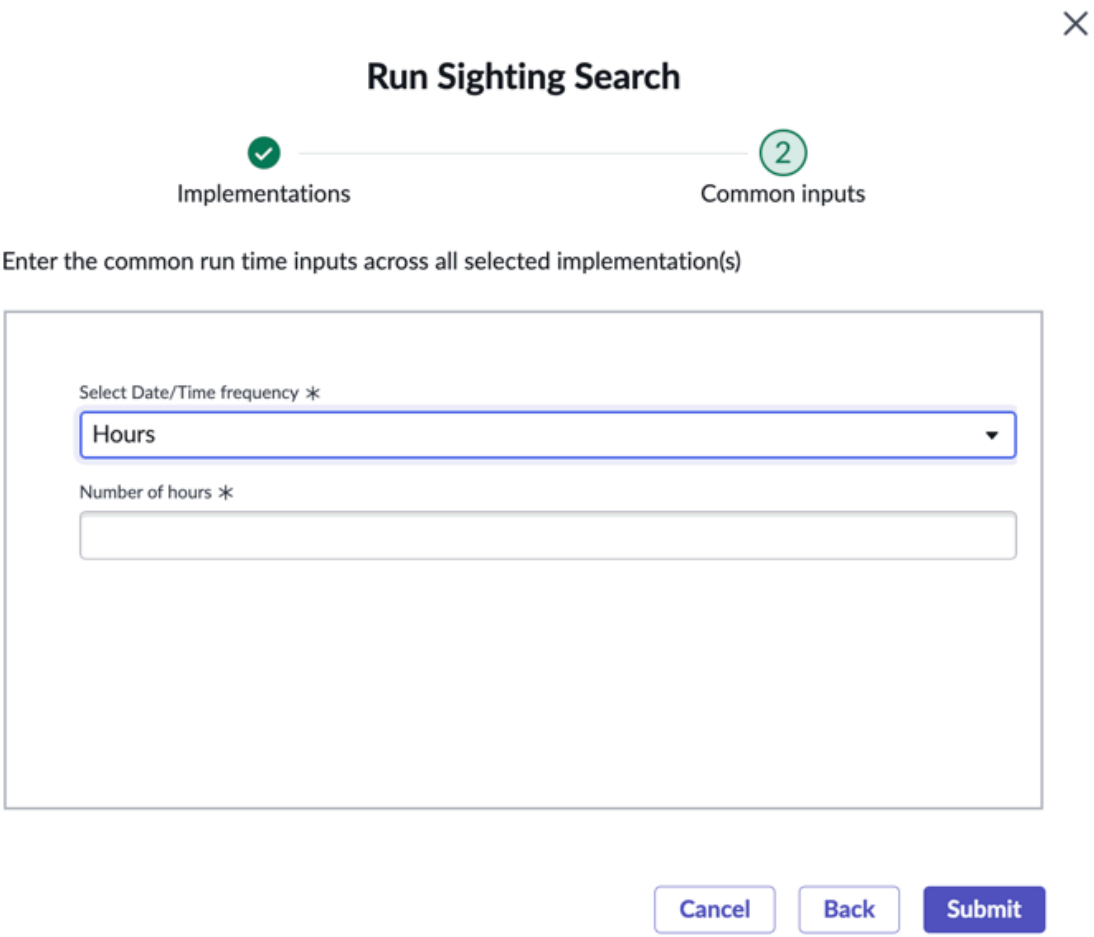


2. **Entradas comuns**: adicione entradas comuns para as implementações selecionadas ou para todas as implementações aplicáveis selecionadas. Esta é a tela 2 da sua implementação. Por exemplo, a partir de agora, somente a **Pesquisa de detecções** tem a tela de entradas comuns. Esta implementação é uma combinação da tela 1 (implementações) e da tela 2 (entradas comuns).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tela 1 + Tela 2



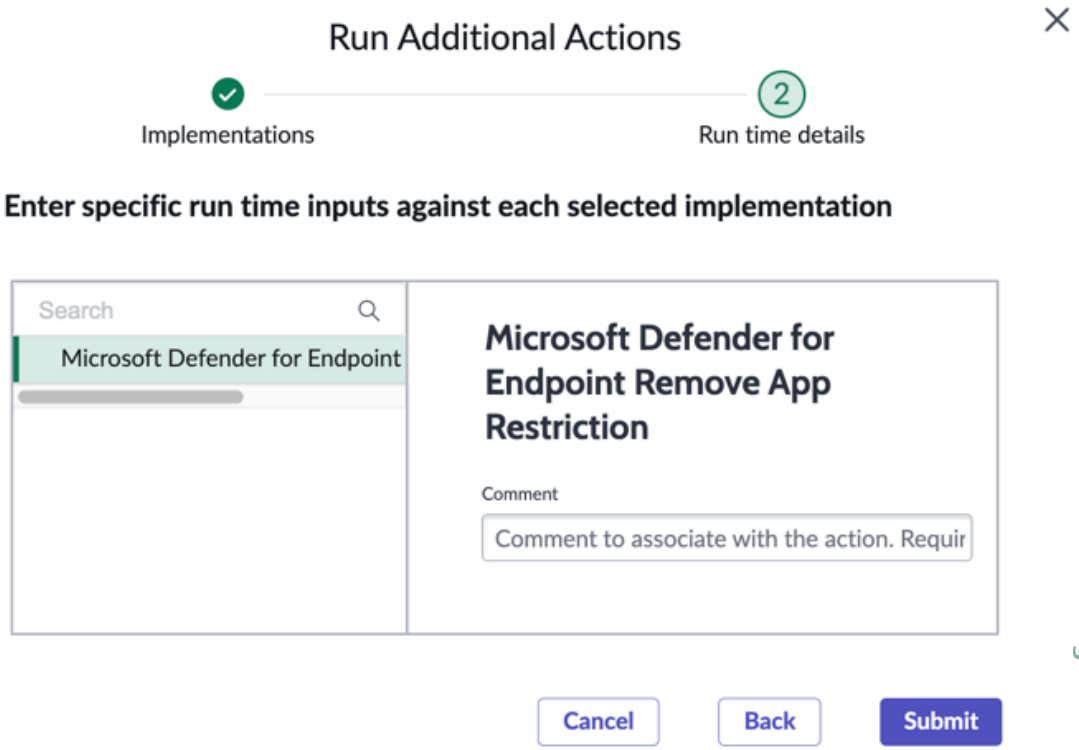
3. **Detalhes do tempo de execução**: adicione entradas de tempo de execução específicas para as implementações selecionadas que são diferentes umas das outras. Esta é a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

tela 3 da sua implementação. Esta implementação é uma combinação da tela 1 (Implementações) e da tela 3 (entradas de tempo de execução específicas).

Entradas específicas



Nota: Nem todas as três etapas são sempre necessárias. Dependendo da capacidade e do tipo de entradas necessárias, a etapa de detalhes do tempo de execução e a etapa de entradas comuns ficarão visíveis.

Recursos da experiência unificada e telas modais

A tabela a seguir descreve as capacidades e as telas aplicáveis.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Executar pesquisa de ameaças	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis a Executar pesquisa de ameaças. Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• Total de vírus • Hybrid Analysis • Security Incident Response Integration with Zscaler • Phistank • Metadefender • Ameaça • Estou penhorado? • Crowd-Strike Falcon Intelligence

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
Executar Aprimoramento Observável	Somente a Tela 1 - Selecionar implementações é aplicável Não há entradas comuns ou entradas específicas de implementação aplicáveis a Executar aprimoramento de observável. Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• MISP • Endpoint do Microsoft Defender • Shodan • RiskIQ • WHOIS • Reverter WHOIS
Executar pesquisa de detecções/Executar pesquisa de detecções na Web/Executar pesquisa de detecções por e-mail	Tela 1 – **Selecionar implementações** e Tela 2 – **Entradas comuns** são aplicáveis. A pesquisa de detecções usa a frequência de data e hora como entradas comuns em várias implementações do Splunk e outras integrações. Esta tela será apresentada ao analista de segurança para capturar frequências de data e hora. Para integrações que não exigem essas entradas, por exemplo, FireEye HX, elas serão ignoradas. Depois de selecionar uma ou mais implementações e fornecer entradas comuns, o Analista de segurança poderá enviar a ação.	• Aprimoramento de Splunk-incident • Carbon Black • Pesquisa elástica • FireEye HX • ESM da McAFee • MSFT Defender para endpoint • Detecção do Splunk • Pesquisa de detecções do QRadar • MISP
Enviar para área restrita	Tela 1 – Selecionar implementações e Tela 3 – Entradas específicas de implementação são aplicáveis. Enviar para área restrita usa entradas diferentes para implementações diferentes. Não há entradas comuns	• Integração do CrowdStrike Falcon X Sandbox • Security Incident Response Integration with Zscaler

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	para esta capacidade no momento. Por exemplo, quando o analista seleciona Crowdstrike Falcon X Quick Scan, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux e Zscaler, as entradas variam. A verificação rápida do Crowdstrike Falcon X e o Zscaler não precisam de mais entradas de tempo de execução. O Crowdstrike Falcon X Windows 64 usa entradas de tempo de execução opcionais que diferem do Crowdstrike Falcon X Linux. Portanto, eles podem ser fornecidos na tela 3 especificamente em relação a implementações individuais selecionadas conforme aplicável.	
Publicar na Watchlist	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis a **Publicar na lista de observação**. Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	Host do Crowdstrike Falcon
Permitir/bloquear solicitação	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis à **solicitação de permissão/bloqueio**.	• NGFW da Rede Palo Alto • NGFW do ponto de verificação • Security Incident Response Integration with Zscaler

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	
Obter detalhes do host	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter detalhes do host. Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• FireEye HX • Microsoft Defender para Ponto de Extremidade
Obter arquivo	Tela 1 – Selecionar implementações e Tela 2 – Entradas comuns são aplicáveis. Obter arquivo usa o nome do arquivo e o caminho como entradas comuns. Depois de selecionar uma ou mais implementações e fornecer entradas comuns, o Analista de segurança poderá enviar a ação.	FireEye HX
Obter estatísticas de rede	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter estatísticas de rede. Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analis-	• FireEye HX • NetStat

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	ta de segurança poderá enviar a ação.	
Obter processos em execução	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para obter processos em execução. Portanto, somente a tela 1 é apresentada ao analista de segurança para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista de segurança poderá enviar a ação.	• FireEye HX • Carbon Black • Comando do Sistema
Obter serviços em execução	Somente a Tela 1 - Selecionar implementações é aplicável. Não há entradas comuns ou entradas específicas de implementação aplicáveis para Obter serviços em execução. Portanto, somente a tela 1 é apresentada ao analista para selecionar uma ou mais implementações. Depois de selecionar as implementações, o analista poderá enviar a ação.	FireEye HX
Isolar host/Remover isolamento de host	Tela 1 – Selecionar implementações e Tela 3 – Entradas específicas de implementação são aplicáveis. Isolar host/desfazer isolamento de host usa entradas diferentes para implementações diferentes. Não há entradas comuns para esta capacidade no momento. Por exemplo, quando o analista seleciona FireEye HX e Microsoft Defen-	• FireEye HX • Endpoint do Microsoft Defender • Carbon Black

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	der para endpoint, as entradas variam. O FireEye HX não precisa de entradas de tempo de execução. Por outro lado, o Microsoft Defender usa entradas como Tipo de isolamento e Comentários. Portanto, eles podem ser fornecidos na tela 3 especificamente em relação a implementações individuais selecionadas conforme aplicável.	
Executar ações adicionais	Tela 1 – Selecionar implementações e Tela 3 – Entradas específicas de implementação são aplicáveis. Executar ações adicionais O host usa entradas diferentes para implementações diferentes. Não há entradas comuns para esta capacidade no momento. Por exemplo, quando o analista seleciona o script de detalhes investigativos padrão do FireEye HX, a aquisição de triagem do FireEye HX e o descarregamento do registro do Crowdstrike Falcon Insight, as entradas variam. O script de detalhes investigativos padrão do FireEye HX e a aquisição de triagem do FireEye HX aceitam comentários como a entrada que pode ser diferente para ambos. O descarregamento do registro do Crowdstrike Falcon Insight usa a subchave como entrada. Portanto, eles podem ser fornecidos na tela 3 especificamente em relação a implementações individuais selecionadas conforme aplicável.	• FireEye HX • Microsoft Defender para Ponto de Extremidade • Crowdstrike Falcon Insight

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidade	Telas de estruturas de UX aplicáveis	Integrações compatíveis
	Nota: Atualmente, oferece suporte a apenas uma única seleção de implementação. Em versões futuras, a seleção múltipla de implementação será compatível.	

Exemplo de experiência unificada

Este exemplo demonstra as capacidades da estrutura de experiência unificada.

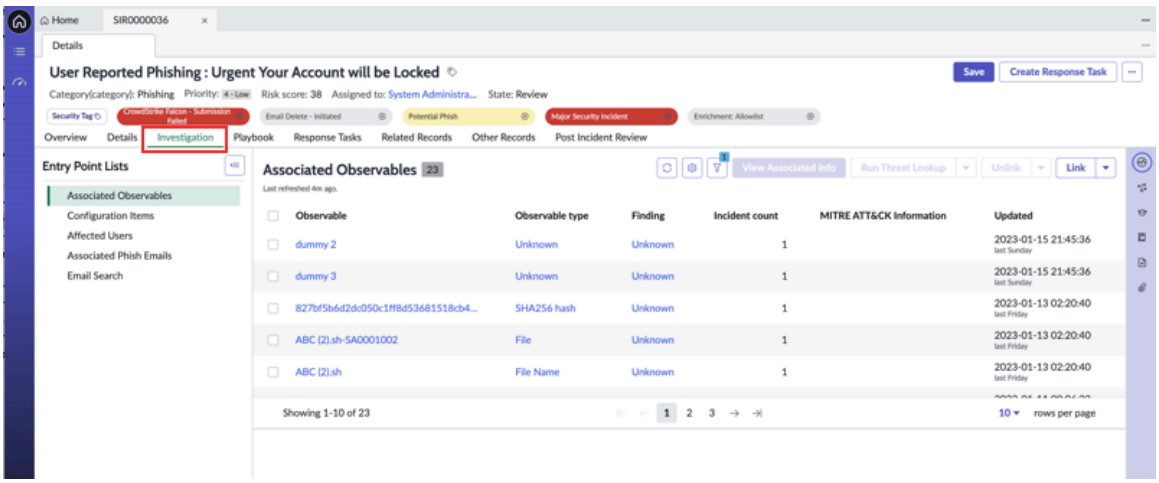
Exemplo 1: Selecionar implementações: pesquisa de ameaças

O exemplo abaixo demonstra as implementações.

Exemplo 1: somente tela 1: pesquisa de ameaças

Você pode executar a ação **Executar pesquisa de ameaças** relacionadas a capacidades de integração usando a guia **Investigação** do Espaço SIR.

1. Na guia **Investigação**, navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página.
2. Selecione qualquer ponto de entrada e execute a ação da capacidade de integração.



Nota: Você também pode navegar até a guia **Registros relacionados** no espaço para executar a ação de capacidades de integrações.

A**pesquisa de ameaças** é um dos exemplos que são descritos em detalhes sobre como executar as integrações.

Selecionar implementações

Selecione uma ou mais implementações conforme aplicável.

Antes de Iniciar
Função necessária: sn_si.analyst

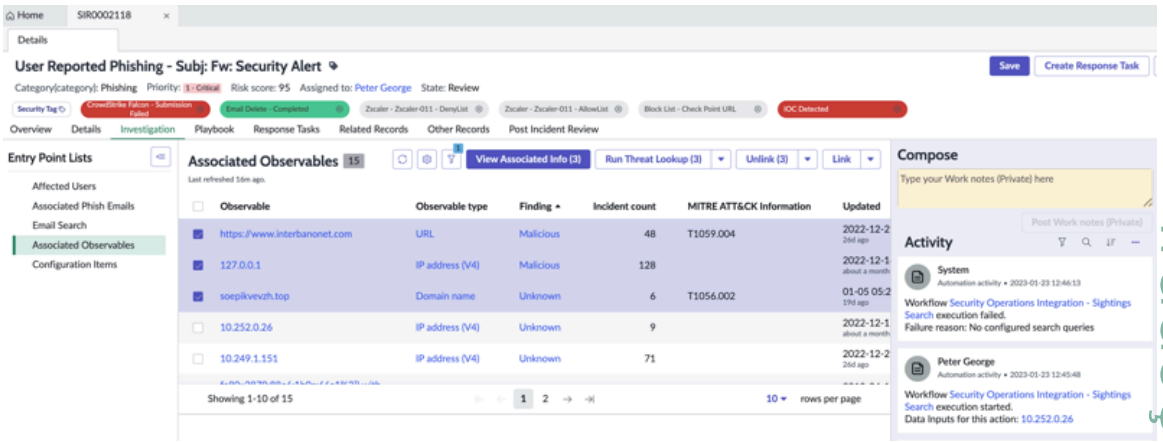
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As implementações disponíveis são listadas. Selecione as implementações. Depois de selecioná-las, somente os registros compatíveis serão enviados em relação a cada implementação selecionada.

Procedimento

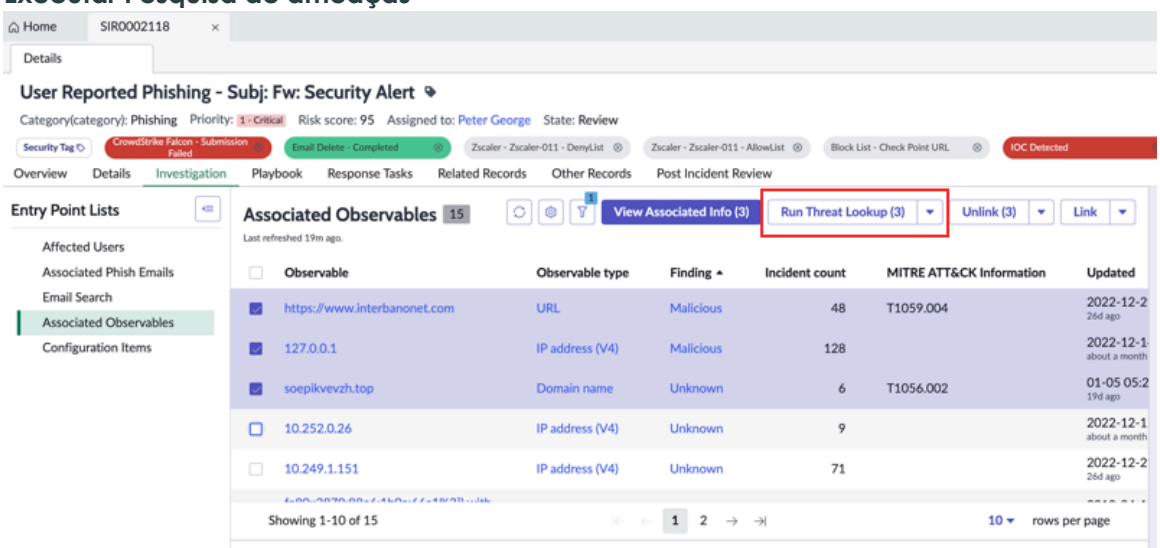
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para a guia **Investigação** do espaço.
   A guia de investigação com as listas de pontos de entrada é exibida.



4. Selecione o observável associado nas listas de ponto de entrada.
   Por exemplo, selecione **Observáveis Associados** lista relacionada. Os registros de observáveis correspondentes são exibidos.

> **Nota:** Você pode selecionar uma implementação para executar uma pesquisa nos observáveis selecionados ou pode executar a pesquisa selecionando todas as implementações.

Executar Pesquisa de ameaças



5. Marque a caixa de seleção de qualquer observável que você deseja executar a pesquisa de ameaças.
6. Navegue até o menu suspenso de ações de listas relacionadas que é exibido na parte superior da página de listas relacionadas.

Tradução automática

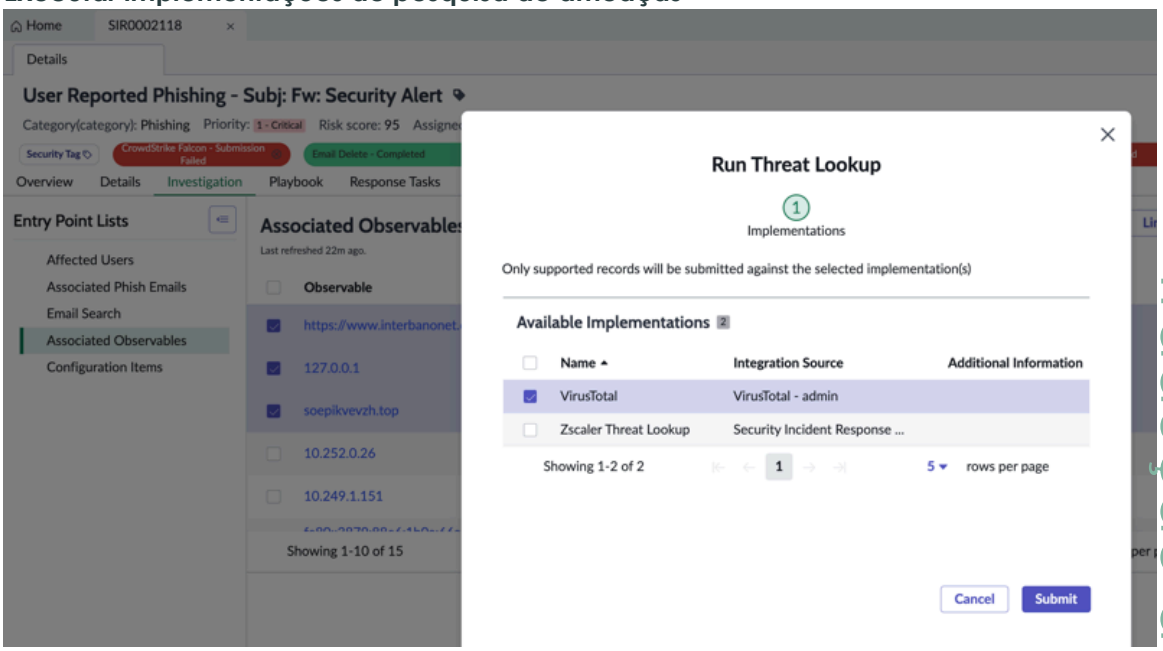
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Executar pesquisa de ameaças** para executar a ação de capacidades de integração relacionadas a informações sobre ameaças.

   Nota: A capacidade Executar pesquisas de ameaças realiza pesquisas de inteligência contra ameaças para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

   A tela do modal **Executar pesquisa de ameaças** é exibida.

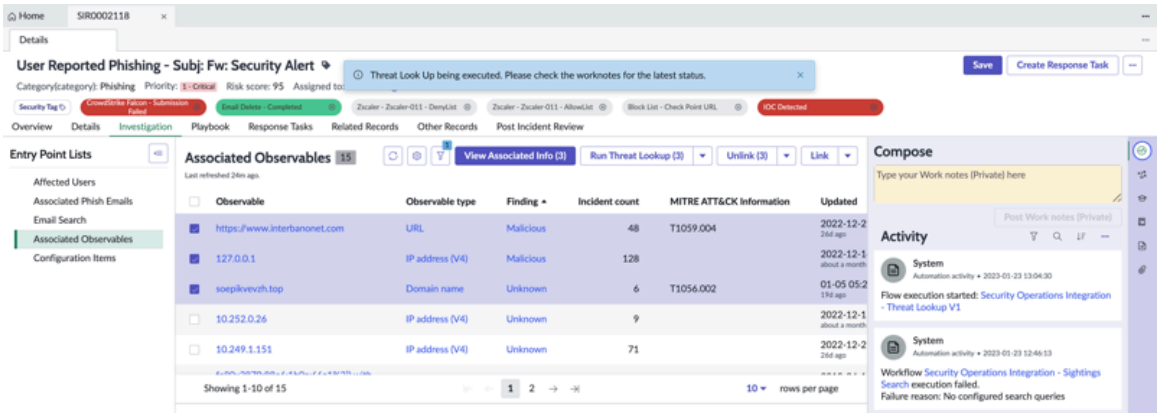
Executar implementações de pesquisa de ameaças



8. Selecione uma ou mais implementações na lista.
9. Clique em **Enviar**.
   Depois que os registros selecionados são enviados, uma mensagem é exibida informando que a pesquisa está sendo executada. Depois que a implementação é processada no back-end, os resultados são exibidos na seção da lista relacionada **Resultados de pesquisa de ameaças**. Além disso, a respectiva atividade de implementação é exibida na seção **Atividade**. Duas atividades são exibidas, uma é quando a execução da implementação é iniciada e a segunda é quando a execução é concluída.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: As listas relacionadas a informações sobre **ameaças**, como as listas relacionadas a observáveis associados, são exibidas na seção **Resultados da pesquisa de ameaças** e as listas relacionadas à **Pesquisa** de detecções são exibidas na seção **Resultados** da pesquisa de detecções em Registros relacionados.

Exemplo 2: entradas comuns: pesquisa de detecções

O exemplo abaixo demonstra a ação da capacidade de entradas comuns.

Você pode executar a ação **Executar pesquisa de detecções** relacionadas a capacidades de integração usando a guia **Investigação** do Espaço SIR.

1. Na guia **Investigação**, navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página.
2. Selecione o respectivo ponto de entrada e execute a ação da capacidade de integração.

Nota: Você também pode navegar até a guia **Registros relacionados** no espaço para executar a ação de capacidades de integrações.

Adicionar entradas comuns a uma implementação

Adicione entradas de tempo de execução comuns que se apliquem a todas as implementações selecionadas, conforme aplicável.

Antes de Iniciar

Função necessária: sn_si.analyst

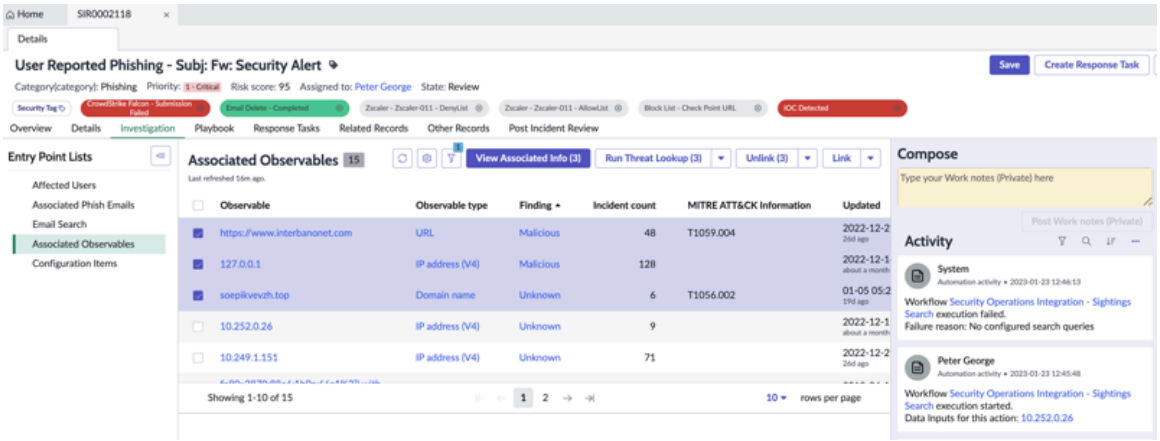
As implementações disponíveis são listadas. Selecione as implementações. Depois de selecioná-las, somente os registros compatíveis serão enviados em relação a cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para a guia **Investigação** do espaço.
   A guia de investigação com as listas de pontos de entrada é exibida.

Tradução automática

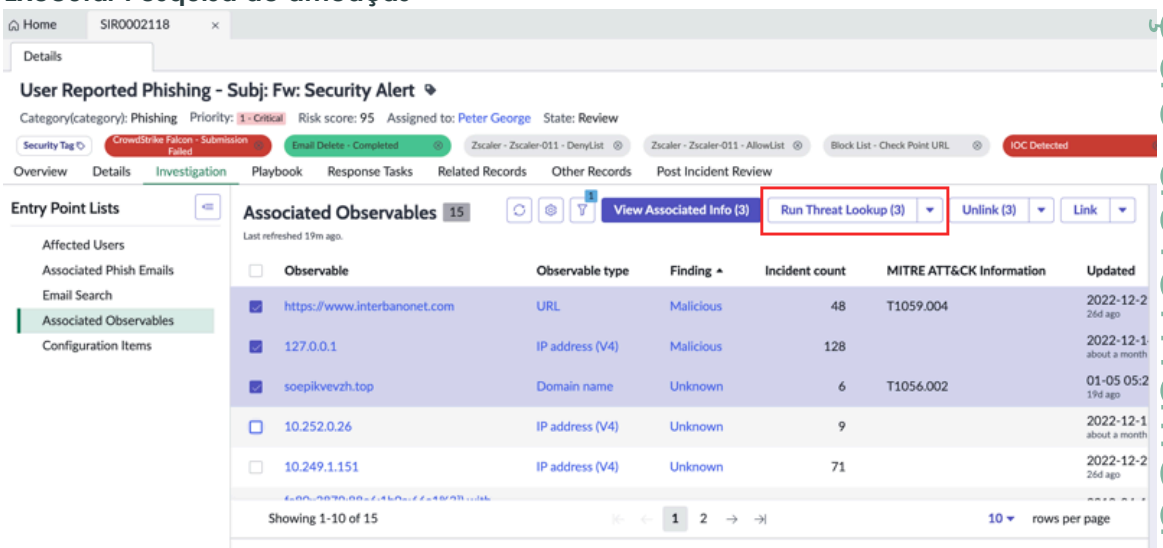
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione o observável associado nas listas de ponto de entrada.
   Por exemplo, selecione **Observáveis Associados** lista relacionada. Os registros de observáveis correspondentes são exibidos.

   Nota: Você pode selecionar uma implementação para executar uma pesquisa de detecções para os observáveis selecionados ou selecionando várias implementações.

Executar Pesquisa de ameaças

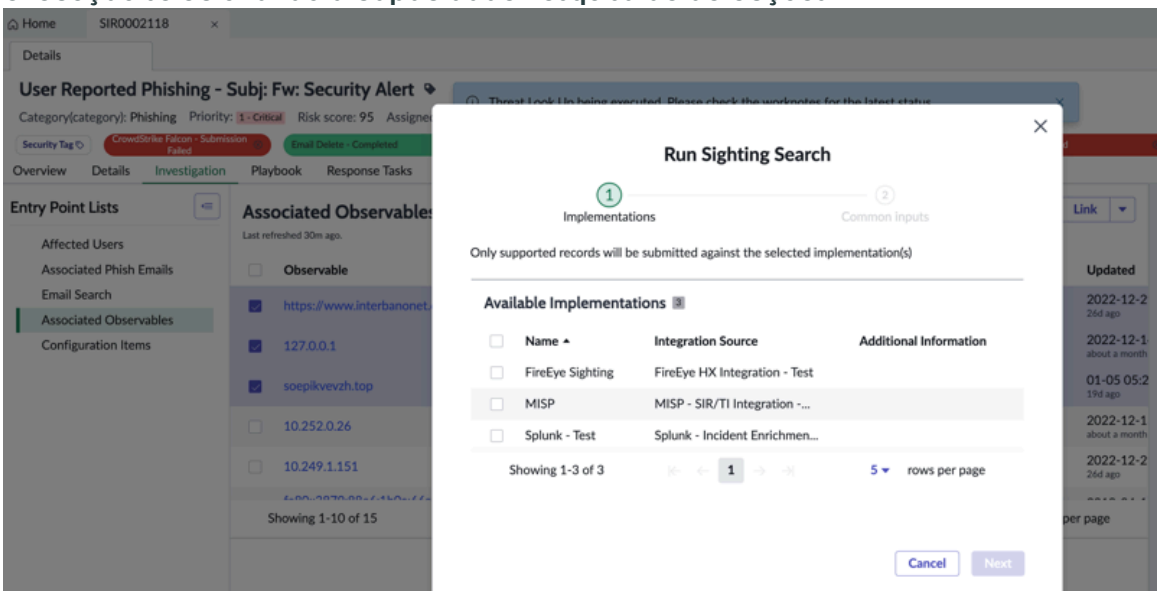


5. Marque a caixa de seleção de qualquer observável que você deseja executar a pesquisa de ameaças.
6. Selecione **Executar pesquisa de detecções** para realizar a pesquisa de e-mail.
   A caixa de diálogo do modal Executar implementações de pesquisa de detecções é exibida.

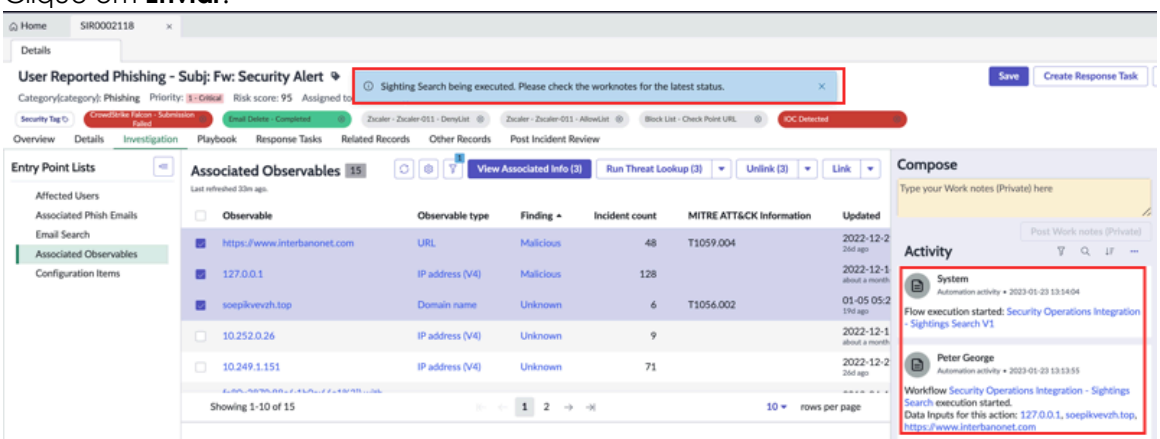
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um exemplo que mostra como adicionar entradas comuns de tempo de execução selecionando a capacidade Pesquisa de detecções



7. Selecione uma ou mais implementações na lista.
8. Clique em **Avançar**.
   Depois que os registros selecionados forem enviados, será exibida uma mensagem informando que a pesquisa de detecções está sendo solicitada. Depois que a implementação é processada no back-end, os resultados são exibidos na seção da lista relacionada **Pesquisa de detecções**. Além disso, a respectiva atividade de implementação é exibida na seção Atividade. Duas atividades são exibidas, uma é quando a execução da implementação é iniciada e a segunda é quando a execução é concluída.
9. Selecione o valor de entrada de tempo de execução comum.
10. Clique em **Enviar**.



Depois que os registros selecionados forem enviados, será exibida uma mensagem informando que a pesquisa de detecções está sendo solicitada. Depois que a implementação é processada no back-end, os resultados são exibidos na seção da lista relacionada **Resultados da pesquisa de detecções**. Além disso, o respectivo status de processamento da atividade de implementação é exibido na seção **Atividade**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo 3: adicionar entradas de detalhes de tempo de execução específicas a uma implementação: executar ações adicionais

Adicionar entradas de detalhes de tempo de execução específicas a uma implementação, Executar ações adicionais.

Você pode executar a ação **Executar ações adicionais** relacionadas às capacidades de integração usando a guia **Investigação** do Espaço SIR.

1. Na guia **Investigação**, navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página.
2. Selecione o respectivo ponto de entrada e execute a ação da capacidade de integração.

> **Nota:** Você também pode navegar até a guia **Registros relacionados** no espaço para executar a ação de capacidades de integrações.

Adicionar entradas específicas a uma implementação

Adicione entradas de tempo de execução específicas para cada implementação selecionada, conforme aplicável.

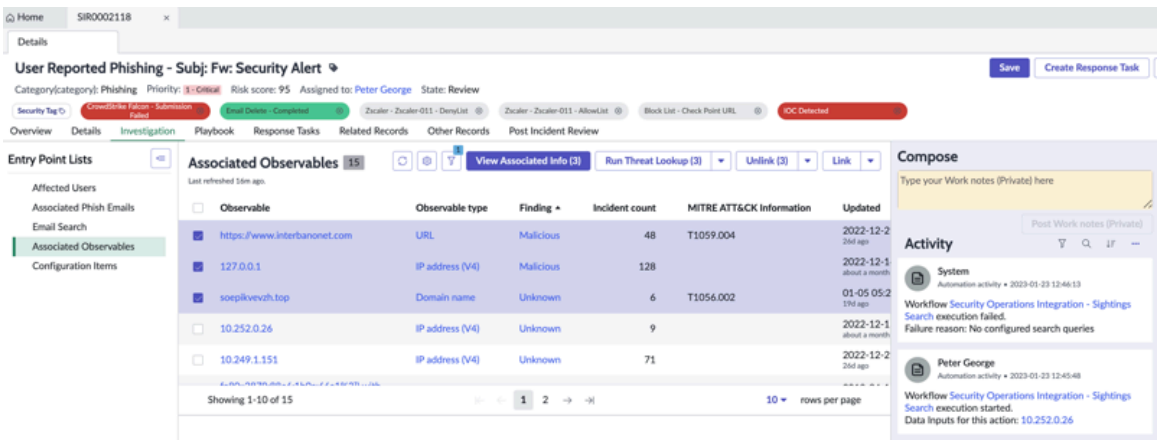
Antes de Iniciar

Função necessária: sn_si.analyst

As implementações disponíveis são listadas. Selecione as implementações. Depois de selecioná-las, somente os registros compatíveis serão enviados em relação a cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para a guia **Investigação** do espaço.
   A guia de investigação com as listas de pontos de entrada é exibida.

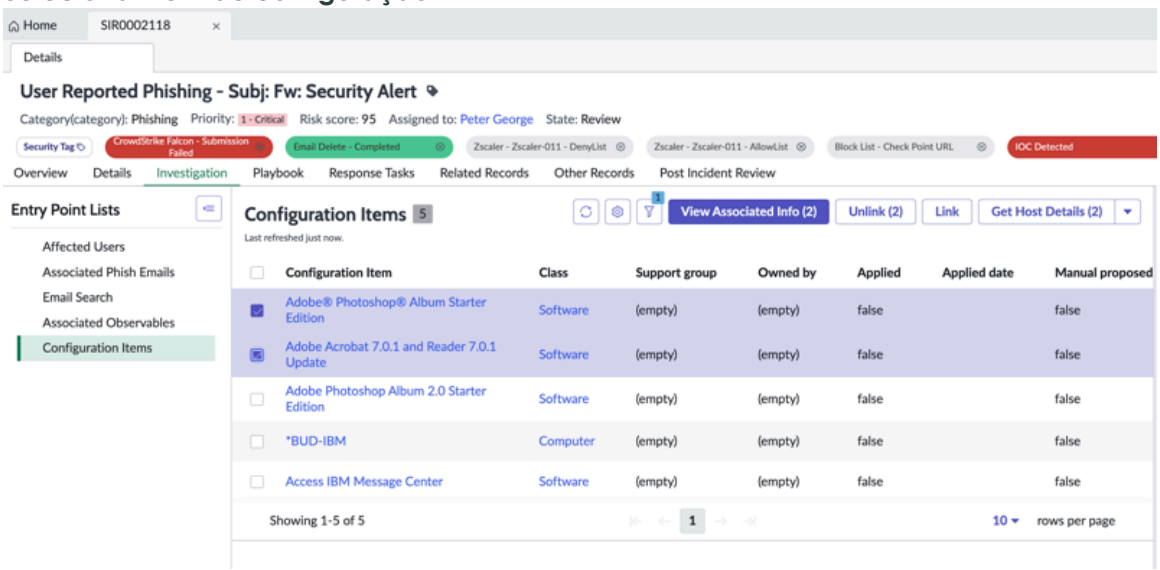


4. Selecione o item de configuração na lista de pontos de entrada.
   Por exemplo, selecione a lista de ponto de entrada **do item de configuração**. Os registros de itens de configuração correspondentes são exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

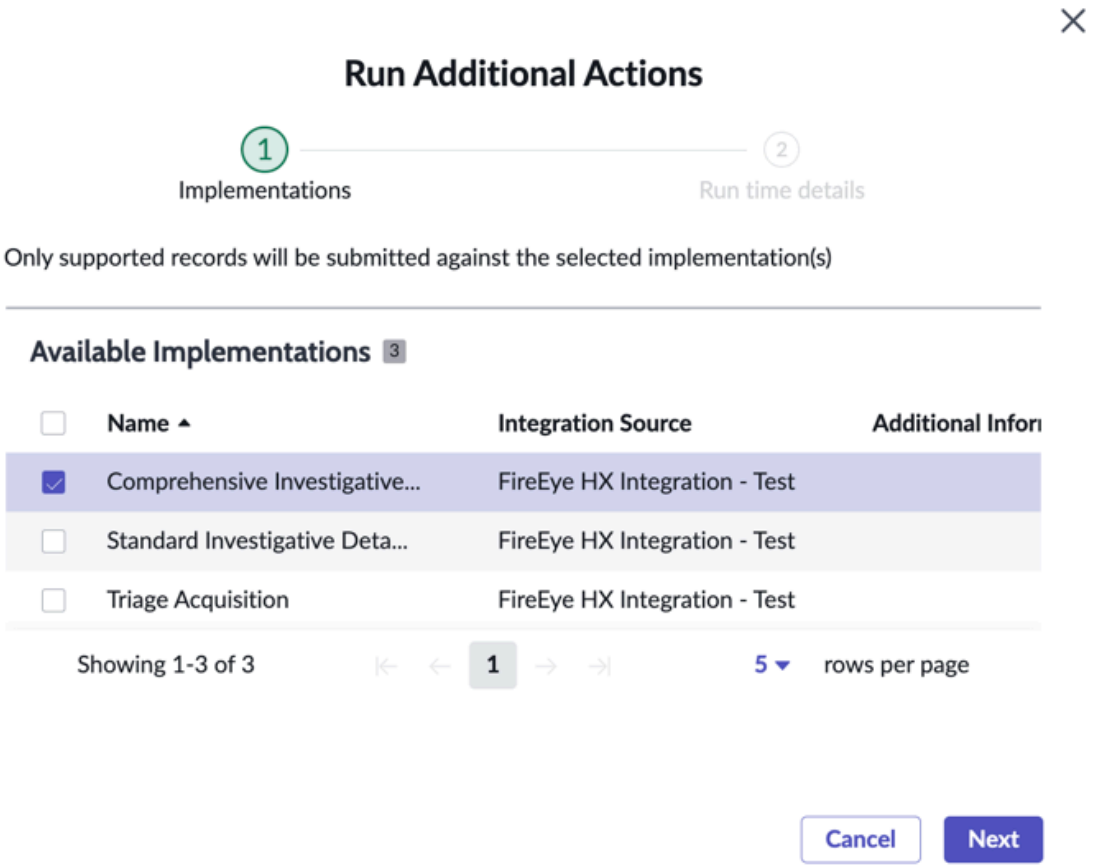
Selecionar item de configuração



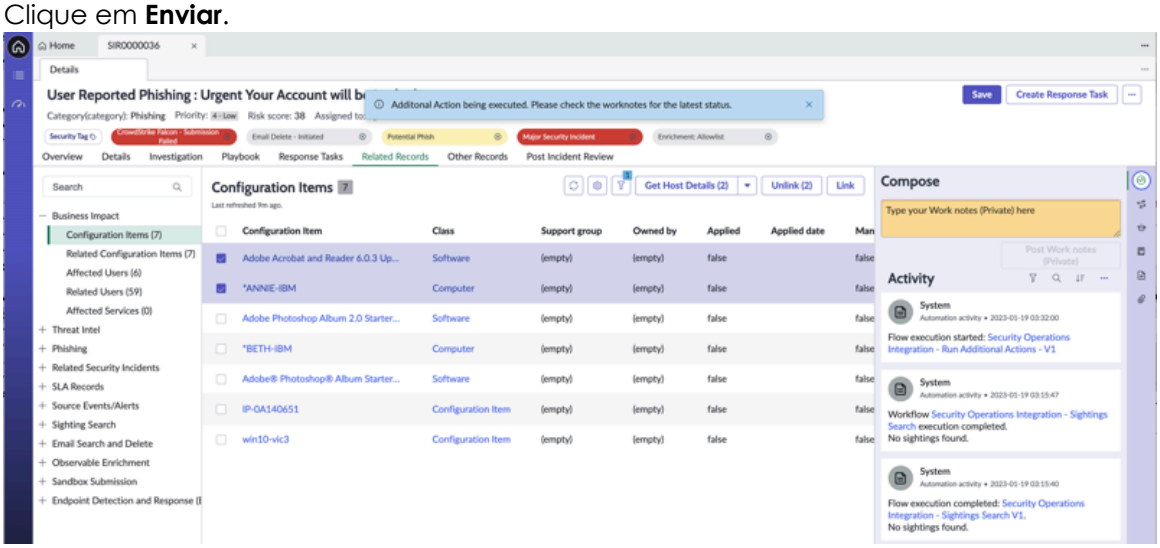
5. Selecione qualquer **item de configuração**.
6. Navegue até as listas suspensas relacionadas que são exibidas na parte superior da página.
   Para o item de configuração (IC) de incidente de segurança, as listas suspensas contêm a seguinte lista de ações de capacidades. As ações de IC listadas coletam os resultados e os armazenam como dados de aprimoramento em um incidente de segurança:
   - Obter arquivo: esta capacidade executa a ação para obter arquivos com um valor de hash específico ou um nome de arquivo.
   - Isolar host: esta capacidade restringe as conexões do sistema a outros dispositivos.
   - Obter detalhes do host: esta capacidade recupera os detalhes do host, detalhes dos usuários conectados e outros recursos de enriquecimento.
   - Executar ações adicionais: esta capacidade executa as ações adicionais além das ações padrão.
   - Obter estatísticas de rede: esta capacidade recupera as estatísticas de rede de um recurso afetado.
   - Obter processo em execução: esta capacidade recupera uma lista de processos em execução em um item de configuração (IC) de um host.
   - Obter usuários conectados: esta capacidade reúne os dados de usuários conectados e os relaciona ao incidente de segurança.
7. Selecione **Executar ações adicionais** para executar a ação de capacidades de integração relacionadas a inteligência de ameaças.
   A caixa de diálogo modal Executar implementações adicionais é exibida.
8. Selecione uma ou mais implementações na lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Clique em **Avançar**.
   Agora você será movido para a próxima etapa para adicionar os detalhes do tempo de execução.
10. Insira um comentário para associar à ação.
11. Clique em **Enviar**.



Depois que os registros selecionados são enviados, uma mensagem é exibida informando que a solicitação de ação adicional está sendo executada. Além disso, o respectivo andamento da ação de implementação é exibido na seção **Atividade**.

12. Exiba os resultados da seção da lista relacionada ao EDR.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

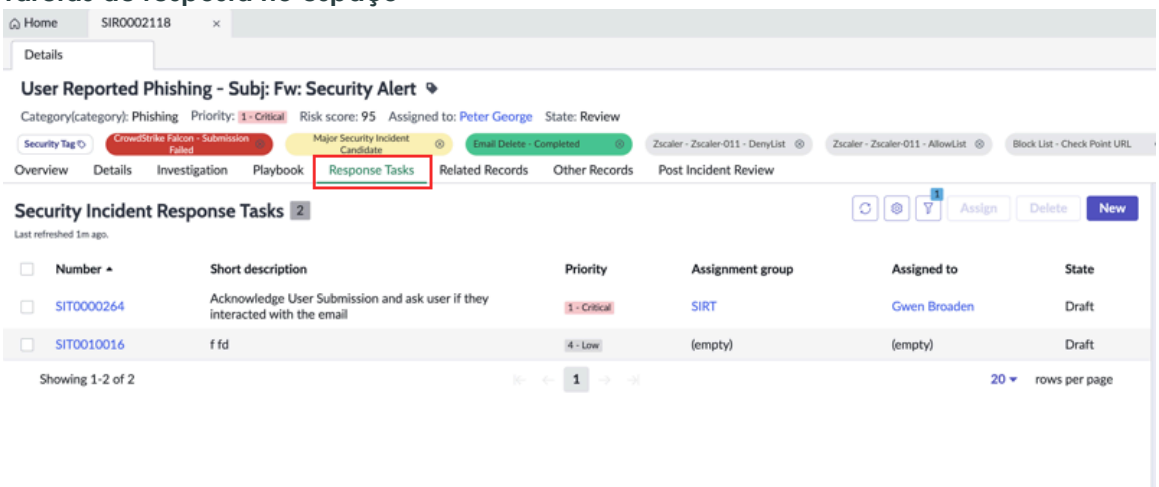
Tarefas do Security Incident Response

Todas as tarefas de resposta associadas a um incidente de segurança são exibidas na seção Tarefas de resposta.

O analista será capaz de:

- criar uma nova tarefa de resposta
- atribuir tarefas de resposta a si mesmo ou a outros
- excluir tarefas de resposta

Tarefas de resposta no espaço



Nota: Para fazer edições rápidas nas tarefas de resposta. Selecione a tarefa de resposta e uma lista de tarefas de resposta será exibida. Selecione o registro, faça as mudanças e salve a tarefa de resposta.

Criar uma tarefa de resposta

Crie tarefas de resposta para rastrear ações separadas a serem executadas para responder ao problema de segurança.

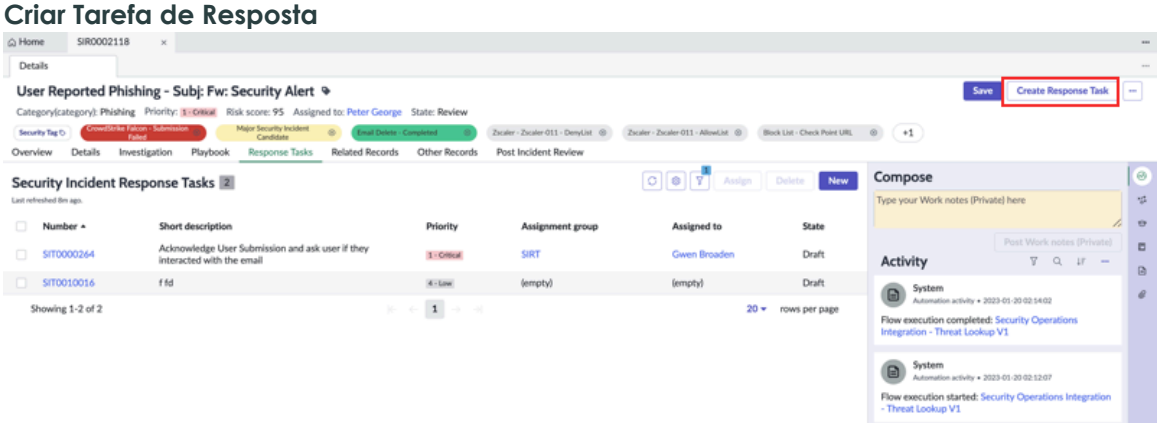
Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique em **Criar tarefa de resposta** nas ações de IU.

Criar Tarefa de Resposta



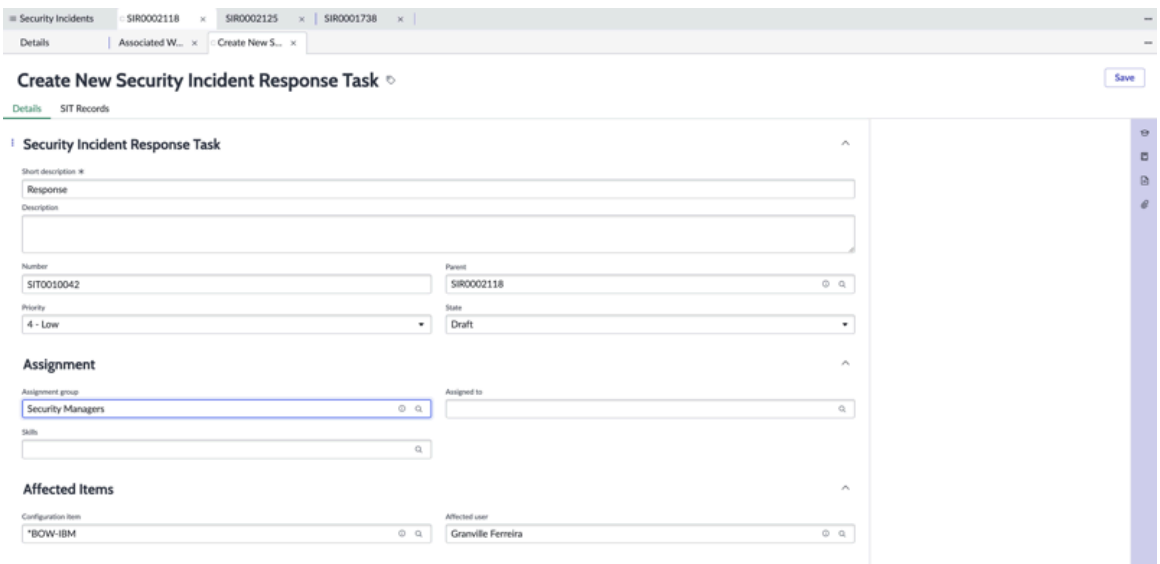
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

Incidente de segurança

Campo	Descrição
Descrição resumida	Uma descrição da tarefa Security Incident Response.
Descrição	Uma descrição para a tarefa selecionada.
Número	Número exclusivo que é gerado automaticamente para um incidente de segurança.
Primário	O número do incidente de segurança relacionado.
Prioridade	A prioridade usada para determinar quando esta tarefa é executada.
Estado	O estado atual da tarefa de resposta de segurança. Por padrão, o estado inicial é **Rascunho**.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuído a	O indivíduo atribuído para executar a tarefa.
Habilidades	A habilidade necessária para executar esta tarefa. Pesquise na pesquisa e selecione a habilidade necessária.
Itens afetados	Os itens afetados pelo problema de segurança.
Item de Configuração	O item de configuração afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.



4. Clique em **Salvar**.
A nova Tarefa de resposta (SIT) é criada.

Tradução automática

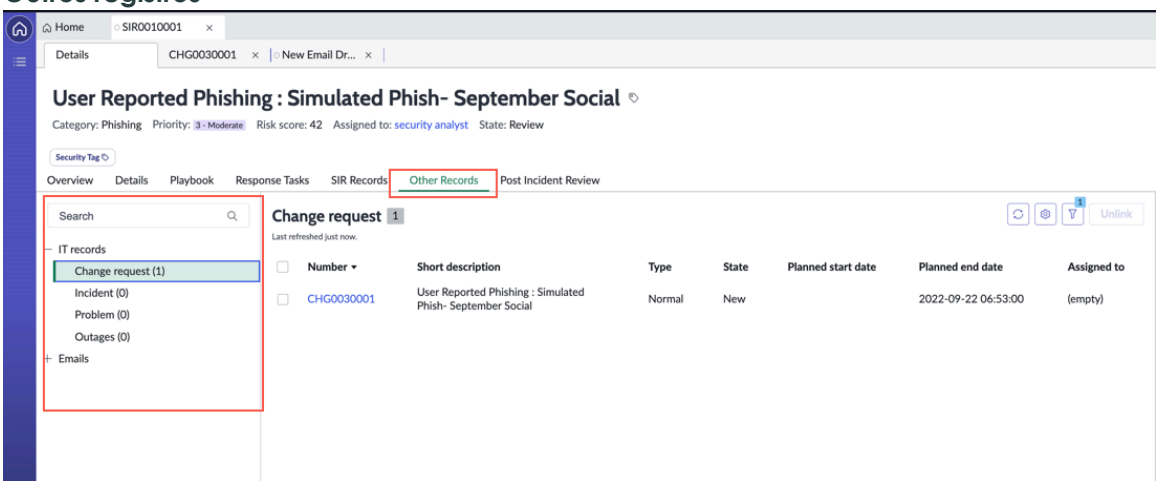
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Outros registros do Security Incident Response

Esta seção exibe os outros registros, como registros relacionados a TI e registros de e-mail. Em Registros de TI, Incidente, Solicitação de mudança, Problema e Indisponibilidades são exibidos.

Em E-mail, Rascunho, E-mails enviados e E-mails recebidos são exibidos.

Outros registros



Criar um incidente

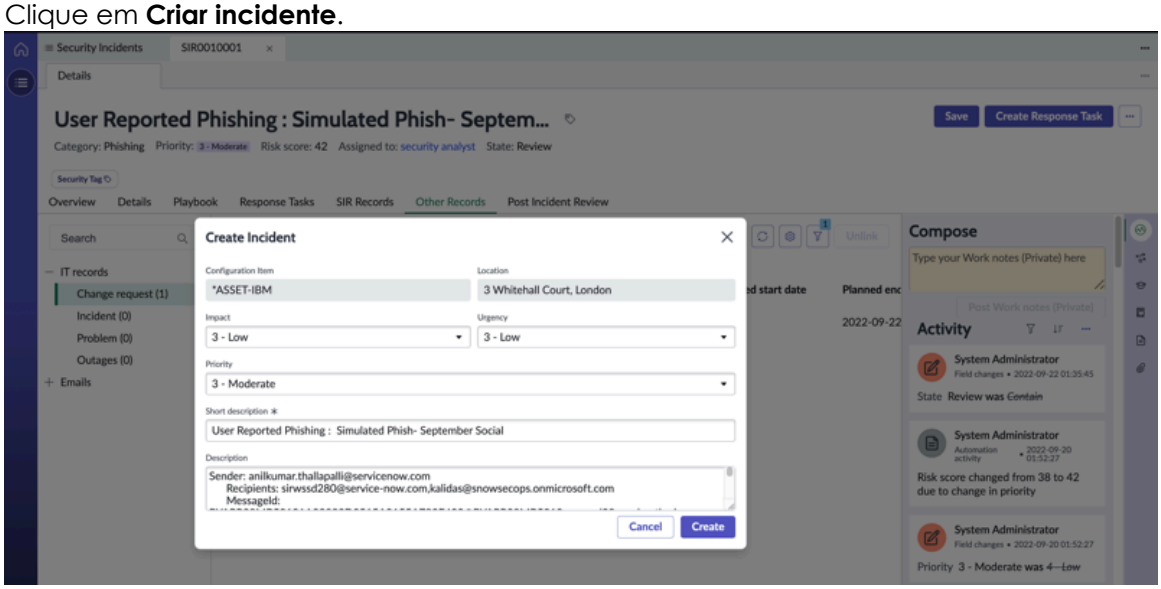
Crie um incidente dentro de um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique em **Criar incidente**.

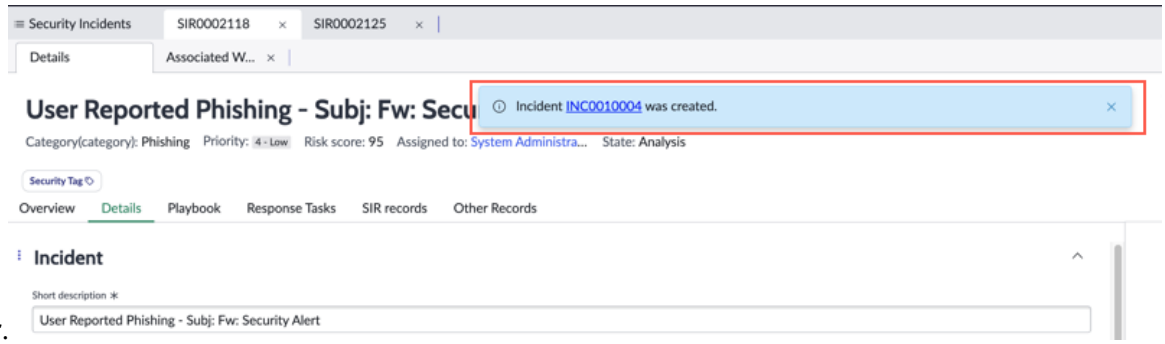


4. Insira os detalhes como Item de configuração, Impacto, Urgência, Local, Prioridade e Descrição resumida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Criar**.



6. Um incidente é criado.

Como criar tarefa de problema

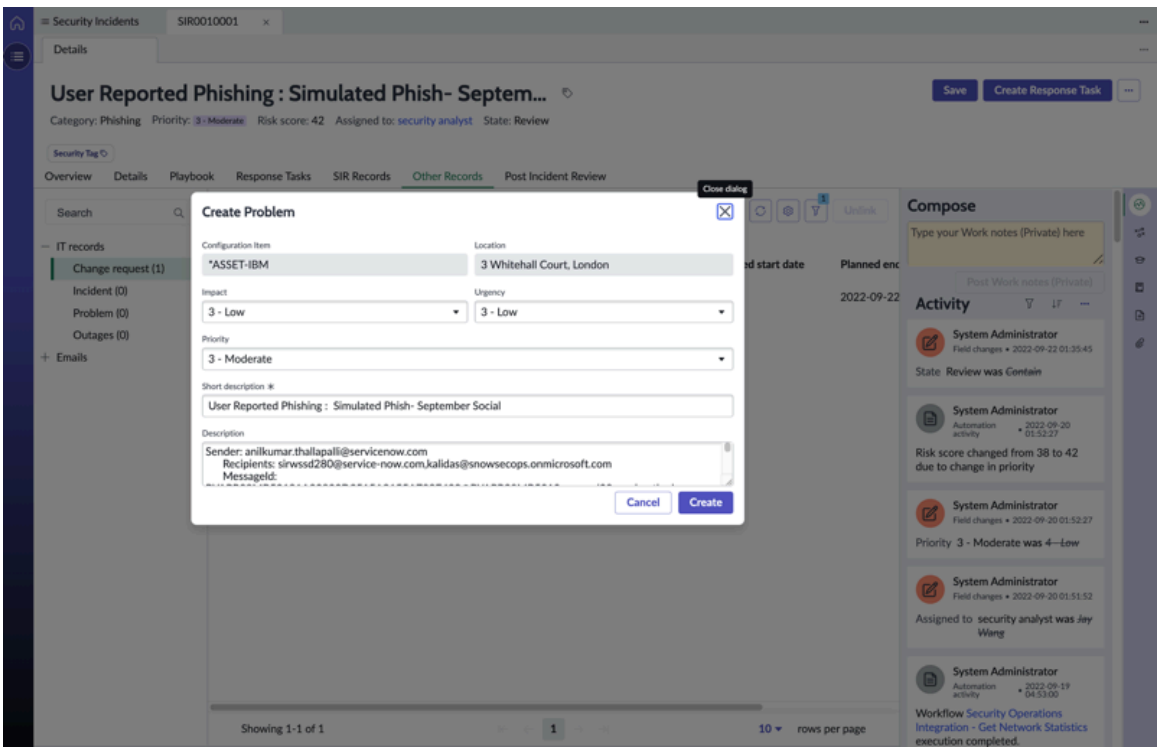
Crie uma tarefa de problema.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique **em Criar problema**.

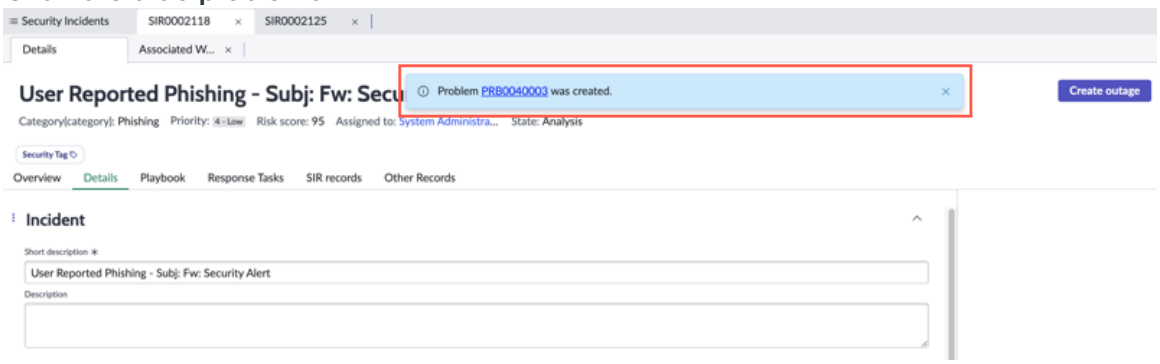


4. Preencha os detalhes como Item de configuração, Local, Impacto, Urgência, Prioridade e Descrição resumida.
5. Clique em **Criar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar tarefa do problema



6. Uma tarefa de problema é criada.

Criar uma solicitação de mudança

Crie uma solicitação de mudança.

Antes de Iniciar

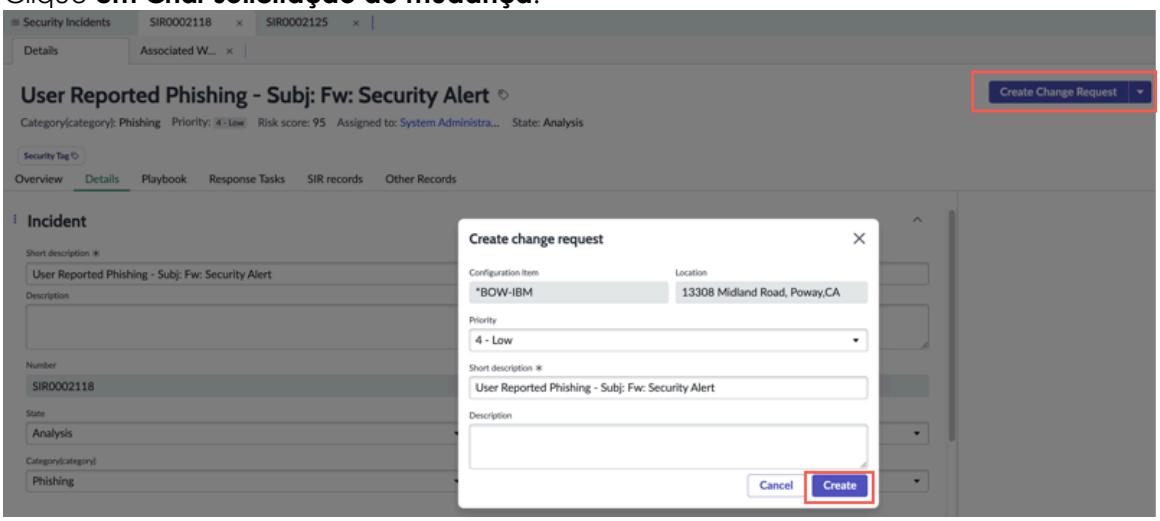
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.

2. Abra um registro de incidente.

3. Clique **em Criar solicitação de mudança**.

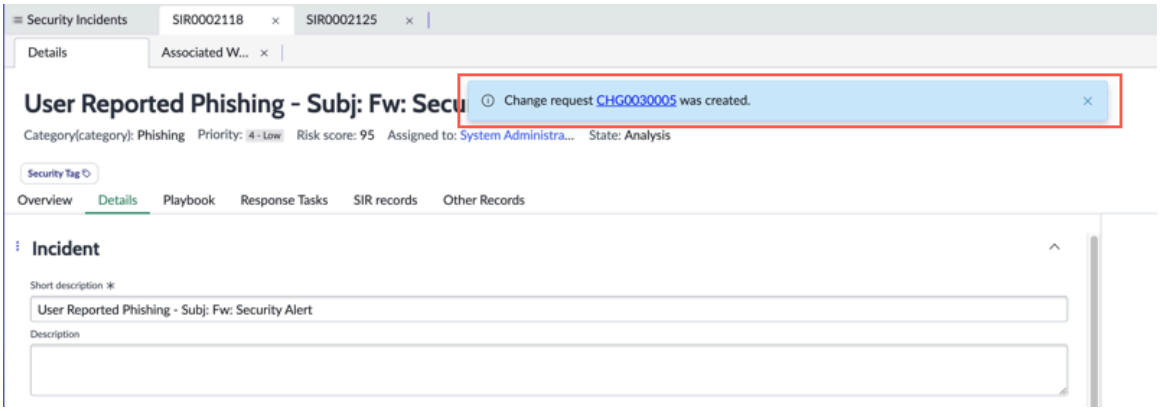


4. Insira os detalhes como Item de configuração, Local, Prioridade e Descrição resumida.

5. Clique em **Criar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Uma solicitação de mudança é criada.

Criar indisponibilidade

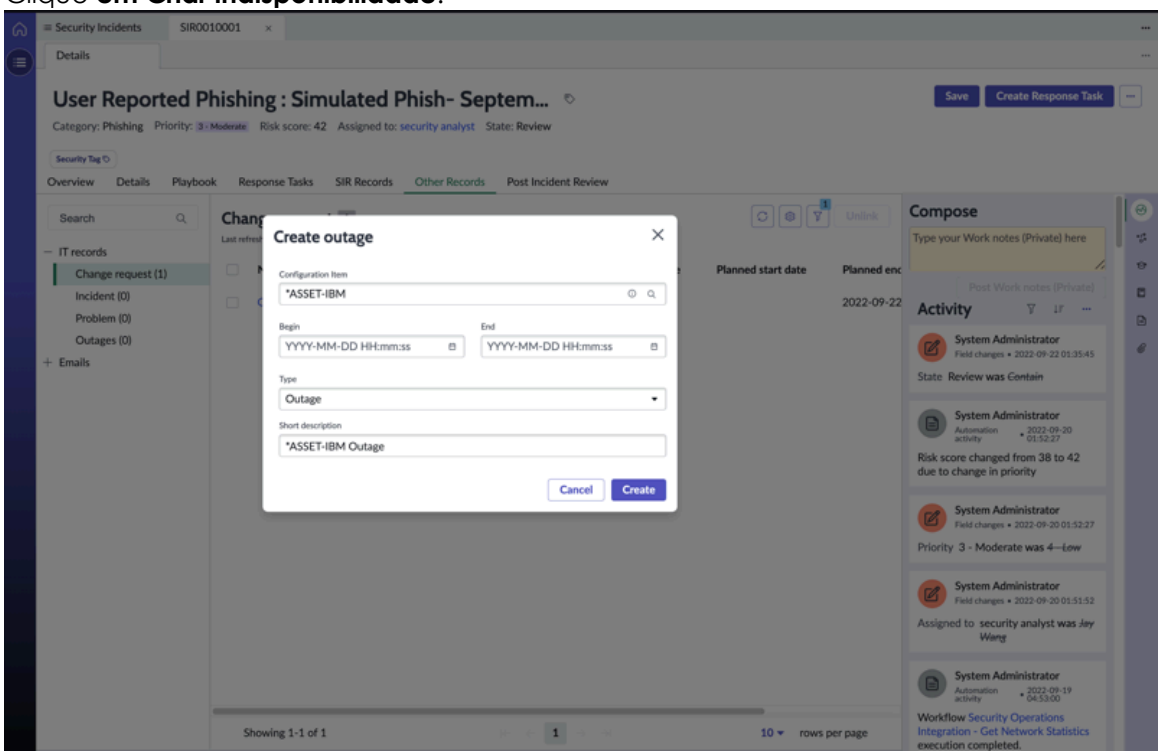
Crie uma indisponibilidade a partir de um incidente para rastrear o tempo de inatividade de um item de configuração.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique **em Criar indisponibilidade**.

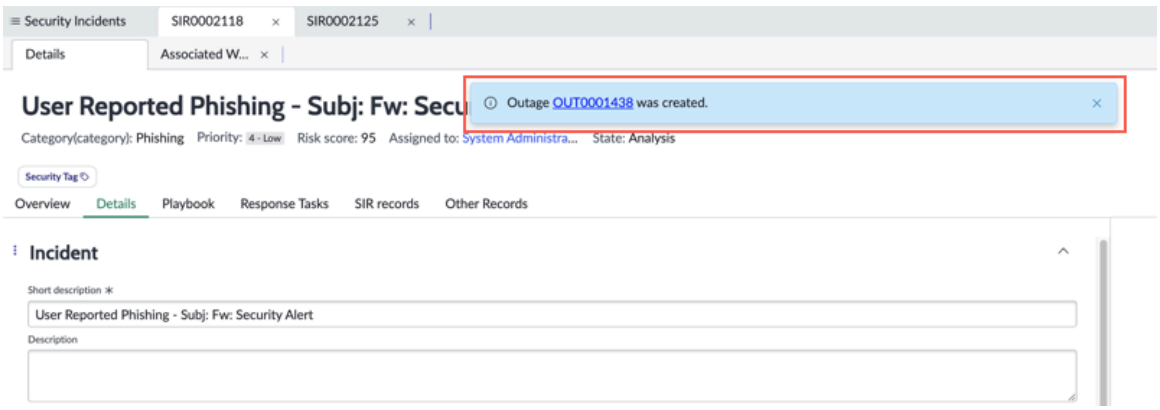


4. Insira os detalhes como Item de configuração, Data de início, Data de término, Tipo e Descrição resumida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Criar**.



Compor e-mails

Como analista, você pode compor e-mails diretamente de incidentes de segurança.

Antes de Iniciar

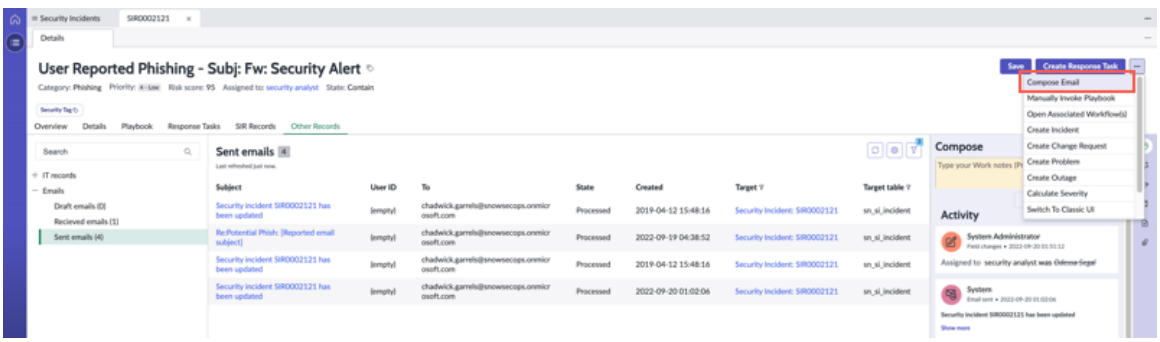
Função necessária: sn_si.analyst

Procedimento

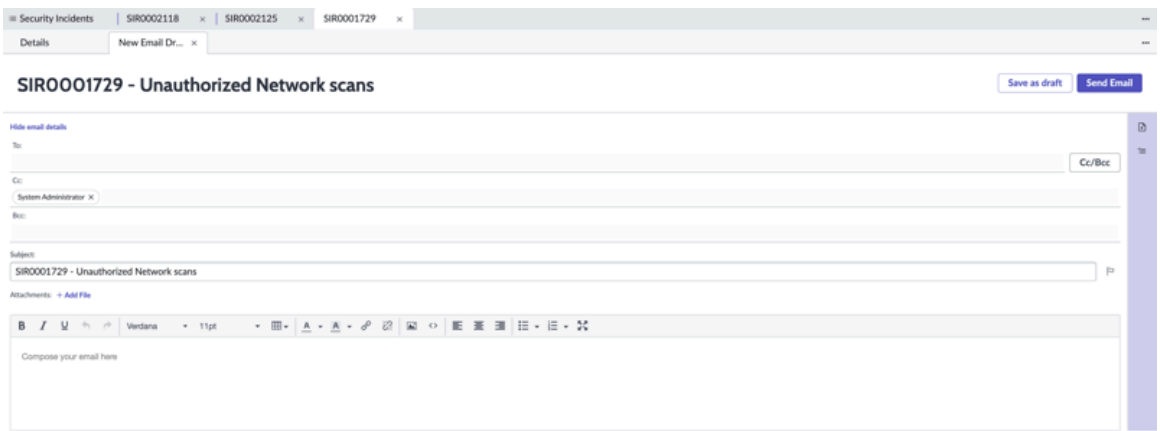
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.

2. Selecione e abra o incidente para o qual você deseja compor um e-mail.

3. Clique no estouro e selecione **Compor e-mail**.



4. Insira os campos **Para** e **CC**.

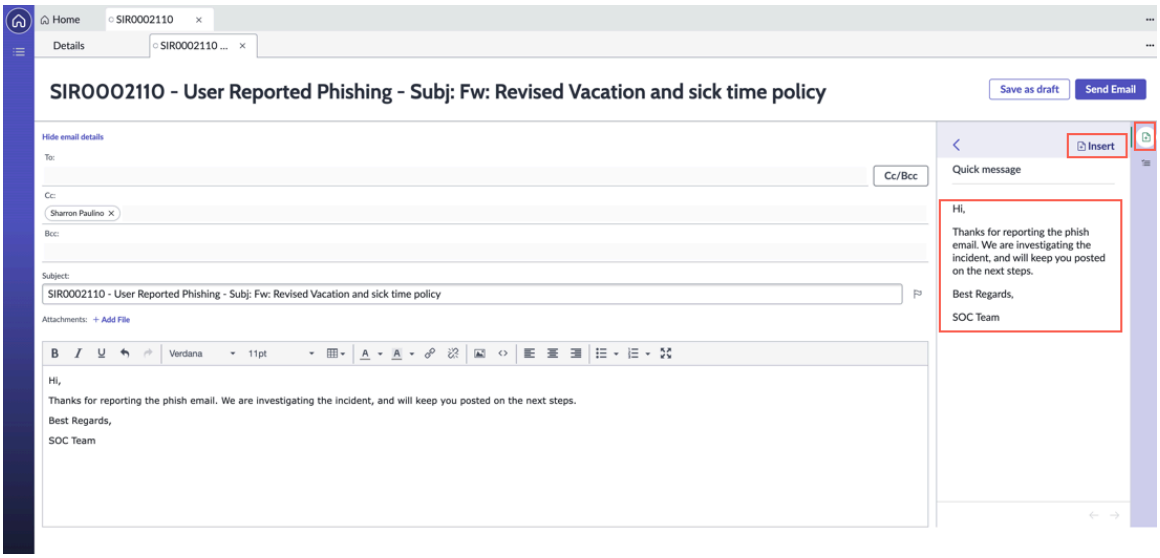


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Adicione** anexos, se houver.

6. No formulário E-mail, clique em **Mensagens rápidas** para exibir as mensagens rápidas que são exibidas no lado direito da seção **Compor e-mails**.
   As mensagens rápidas disponíveis são exibidas. Selecione a mensagem e clique em **Inserir**.
   As mensagens são inseridas no corpo do e-mail.



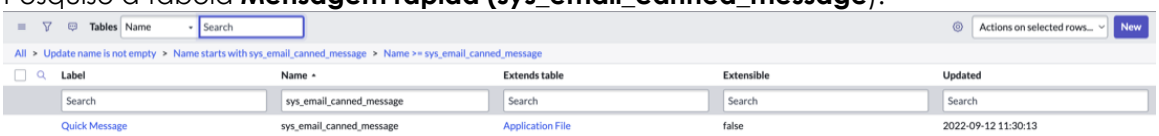
7. Escreva seu e-mail e clique em **Enviar e-mail**.

> **Nota:** Você pode salvar um e-mail como rascunho. Esses rascunhos de e-mail estarão disponíveis na guia Outros registros.

Como configurar Mensagens rápidas:

a. Navegar até **Definições do sistema** > **Tabelas**.

b. Pesquise a tabela **Mensagem rápida (sys_email_canned_message)**.



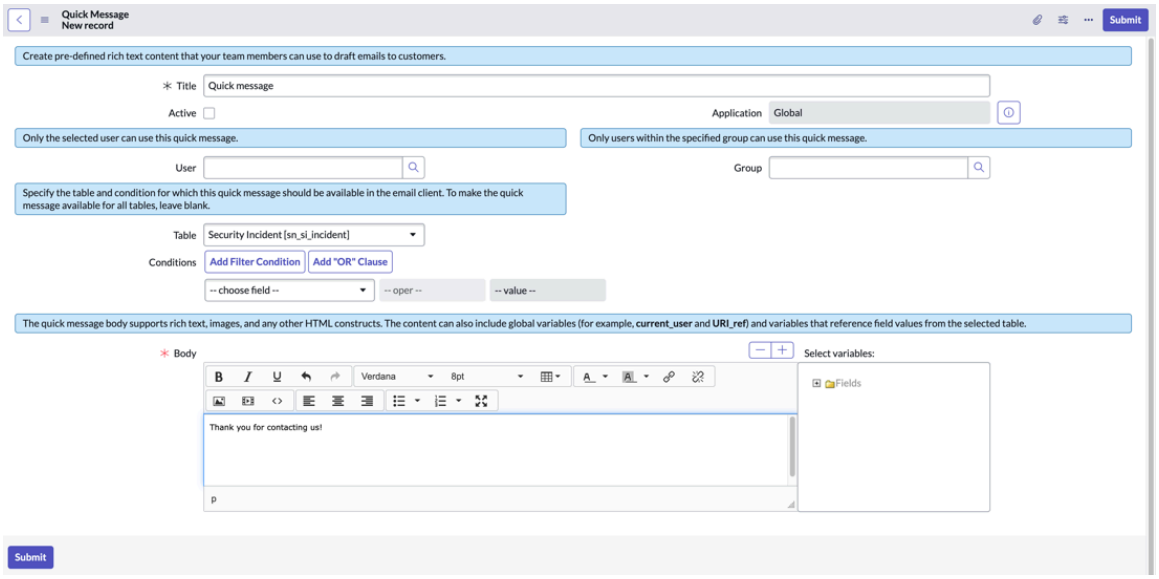
c. Ir para **Links relacionados** > **Mostrar lista**.

d. Criar **novo**.

e. Insira o **Título**, **o corpo da mensagem**, marque a caixa de seleção **Tabela: Incidente de segurança (sn_si_incident)** e **Ativo**.

Tradução automática

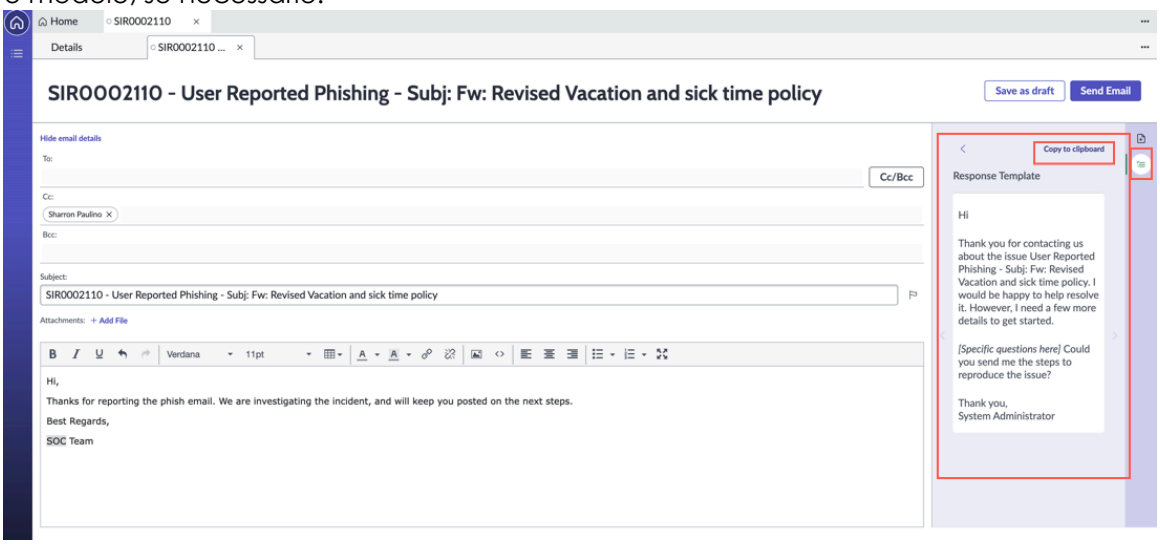
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Clique em **Enviar**.
Depois que uma nova entrada é criada na tabela, a mensagem rápida aparece no menu contextual.

8. Clique em **Modelos** para adicionar qualquer modelo, se necessário.

9. Selecione o **modelo de resposta**, clique em **Copiar para a área de transferência** e aplique o modelo, se necessário.



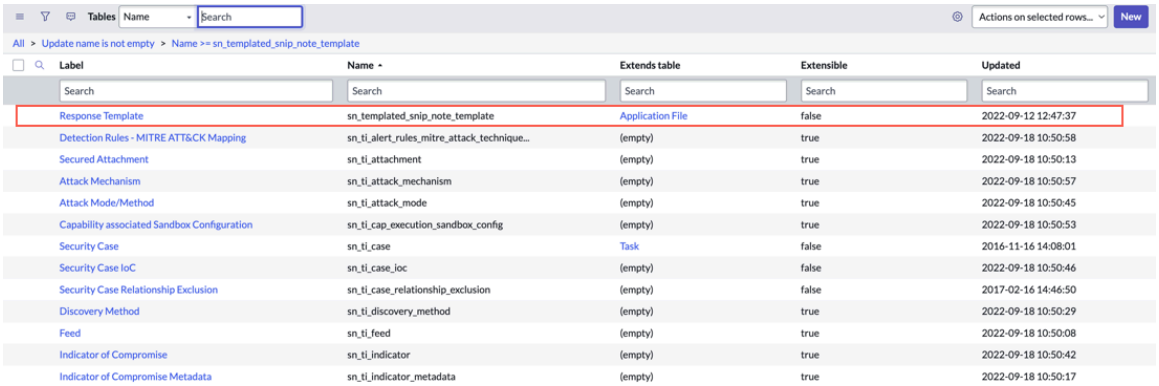
Como configurar Modelos de resposta:

a. Navegar até **Definições do sistema** > **Tabelas**.

b. Pesquise a tabela **Modelo de resposta (sn_templated_snip_note_template)**.

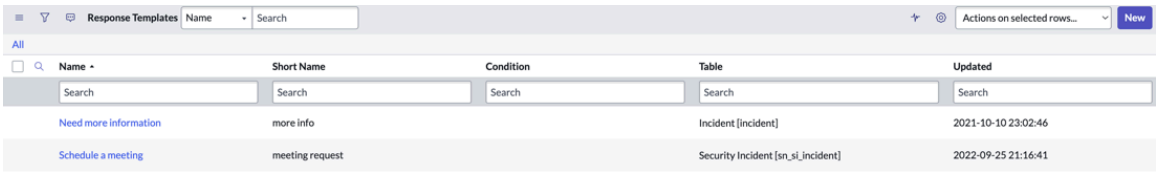
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

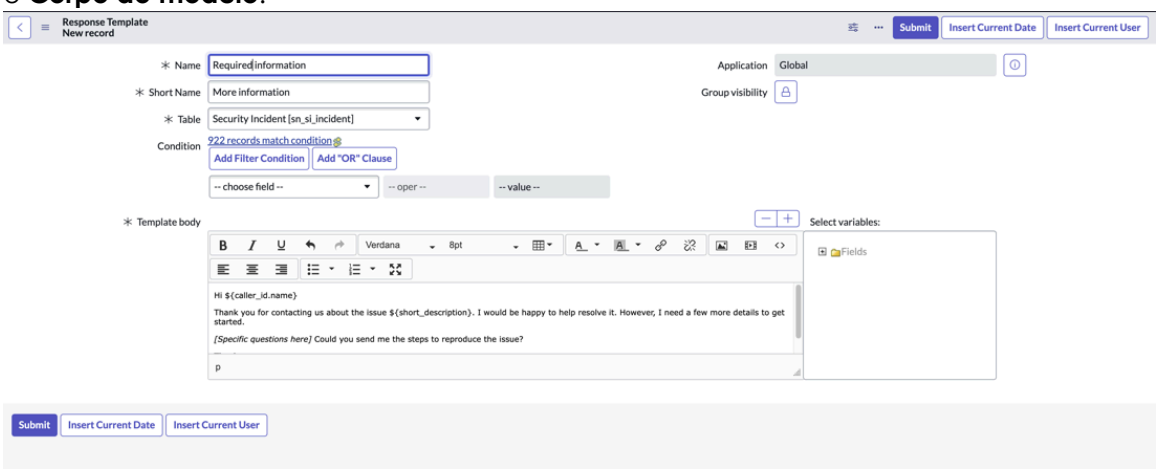


c. Ir para **Links relacionados** > **Mostrar lista**.

d. Criar **novo**.



e. Insira o **Nome**, **Nome Curto**, selecione a **Tabela: Incidente de segurança (sn_si_incident)** e **Corpo do modelo**.



f. Clique em **Enviar**.
Depois que uma nova entrada é criada na tabela, o novo modelo aparece no menu contextual.

Análise pós-incidente do Security Incident Response

A revisão pós-incidente aparece quando um incidente é movido para um estado de Revisão.

Para obter informações mais detalhadas sobre como conduzir as atividades pós-incidente, consulte Relatório de análise pós-incidente

A análise pós-incidente consiste nas seguintes seções:

1. Avaliações
2. Relatórios

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No espaço do Security Incident Response, você poderá solicitar e fazer avaliações usando essas duas novas ações de IU.

Nome	Descrição
Avaliações	A avaliação exibe todas as avaliações associadas às outras avaliações do incidente de segurança. O analista poderá fazer avaliações e solicitar avaliações. • **Fazer avaliações**: clique em **Fazer avaliações** para fazer as avaliações (se aplicável) e concluir a avaliação. Antes de concluir a avaliação, o estado do incidente de segurança é Pronto para receber e a data de vencimento do incidente é indicada em vermelho. • Solicitar avaliações: clique em **Solicitar avaliação** para qualquer avaliação adicional e você poderá adicionar os novos usuários que deseja solicitar. **Nota:** Usuários que já solicitaram não aparecerão nesta seção. Qualquer avaliação para este incidente foi configurada com base nas condições definidas na análise pós-incidente, podendo ser obrigatória ou opcional.
Relatórios	Modifique as configurações de tempo de execução e gere o relatório. Selecione a instância de relatório, modifique os filtros e salve o relatório. O analista pode visualizar e baixar o relatório PIR.

Integração de TISC no espaço SIR

A seção a seguir inclui informações sobre a integração da Central de segurança de inteligência contra ameaças de dentro do contexto do espaço SIR.

Enviar dados do espaço SIR para TISC

Saiba como os dados são colaborados e compartilhados entre os espaços da Central de segurança de inteligência contra ameaças (TISC) e do Security Incident Response (SIR) seguindo os procedimentos explicados nas seções a seguir.

Propriedades do sistema para enviar dados

Revise as propriedades do sistema para integrações de TISC a serem combinadas com o SIRW. Você pode configurar essas propriedades para controlar como ambas as aplicações gerenciam as integrações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Considerações principais

As propriedades do sistema para integrações de TISC fornecem opções de configuração avançadas sobre como a aplicação lida com observáveis e enriquecimentos.

1. Para definir as propriedades do sistema de integrações de TISC no SIRW, navegue até as **Propriedades do sistema** para Inteligência contra ameaças e acesse a tabela [sys_properties].
2. As propriedades do sistema controlam e lidam com o comportamento de cada operação de envio de dados individual.
3. Quando a propriedade está habilitada, os dados são enviados automaticamente quando os dados de observáveis ou de aprimoramento são gerados no espaço SIR.
4. Se a propriedade estiver desabilitada, os dados serão enviados por push manualmente e permitirão que os usuários enviem dados por push usando as ações de IU do Espaço SIR.

As listas a seguir mostram as propriedades do sistema para integração de TISC - SIR:

- Inserir dados de observáveis automaticamente e manualmente a partir do SIR: habilite a propriedade sn_ti.allow_observable_and_enrichment_records_push para enviar os dados automaticamente ou manualmente. Se desabilitada, esta propriedade desabilitará os modos automático e manual para todos os envios por push de dados do SIR.
- Enviar resultados de pesquisa de ameaças: habilite esta propriedade do sistema sn_ti.automatic_push_threat_lookup_results para enviar dados de pesquisa de ameaças automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados de pesquisa de ameaças manualmente.
- Envio por push dos resultados da pesquisa de detecções para o TISC: habilite sn_ti.automatic_push_sighting_results_to_tisc desta propriedade do sistema para enviar dados de pesquisa de detecções automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados de pesquisa de detecções manualmente.
- Enviar observáveis: habilite sn_ti.automatic_push_observable_to_tisc desta propriedade do sistema para enviar dados de observáveis automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados dos observáveis manualmente.
- Envio por push de resultados de aprimoramento: habilite sn_ti.automatic_push_enichment_results desta propriedade do sistema para enviar dados de resultados de aprimoramento automaticamente para o TISC. Se desabilitado, os analistas de segurança ainda poderão enviar os dados de resultados de aprimoramento manualmente.

Adicionar incidente de segurança ao caso de TISC

Adicione incidentes de segurança aos registros de caso de TISC.

Antes de Iniciar

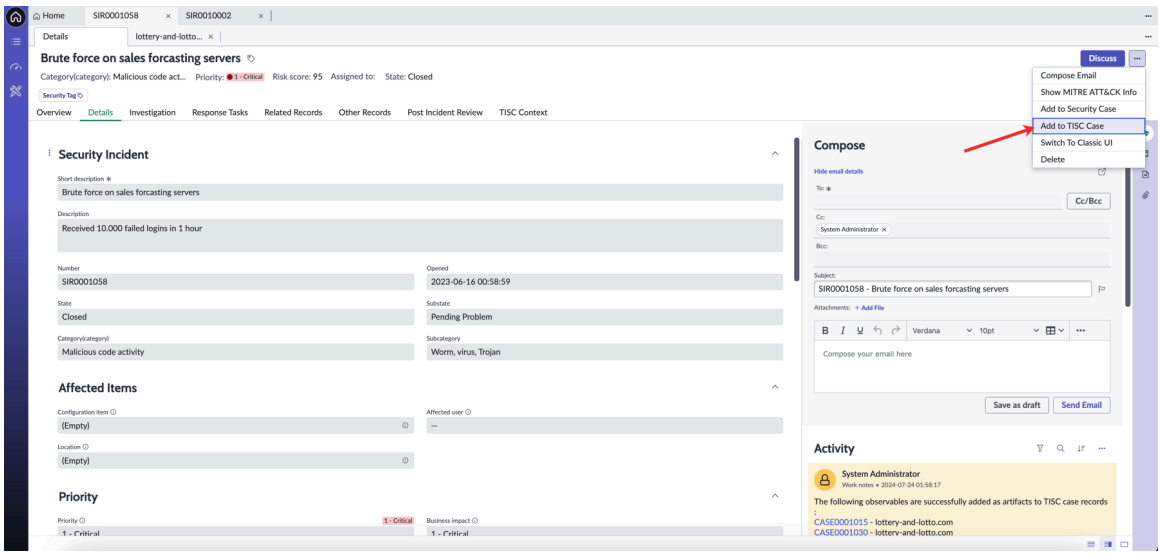
Função necessária: sn_si.analyst, sn_sec_tisc.case_write

Procedimento

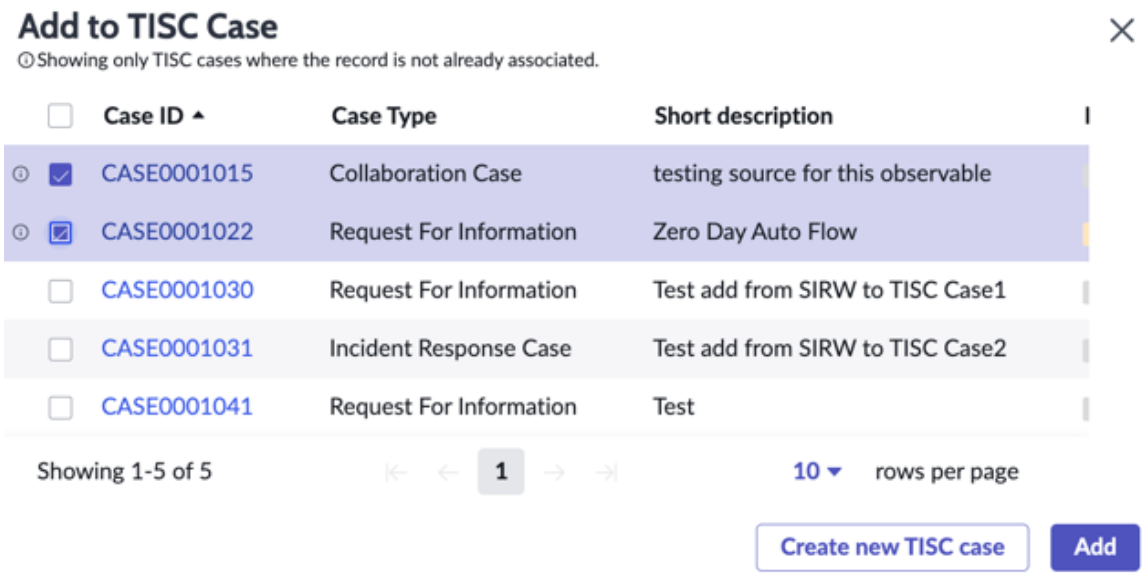
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Todos**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente, navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique no ícone **Mais ações**.
4. Clique na ação **Adicionar ao caso de TISC**.
   A caixa de diálogo Adicionar ao caso de TISC é exibida e mostra somente os casos de TISC em que o incidente ainda não está associado.



5. Selecione o(s) caso(s) na caixa de diálogo **Adicionar ao caso**.

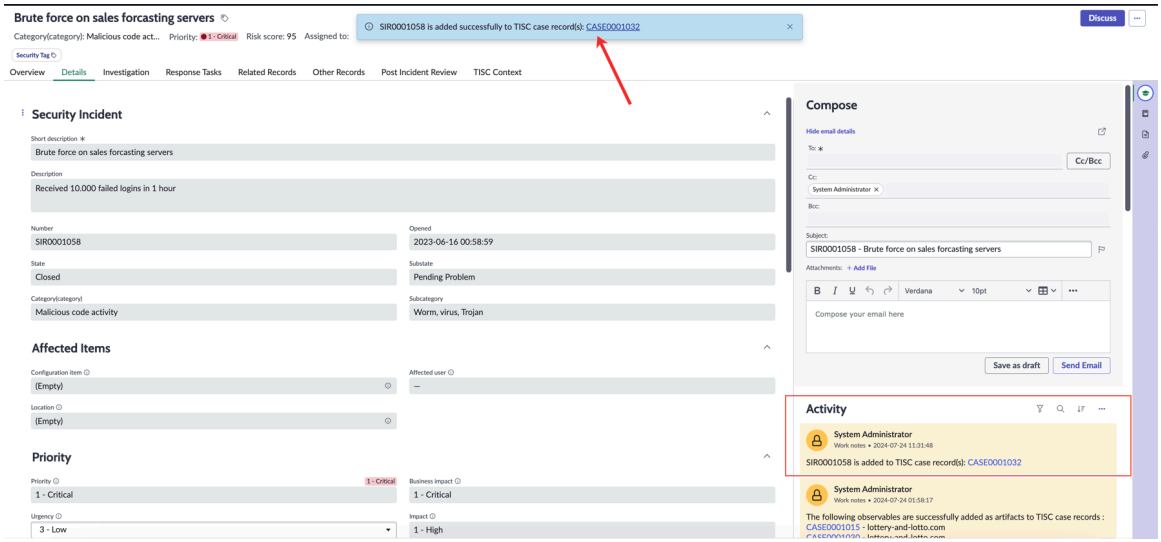


Nota: Crie um novo caso de TISC se não houver registros de caso. Para obter mais informações sobre como criar caso(s), consulte Criação de casos usando o Workbench do analista de ameaças.

6. Clique em **Adicionar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Clique no registro de caso para exibir o caso no TISC na mensagem de informações exibida ou no fluxo de **atividades**.

> **Nota:** Para exibir os incidentes de segurança vinculados, clique no registro de caso específico no fluxo de **atividades** do incidente de segurança. Ao clicar aqui, você será direcionado para o registro de caso no espaço de TISC e os incidentes de segurança serão adicionados na guia **Artefatos** do módulo Gestão de casos.

Adicionar observáveis ao caso de TISC

Adicione observáveis aos registros de caso de TISC.

Antes de Iniciar

Função necessária: sn_si.analyst, sn_sec_tisc.case_write

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Todos**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente, navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Clique na guia **Registros relacionados** no espaço.
   Você pode executar a ação de adicionar observáveis a casos de TISC usando várias guias do espaço do Security Incident Response Workspace.

> **Nota:** Você pode navegar até o
>
> - Página de detalhes de observáveis na guia Registros relacionados.
> - Clique na guia**Investigação** e navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página e selecione **Observáveis associados** para adicionar observáveis ao caso de TISC.

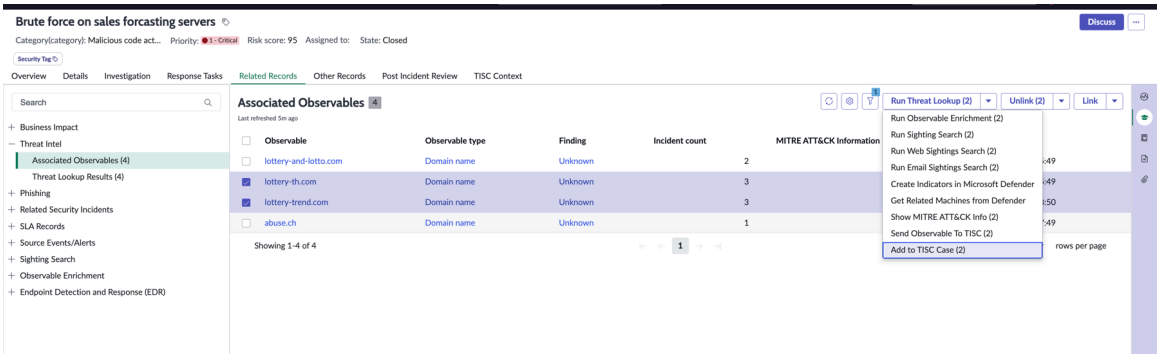
4. Por exemplo, selecione **Inteligência sobre ameaça** > **Observáveis Associados**.
5. Selecione um ou vários observáveis para adicionar os observáveis selecionados aos registros de caso.

Tradução automática

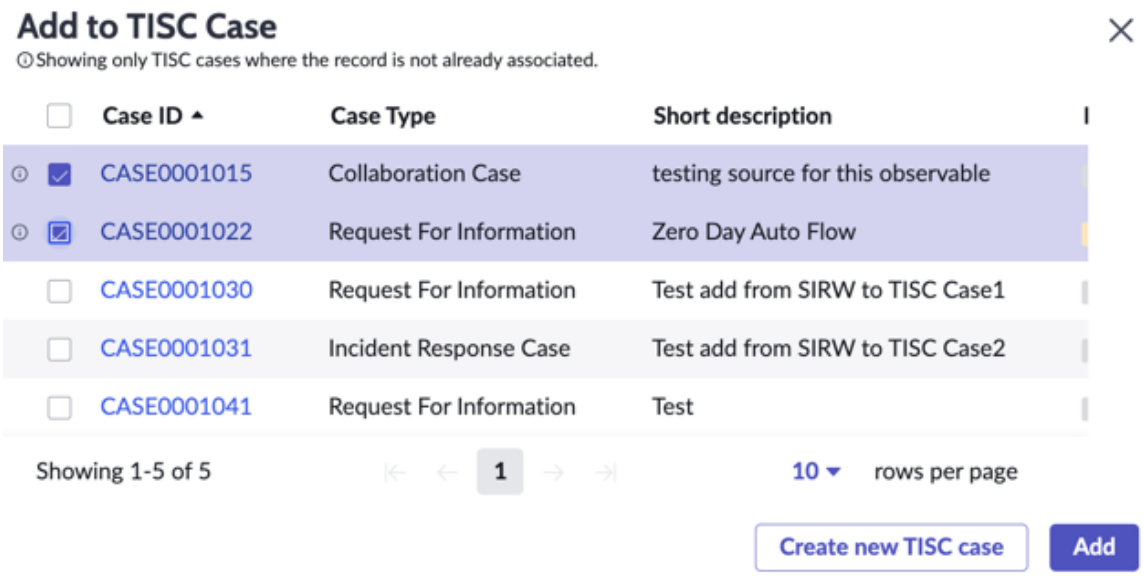
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você também pode clicar em qualquer registro de observável e abrir a página de detalhes de observáveis em uma guia diferente. Você pode adicionar registros de caso aqui clicando em Adicionar ao caso de TISC.

6. Clique no botão de divisão **Ações de capacidade**.
7. Selecione **Adicionar ao caso de TISC**.



8. Selecione o(s) caso(s) na caixa de diálogo **Adicionar ao caso**.



Nota: Crie um novo caso de TISC se não houver registros de caso. Para obter mais informações sobre como criar caso(s), consulte Criação de casos usando o Workbench do analista de ameaças.

9. Clique em **Adicionar**.
10. Clique no registro de caso para exibir o caso no TISC na mensagem de informações exibida ou no fluxo de **atividades**.

Nota: Se o observável não tiver um observável de TISC correspondente, o observável selecionado no espaço SIR será enviado para o TISC automaticamente e, posteriormente, será adicionado ao(s) registro(s) de caso de TISC selecionado(s). Para exibir os observáveis vinculados, clique no registro de caso específico no Fluxo de **atividades**. Ao clicar aqui, você será direcionado para o registro de caso no espaço de TISC e os observáveis serão adicionados na guia **Artefatos** do módulo Gestão de casos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Você enviou com sucesso os dados de observáveis para a gestão de casos da Central de segurança de inteligência contra ameaças.

Enviar observáveis para TISC

Usando este recurso, o analista de segurança pode enviar por push os dados de observáveis do SIR para o TISC. Usando o contexto de TISC, você pode verificar se os observáveis estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados por push sempre que necessário.

Antes de Iniciar

Função necessária: sn_si.analyst

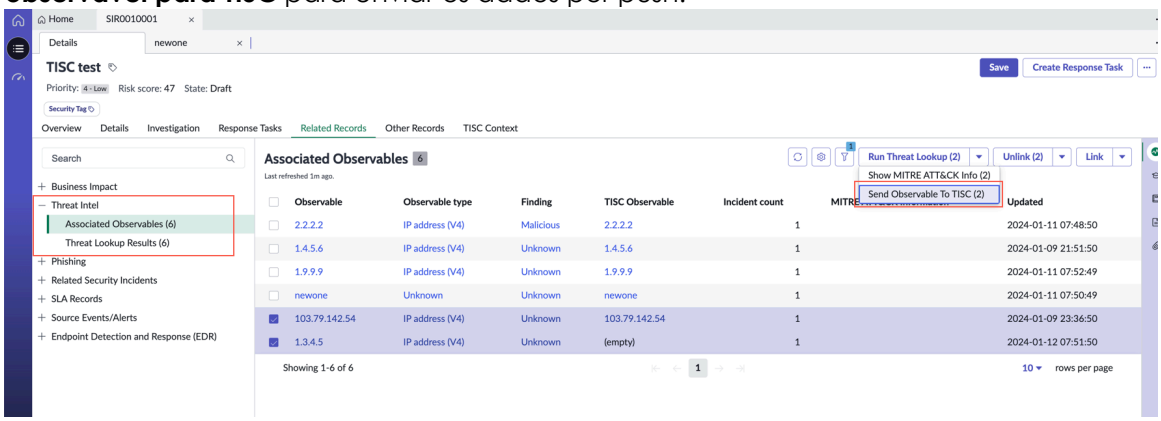
Procedimento

1. Navegue até a guia **Registros relacionados** no espaço SIR para executar a ação da capacidade de integração de TISC.

   Nota:

   - Você também pode navegar até a guia **Investigação** e navegar até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página e selecionar **Observáveis associados** para executar a operação de envio.
   - Na guia **Investigação**, clique em **Exibir informações relacionadas** para exibir todas as pesquisas de ameaças associadas, pesquisa de detecções e dados de enriquecimento do observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Por exemplo, selecione **Inteligência sobre ameaça** > **Observáveis Associados** para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros de observável para executar a operação **Enviar observável para TISC** para enviar os dados por push.



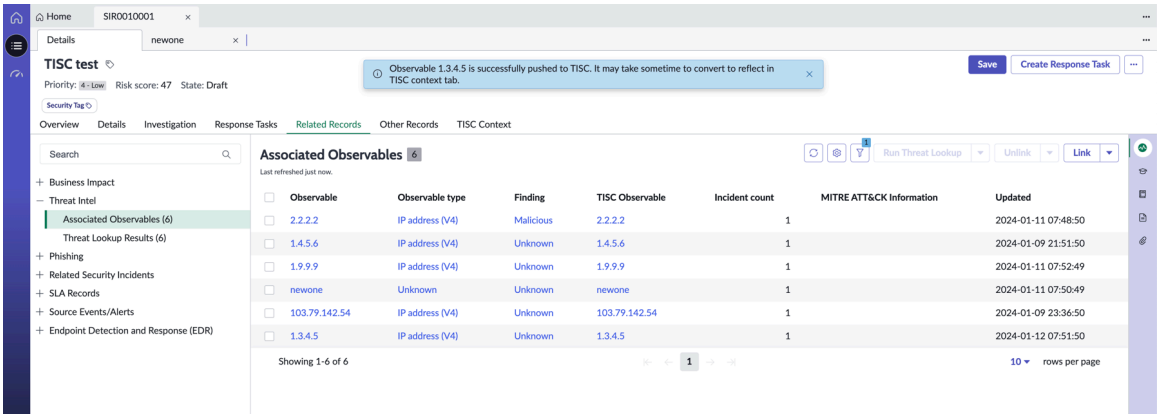
4. Clique **em Enviar observável para TISC**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se o observável selecionado não estiver presente no TISC, primeiro o observável será criado como origem de observável e, quando o observável de origem criar o registro de observável de TISC, o registro de observável será automaticamente associado ao observável recém-criado.
- Depois que a operação de envio do observável é executada, uma mensagem informativa é exibida informando que `o observável 0.0.0.0 foi enviado por push com sucesso para o TISC. Pode levar algum tempo para converter para refletir na guia de contexto de TISC.`



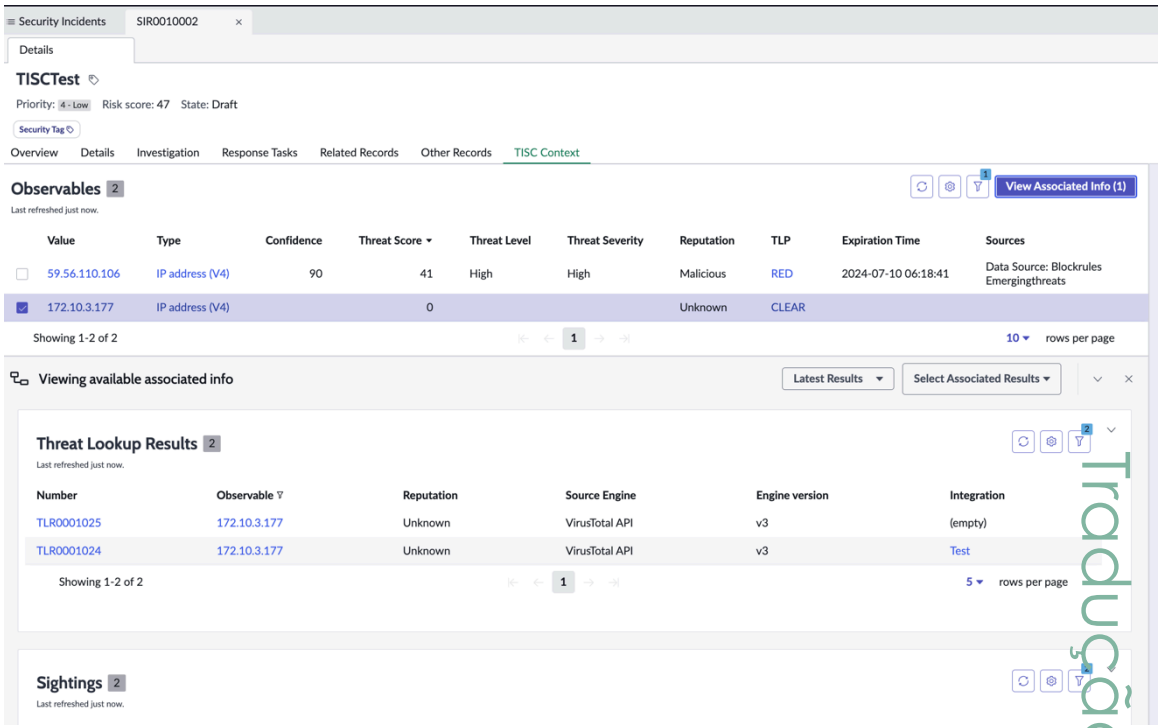
5. Selecione **Contexto de TISC**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: :

- Agora você verá o observável que é enviado por push para o TISC da aplicação SIR.



- **Em uma operação de envio manual**: os dados do observável só podem ser enviados se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de envio automático**: os dados do observável ou de aprimoramento serão enviados automaticamente quando estiverem associados ao incidente de segurança.
- **O contexto do TISC** mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas do SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento do observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento do observável associado dos observáveis selecionados.

6. Exibe os resultados.

Enviar pesquisa de ameaças para TISC

Usando este recurso, o analista de segurança pode enviar os dados de pesquisa de ameaças do SIR para o TISC. Usando o contexto de TISC, você pode verificar se os resultados da pesquisa de ameaças estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados por push sempre que necessário.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

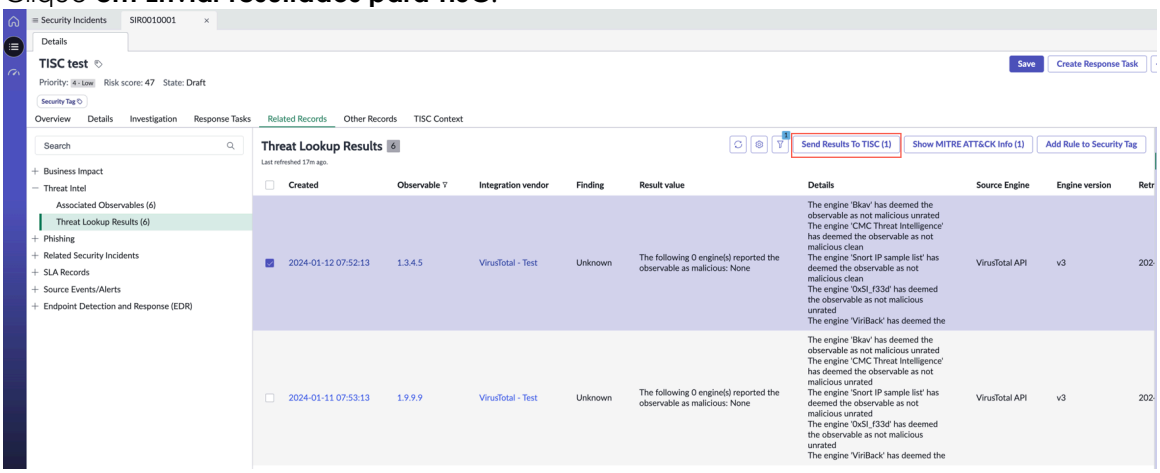
Procedimento

1. Navegue até a guia **Registros relacionados** no espaço SIR para executar a ação da capacidade de integração de TISC.

Nota:

- Você também pode navegar até a guia **Investigação** e navegar até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página e selecionar **Observáveis associados** para executar a operação de envio.
- Na guia **Investigação**, clique em **Exibir informações associadas** para exibir todas as pesquisas de ameaças associadas, pesquisa de detecções e dados de enriquecimento do observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Selecionar **Inteligência sobre ameaça** > **Resultados da Pesquisa de ameaças** para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros de resultados de pesquisa de ameaças.
4. Clique **em Enviar resultados para TISC**.



Nota:

- Se o observável de pesquisa de ameaças selecionado não estiver presente no TISC, no modo manual, primeiro o observável será criado como origem de observável e, quando o observável de origem criar o registro de observável de TISC, o registro de observável será automaticamente associado ao observável recém-criado. Além disso, a pesquisa de ameaças selecionada também será enviada para o observável de pesquisa de ameaças recém-criado no modo manual.
- Em um modo automático, os observáveis não serão enviados se o observável estiver presente, então as pesquisas de ameaças serão enviadas automaticamente. Se os observáveis não estiverem presentes, as pesquisas de ameaças não serão enviadas por push.

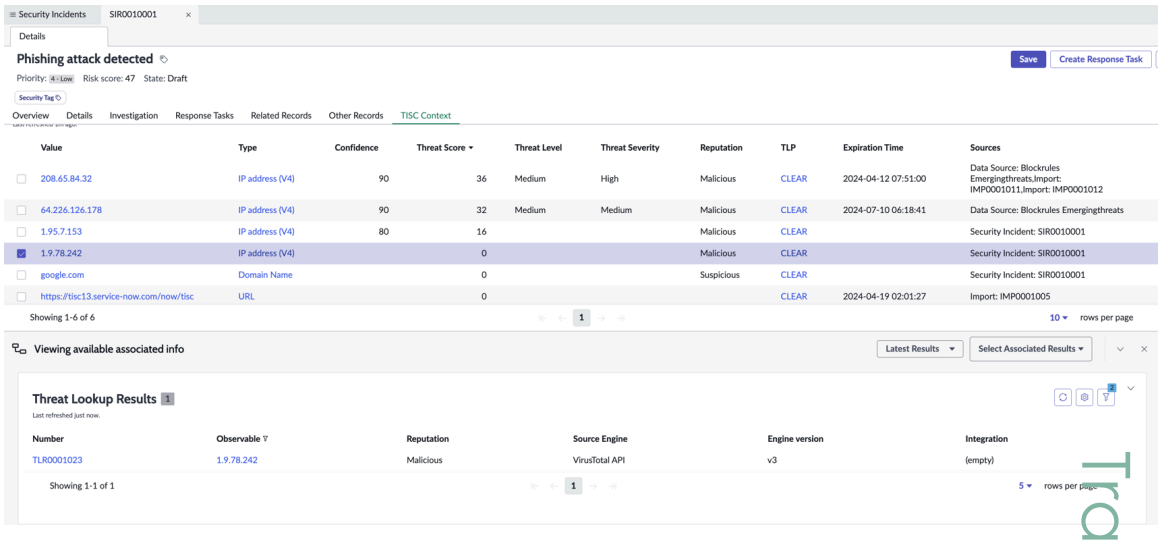
5. É exibida uma mensagem de confirmação de que `O observável (1.9.78.242) para o registro de pesquisa de ameaças selecionado não existe no TISC. Levará algum tempo para criar um observável e associar automaticamente o registro de pesquisa de ameaças do observável no TISC.`
   Depois que isso for processado e enviado por push, você poderá ver os resultados.
6. Selecione **Contexto de TISC**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: :

- Agora você verá o observável que é enviado por push para o TISC da aplicação SIR.



- **Em uma operação de envio manual**: os dados do observável só podem ser enviados se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de envio automático**: os dados do observável ou de aprimoramento serão enviados automaticamente quando estiverem associados a um incidente de segurança.
- **O contexto do TISC** mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas do SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento do observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento do observável associado dos observáveis selecionados.

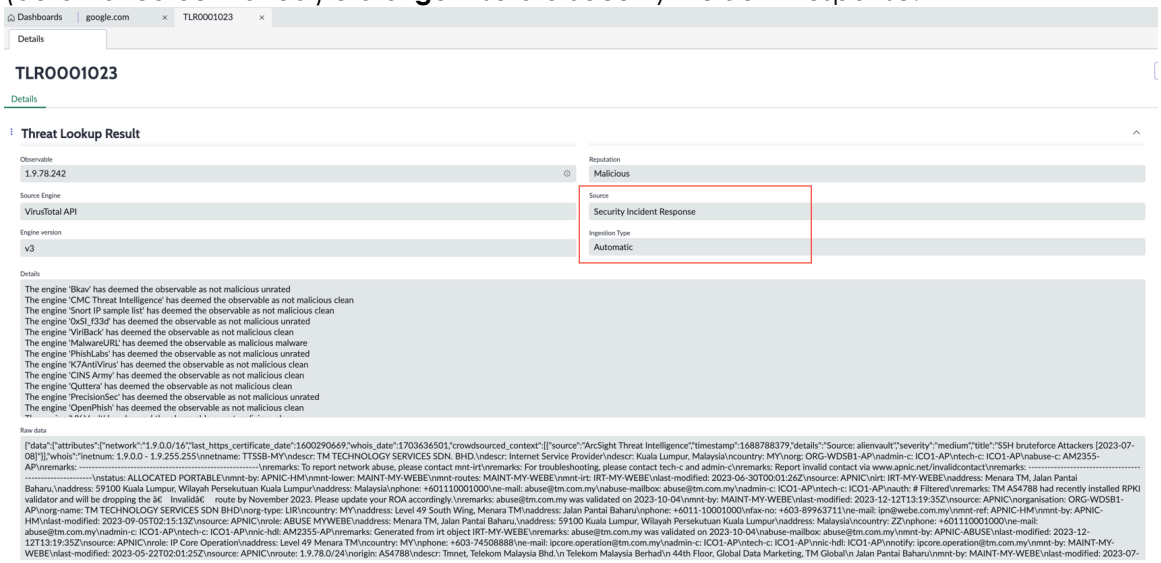
7. A exibição de lista mostra todos os resultados da pesquisa de ameaças, no entanto, selecione qualquer registro e clique no botão **Exibir informações associadas**.

8. Exibir os resultados da pesquisa de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Clique em qualquer registro de resultados de pesquisa de ameaças para exibir o registro na exibição do formulário, que também mostra o envio por push ou o **tipo de ingestão** (automático ou manual) e a **origem** será o Security Incident Response.



Enviar pesquisa de detecções para TISC

Usando este recurso, o analista de segurança pode enviar os dados de pesquisa de detecções do SIR para o TISC. Usando o contexto TISC, o analista pode verificar se os dados de pesquisa de detecções estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados por push sempre que necessário.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegue até a guia **Registros relacionados** no espaço SIR para executar a ação da capacidade de integração de TISC.

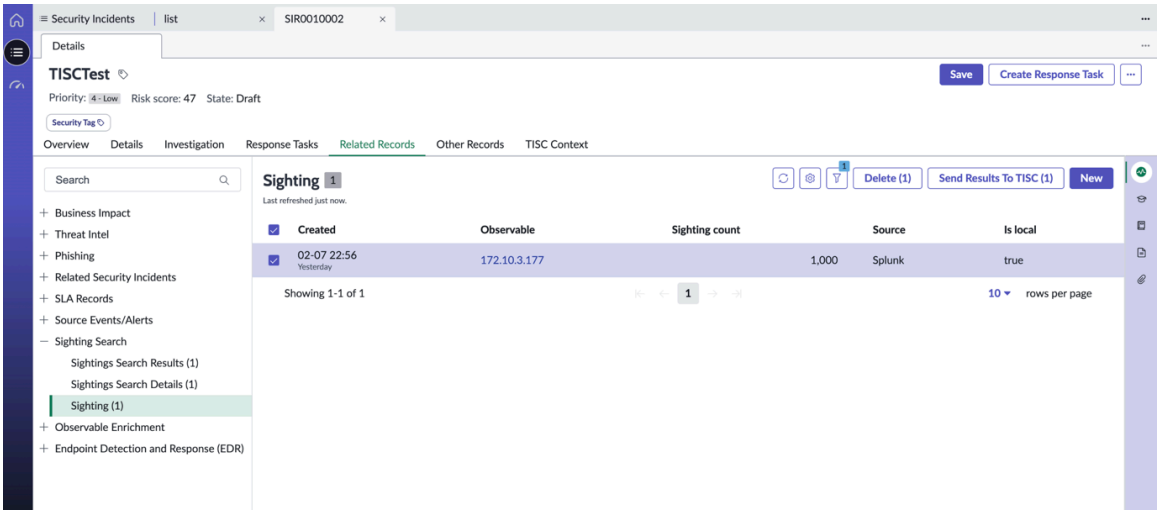
Nota:

- Você também pode navegar até a guia **Investigação** e navegar até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página e selecionar **Observáveis associados** para executar a operação de envio.
- Na guia **Investigação**, clique em **Exibir informações associadas** para exibir todas as pesquisas de ameaças associadas, pesquisa de detecções e dados de enriquecimento do observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Selecionar **Pesquisa de detecções** > **Resultados da pesquisa de detecções** para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros de Resultados da pesquisa de detecções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

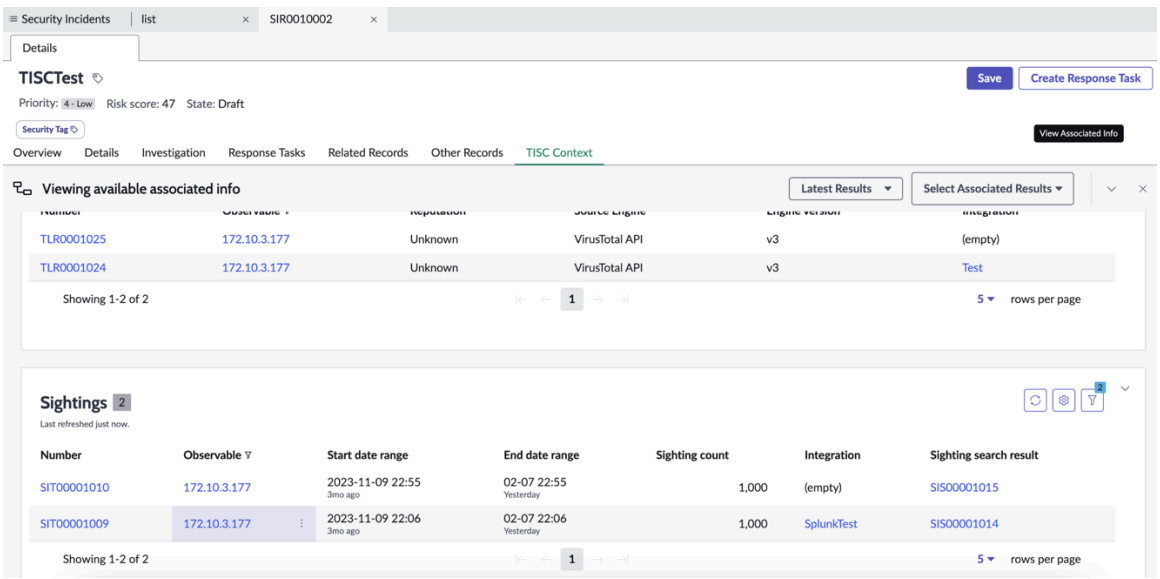


4. Clique **em Enviar resultados para TISC**.

Nota:

- Se o observável de pesquisa de detecções selecionado não estiver presente no TISC, no modo manual, primeiro o observável será criado como origem de observável e, depois que o observável de origem criar o registro de observável de TISC, o registro de observável será automaticamente associado ao observável recém-criado. Além disso, a pesquisa de detecções selecionada também será enviada para o observável de pesquisa de ameaças recém-criado no modo manual.
- Em um modo automático, os observáveis não serão enviados se o observável estiver presente, então as pesquisas de ameaças serão enviadas automaticamente. Se os observáveis não estiverem presentes, as pesquisas de ameaças não serão enviadas por push.

5. Selecione **Contexto de TISC**.



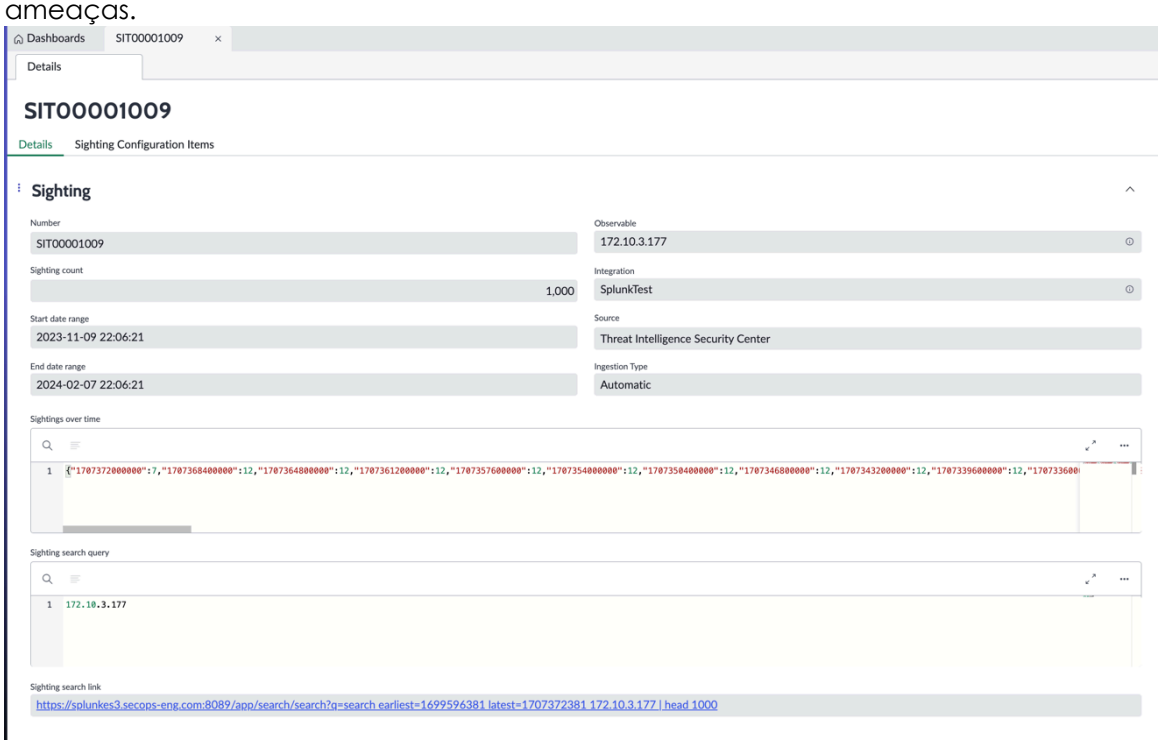
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: :

- Agora você verá o observável que é enviado por push para o TISC da aplicação SIR.
- **Em uma operação de envio manual**: os dados do observável só podem ser enviados se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de envio automático**: os dados do observável ou de aprimoramento serão enviados automaticamente quando estiverem associados ao incidente de segurança.
- **O contexto do TISC** mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas do SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento do observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento do observável associado dos observáveis selecionados.

6. Depois que o registro for processado, selecione-o e clique em **Exibir informações associadas**.
7. Exibe os resultados.
8. Clique em qualquer registro de resultados de pesquisa de detecções para exibir o registro na exibição do formulário, que também mostra o envio por push ou o **tipo de ingestão** (automático ou manual) e a **origem** será a Central de segurança de inteligência contra ameaças.



Enviar aprimoramento de observável para TISC

Usando este recurso, o analista de segurança pode enviar os dados de pesquisa de detecções do SIR para o TISC. Usando o contexto TISC, o analista pode verificar se os dados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de pesquisa de detecções estão presentes no TISC. Caso contrário, o analista de segurança pode enviar os dados por push sempre que necessário.

Antes de Iniciar
Função necessária: sn_si.analyst

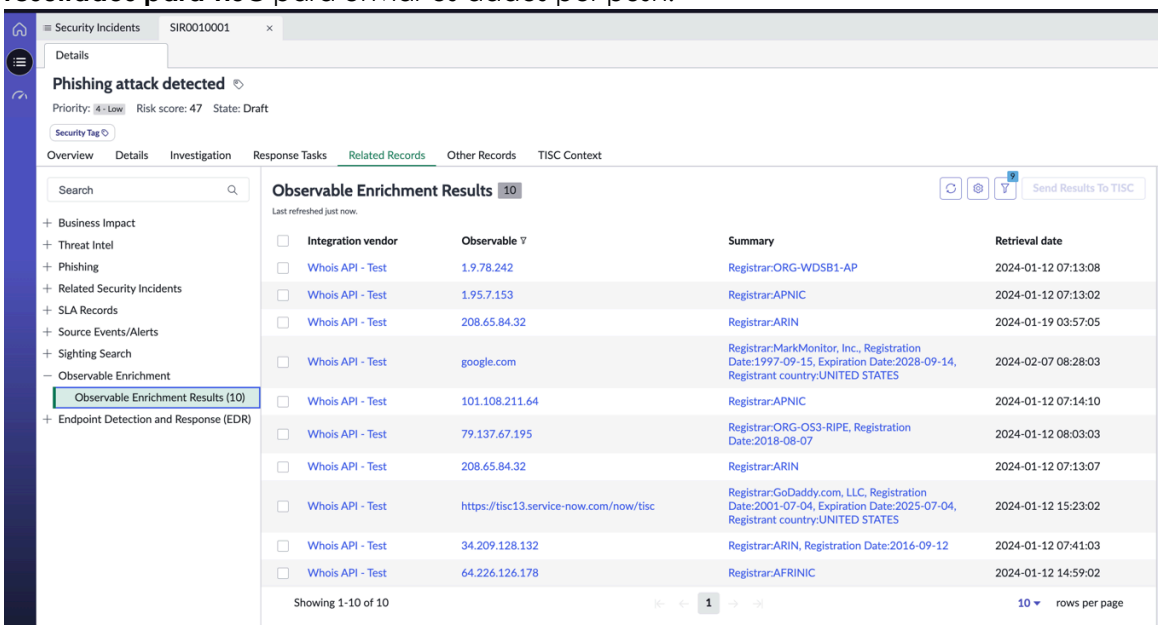
Procedimento

1. Navegue até a guia **Registros relacionados** no espaço SIR para executar a ação da capacidade de integração de TISC.

   Nota:

   - Você também pode navegar até a guia **Investigação** e navegar até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página e selecionar **Observáveis associados** para executar a operação de envio.
   - Na guia **Investigação**, clique em **Exibir informações associadas** para exibir todas as pesquisas de ameaças associadas, pesquisa de detecções e dados de enriquecimento do observável selecionado. Para obter mais informações, consulte Explorar tela de investigação.

2. Selecionar **Aprimoramento de Observável** > **Resultados de enriquecimento observável** para executar a operação de envio e enviar manualmente os dados para o TISC.
3. Selecione um ou mais registros de observáveis para executar a operação **Enviar resultados para TISC** para enviar os dados por push.



4. Clique **em Enviar resultados para TISC**.

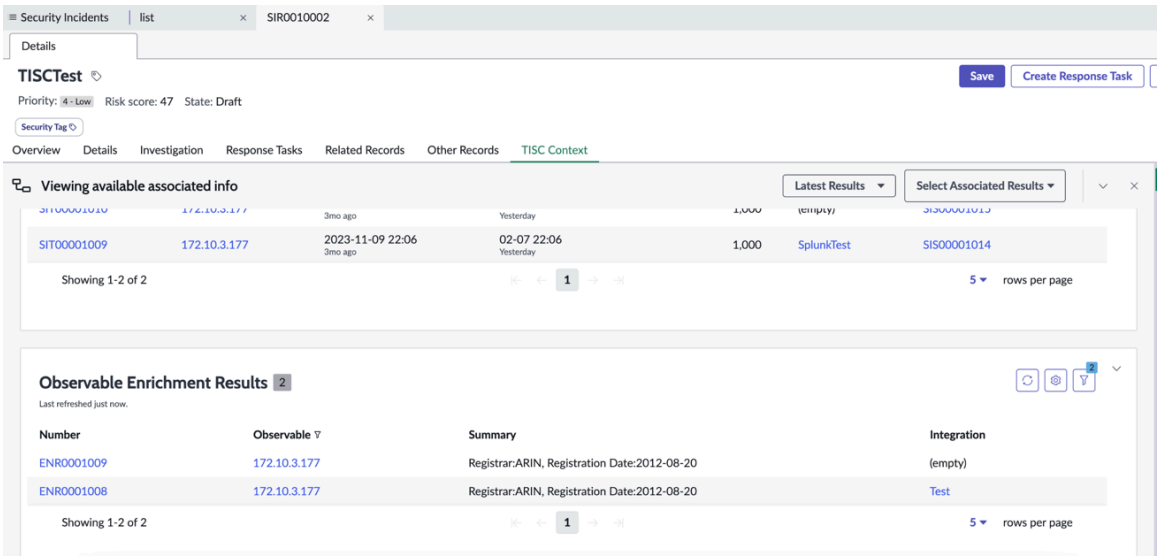
   Nota:

   - Se o observável selecionado não estiver presente no TISC, primeiro o observável será criado como origem de observável e, quando o observável de origem criar o registro de observável de TISC, o registro de observável será automaticamente associado ao observável recém-criado.
   - Depois que a operação de envio do observável é executada, uma mensagem informativa é exibida informando que `o observável 0.0.0.0 foi enviado por push com sucesso para o TISC. Pode levar algum tempo para converter para refletir na guia de contexto de TISC.`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Contexto de TISC**.



Nota: :

- Agora você verá o observável que é enviado por push para o TISC da aplicação SIR.
- **Em uma operação de envio manual**: os dados do observável só podem ser enviados se estiverem vinculados aos incidentes de segurança. Depois que o observável é enviado do SIR, esses dados podem ser identificados usando fontes que terão referência ao incidente de segurança vinculado ao observável.
- **Em uma operação de envio automático**: os dados do observável ou de aprimoramento serão enviados automaticamente quando estiverem associados ao incidente de segurança.
- **O contexto do TISC** mostra todos os observáveis associados ao SIR que também estão presentes no TISC.
- Usando o contexto do TISC, os analistas do SIR podem ver todos os dados de aprimoramento do TISC, incluindo pesquisas de ameaças, pesquisa de detecções e resultados de aprimoramento do observável.
- **Exibir informações associadas** mostrará todos os dados de aprimoramento do observável associado dos observáveis selecionados.

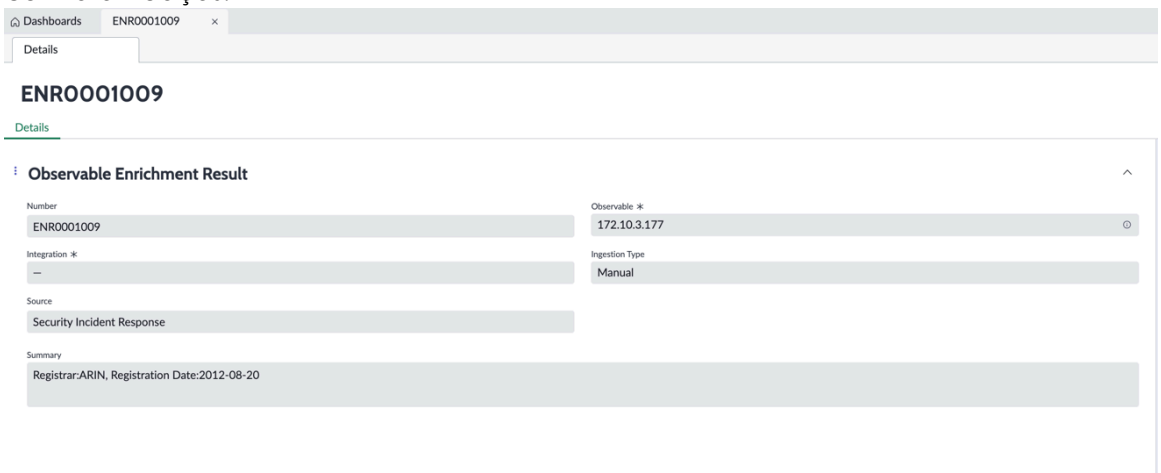
6. Exibe os resultados.

7. Clique em qualquer registro de resultados de aprimoramento de observável para exibir o registro na exibição do formulário, que também mostra o envio por push ou o **tipo de**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ingestão (automático ou manual) e a **origem** será Central de segurança de inteligência contra ameaças.



Trabalhando com contexto de TISC

O contexto do TISC facilita a exibição de dados de inteligência contra ameaças, como observáveis, no espaço de resposta a incidentes de segurança.

Isso ajuda os analistas de segurança a detectar, investigar e responder a incidentes de segurança com mais eficiência no espaço.

O contexto de TISC no espaço do Security Incident Response permite que os analistas de segurança adicionem incidentes de segurança ou observáveis a casos de TISC diretamente do espaço, além de exibir os resultados de enriquecimento e exibir informações relacionadas a observáveis que são agentes de ameaça, padrões de ataque, campanhas, e assim por diante.

Usando esta seção, você pode fazer o seguinte:

1. Associar observáveis a um caso de TISC.
2. Exibir informações de observáveis associados.
3. Exibir resultados de aprimoramento de observáveis.

Para obter informações e procedimentos mais detalhados, consulte as seções a seguir e, para obter mais informações sobre como a integração funciona entre os espaços de TISC e SIR, consulte TISC integration with SIR Workspace em Central de segurança de inteligência contra ameaças.

Adicionar observáveis ao caso de TISC

Use esta seção para adicionar incidentes ou observáveis de segurança a um caso de TISC.

Antes de Iniciar

Função necessária: sn_si.analyst

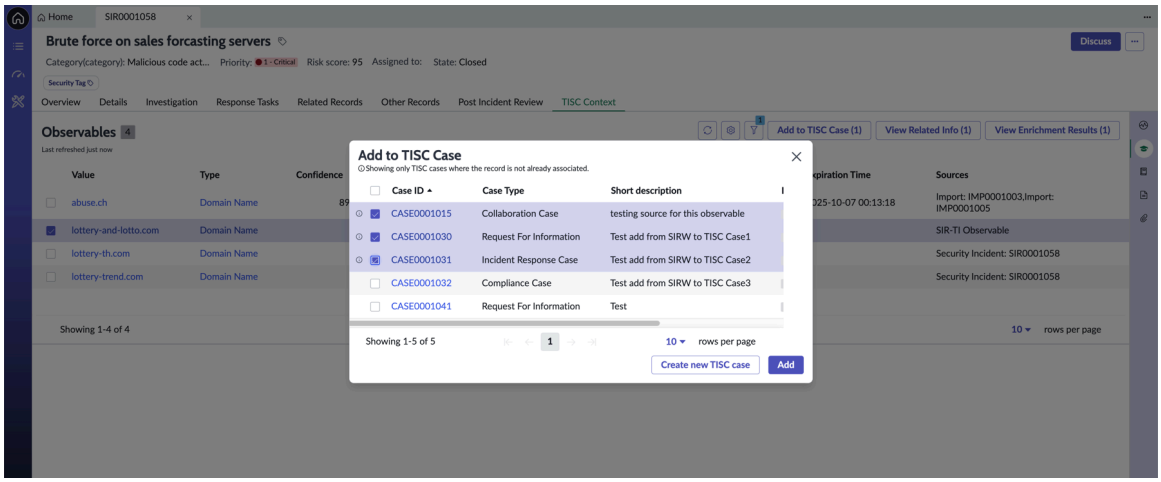
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Todos**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente, filtrando usando a seção Filtros rápidos ou navegando por um estado de incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione a guia **Contexto de TISC**.
4. Clique no botão **Adicionar ao caso de TISC**.
   A caixa de diálogo Adicionar ao caso de TISC é exibida e mostra somente os casos de TISC em que o registro ainda não está associado.
5. Selecione os observáveis.
6. Selecione o(s) caso(s) e clique em **Adicionar** para adicionar os casos aos observáveis e associá-los ao incidente de segurança.



Nota: Você também pode criar um novo caso clicando em **Criar novo caso de TISC**, caso não tenha nenhum caso existente.

As seguintes mensagens de confirmação são exibidas:

- Os observáveis a seguir foram adicionados como artefatos com sucesso.
- Os seguintes observáveis são enviados para o TISC e posteriormente adicionados aos registros de casos de TISC selecionados.

Nota: O processamento e a associação das atividades de observáveis são publicados no fluxo de atividades conforme e quando a associação é concluída.

7. Exiba os registros de casos associados fazendo login no Espaço da Central de segurança de inteligência contra ameaças para obter outras etapas.
   Para obter mais informações, consulte TISC integration with SIR Workspace.

Nota:

No espaço do Security Incident Response, você também pode associar observáveis a registros de caso das guias **Investigação** e **Registros relacionados**.

Nota: Para associar observáveis da **investigação**, siga o procedimento abaixo e para associar dos **Registros relacionados** explicados aqui Adicionar observáveis ao caso de TISC.Você também pode navegar até a guia **Investigação** e navegar até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página e selecionar **Observáveis associados** para adicionar observáveis ao caso de TISC.

Exibir informações relacionadas do TISC

Use esta seção para exibir as informações relacionadas, como agentes de ameaça relacionados, padrões de ataque, campanhas e casos do TISC no espaço SIR.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

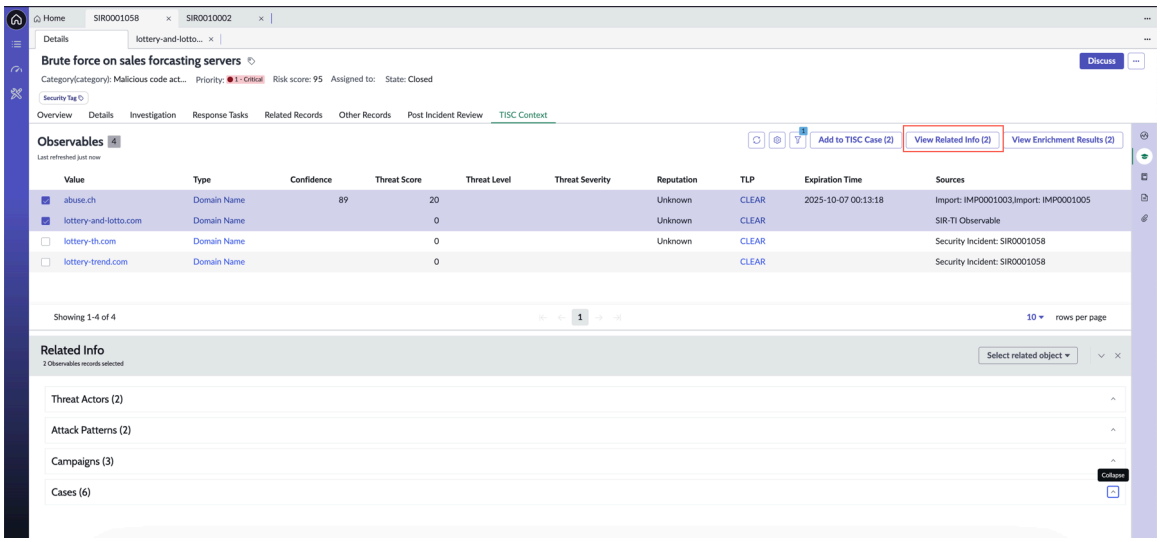
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Todos**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente, navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Depois que o incidente estiver aberto, navegue até a guia **Contexto de TISC**.
   Exibição de informações relacionadas à exibição:

   Nos detalhes do incidente, você pode exibir informações relacionadas em várias seções.

   a. Selecione um ou mais observáveis.

   b. Clique no botão **Exibir informações relacionadas**.
   Esta seção exibe as informações associadas que estão relacionadas aos observáveis selecionados.

Nome	Descrição
Agentes da ameaça	Mostra informações do TISC para agentes de ameaça relacionados aos observáveis selecionados.
Padrões de ataque	Mostra informações do TISC para Padrões de ataque relacionados aos observáveis selecionados.
Campanhas	Mostra informações do TISC para campanhas relacionadas aos observáveis selecionados.
Casos	Mostra informações de TISC para casos de TISC relacionados aos observáveis selecionados.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir resultados de enriquecimento

Use esta seção para exibir os resultados de aprimoramento de observáveis, como resultados de pesquisa de ameaças, detecções e resultados de aprimoramento de observáveis do TISC no espaço SIR.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

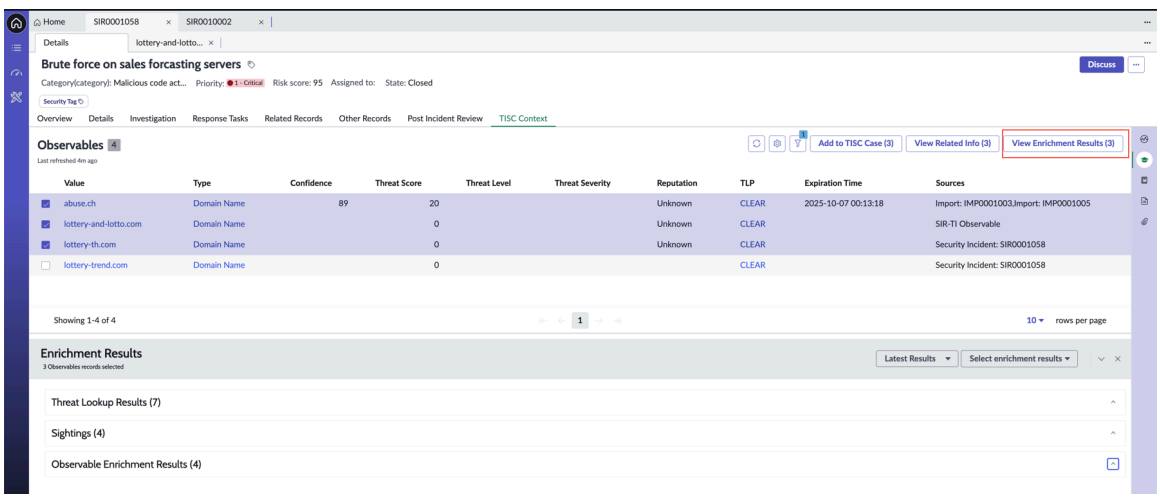
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Todos**.
2. Localize e abra qualquer incidente de segurança específico que você esteja investigando.
   Isso também pode ser feito pesquisando o ID do incidente, navegando na seção Filtros rápidos ou filtrando pelo estado do incidente.
3. Depois que o incidente estiver aberto, navegue até a guia **Contexto de TISC**.
   Exibição de resultados de aprimoramento:

   Nos detalhes do incidente, você pode exibir informações relacionadas em várias seções.

   a. Selecione um ou mais observáveis.

   b. Clique no botão **Exibir resultados** de aprimoramento.
   Esta seção exibe os detalhes relacionados aos observáveis selecionados.

Nome	Descrição
Resultados da Pesquisa de ameaças	Lista todos os resultados de pesquisa de ameaças associados para observáveis de TISC selecionados.
Detecções	Lista todas as vistas associadas aos observáveis de TISC selecionados.
Resultados de enriquecimento observável	Lista todos os resultados de enriquecimento de observáveis associados para observáveis de TISC selecionados.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como iniciar um bate-papo na barra lateral no Security Incident Response

Usando a barra lateral, os analistas de segurança podem colaborar com outras pessoas em tempo real com base em um registro baseado em tarefa ou em interação do espaço. Essas discussões da barra lateral facilitam a troca de informações e conhecimento para ajudar a resolver problemas mais rapidamente e com resultados de maior qualidade.

Antes de Iniciar

Função necessária: sn_si.read

Verifique se você ativou o plug-in Conjunto de recursos padrão do Omni-Experience. Para obter mais informações, consulte Instalação de Barra lateral .

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione o ícone de exibição de de lista.
3. Abra um incidente de segurança para o qual você deseja iniciar uma discussão na barra lateral.
4. Selecione **Discutir**.
   A caixa de diálogo Iniciar uma discussão na barra lateral é exibida.

   Nota: A integração da barra lateral com o Microsoft Teams permite que os usuários da barra lateral e do Microsoft Teams se comuniquem em suas respectivas plataformas. Para obter mais informações, consulte Barra lateral e Microsoft Teams .

5. Na caixa de diálogo Iniciar uma discussão na barra lateral, preencha os campos.

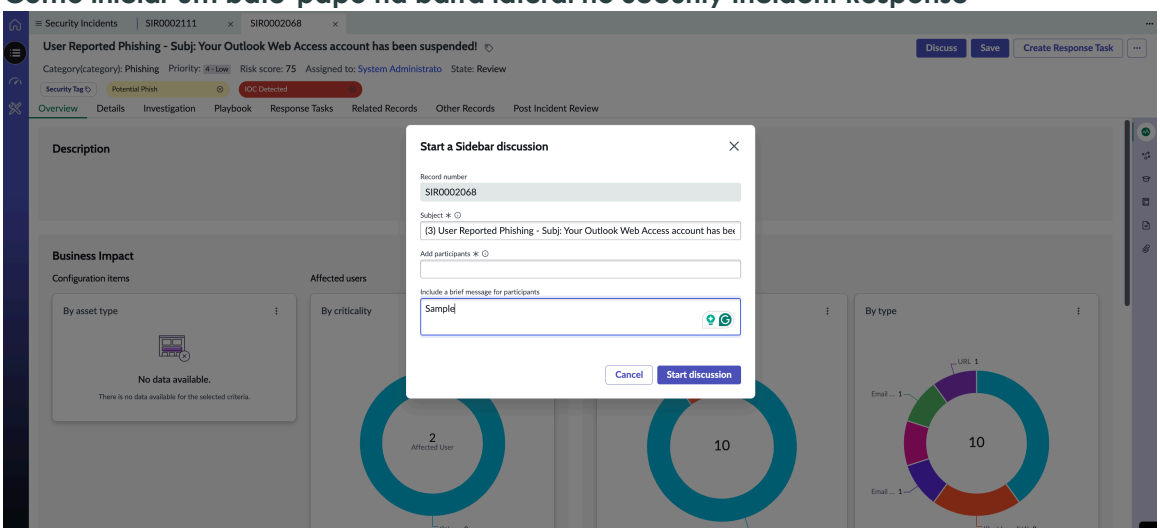
Campo	Descrição
Número de registro	O número da tarefa ou do incidente associado à discussão da barra lateral.
Assunto	Forneça um título para a discussão na barra lateral.
Adicionar participantes	Opção para adicionar participantes à discussão na barra lateral. Se você tiver integrado o bate-papo da barra lateral com o Microsoft Teams, também poderá adicionar participantes do Microsoft Teams.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ É necessário adicionar pelo menos um participante para criar uma nova discussão. ◦ Se a barra lateral e o Microsoft Teams estiverem integrados, os usuários do Microsoft Teams serão diferenciados dos usuários da barra lateral com um ícone do Microsoft Teams. ◦ Por padrão, todos os usuários com acesso de leitura aos registros SIR também terão acesso aos bate-papos da barra lateral, mas isso pode ser controlado usando a consulta de membro. Para obter mais informações, consulte Configurar consulta de membro Barra lateral .
Incluir uma breve mensagem	Envie um resumo curto do problema para que seja abordado na discussão da barra lateral.

Como iniciar um bate-papo na barra lateral no Security Incident Response



6. Selecione **Iniciar discussão**.
7. Você pode executar configurações adicionais, como ações rápidas.
   Para limitar o uso da ação, você pode usar o campo **Aplicar ao grupo** na página de ação rápida. Para obter mais informações, consulte Como criar uma ação rápida .

Playbook de incidente de segurança

Invoque o fluxo do playbook de incidente de segurança automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook funciona somente para os processos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados do Flow Designer existentes, ele continuará a funcionar e as atividades continuarão a ser renderizadas como tarefas de resposta.

Existem duas maneiras de associar o playbook ao incidente de segurança:

- Invocar playbook automaticamente
- Adicionar playbook manualmente

Invocar playbook automaticamente

Para que um Playbook seja invocado automaticamente, um processo precisa ser definido usando o **Designer de automação de processos (PAD)**e, quando a condição do gatilho for atendida, a guia do playbook será renderizada automaticamente com as atividades do playbook sendo exibidas.

Adicionar playbook manualmente

Para que um Playbook seja invocado manualmente, navegue até o menu suspenso Ação de IU Formulário e selecione **Adicionar Playbook**. Para obter mais informações, consulte, Adicionar Playbook

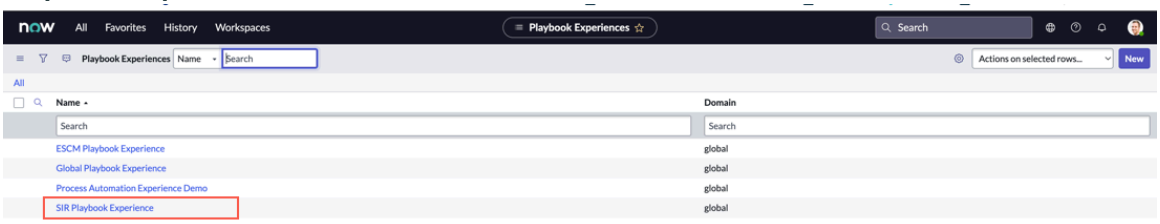
Nota: Se já houver um playbook disponível, os novos playbooks adicionados serão executados em paralelo aos playbooks existentes.

- No playbook, o analista pode filtrar os cartões do playbook por status.
- O analista pode cancelar um playbook selecionando-o no ícone de elipse.
- Em cada atividade, o analista poderá executar as ações definidas nos cartões de atividade, como Ignorar, Marcar como concluído, Cancelar ou ações de Orquestração, como Enviar para área restrita, Pesquisar e-mails e assim por diante.
- Cada uma dessas ações é definida na definição de atividade e o cartão completo visível é personalizável no momento da criação da própria definição de atividade.

Nota: Todas as definições de atividade futura e as próximas etapas a serem executadas são exibidas com um ícone de cadeado e estão no modo somente leitura para o usuário. O modo de exibição do playbook é controlado por uma configuração conforme explicado abaixo.

1. Navegar até **Todos** > **Playbook Experiences**.
2. Na página Playbook Experiences, selecione uma **SIR Playbook Experience**.

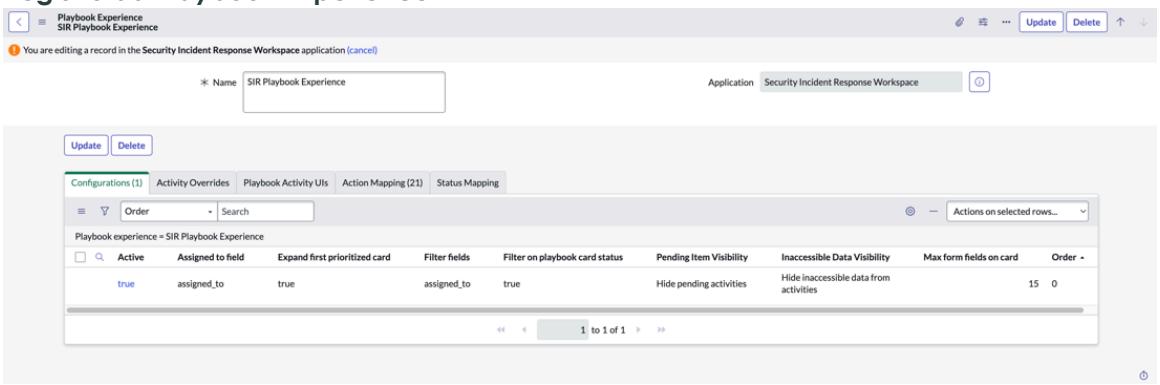
Playbook Experience



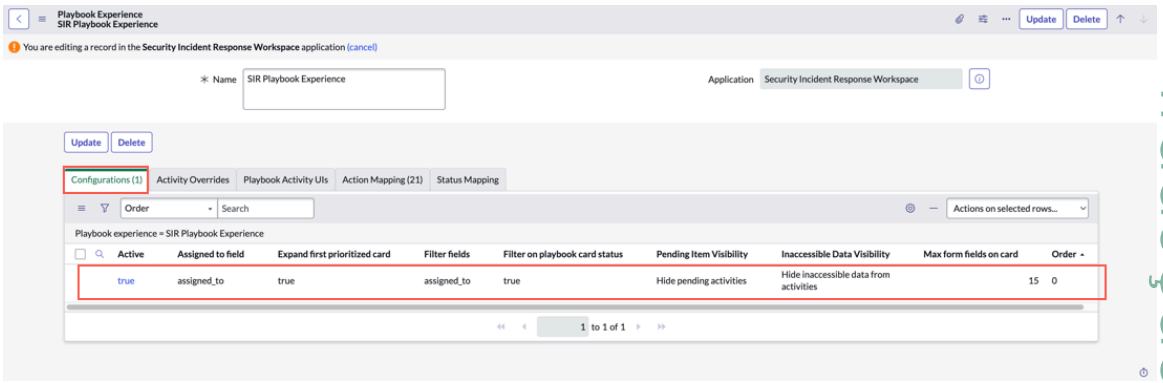
A página **Playbook Experience SIR da Playbook Experience** é exibida.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro da Playbook Experience

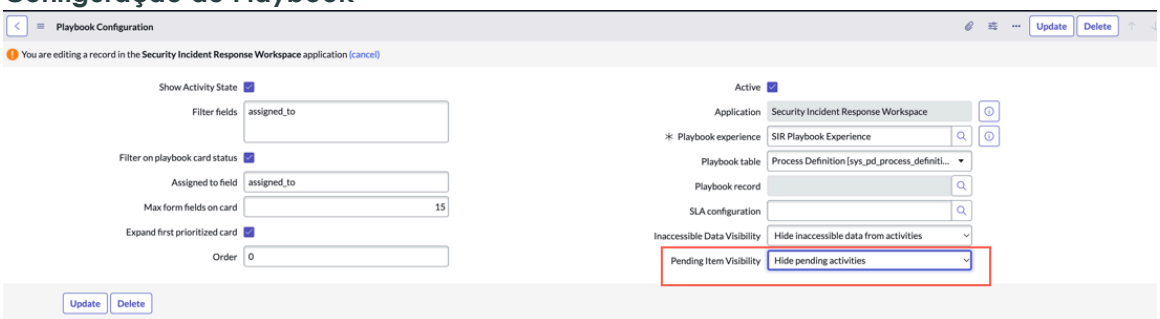


3. Clique no registro de **configuração**.



4. Na guia Configuração, clique em SIR Configuração da Playbook Experience.

Configuração do Playbook



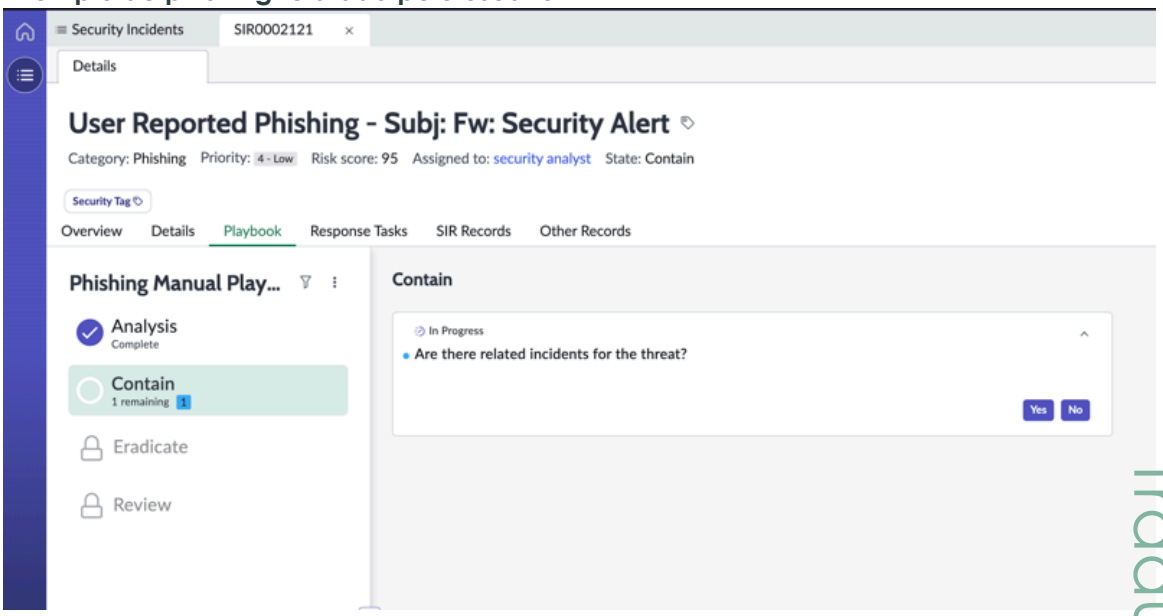
5. Navegue até a lista suspensa do campo **Visibilidade de item pendente**, selecione a opção desejada e salve o registro. Escolhas das seguintes opções:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

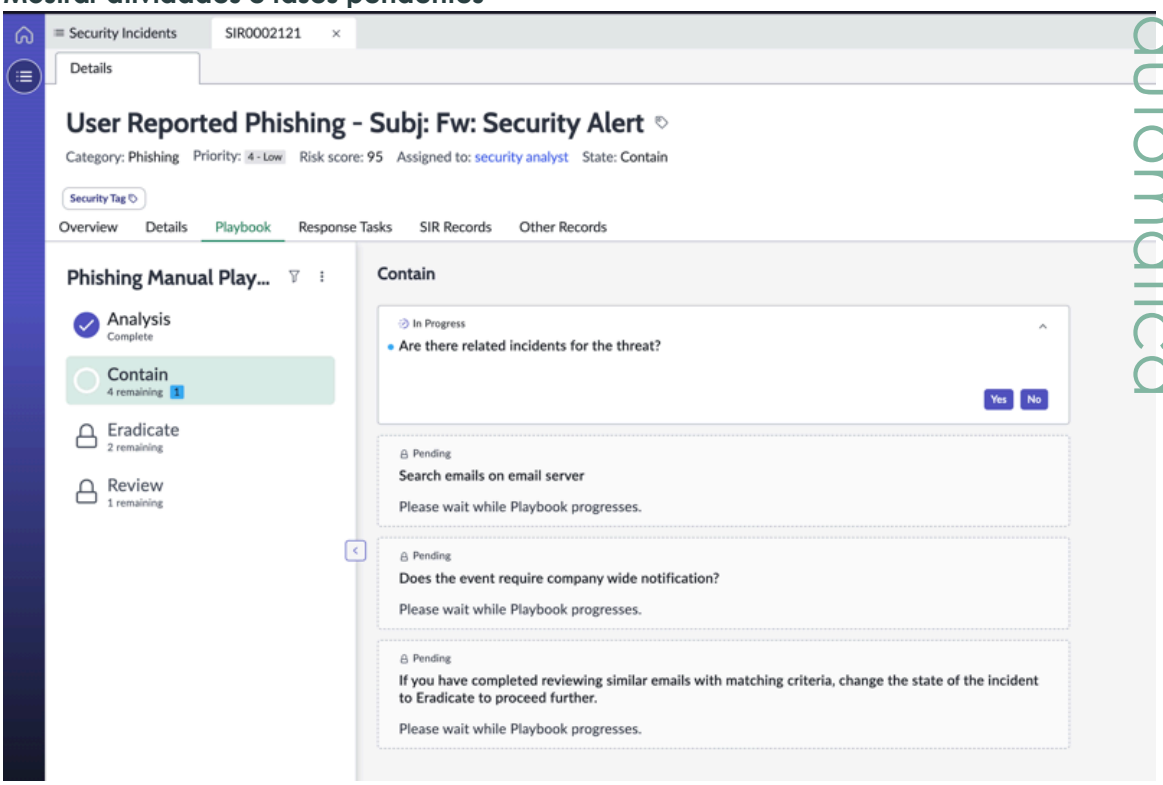
- **Ocultar atividades pendentes**: selecione esta opção para ocultar as atividades pendentes que você deseja ver na seção de playbook do espaço.

Exemplo de phishing relatado pelo usuário



- **Mostrar fases e atividades pendentes**: selecione esta opção para mostrar as fases e atividades pendentes que você gostaria de ver na seção de playbook do espaço.

Mostrar atividades e fases pendentes

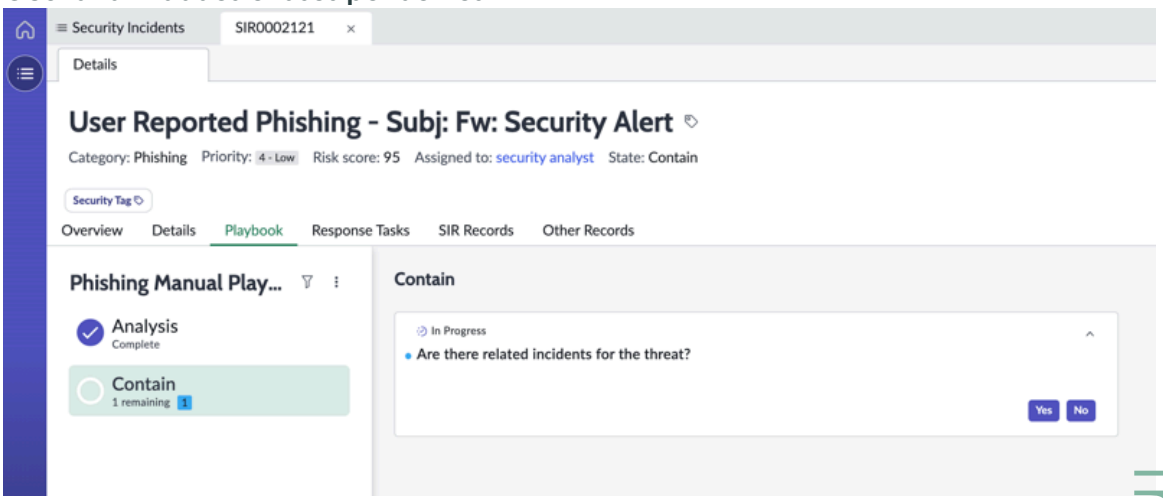


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

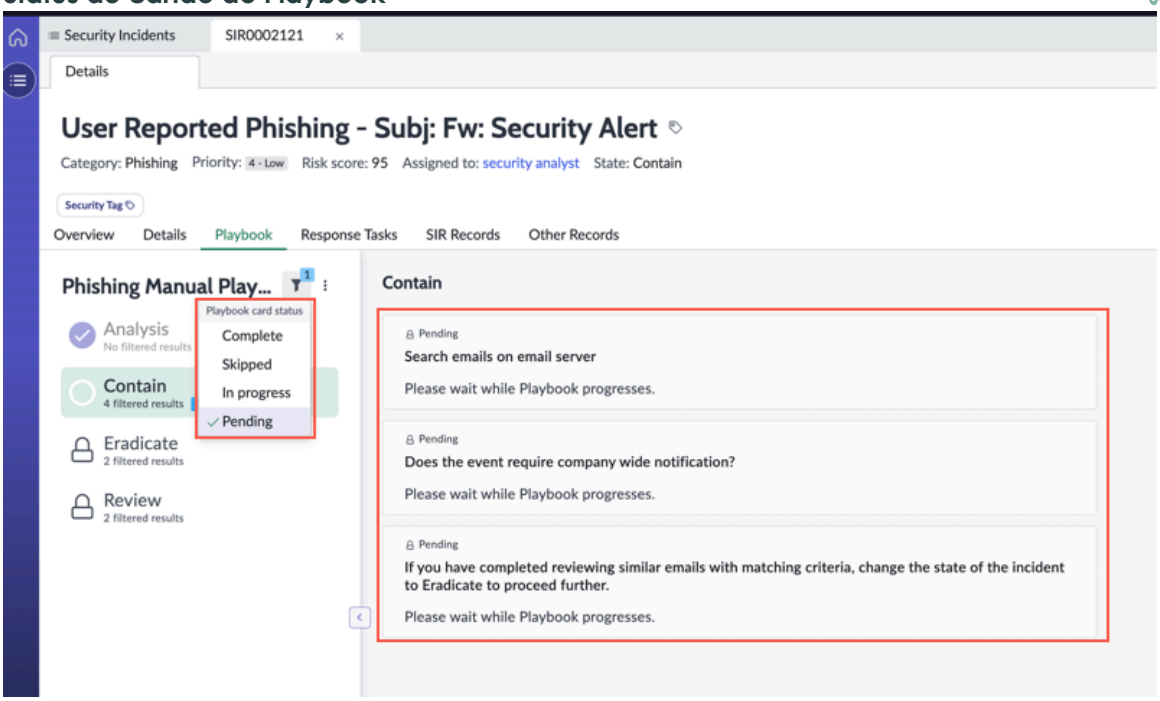
- **Ocultar atividades e fases pendentes**: selecione esta opção para ocultar as atividades e fases pendentes que você gostaria de ver na seção de playbook do espaço.

Ocultar atividades e fases pendentes



6. Na seção Playbook, use a opção de filtro para filtrar as atividades por status do cartão do Playbook (definição de atividade).

Status do cartão do Playbook



Adicionar Playbook

Use esta seção para adicionar o playbook manualmente.

Antes de Iniciar

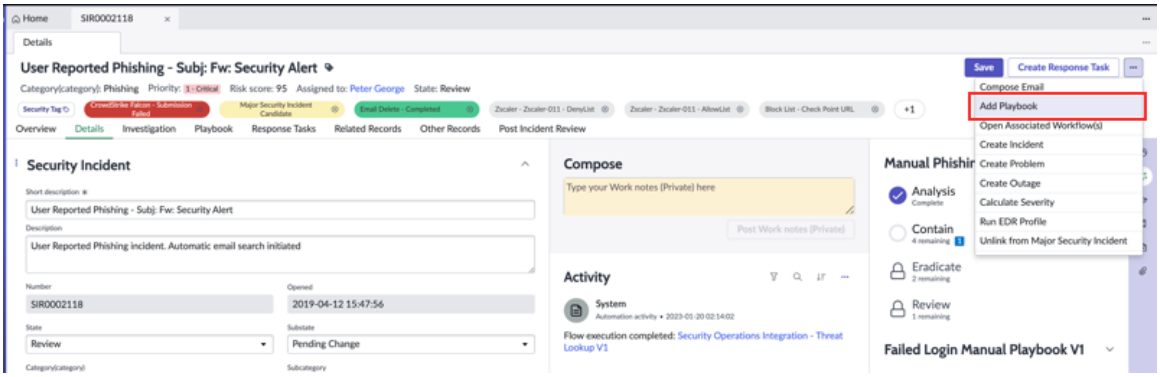
Função necessária: sn_si.analyst

Tradução automática

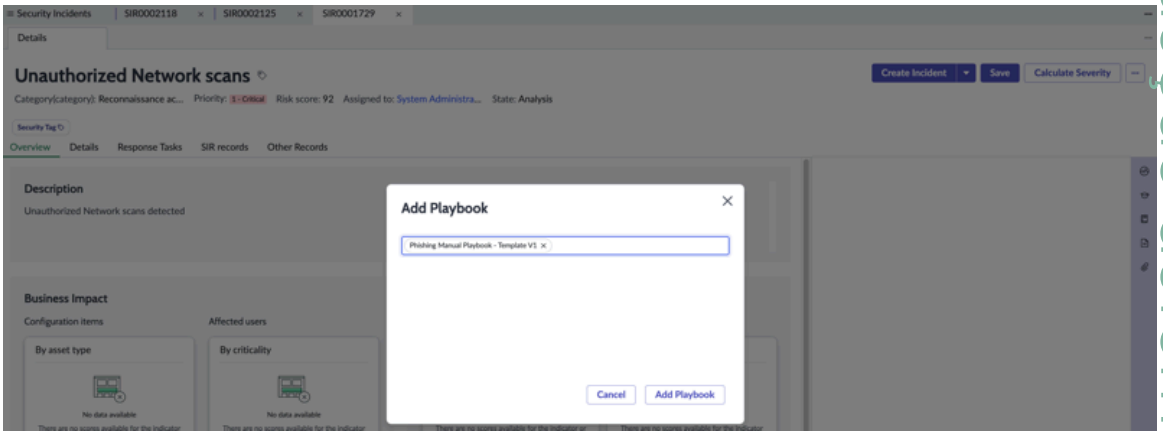
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Espaço de trabalho do analista de segurança**.
2. Abra um registro de incidentes
3. Clique **em Adicionar Playbook**.



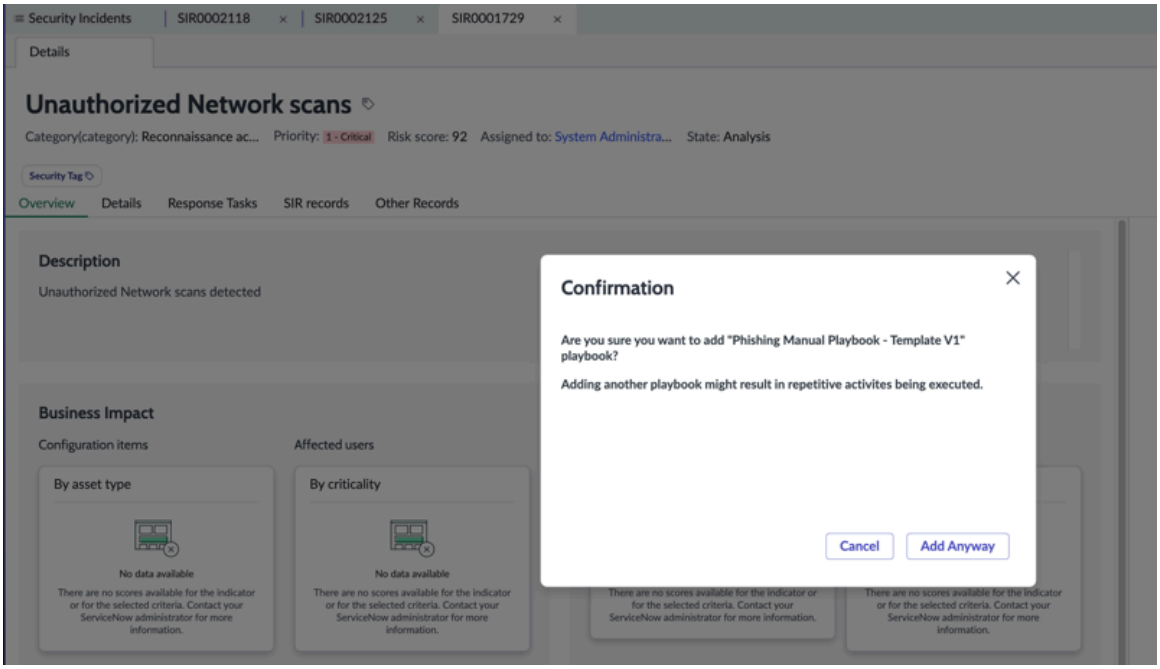
A caixa de diálogo **Adicionar Playbook** é exibida.



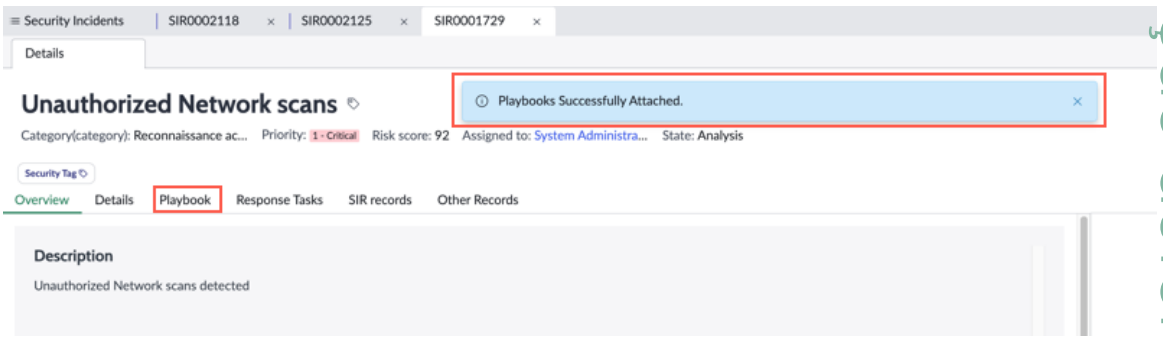
4. Selecione o modelo de playbook.
5. Clique **em Adicionar Playbook**.
   Uma caixa de diálogo de mensagem de confirmação é exibida para você confirmar.
6. Clique **em Adicionar mesmo assim**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



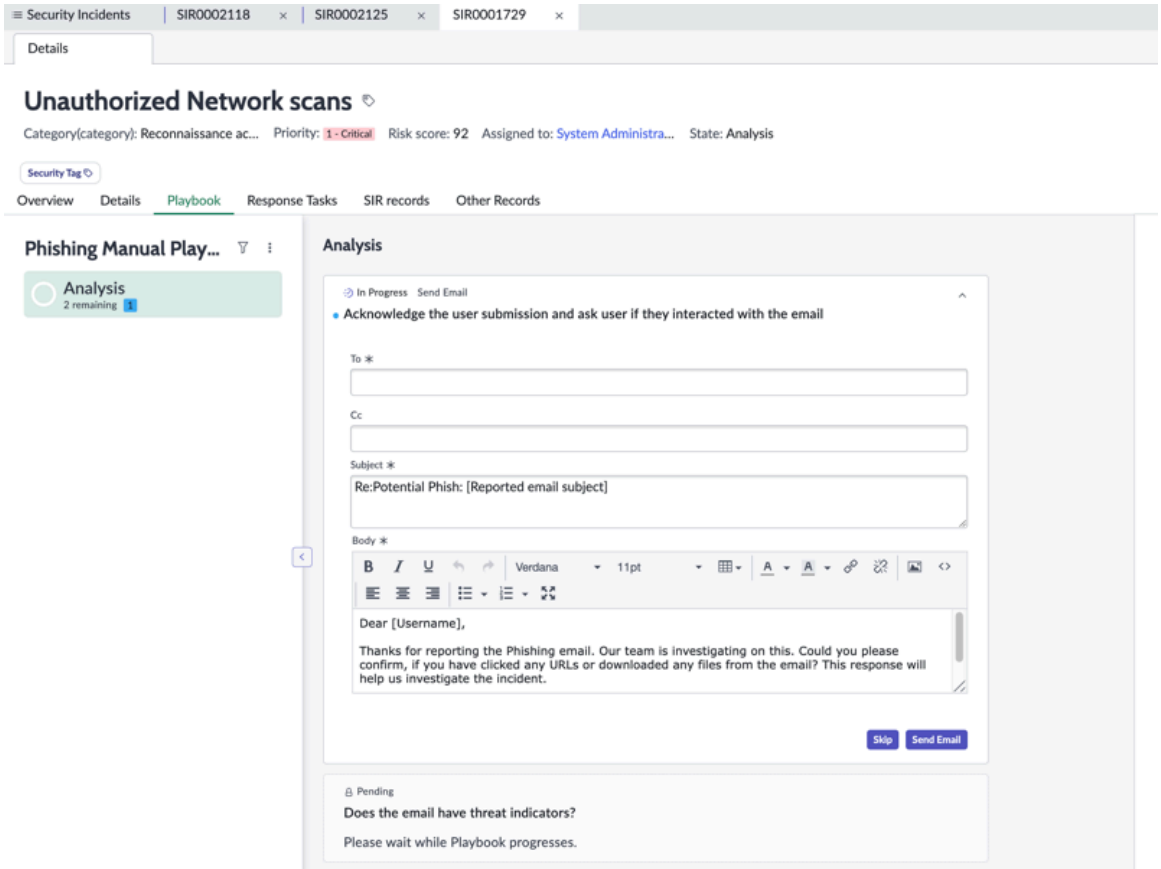
7. O **Playbook** é adicionado ao lado da guia **Detalhes**.



8. Clique na guia **Playbook**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Execute a série de atividades listada para passar para o próximo nível.

> **Nota:** Se um incidente de segurança estiver associado a um playbook, até que o playbook associado seja fechado ou cancelado, o usuário não poderá associar novamente o mesmo playbook ao mesmo incidente de segurança.

Pré-requisitos para os Playbooks

Você precisa das seguintes funções e plug-ins para criar os Playbooks.

Função necessária: administrador

- Habilite o plug-in Designer de automação de processos (PAD) [com.glide.pad.license].
- Habilite os seguintes plug-ins para uma Playbook Experience:
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Habilite o spoke das Operações de segurança para acessar fluxos [com.snc.secops.spoke].
- Enterprise Security Case Management PAD Commons.

Certifique-se de ter lido a documentação da plataforma na Playbook Experience e no Designer de automação de processos antes de começar com este guia.

Como recriar playbooks existentes no Workflow Studio

Você não pode converter fluxos existentes diretamente em playbooks em Workflow Studio. Cada etapa do Flow Designer que cria uma tarefa de resposta para orientar o analista deve ser dividida em ações ou subfluxos separados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você não tem permissão para converter fluxos existentes diretamente em playbooks em Workflow Studio. Cada etapa do Flow Designer que cria uma tarefa de resposta para orientar o analista deve ser dividida em ações ou subfluxos separados. Ao usar esses subfluxos ou ações granulares, você deve criar definições de atividade. Depois de criar essas definições de atividade, elas são adicionadas como atividades na fase na definição do processo. Você pode reutilizar definições de atividade em vários playbooks.

Você pode personalizar cada atividade para renderizar as ações necessárias nelas e a aparência do cartão ao criar a definição da atividade. A atividade pode mostrar clientes de e-mail, tabelas, ações, artigos da base de conhecimento, URLs e assim por diante. Você pode definir como a definição de atividade e a ação ou subfluxos subjacentes são criados.

Para obter mais informações, consulte as seções a seguir.

- Definições de atividades
- Designer de automação de processos

Definições de Atividades

O Now Platform fornece algumas definições de atividade no sistema de base. Além disso, para os playbooks do sistema base do Espaço SIR, há algumas definições de atividade definidas no sistema base na aplicação Gestão de casos de segurança empresarial PAD Commons.

Função necessária: sn_si.admin.

Esta é a lista de definições de atividades que fazem parte do sistema de base:

Definição de Atividade	Tabela	Descrição	Aplicação
Aguardar condição sem experiência	Global[global]	Aguardar condição sem experiência	Componentes comuns do PAD de gestão de casos de segurança empresarial
Enviar para área restrita FCS X	Incidente de segurança [sn_si_incident]	Enviar para área restrita	Componentes comuns do PAD de gestão de casos de segurança empresarial
Enviar e-mail	Incidente de segurança [sn_si_incident]	Atividade de envio de e-mail para playbooks SIR.	Componentes comuns do PAD de gestão de casos de segurança empresarial
Pesquisar E-mail	Incidente de segurança [sn_si_incident]	Pesquisar e-mails no servidor de e-mail	Componentes comuns do PAD de gestão de casos de segurança empresarial
Atualizar estado da tarefa	Incidente de segurança [sn_si_incident]	Atualizar o estado da tarefa	Componentes comuns do PAD de gestão de casos de segurança empresarial

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de Atividade	Tabela	Descrição	Aplicação
Excluir e-mail	Incidente de segurança [sn_si_incident]	Excluir e-mails	Componentes comuns do PAD de gestão de casos de segurança empresarial
Resultado Sim Não	Tarefa [task]	Resultado esperado	Componentes comuns do PAD de gestão de casos de segurança empresarial

Exemplo de definição de atividade: enviar e-mail

A seguir está um exemplo de definição da atividade Enviar e-mail.

Básico

Os detalhes básicos capturam o nome (rótulo), a aplicação, a descrição, a tabela e de todas as aplicações a partir das quais ele pode ser acessado.

Adicione o plano de automação, a experiência de atividade e envie. Após o envio, edite o documento para adicionar mais detalhes em cada guia.

Plano de Automação

O plano de automação associa a ação de back-end ou subfluxos criados usando o Flow Designer. Este exemplo usa: **Enviar e-mail - Subfluxo de atividade ESCM**.

Este subfluxo permite o envio de um e-mail. Ele tem a lógica principal para enviar um e-mail. Ele tem todos os campos de entrada e de saída definidos.

Todos os campos de entrada são mostrados na seção do plano de automação. Cada campo de entrada pode ser habilitado para ficar visível somente para o administrador, no modal padrão, no modal padrão e no painel de configuração:

- **Somente visibilidade de administrador**: quando definido como administrador, somente o administrador pode exibi-lo.
- **Incluir no modelo padrão**: quando definido para exibir no modal padrão, ele aparece somente no modal de propriedades.
- **Incluir no modelo padrão e no painel de configuração**: quando definido para exibir no modal padrão e no painel de configuração, ele aparece no painel de configuração do PAD e no modal de propriedades. Para obter mais informações, consulte Definições de atividade

Você pode definir os campos de entrada no momento da própria definição da atividade, desde que não precise alterar esses valores no momento da configuração. Isso ajuda o proprietário do processo de negócios a economizar tempo ao configurar uma atividade em um processo.

Experiência de Atividade

A guia de experiência de atividade define como o cartão de atividade é renderizado em tempo de execução. O sistema de base fornece os seguintes tipos de experiência:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Aprovação
- Item do catálogo
- Criar registro
- Instrucional
- Conhecimento
- Lista
- Notificação
- Registro

Com base no tipo de experiência selecionado, os outros campos são preenchidos. Para obter mais informações, consulte a documentação da Now Platform.

Neste exemplo, o tipo de **registro** está selecionado.

Nota: Por exemplo, se você quiser renderizar uma tabela, poderá escolher lista como o tipo de experiência.

Registro Associado

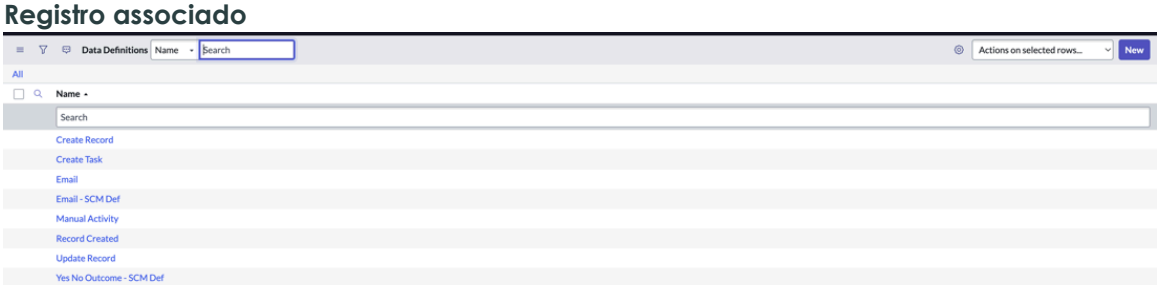
Use este registro para armazenar os dados associados pertencentes à atividade atual. Isso capturaria os dados de tempo de execução, bem como o status da experiência.

- Tabela associada: dados de fluxo
- Registro associado: VL
- Tabela de status da experiência: dados de fluxo
- Registro de status da experiência: VL

Neste exemplo, a tabela de dados de fluxo é usada para capturar os dados de tempo de execução. Os dados de tempo de execução podem variar de acordo com o caso de uso. Neste exemplo, os dados de tempo de execução são campos como Para, cc, Assunto e corpo. Para cada caso de uso, uma definição de dados de fluxo precisa ser criada para definir o tipo dos dados de tempo de execução.

1. Navegue até o painel esquerdo e insira **sys_flow_data_definition.list**. Exibe a lista de definições criadas para a tabela de dados de fluxo.

Registro associado

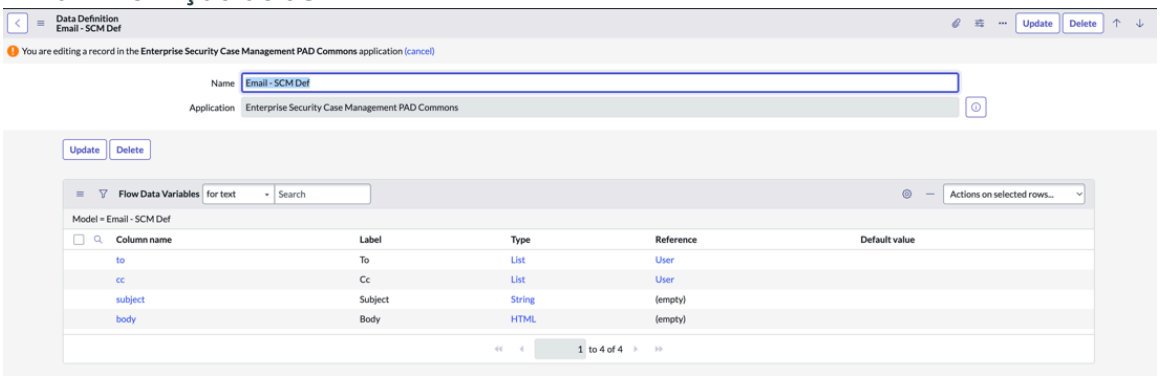


2. Abra **E-mail - Def SCM** para exibir a definição relacionada a este exemplo.

Tradução automática

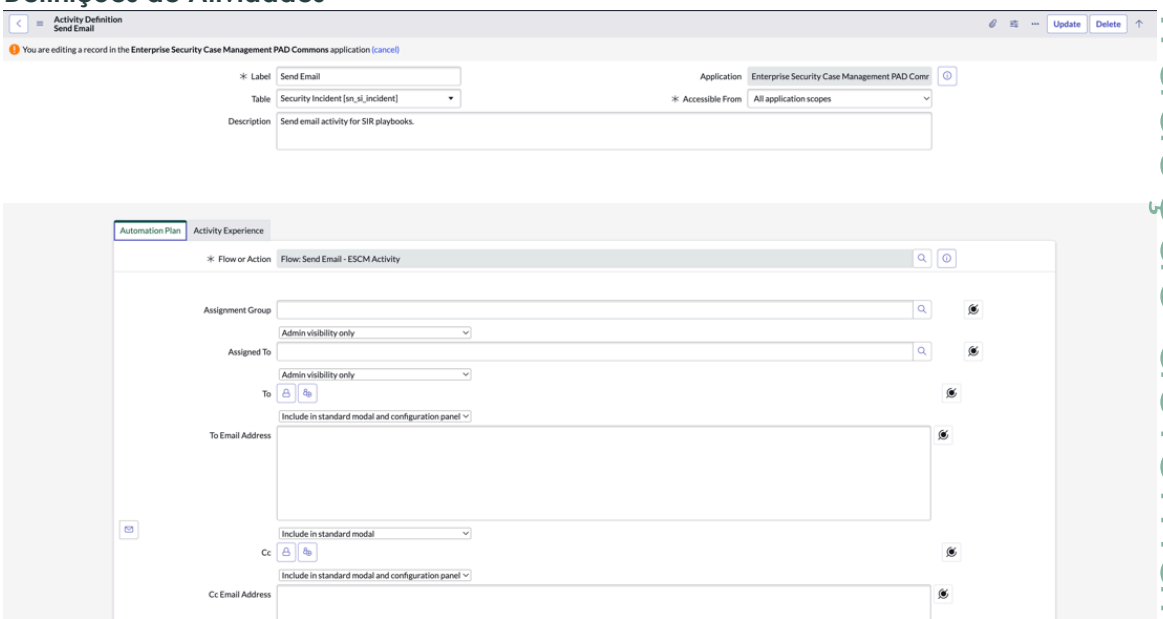
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

E-mail - Definição de SCM



Esta definição de dados de fluxo deve ser usada pelo subfluxo ou pela ação que está associada a esta definição de atividade (plano de automação de referência) para capturar os dados de tempo de execução.

Definições de Atividades



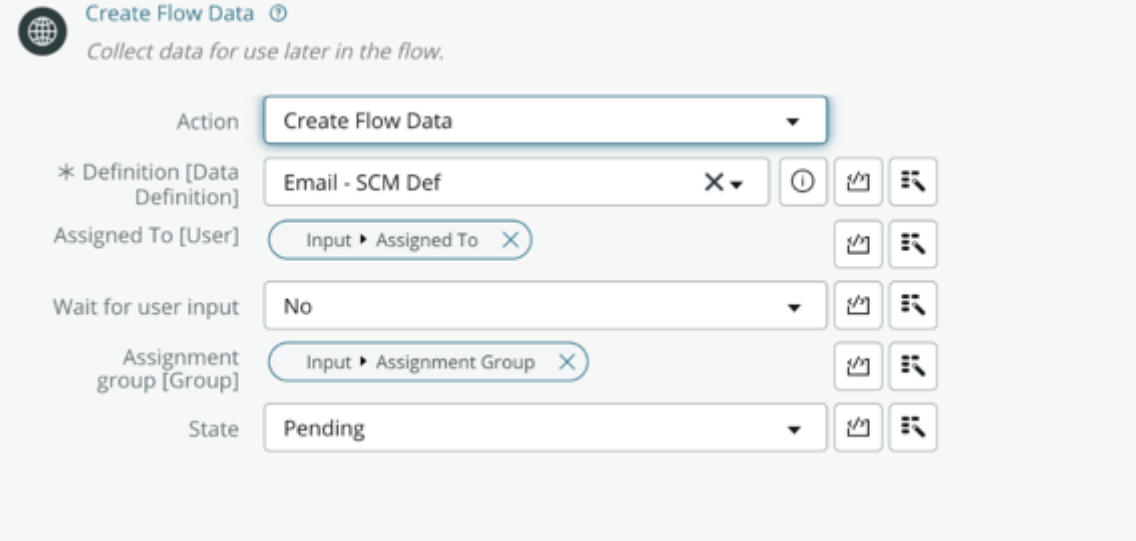
3. Neste exemplo, abra o subfluxo: **Enviar e-mail - Atividade ESCM**. Na etapa **Criar dados de fluxo**, a definição de dados de fluxo que você criou é mapeada em relação ao campo **Definição**. Este registro de dados de fluxo é usado em todo o subfluxo. Neste exemplo, o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

status do cartão de atividade (status de experiência) é capturado na tabela de dados de fluxo.

Enviar e-mail - Atividade ESCM



Nota: Se você quiser capturar os dados de tempo de execução em um registro de tabela diferente que não seja a tabela de dados de fluxo, digamos, por exemplo, em uma tarefa de resposta. Você pode selecionar a tabela associada como tabela de tarefa de resposta. O registro associado deve ser definido como o registro de tarefa de resposta criado pelo subfluxo.

Da mesma forma, a tabela de status de experiência captura o status do cartão de atividade. No sistema base, o campo de estado da tabela de dados de fluxo é mapeado para o status do cartão de atividade. Portanto, quando a tabela de dados de fluxo é usada para capturar o status da experiência, ela atualiza automaticamente o status do cartão de atividade. Você também pode usar uma tabela diferente da tabela de dados de fluxo para capturar o status da experiência.

Por exemplo, se você quiser mapear o status da tarefa de resposta para o status do cartão de atividade, isso será possível. Para fazer isso:

1. Navegar até **Todos** > **Playbook Experiences**.

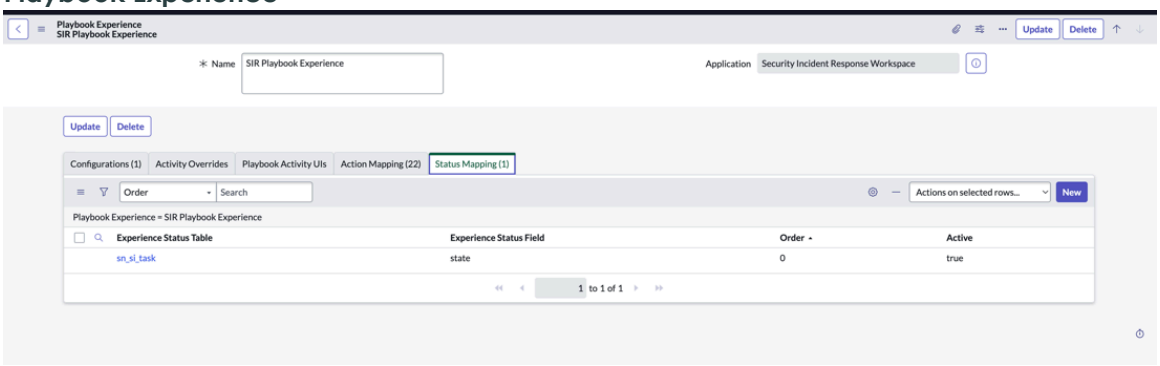
Playbook Experiences

2. Abra **a Playbook Experience de SIR**.
3. Abra a lista relacionada **Mapeamento de status**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook Experience

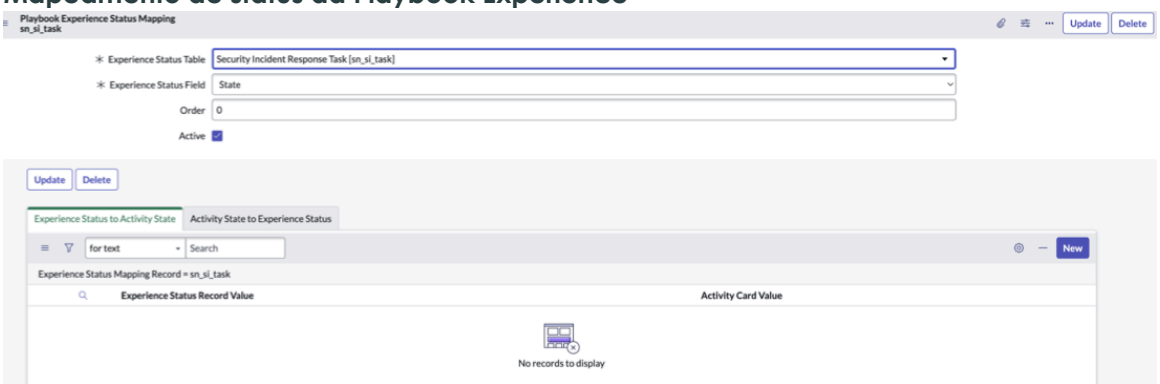


4. Insira o campo **Tarefa de resposta** em relação à tabela de status de experiência.
5. Insira o campo **Estado em** relação ao Status da experiência.

Status da experiência

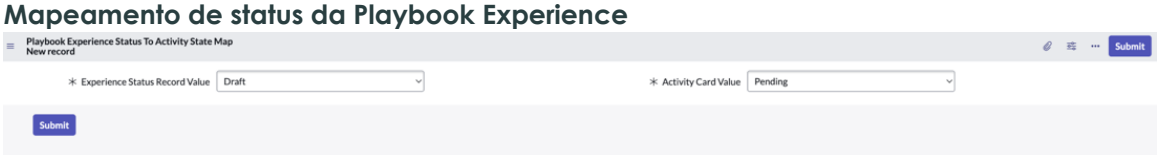
6. Clique em **Enviar**. O registro foi criado.

Mapeamento de status da Playbook Experience



7. Em Status de experiência para estado de atividade, mapeie os estados da tarefa de resposta para o status do cartão de atividade.
8. O lado esquerdo mostra os estados da Tarefa de resposta e o lado direito mostra o status do cartão de atividade.

Mapeamento de status da Playbook Experience



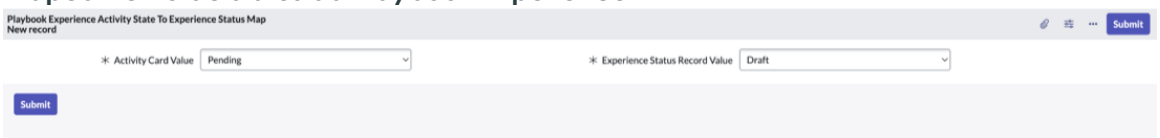
9. O mapeamento pode ser bidirecional. Na lista relacionada Estado da atividade para experiência também, mapeie os status corretamente. Esta etapa é o inverso da etapa

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

anterior. Nesse caso, o lado esquerdo mostra o status do cartão de atividade e o lado direito mostra o status da tarefa de resposta.

Mapeamento de status da Playbook Experience



Detalhes

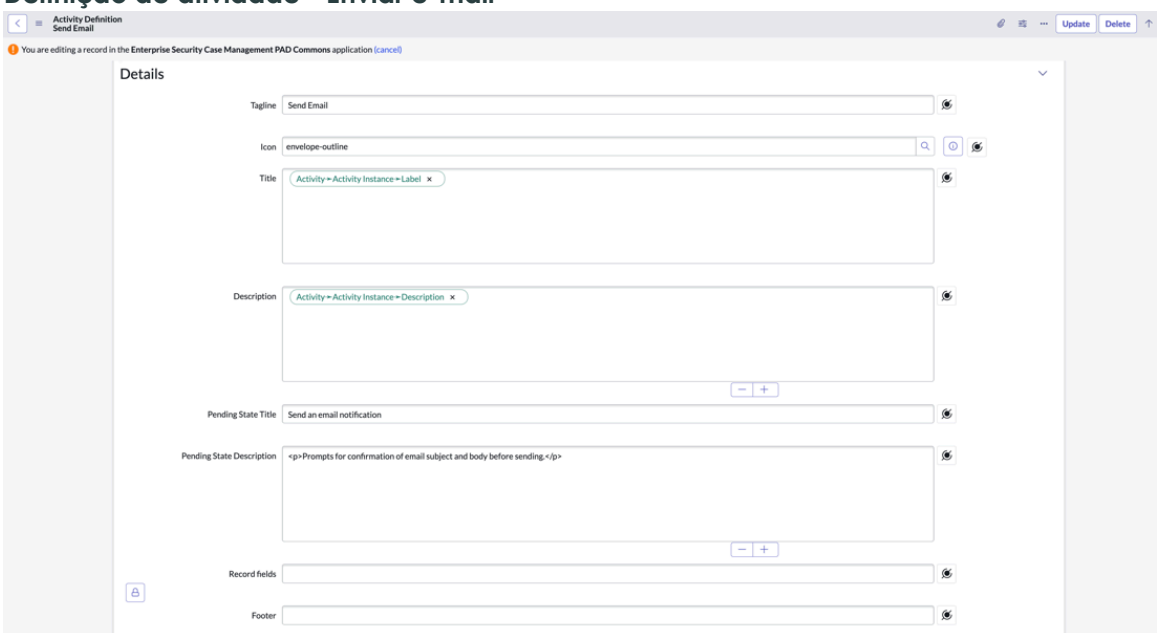
- Slogan: Enviar e-mail
- Ícone: contorno de envelope (não mostrado na interface do usuário)
- Título: **Atividade** > **Instância de atividade** > **Rótulo**. Aqui, selecionamos o rótulo da instância de atividade. Esta referência com pontos substituirá o valor do rótulo como o título dinamicamente em tempo de execução.
- Descrição: **Atividade** > **Instância de atividade** > **Descrição**. Aqui, selecionamos a descrição da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como o título dinamicamente em tempo de execução.
- Título do estado pendente: envie uma notificação por e-mail. Este é o título quando a atividade está no status Pendente.
- Descrição do estado pendente: solicita a confirmação do assunto e do corpo do e-mail antes do envio. Esta é a descrição do cartão de atividade quando o status é pendente Campos de registro: há campos de registro selecionados neste exemplo.

  Campos de registro são listas separadas por vírgulas de nomes de campos a serem exibidos para o registro associado em uma lista de pares de nome-valor. Os dados são pré-buscados no servidor, a referência com pontos é compatível e as permissões **canRead()**são avaliadas em cada campo.

- Rodapé: não há rodapé definido para este exemplo.

  Rodapé é um texto em uma área cinza do rodapé do cartão. Você pode adicionar qualquer informação significativa ao mostrado.

Definição de atividade - Enviar e-mail



Tradução automática

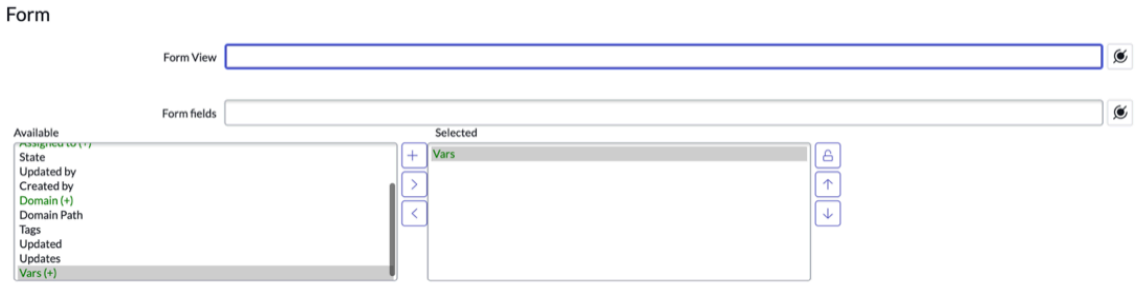
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário

- Exibição de formulário: collect_data
- Campos de formulário:

Este exemplo usa a exibição collect_data para mostrar os campos que devem ser apresentados ao usuário para inserir entradas. A exibição Collect_data é uma exibição fornecida pela plataforma que corresponde à tabela de dados de fluxo. Como alternativa, você pode deixar a Exibição de formulário em branco e selecionar Variáveis na lista de valores disponíveis em Campos de formulário. (clique no ícone de cadeado para abrir a lista de valores disponíveis).

Exibição de formulário



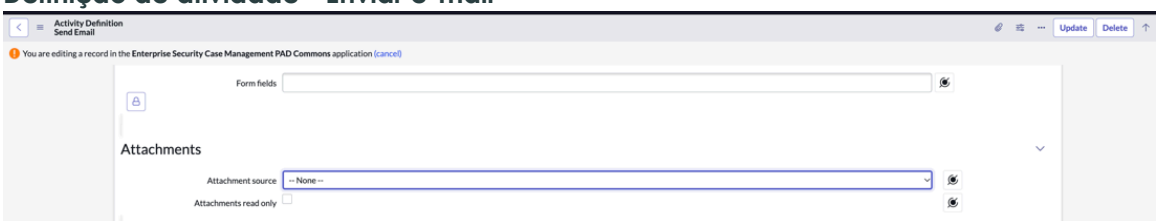
Anexos

Neste exemplo:

- A origem do anexo está vazia.
- Anexo somente leitura não selecionado.

1. Origem do anexo - Menu suspenso. Quais anexos serão mostrados no cartão: aqueles anexados ao registro primário, ao registro associado ou a nenhum.
2. Anexo Somente leitura - Verdadeiro ou Falso. Evite que o usuário renomeie ou exclua os anexos existentes.

Definição de atividade - Enviar e-mail



Recursos

Neste exemplo,

- Mostrar ANS - Limpo
- Mostrar check-list - Limpo
- É automatizado - Limpo

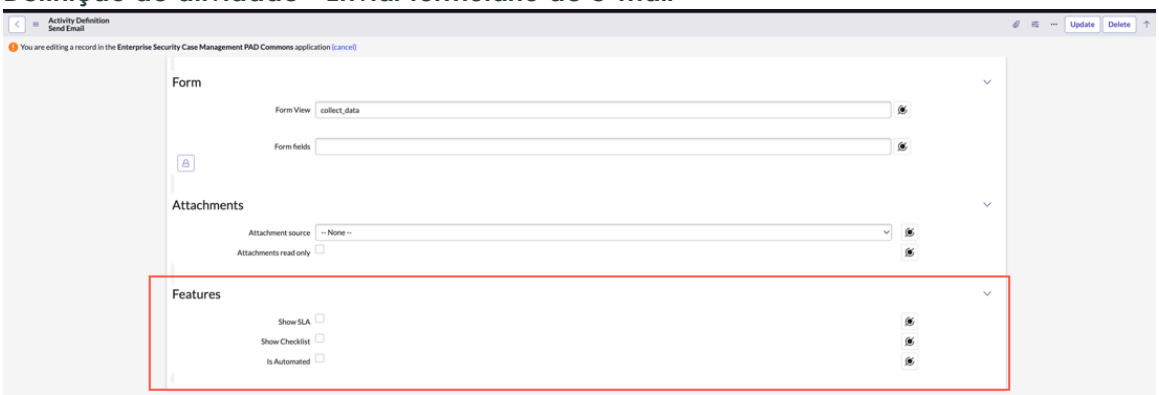
Mostrar ANS: verdadeiro/falso. Renderiza um temporizador de ANS no cabeçalho do cartão para o registro associado. O ANS é escolhido de acordo com o registro de configuração de ANS especificado na configuração do Playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Mostrar check-list - verdadeiro ou falso. Renderiza qualquer check-list anexada ao registro associado. A check-list é editável e as mudanças são salvas sem exigir uma ação declarativa.
2. É automatizado - Verdadeiro ou Falso. Se verdadeiro, o **slogan**e o **ícone**serão substituídos pelo texto **Tarefa automatizada** e um ícone automatizado.

Definição de atividade - Enviar formulário de e-mail

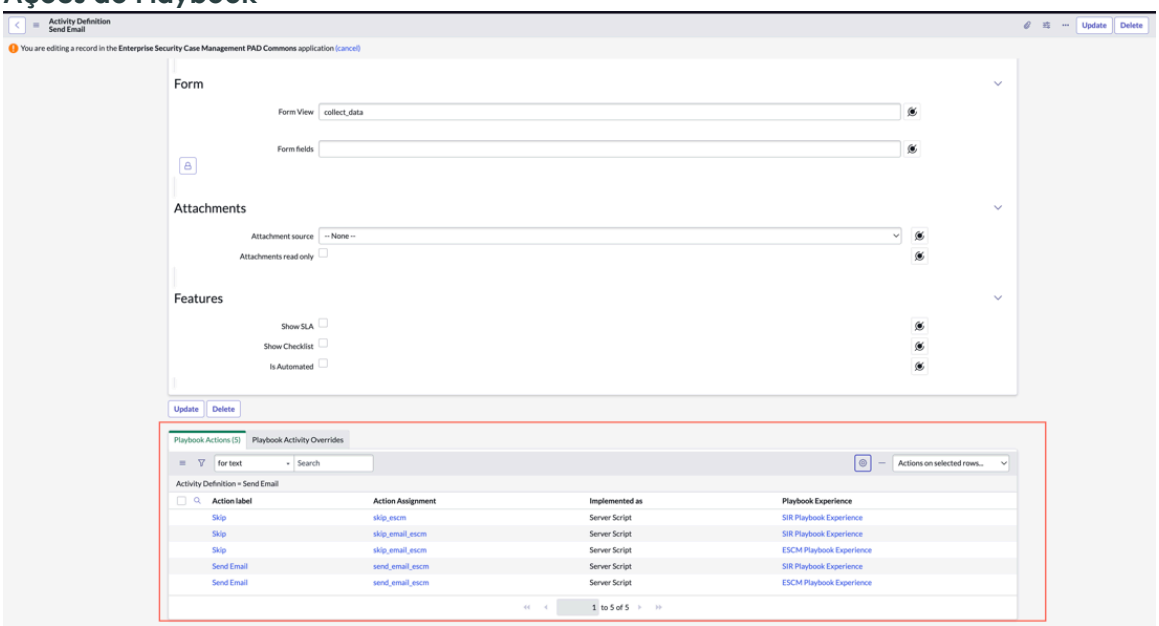


Ações do playbook na definição de atividade

Esta seção tem as ações que serão renderizadas no cartão de atividade. Este exemplo tem as ações **Ignorar**e **Enviar e-mail**.

Para adicionar uma nova ação ao cartão de atividade, você deve criar um registro na lista relacionada **Ações do Playbook**, presente na parte inferior da página.

Ações do Playbook



1. Clique em **Nova**.
2. Selecione a ação de atividade existente no campo Atribuição de ação.
3. Selecione a **Playbook Experience SIR** no campo Playbook Experience.

Criar uma Ação de Atividade

A seguir está o procedimento para criar uma ação de atividade.

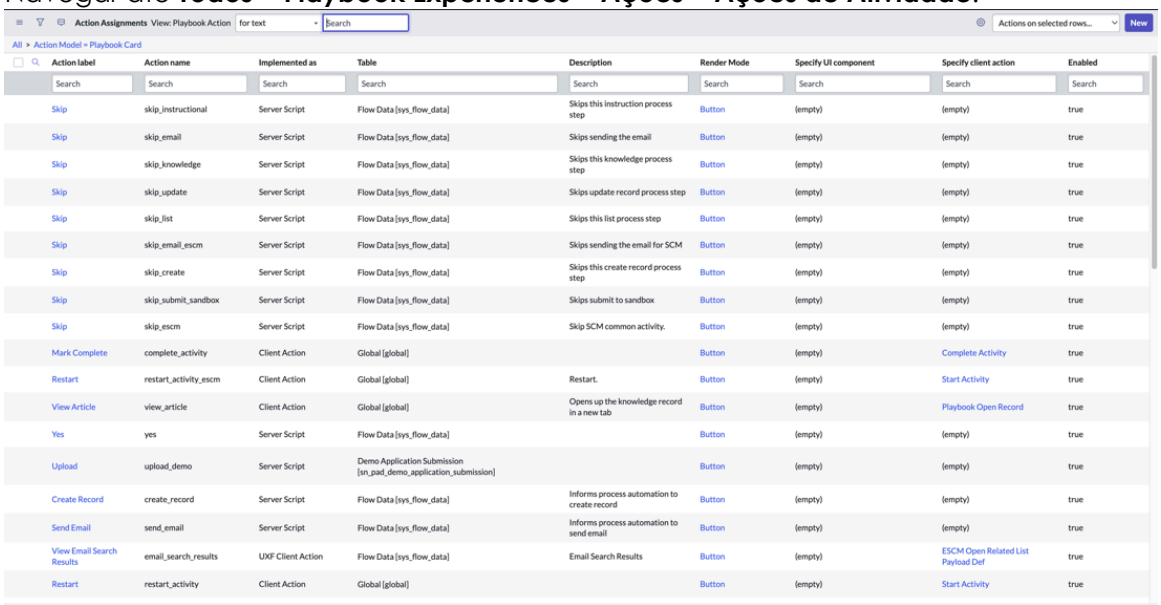
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Playbook Experiences** > **Ações** > **Ações de Atividade**.



Action Assignments View: Playbook Action | for text | Search | Actions on selected rows... | New

All > Action Model = Playbook Card

Action label	Action name	Implemented as	Table	Description	Render Mode	Specify UI component	Specify client action	Enabled
Search	Search	Search	Search	Search	Search	Search	Search	Search
Skip	skip_instructional	Server Script	Flow Data [sys_flow_data]	Skips this instruction process step	Button	(empty)	(empty)	true
Skip	skip_email	Server Script	Flow Data [sys_flow_data]	Skips sending the email	Button	(empty)	(empty)	true
Skip	skip_knowledge	Server Script	Flow Data [sys_flow_data]	Skips this knowledge process step	Button	(empty)	(empty)	true
Skip	skip_update	Server Script	Flow Data [sys_flow_data]	Skips update record process step	Button	(empty)	(empty)	true
Skip	skip_list	Server Script	Flow Data [sys_flow_data]	Skips this list process step	Button	(empty)	(empty)	true
Skip	skip_email_escm	Server Script	Flow Data [sys_flow_data]	Skips sending the email for SCM	Button	(empty)	(empty)	true
Skip	skip_create	Server Script	Flow Data [sys_flow_data]	Skips this create record process step	Button	(empty)	(empty)	true
Skip	skip_submit_sandbox	Server Script	Flow Data [sys_flow_data]	Skips submit to sandbox	Button	(empty)	(empty)	true
Skip	skip_escm	Server Script	Flow Data [sys_flow_data]	Skip SCM common activity.	Button	(empty)	(empty)	true
Mark Complete	complete_activity	Client Action	Global [global]		Button	(empty)	Complete Activity	true
Restart	restart_activity_escm	Client Action	Global [global]	Restart.	Button	(empty)	Start Activity	true
View Article	view_article	Client Action	Global [global]	Opens up the knowledge record in a new tab	Button	(empty)	Playbook Open Record	true
Yes	yes	Server Script	Flow Data [sys_flow_data]		Button	(empty)	(empty)	true
Upload	upload_demo	Server Script	Demo Application Submission [sn_pad_demo_application_submission]		Button	(empty)	(empty)	true
Create Record	create_record	Server Script	Flow Data [sys_flow_data]	Informs process automation to create record	Button	(empty)	(empty)	true
Send Email	send_email	Server Script	Flow Data [sys_flow_data]	Informs process automation to send email	Button	(empty)	(empty)	true
View Email Search Results	email_search_results	UXF Client Action	Flow Data [sys_flow_data]	Email Search Results	Button	(empty)	ESCM Open Related List Payload Def	true
Restart	restart_activity	Client Action	Global [global]		Button	(empty)	Start Activity	true

2. Clique em **Nova**.

   Consulte a documentação da Now Platform para saber como criar essas ações. Neste exemplo, Ignorar é implementado como um script de servidor.

3. **Substituição de playbook:**

   Se você quiser substituir o tipo de experiência de atividade existente, é possível. Para obter mais informações, consulte a documentação da Now Platform. Não há substituições de Playbook para este exemplo.

Enviar para área restrita FCS X

Enviar para área restrita do FCS X é um exemplo de um processo de definição de atividade.

Básico

Os detalhes básicos capturam o nome (rótulo), aplicação, descrição, tabela e a partir do qual todas as aplicações podem ser acessadas.

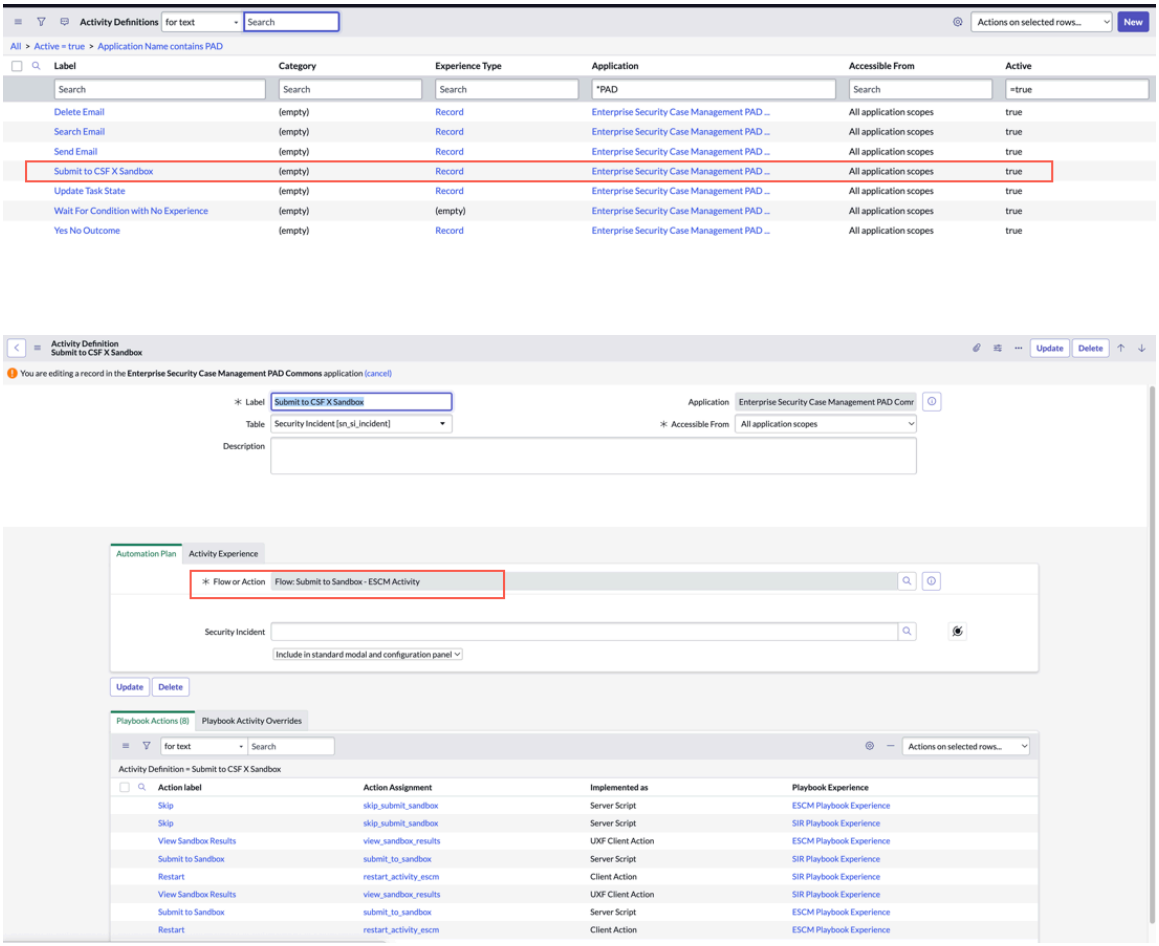
Adicione o plano de automação, a experiência de atividade e envie. Depois de enviado, edite o documento para adicionar mais detalhes em relação a cada guia.

Plano de Automação

O plano de automação associa a ação de back-end/subfluxo criado usando o Flow Designer. Este exemplo usa **o subfluxo Enviar para área restrita - Atividade ESCM**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este subfluxo permite o envio de observáveis mal-intencionados para a área restrita. Ele tem todos os campos de entrada e de saída definidos.

Incidente de segurança é o campo de entrada.

Experiência de Atividade

Neste exemplo, o tipo de **registro** está selecionado.

Registro Associado

O registro associado serve para armazenar os dados associados pertencentes à atividade atual. Isso capturaria os dados de tempo de execução, bem como o status da experiência.

- Tabela associada: dados de fluxo
- Registro associado: VL
- Tabela de status da experiência: dados de fluxo
- Registro de status da experiência: VL

Detalhes

- Slogan: Enviar e-mail
- Ícone: contorno de envelope
- Título: **Atividade** > **Instância de atividade** > **Rótulo**. Aqui, selecionamos o rótulo da instância de atividade. Esta referência com pontos substituirá o valor do rótulo como o título dinamicamente no tempo de execução.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Descrição: VL (a saída do subfluxo está mapeada)
- Título do estado pendente: em branco
- Descrição do estado pendente: em branco
- Campos do Registro
- Rodapé

Formulário

- Exibição de formulário: em branco
- Campos de formulário: em branco

Anexos

Neste exemplo:

- Origem do anexo - Nenhum
- Anexo Somente leitura - Desmarcado

1. Origem do anexo - este é um menu suspenso. Quais anexos serão mostrados no cartão: aqueles anexados ao registro primário, ao registro associado ou a nenhum.
2. Anexo Somente leitura - Verdadeiro/Falso. Evite que o usuário renomeie ou exclua os anexos existentes.

Recursos

Neste exemplo,

- Mostrar ANS - Desmarcado
- Mostrar check-list - Desmarcado
- É automatizado - Desmarcado

Ações do playbook na definição de atividade

Esta seção tem as ações que serão renderizadas no cartão de atividade.

Este exemplo tem as ações Ignorar, Exibir resultados da área restrita, Enviar para área restrita e Reiniciar.

Para adicionar uma nova ação ao cartão de atividade, você precisa criar um novo registro na lista relacionada Ações do Playbook, presente na parte inferior da página.

Substituição de playbook

Não há substituições de Playbook para este exemplo.

Playbooks de amostra para o espaço SIR

Você pode criar ou configurar playbooks para o Espaço SIR de forma rápida e fácil sem escrever códigos complicados. Você pode usar esses playbooks para resolver ameaças à segurança passo a passo. Você pode invocar o fluxo do playbook de incidente de segurança automaticamente ou manualmente.

O Security Incident Response fornece os seguintes playbooks com o sistema de base:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Playbook para phishing manual
- Playbook for Automated Phishing
- Playbook para malware manual
- Playbook para malware automatizado
- Playbook para login manual com falha

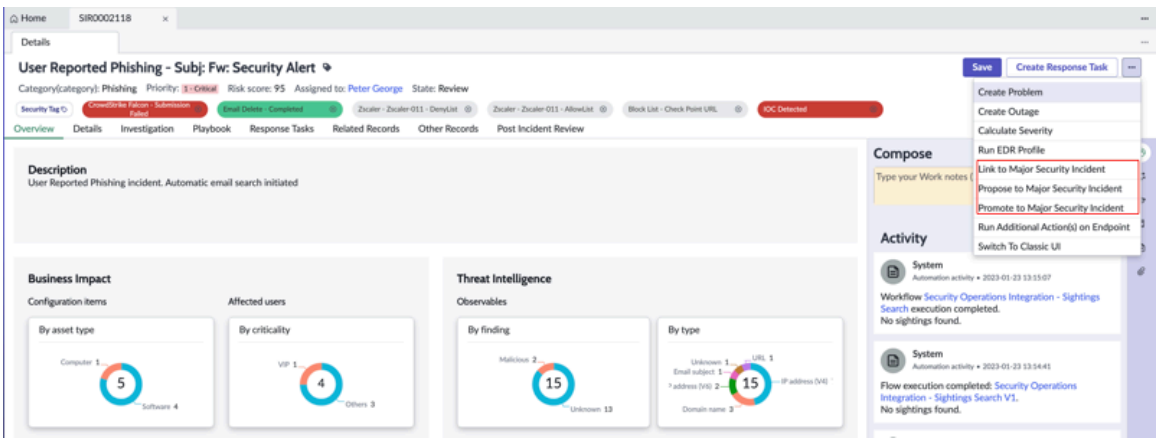
Trabalhando com Registros MSI

Usando o espaço do Security Incident Response, você pode propor, promover ou vincular incidentes de segurança como incidentes de segurança graves quando os incidentes são identificados como ameaças críticas à organização.

Depois de instalar Gestão de incidentes graves de segurança (MSIM) em sua instância Now Platform, você pode lidar com a transição de incidentes de segurança para incidentes graves.

As ações de IU Gestão de incidentes graves de segurança (MSIM) são exibidas no canto superior direito da faixa do formulário de incidente de segurança do espaço SIR. Selecione a ação de IU conforme aplicável.

Nota: Algumas ações são contextuais. Por exemplo, a ação Desvincular está disponível somente quando o incidente de segurança já foi proposto, promovido ou vinculado a um incidente de segurança grave.



Propor como incidente de segurança grave

Proponha um incidente de segurança como um incidente de segurança grave (MSI).

Antes de Iniciar

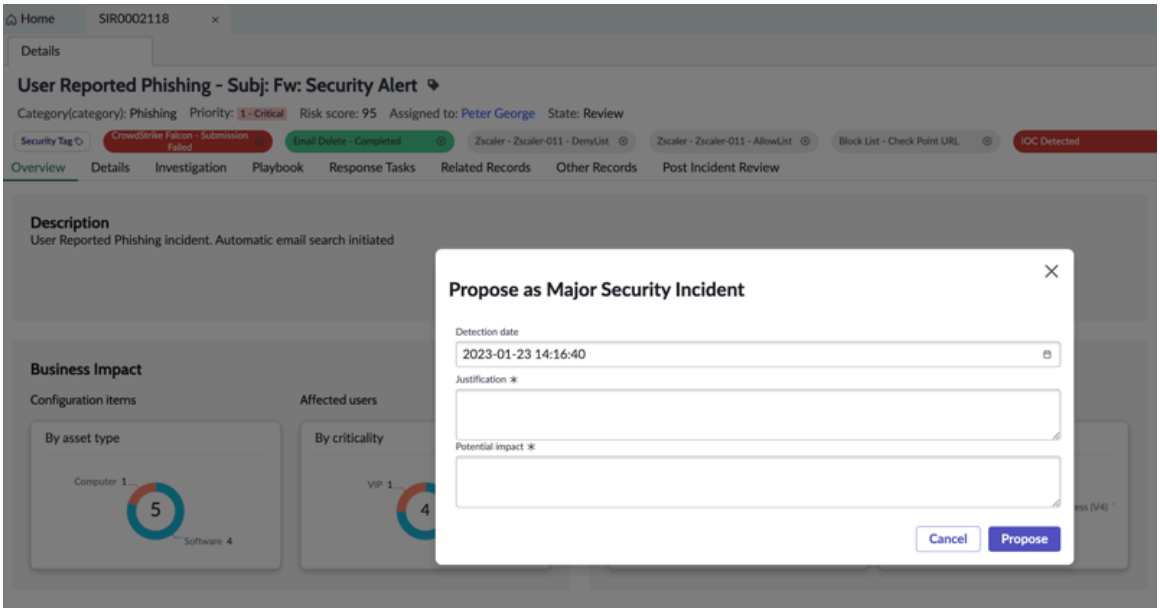
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique **em Propor para incidente de segurança grave**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos como Data de detecção, Justificativa e Impacto potencial.
5. Clique **em Propor**.
   O registro de incidente é proposto como um candidato a incidente de segurança grave. Depois que o registro de incidente é proposto como um candidato a incidente de segurança grave, o marcador **Candidato** a incidente de segurança grave é aplicado e exibido na faixa do formulário de incidente de segurança.

> **Nota:** Clique **em Desvincular do incidente de segurança grave** para desvincular o incidente se você não quiser propor ou não tiver nenhum impacto crítico. O incidente será desvinculado e listado na exibição de lista para o analista de segurança para correção.

Promover a incidente de segurança grave

Promova um incidente de segurança a incidente de segurança grave.

Antes de Iniciar

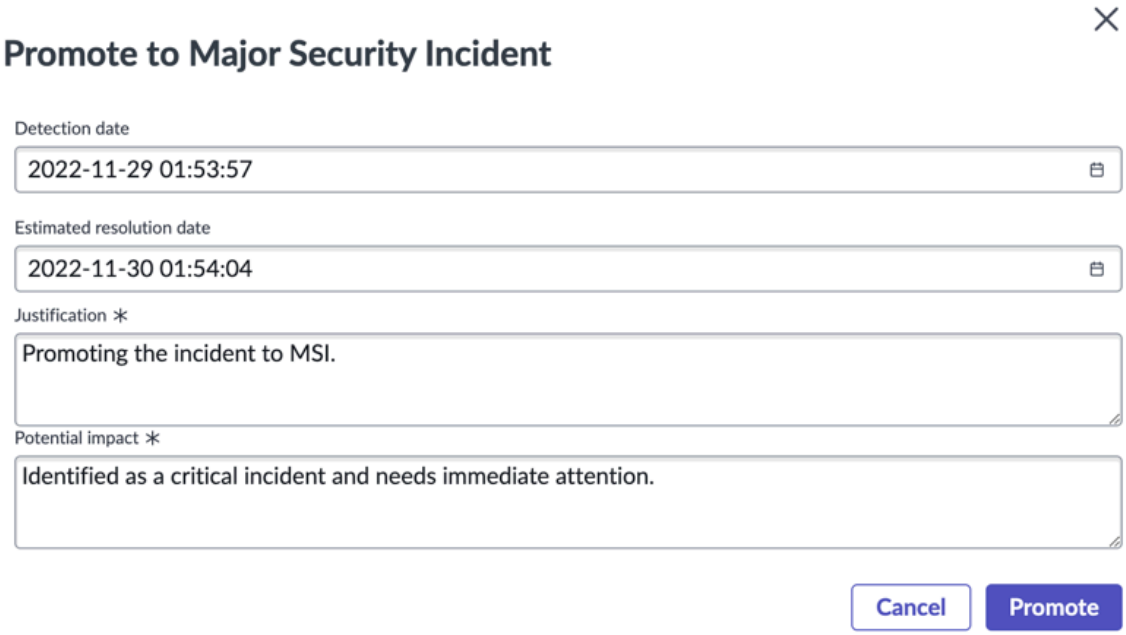
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique **em Promover a incidente de segurança grave**.
4. No formulário, preencha os campos como Data de detecção, Data de resolução estimada, Justificativa e Impacto potencial.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique **em Promover**.
   O registro de incidente é promovido como um incidente de segurança grave.
   Depois que o registro de incidente é promovido como um incidente de segurança grave, o marcador **de incidente** de segurança grave é aplicado e exibido na faixa do formulário.

> **Nota:** Você também pode desvincular o incidente de segurança grave se o incidente não for crítico. O incidente será desvinculado e listado na exibição de lista para correção do analista de segurança.

Link para o incidente de segurança grave

Vincule um incidente de segurança a um incidente de segurança grave como incidente(s) de segurança secundário(s).

Antes de Iniciar

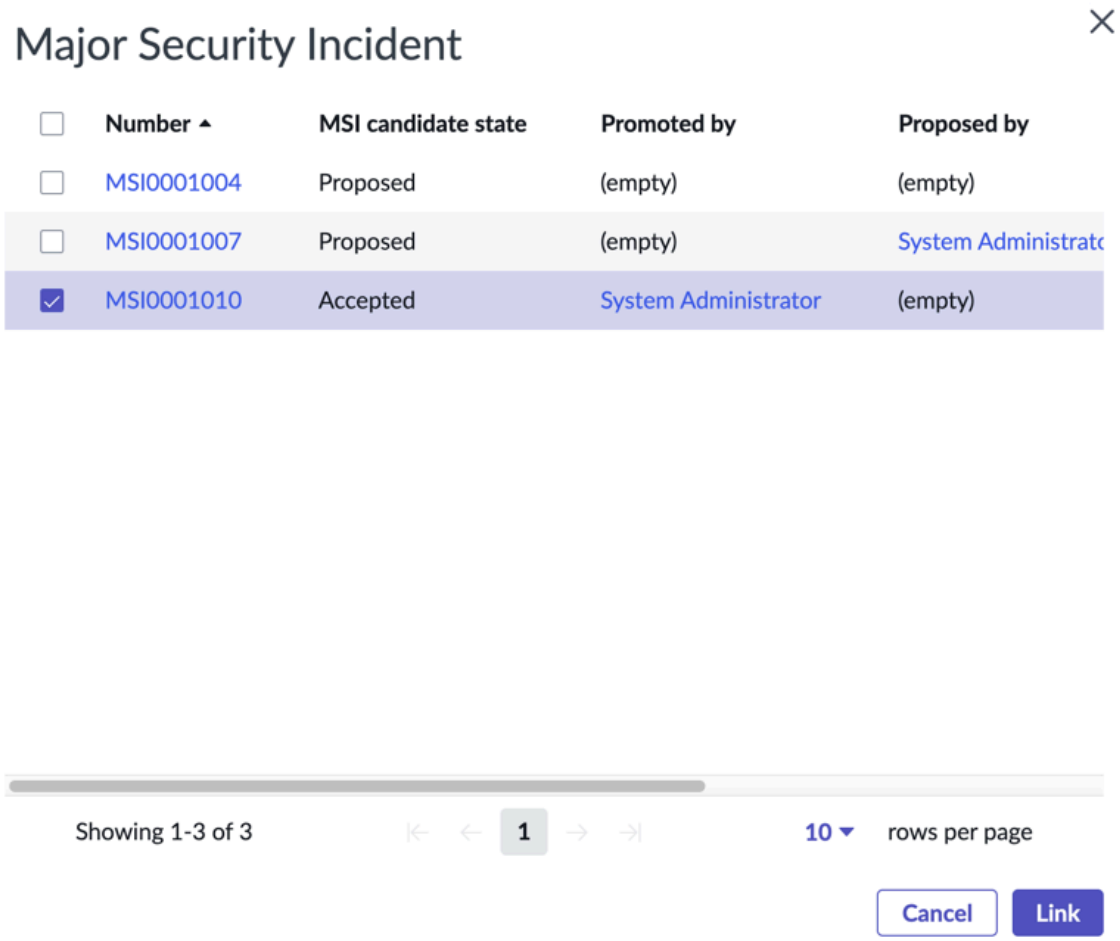
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique **em Vincular ao incidente de segurança grave**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione os incidentes a serem vinculados a um incidente de segurança grave.
5. Clique em **Vincular**.
6. O registro de incidente está vinculado como um incidente secundário do incidente de segurança grave.
   Depois que o incidente é vinculado como um incidente secundário a um incidente de segurança grave, o marcador de **incidente** de segurança grave é aplicado e exibido na faixa do formulário.

Como trabalhar com ações de IU de formulário

A seguir estão as ações de IU que são exibidas no formulário de incidente de segurança.

Para navegar até o formulário Ações de IU:

1. Ir para **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione qualquer incidente de segurança na exibição de lista.
3. Todas as ações de IU estão presentes no canto superior direito do formulário de incidente de segurança.

Ações de IU de formulário do espaço

Nome do Campo	Descrição
Discutir	Crie ou inicie uma discussão na barra lateral para o incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
Salvar	Salve ou atualize o registro do Security Incident Response após fazer qualquer mudança.
Criar Tarefa de Resposta	Crie uma tarefa de resposta para o incidente de segurança.
Compor e-mails	Escreva e-mails para o incidente de segurança.
Adicionar Playbook	Adicione o playbook manualmente para o incidente de segurança.
Criar incidente	Crie um incidente dentro do incidente de segurança.
Criar caso de Atendimento ao cliente	Crie um caso de atendimento ao cliente para o incidente de segurança que será rastreado pela equipe de Customer Service Management (CSM). **Nota:** Esta opção está disponível somente quando o Customer Service Management (CSM) está instalado.
Abrir Fluxo(s) de Trabalho Associado(s)	Abra qualquer contexto de fluxo de trabalho associado ao incidente de segurança. Esta opção ficará visível somente se houver fluxos de trabalho.
Criar solicitação de mudança	Crie uma solicitação de mudança no incidente de segurança.
Criar problema	Crie um problema no incidente de segurança.
Criar indisponibilidade	Crie uma indisponibilidade no incidente de segurança.
Calcular Gravidade	Calcule a gravidade de um incidente de segurança usando calculadoras predefinidas. A severidade é calculada com base nas regras predefinidas nas calculadoras. A gravidade de um incidente é baseada na pontuação de risco, no impacto nos negócios e na prioridade.
Executar perfil de EDR	Selecione e execute o perfil de EDR para a integração necessária. **Nota:** Esta opção está disponível somente quando integrações estão instaladas.
Link para o incidente de segurança grave	Vincule um incidente de segurança a um incidente de segurança grave.
Relatar evento de risco	Relate este incidente de segurança como um evento de risco para a equipe de gestão de riscos. A equipe de gestão de riscos analisa o evento e garante que esses eventos e as perdas associadas não ocorram novamente. **Nota:** Esta opção está disponível somente quando a Gestão de riscos está instalada.
Desvincular de um incidente de segurança grave	Desvincular do incidente de segurança grave.

Tradução automática

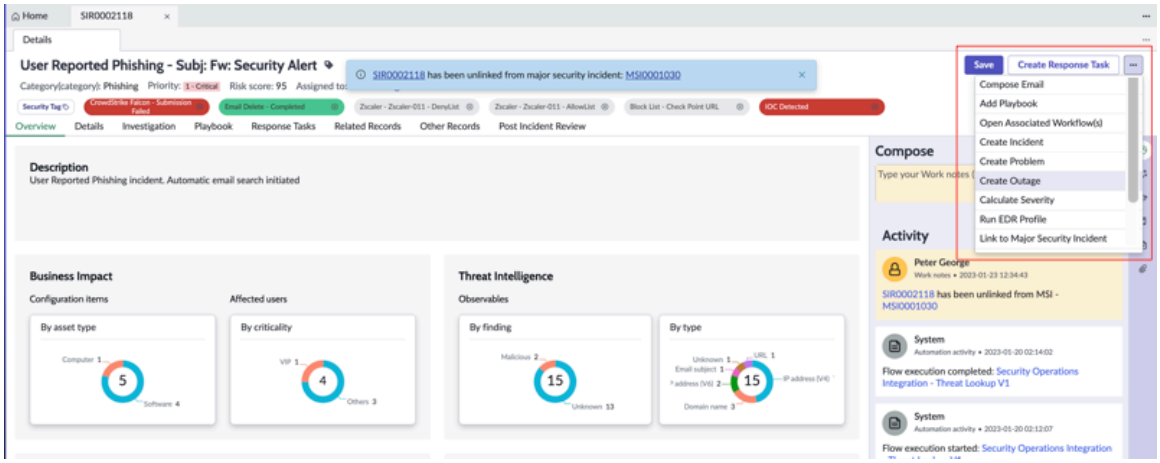
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
Propor como incidente de segurança grave	Propor um incidente de segurança como um incidente de segurança grave.
Promover a incidente de segurança grave	Promova um incidente de segurança como um incidente de segurança grave.
Executar ações adicionais no endpoint	Execute ações adicionais no endpoint. **Nota:** Esta opção está disponível somente quando as integrações de endpoint estão instaladas. Por exemplo: FireEye HX
Criar um novo evento no MISP	Crie e modifique eventos no MISP automaticamente ou manualmente. **Nota:** Esta opção está disponível somente quando a integração MISP está instalada.
Associar técnica do MITRE ATT&K	Associe as técnicas do MITRE ATT&K ao incidente de segurança. **Nota:** Esta opção está disponível quando o MITRE ATT&K está instalado.
Mostrar informações do MITRE ATT&K	Mostra as informações do MITRE ATT&K associadas ao incidente de segurança. **Nota:** Esta opção está disponível quando o MITRE ATT&K está instalado.
Adicionar ao Caso de Segurança	Adicione o incidente de segurança a um caso de segurança existente ou novo. **Nota:** Esta opção está disponível quando a Inteligência contra ameaças está instalada.
Alternar para a IU Clássica	Permita que o analista alterne entre a IU clássica e a nova para que o analista também possa trabalhar nas funcionalidades existentes que ainda não estão disponíveis no novo espaço.
Cancelar	Cancele um incidente de segurança. Depois de selecionar **Cancelar** todos os registros relacionados, como tarefas de resposta, os incidentes de segurança secundários também serão cancelados.
Excluir	Excluir um registro de incidente de segurança.

4. Clique no número de um incidente de segurança para exibir o registro do incidente de segurança. Você pode ver as ações de IU na parte superior da página.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Fluxo de trabalho de fechamento do incidente de segurança

Feche o incidente de segurança atualizando o estado do incidente.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

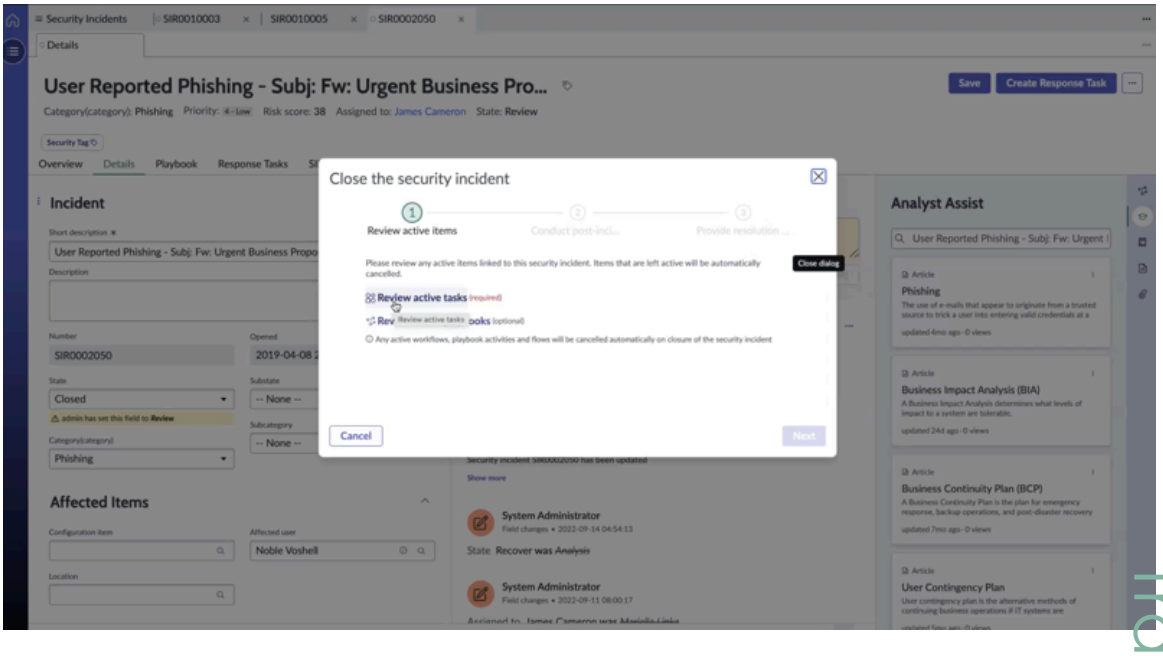
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Por exemplo, vá para **Listas** > **Incidentes de segurança** > **Incidentes abertos**.
3. Abra um incidente que você deseja fechar.
4. Vá para a guia **Detalhes**.
5. Faça o detalhamento ativo do estado do incidente e selecione **Fechar**.
6. Executar as atividades de encerramento.

   - Esta é uma etapa obrigatória para revisar qualquer tarefa antes de encerrar um incidente de segurança. Todas as tarefas de resposta devem ser revisadas pelo analista e encerradas ou canceladas antes de serem encerradas como incidente de segurança. Quando o analista clica em **Revisar tarefas ativas**, ele leva o usuário para a guia **Tarefas de resposta**. Uma mensagem de sessão é exibida avisando que você está no processo de fechar um incidente de segurança. Clique **em continuar**.
   - Clique em **"Continuar"**. A primeira etapa - revisar as tarefas ativas no encerramento do incidente de segurança - está concluída.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

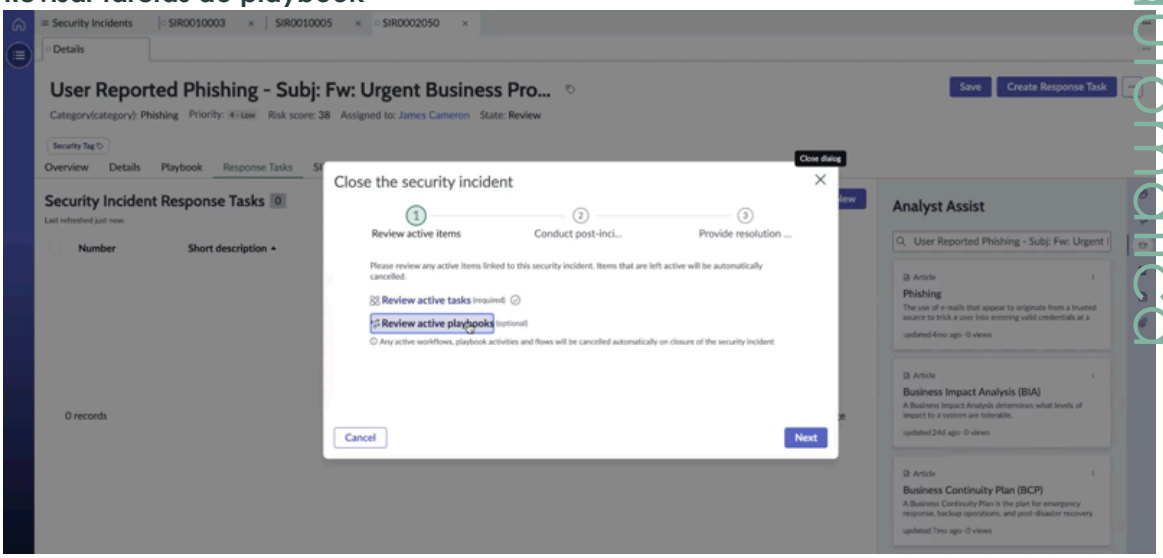
Revisando tarefas de fechamento



- Passe para a próxima etapa para revisar os playbooks ativos para o analista revisar, que é uma etapa opcional. Você pode clicar no link para revisar a tarefa do playbook ativa e fechá-la conforme necessário.

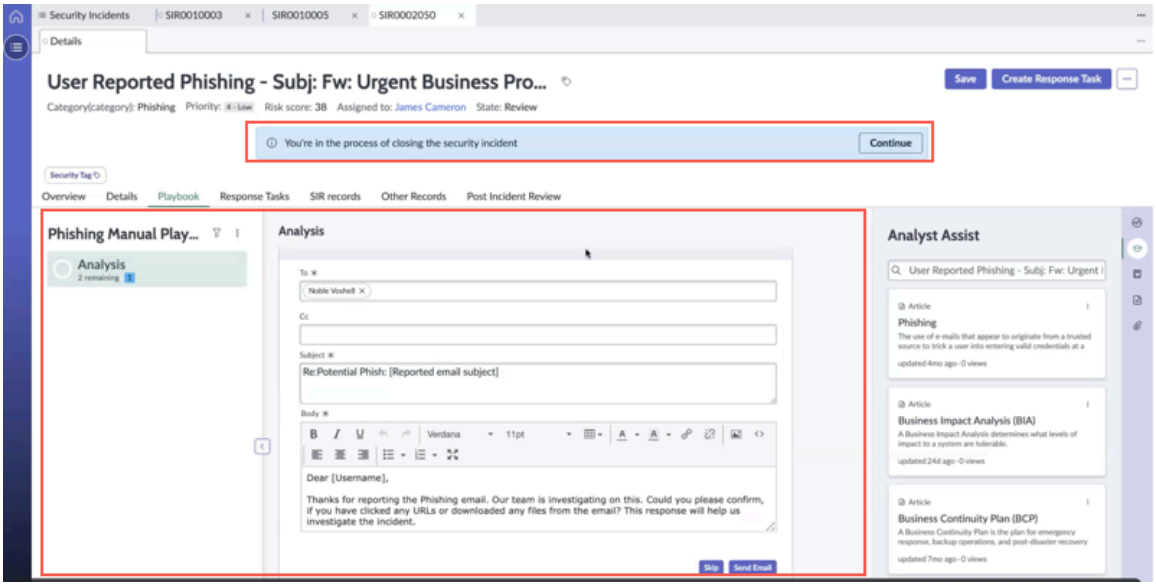
> **Nota:** Todos os fluxos de trabalho, atividades do playbook e fluxos ativos serão cancelados automaticamente no fechamento do incidente de segurança.

Revisar tarefas do playbook



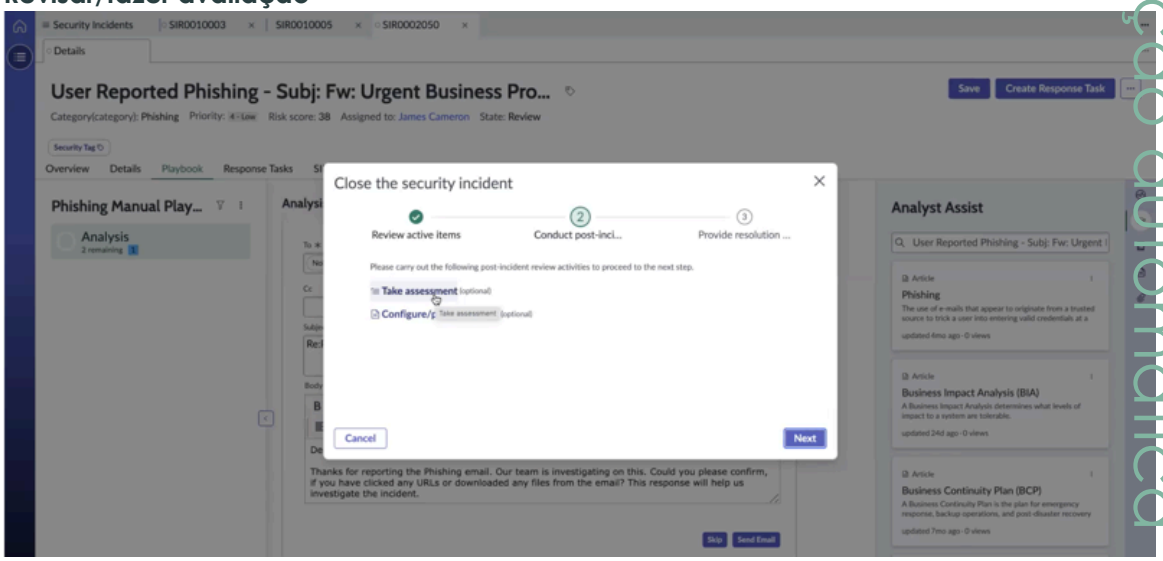
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



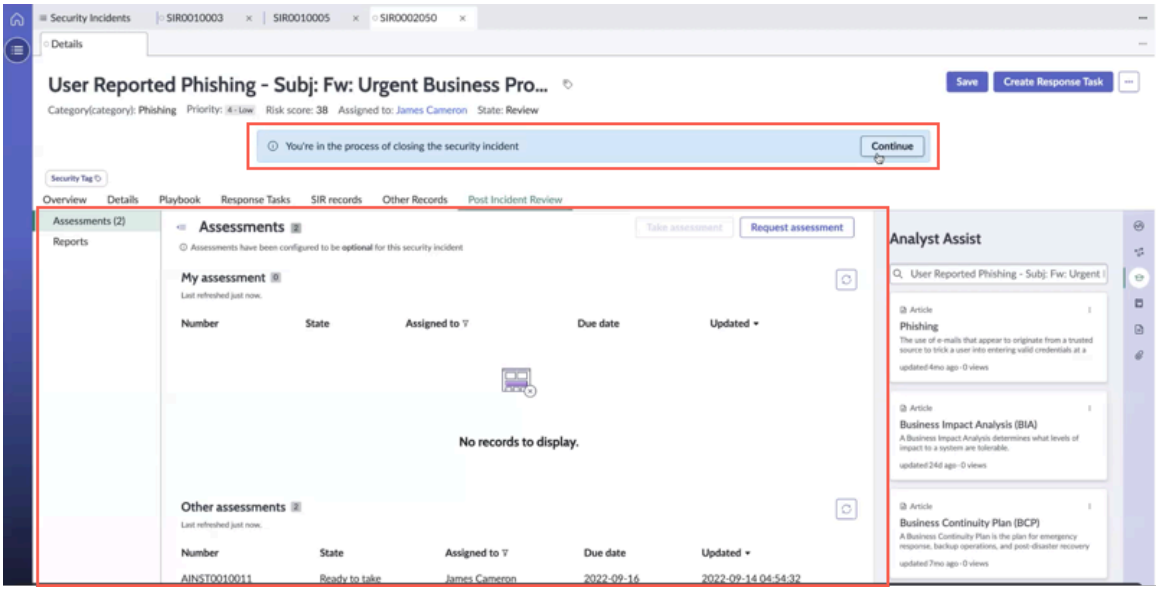
- Relatório de revisão pós-incidente: agora você será movido para revisar as atividades pós-incidente para prosseguir com o fechamento. Se a avaliação for opcional, pule a etapa ou, se for obrigatória, faça a avaliação e conclua-a.

Revisar/fazer avaliação

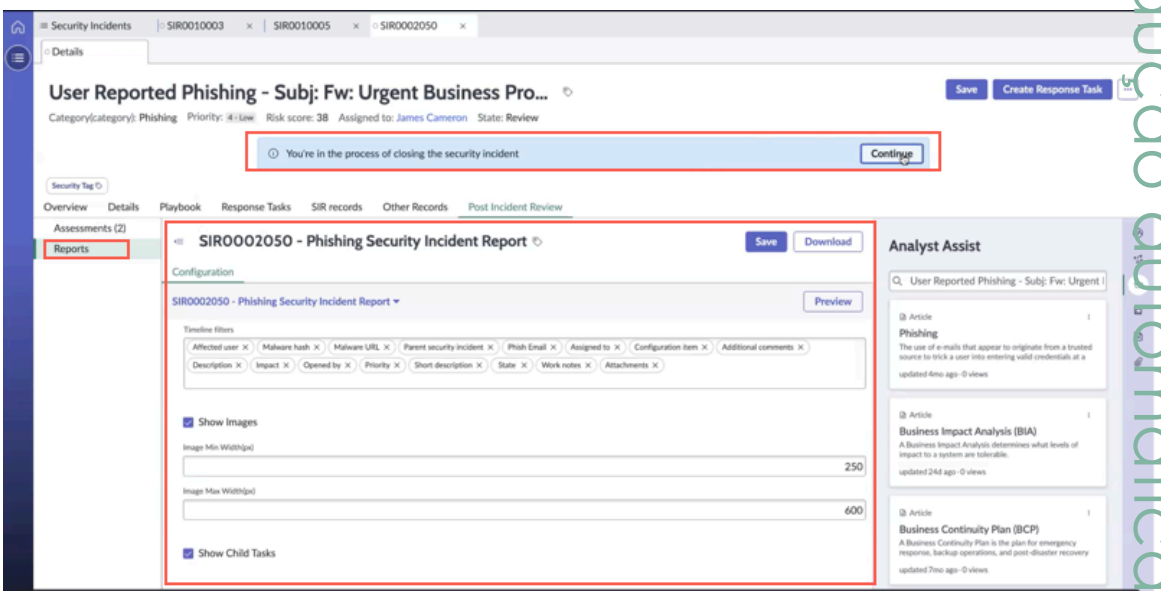


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



◦ Configurar/visualizar relatório: esta é novamente uma etapa opcional. Clique no link para revisar o relatório e prosseguir para a **Próxima** etapa.

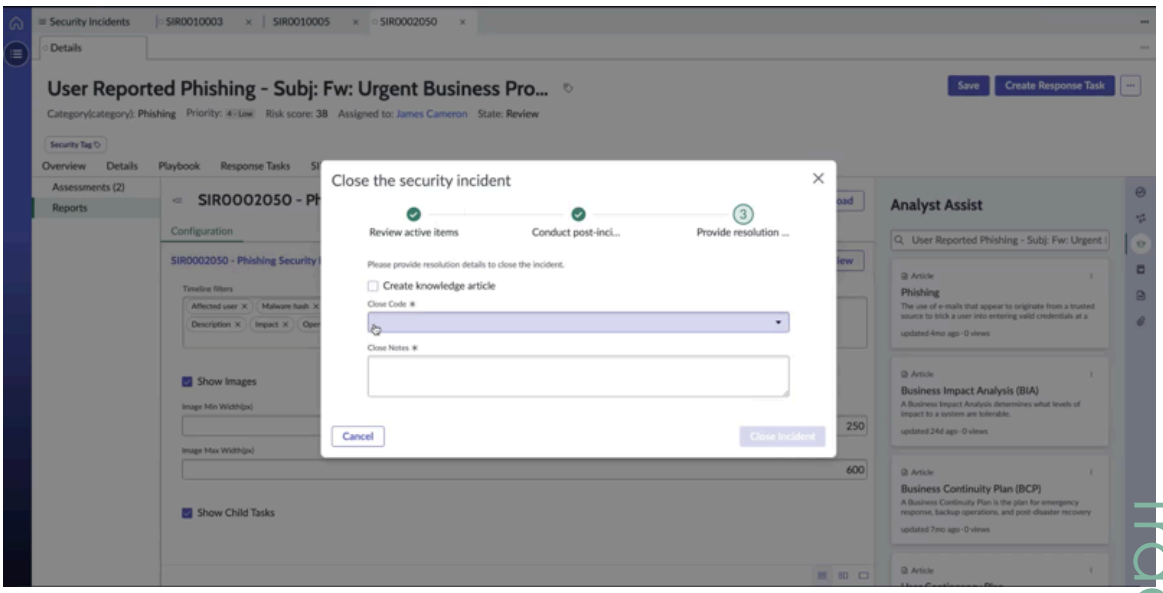


◦ Fornecer detalhes da resolução: o analista pode marcar a caixa de seleção para criar artigos de conhecimento automaticamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Forneça o Código de fechamento, Anotações de fechamento e clique em **Fechar incidente**.



Nota: Por qualquer chance, se o analista cancelar a caixa de diálogo **Fechar o incidente de segurança**, o analista poderá navegar até a guia **Detalhes** e mudar o estado do incidente para **fechar** para continuar com o fechamento.

Exibição de painéis do espaço de SIR

Esta seção apresenta as métricas importantes para analisar seu processo Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto.

Na IU clássica, há alguns painéis padrão disponíveis na página inicial e Performance Analytics Painéis que estão disponíveis quando o plug-in Performance Analytics para Security Incident Response está instalado. Tudo isso agora estará disponível no novo espaço na seção **Painéis SIR**.

Painéis padrão na página inicial:

- Visão geral do Security Incident Response
  - Visão geral do analista
  - Visão geral do gerente (com suporte em versões futuras)
  - Visão geral do CISO (com suporte em versões futuras)
- **Análise da plataforma para** *`Security Incident Response`*
  - Explorador de incidentes de segurança
  - Painel do CISO (versão futura)
  - Gestão de incidentes de segurança
  - KPIs de Gestão de incidentes de segurança premium
  - Eficiência das operações de segurança
  - Análise sensível ao contexto – Painel de SI

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Pode haver alguma repetição de painéis nas análises padrão e de plataforma para painéis de resposta a incidentes de segurança, como o Painel do CISO. Quando o plug-in estiver instalado, haverá conteúdo adicional nesses painéis e não estará disponível como duplicata.

Os usuários precisam instalar o plug-in para que os painéis listados em Análise da plataforma para painéis do Security Incident Response estejam presentes no espaço. Caso contrário, somente os painéis padrão estarão disponíveis.

Na versão atual do Espaço SIR, os seguintes painéis estão disponíveis na seção **Painéis SIR**. Os outros painéis ausentes estarão disponíveis em versões posteriores.

Painéis do Security Incident Response

Painel	Descrição
Painel padrão	
Visão Geral de Análise de Segurança	Com este painel, os analistas de segurança podem exibir incidentes de segurança resumidos com base no trabalho de prioridade crítica do analista, trabalho de alta prioridade, incidentes de segurança atribuídos ao analista, tarefas atribuídas aos analistas e contagem de incidentes.
Performance Analytics (PA) para painéis do Security Incident Response	
Explorador de incidentes de segurança	Com este painel, os gerentes e analistas de segurança podem exibir incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios. Essas exibições permitem que gerentes e analistas obtenham informações rapidamente sobre a frequência com que os ataques estão ocorrendo e quais serviços de negócios são afetados.
Gestão de incidentes de segurança	Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.
Painel do CISO	Proposta para oferecer suporte em uma versão futura.
Eficiência das operações de segurança	Com este painel, gerentes e analistas podem exibir métricas gerais de eficiência e medir o desempenho do SOC.
KPIs de Gestão de incidentes de segurança premium	Com este painel, os gerentes de segurança podem rastrear e visualizar o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painéis do Security Incident Response

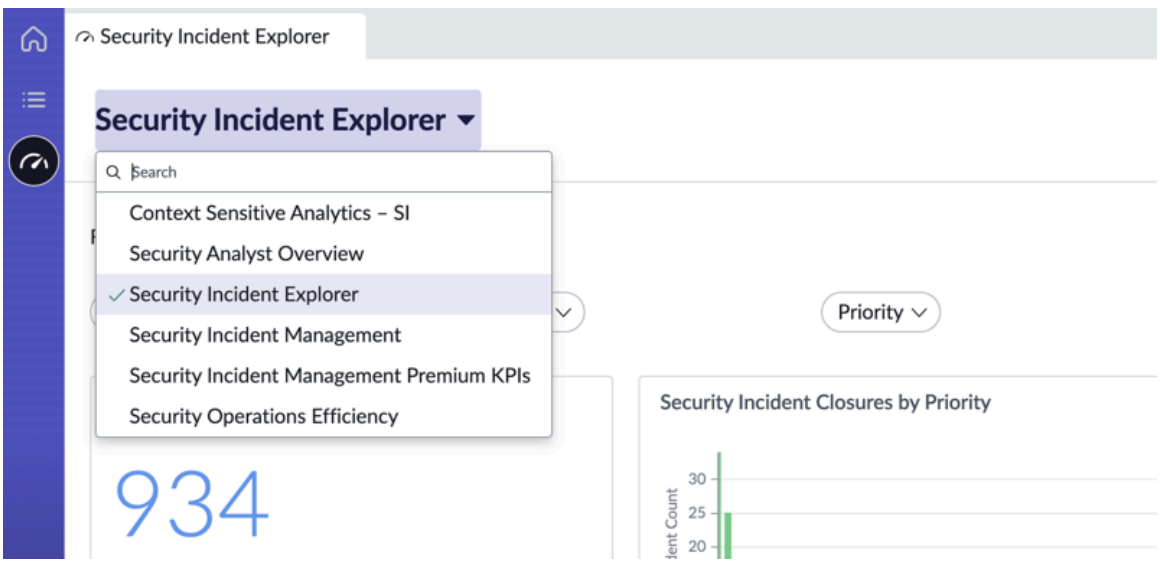
Painel	Descrição
Análise sensível ao contexto – S	Com este painel, gerentes e analistas podem exibir os incidentes de segurança em aberto, a idade média dos incidentes de segurança em aberto, o tempo médio de encerramento de incidentes de segurança, a porcentagem de incidentes de segurança que foram abertos e encerrados no mesmo dia e a porcentagem do incidentes que não foram atualizados nos últimos 5 dias e 30 dias.

Acessar painéis de SIR e PA

O ícone dos **Painéis SIR** é exibido no lado esquerdo da página inicial do espaço.

Nota: Usuários com acesso sn_si.manager ou sn_si.admin podem editar os painéis. Os usuários devem estar dentro do mesmo escopo dos painéis em que o usuário está tentando fazer edições. Por exemplo, se o painel de visão geral do analista de segurança estiver disponível no espaço SIR, o usuário também deverá estar no mesmo escopo do espaço SIR para fazer edições no painel.

1. Navegar até **Espaços** > **Espaço de gestão de incidentes de segurança**.
2. Clique no do **painel SIR Dashboards** .
3. Selecione o painel desejado na lista suspensa.



Você pode editar os painéis, adicionar novos elementos aos painéis e criar seus próprios painéis. Para obter mais informações sobre como usar painéis, consulte Como trabalhar com painéis dinâmicos

Exibir painel Visão geral do analista de segurança

Com este painel, os analistas de segurança podem exibir incidentes de segurança resumidos com base no trabalho de prioridade crítica dos analistas, trabalho de alta

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

prioridade, incidentes de segurança atribuídos ao analista, tarefas atribuídas aos analistas e contagem de incidentes.

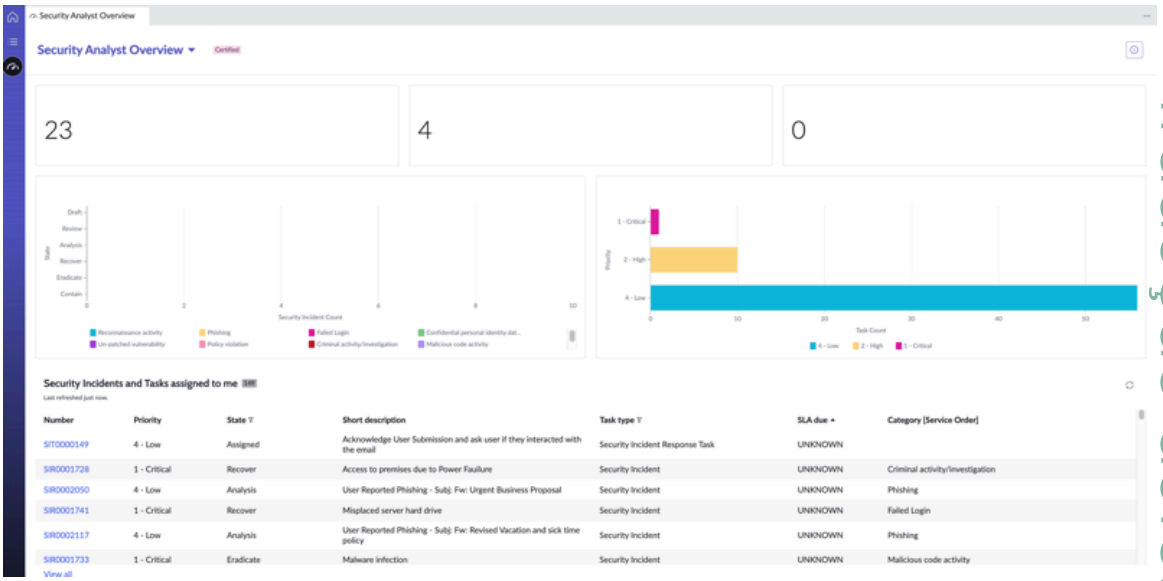
Antes de Iniciar

Por padrão, o painel Visão geral do analista de segurança é exibido para os usuários com acesso sn_si.analyst.

Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do analista de segurança** na lista suspensa.



Exiba o painel Visão geral do analista de segurança para ações futuras. Para obter informações detalhadas sobre o painel Visão geral do analista de segurança, consulte Security Incident Response Soluções Análise da plataforma e relatórios.

Exibir o painel do Explorador de incidentes de segurança

Com este painel, os gerentes de segurança podem exibir incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios.

Antes de Iniciar

Por padrão, o painel do Explorador de incidentes de segurança é exibido para os usuários com acesso sn_si.manager.

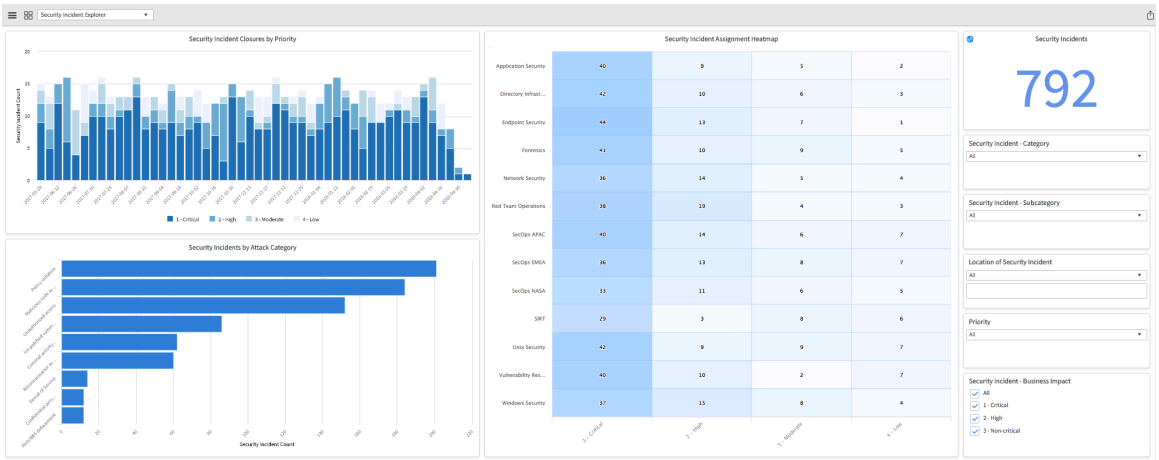
Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Explorador de incidentes de segurança** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba o painel do Explorador de incidentes de segurança para obter outras ações. Para obter informações detalhadas sobre o painel do Explorador de incidentes de segurança, consulte Painel do Explorador de incidentes de segurança

Na versão atual, a seguinte lista de relatórios não é compatível com o painel do Explorador de incidentes de segurança:

- Mapa térmico de atribuição de incidente de segurança — A visualização do mapa térmico não está disponível.
- Mapa de incidentes de segurança - A visualização do mapa não está disponível.

Exibir painel do Gestão de incidentes de segurança

Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Antes de Iniciar

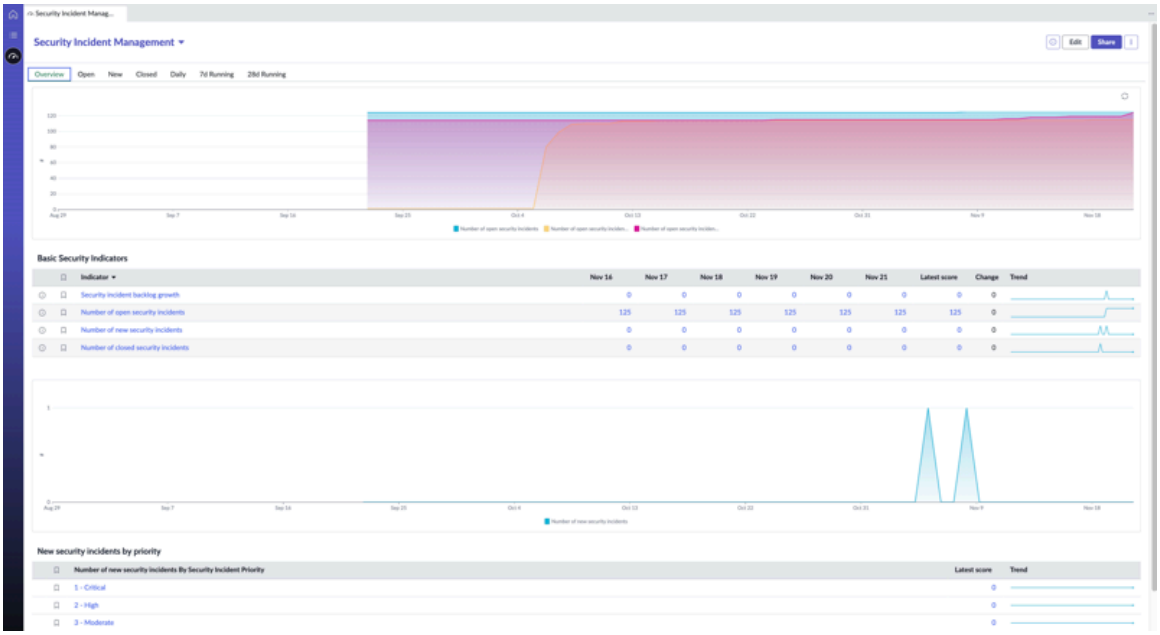
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Gestão de incidentes de segurança** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba o painel do Gestão de incidentes de segurança para obter outras ações. Para obter informações detalhadas sobre o painel do Gestão de incidentes de segurança, consulte Painel do Gestão de incidentes de segurança

Exibir o painel Eficiência das Operações de segurança

Os gerentes do centro de operações de segurança (SOC) podem visualizar as métricas gerais de eficiência e medir o desempenho individual dos membros da equipe de SOC na organização.

Antes de Iniciar

Na versão atual, o relatório a seguir não é compatível com o painel Eficiência das Operações de segurança:

- A análise da fase de Incidente de segurança - Workbench não está disponível

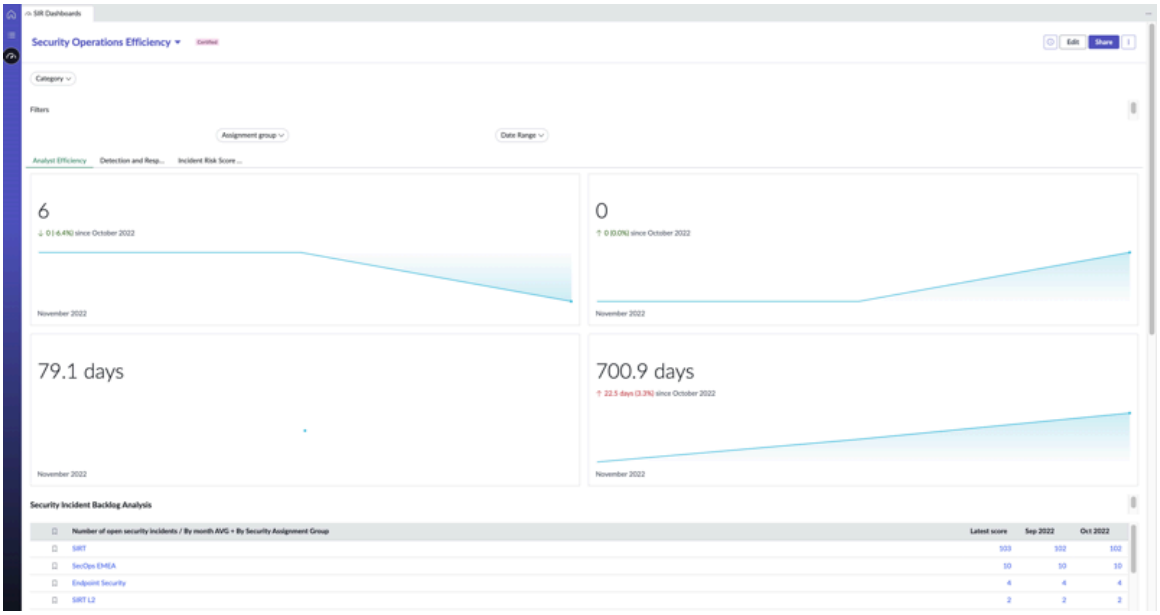
Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Eficiência das Operações de segurança** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba o painel Eficiência das Operações de segurança para ações futuras. Para obter informações detalhadas sobre o painel Eficiência das Operações de segurança, consulte Painel Eficiência das Operaçõesde segurança

Exibir o painel de KPIs premium do Security Incident Response

Com este painel, os gerentes de segurança podem rastrear e visualizar o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Antes de Iniciar

Na versão atual, a lista de relatórios a seguir não é compatível com o painel de KPIs premium do Security Incident Response:

- Processar por estado - Workbench não está disponível
- Processar por Idade - Workbench não está disponível
- Incidentes de segurança abertos por mais de 30 dias por grupo de atribuição e estado - a visualização do mapa térmico não está disponível.
- Incidentes de segurança não atualizados por mais de 30 dias por grupo de atribuição e estado - a visualização do mapa térmico não está disponível.
- Incidentes de segurança com atribuído que não está ativo - a visualização do mapa térmico não está disponível.

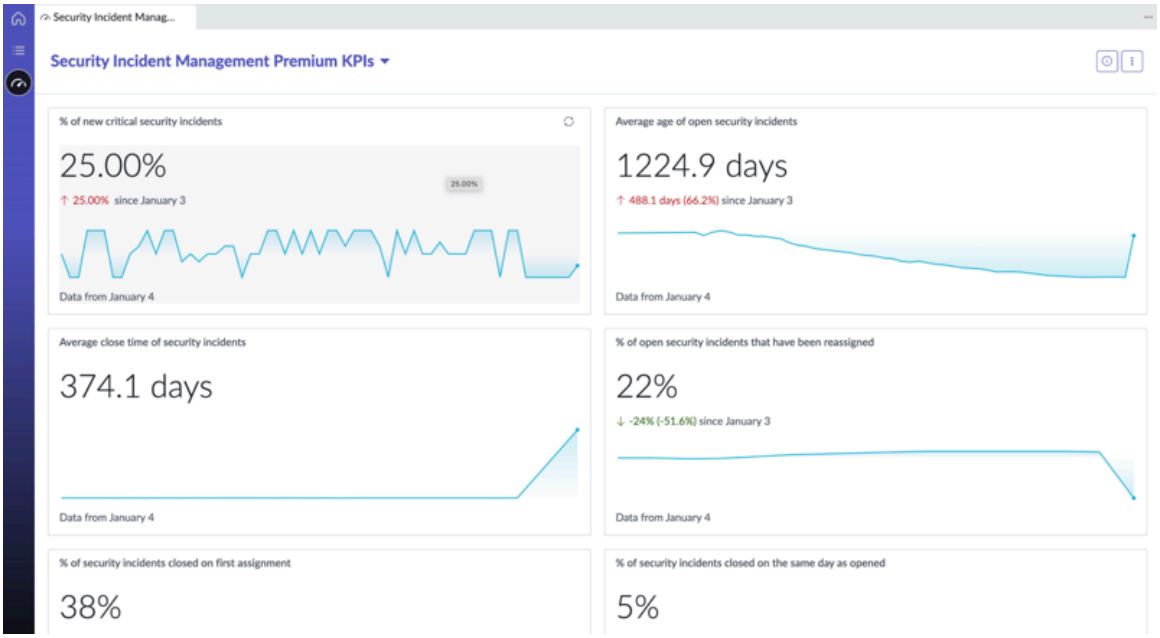
Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Todos** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **KPIs premium do Security Incident Response** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel de KPIs premium do Security Incident Response para ações adicionais. Para obter informações detalhadas sobre o painel de KPIs do Security Incident Response Premium, consulte Paineldo Security Incident Response Premium.

Exibir análise sensível ao contexto - Painel de SI

Com este painel, gerentes e analistas podem exibir os incidentes de segurança em aberto, a idade média dos incidentes de segurança em aberto, o tempo médio de encerramento de incidentes de segurança, a porcentagem de incidentes de segurança que foram abertos e encerrados no mesmo dia e a porcentagem do incidentes que não foram atualizados nos últimos 5 dias e 30 dias.

Antes de Iniciar

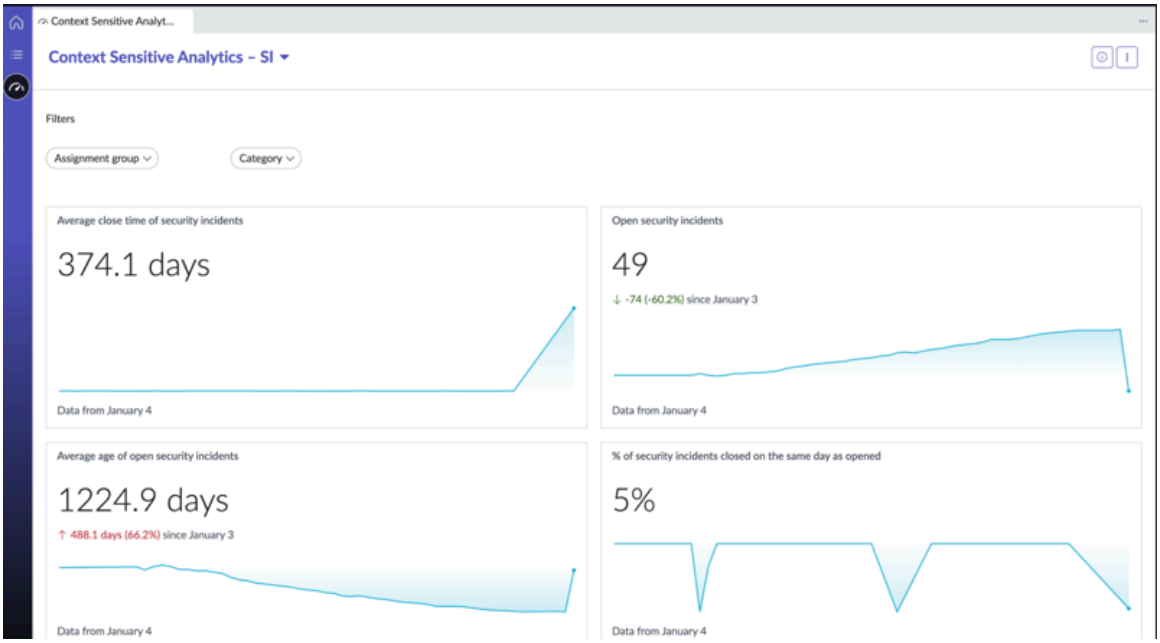
Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Todos** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Análise sensível ao contexto – SI** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel Análise sensível ao contexto – SI para obter outras ações.

Exibir painel do CISO

Este painel fornece aos diretores de segurança da informação (CISOs) uma visão geral de alto nível dos incidentes de segurança e tendências de incidentes semanais na instância na forma de gráficos gráficos. Esses gráficos ajudam a exibir e analisar com eficácia o desempenho do Centro de operações de segurança (SOC).

Antes de Iniciar

- Função necessária: sn_si.admin e sn_si.ciso - Editar e exibir incidentes.
- Certifique-se de ter o aplicativo Performance Analytics para Security Incident Response instalado.

Por Que e Quando Desempenhar Esta Tarefa

Nota: O painel CISO e o painel Visão geral do CISO eram dois diferentes na IU clássica. Mas agora as capacidades dos dois painéis foram mescladas no painel do CISO.

O painel do CISO fornece informações importantes sobre seus incidentes de segurança semanalmente. Você pode configurar indicadores e coletar snapshots de dados dos incidentes que correspondem às condições nas propriedades do indicador. Os dados coletados são visualizados usando widgets no painel.

Você pode visualizar as tendências semanais usando os widgets no painel do CISO. Os dados ou estatísticas das tendências de seus incidentes de segurança são coletados das propriedades do indicador de incidentes semanais que são definidas pela organização. Você pode obter informações importantes usando os seguintes gráficos:

- **Tempo médio de identificação (semanalmente)**: este gráfico ilustra o tempo médio semanal necessário para identificar um incidente de segurança.
- **Tempo médio de contenção (semanalmente)**: este gráfico ilustra o tempo médio semanal necessário para conter um incidente de segurança.
- **Tempo médio para erradicar (semanalmente)**: este gráfico ilustra o tempo médio semanal necessário para erradicar um incidente de segurança.

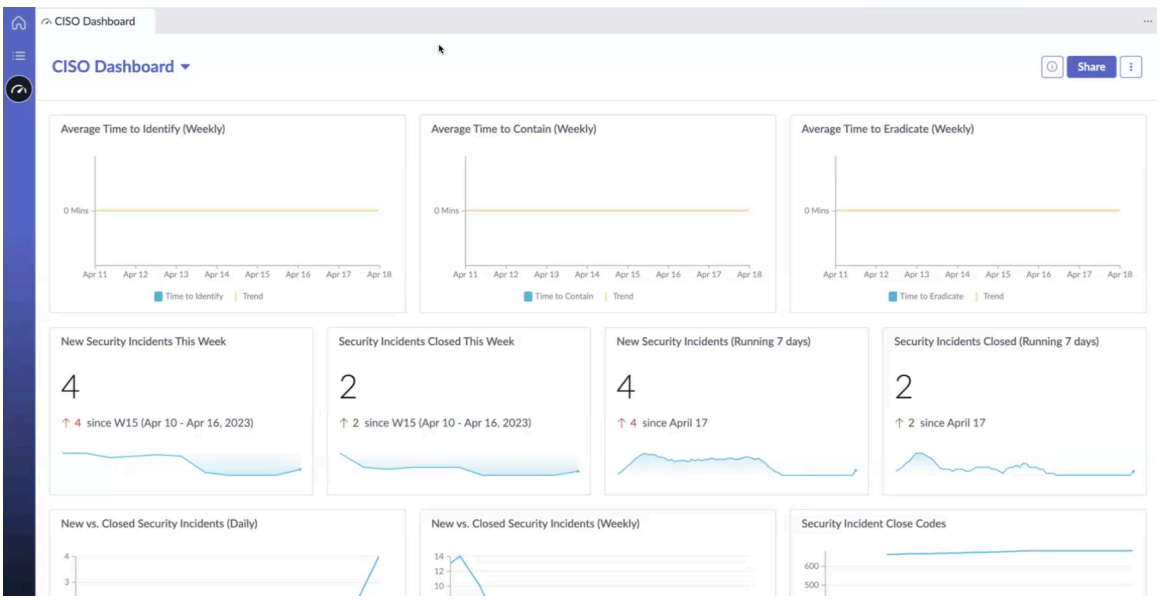
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Novos incidentes de segurança nesta semana**: este gráfico ilustra o número de novos incidentes de segurança nesta semana.
- **Incidentes de segurança encerrados nesta semana**: este gráfico ilustra o número de incidentes de segurança encerrados nesta semana.
- **Novos incidentes de segurança (em execução há 7 dias)**: este gráfico ilustra o número de novos incidentes de segurança em execução por uma semana.
- **Incidentes de segurança encerrados (em execução há 7 dias)**: este gráfico ilustra o número de novos incidentes de segurança que estão encerrados, mas estão em execução há uma semana.
- **Incidentes novos versus encerrados (diariamente)**: este gráfico ilustra a comparação entre os novos incidentes de segurança diários e os incidentes de segurança encerrados diariamente.
- **Incidentes novos versus encerrados (semanalmente)**: este gráfico ilustra a comparação entre os novos incidentes de segurança semanais e os incidentes de segurança encerrados semanalmente.
- **Códigos**encerrados de incidentes de segurança: este gráfico ilustra os códigos encerrados dos incidentes de segurança.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis de SIR** no lado esquerdo da página inicial do espaço.
3. Selecione **Painel do CISO** na lista suspensa.



4. Exiba o painel do CISO para ações futuras.

Exibir o painel Visão geral do relatório do CISO

Este painel fornece aos diretores de segurança da informação (CISOs) uma visão geral de relatório de alto nível dos incidentes de segurança e tendências de incidentes semanais na instância na forma de gráficos gráficos. Esses gráficos ajudam a exibir e analisar com eficácia o desempenho do Centro de operações de segurança (SOC).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin e sn_si.ciso - Editar e exibir incidentes.

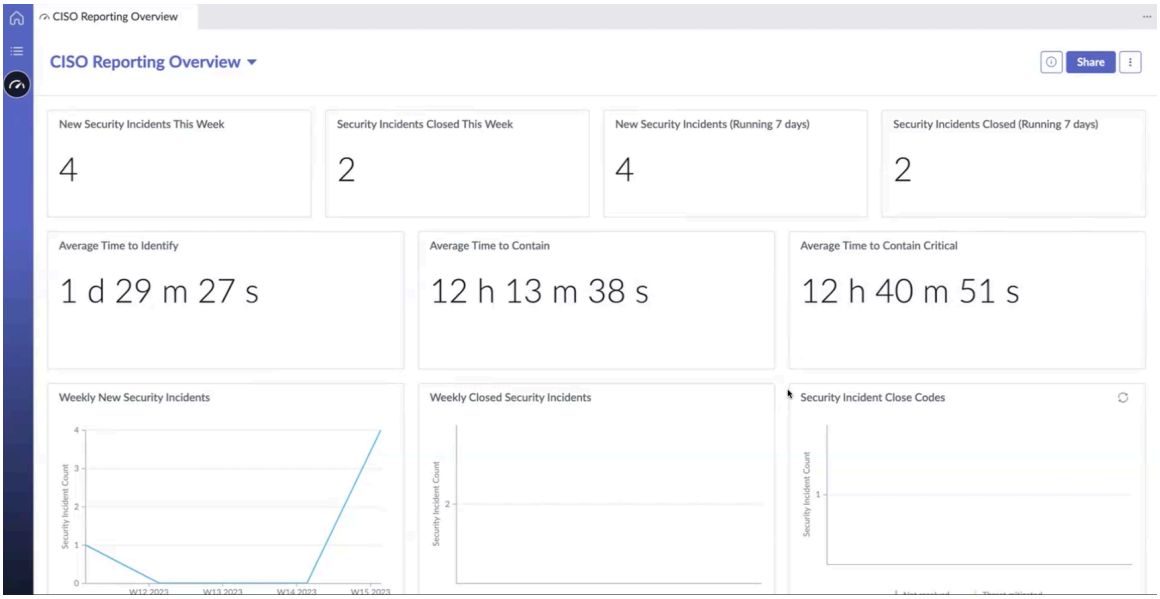
Por Que e Quando Desempenhar Esta Tarefa
O painel Visão geral de relatórios do CISO fornece informações importantes sobre os incidentes de segurança semanalmente e você pode visualizar as tendências semanais usando widgets. Você pode obter informações importantes sobre a Emissão de relatórios do CISO usando os seguintes gráficos:

- **Novos incidentes de segurança nesta semana**: este bloco exibe o relatório do número de novos incidentes de segurança nesta semana.
- **Incidentes de segurança encerrados nesta semana**: este bloco exibe o relatório do número de incidentes de segurança encerrados nesta semana.
- **Novos incidentes de segurança (em execução há 7 dias)**: este bloco exibe o relatório do número de novos incidentes de segurança em execução por uma semana.
- **Incidentes de segurança encerrados (em execução há 7 dias)**: este bloco exibe o relatório do número de novos incidentes de segurança encerrados, mas estão em execução há uma semana.
- **Tempo médio de identificação**: este bloco exibe o relatório do tempo médio semanal necessário para identificar incidentes de segurança.
- **Tempo médio de contenção**: este bloco exibe o relatório do tempo médio semanal necessário para conter incidentes de segurança.
- **Tempo médio para conter incidentes críticos**: este bloco exibe o relatório do tempo médio semanal necessário para conter incidentes de segurança críticos.
- **Novos incidentes de segurança semanais**: este gráfico ilustra o relatório dos novos incidentes de segurança semanais.
- **Incidentes**de segurança encerrados semanalmente: este gráfico ilustra o relatório dos incidentes de segurança encerrados semanalmente.
- **Códigos encerrados de incidentes de segurança**: este gráfico ilustra o relatório dos códigos encerrados dos incidentes de segurança.

Procedimento
1. Navegar até **Todos** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis SIR** no lado esquerdo da página inicial do espaço.
3. Selecione **CISO Reporting Overview** na lista suspensa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel de emissão de relatórios do CISO para ações futuras.

Exibir o painel Visão geral do gerenciador de incidentes de segurança

Este painel fornece aos gerentes uma visão geral de alto nível dos incidentes de segurança críticos ou de alta prioridade no nível da equipe, SLAs que estão prestes a expirar em 24 horas e tendências de incidentes semanais na instância na forma de relatórios e gráficos gráficos.

Antes de Iniciar

Função necessária:

- sn_si.admin - Editar e exibir o painel.
- sn_si.manager — Exibir painel.

Por Que e Quando Desempenhar Esta Tarefa

Você pode analisar os incidentes de segurança críticos ou de alta prioridade, ou SLAs que precisam de atenção imediata. Você também pode visualizar as tendências semanais usando os widgets no painel Visão geral do Gerenciador de incidentes de segurança. Os dados ou estatísticas das tendências semanais ou mensais de seus incidentes de segurança são coletados das tabelas de incidentes definidas pela organização. Você pode obter informações importantes usando os seguintes gráficos:

- **Incidentes de segurança críticos da equipe**: este bloco exibe o número de incidentes de segurança críticos da equipe nesta semana.
- **Incidentes**de alta segurança da equipe: este bloco exibe o número de incidentes de alta segurança da equipe nesta semana.
- **ANS que expiram em 24 horas**: este bloco exibe o número de SLAs que expirarão em 24 horas.
- **Tempo médio de identificação**: este bloco exibe o tempo médio semanal necessário para identificar incidentes de segurança.
- **Tempo médio de contenção**: este bloco exibe o tempo médio semanal necessário para conter incidentes de segurança.
- **Tempo médio para conter incidentes críticos**: este bloco exibe o tempo médio semanal necessário para conter incidentes de segurança críticos.

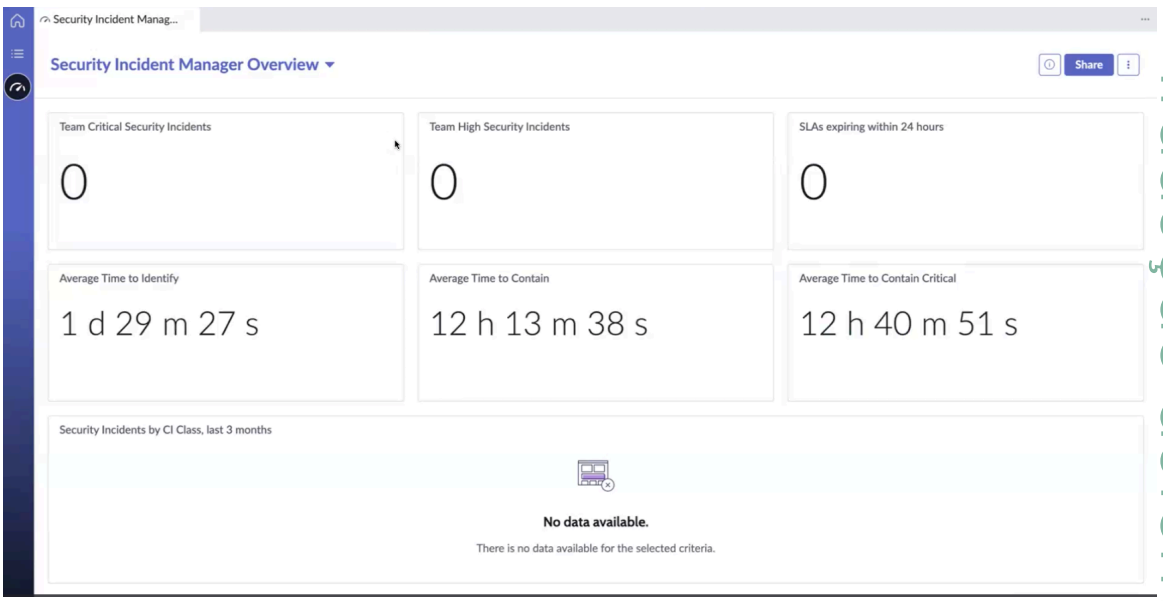
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Incidente de segurança por classe de IC, últimos 3 meses**: este gráfico ilustra as tendências de todos os incidentes de segurança com base na classe de IC nos últimos três meses.
- **Tendência de todos os incidentes de segurança por categoria**: este gráfico ilustra as tendências de todos os incidentes de segurança com base na categoria.
- **Tendência de todos os incidentes de segurança por prioridade**: este gráfico ilustra as tendências de todos os incidentes de segurança com base na prioridade.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Resposta a incidentes de segurança**.
2. Clique no ícone **Painéis SIR** no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do Gerenciador de incidentes de segurança** na lista suspensa.



4. Consulte a Visão geral do Gerenciador de incidentes de segurança para obter outras ações.

Tradução automática

Exibir painel de integridade do Security Incident Response

O recurso do painel de Integridade do Security Incident Response fornece uma exibição centralizada de aspectos críticos relacionados à implementação do processo de resposta a incidentes, problemas/erros encontrados e métricas de desempenho. Ele serve como uma ferramenta vital para monitorar e otimizar a eficácia das capacidades de resposta a incidentes de segurança de uma organização.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst ou sn_si.analytics_read - Exibir painel.

Por Que e Quando Desempenhar Esta Tarefa

Você pode monitorar a integridade dos incidentes de segurança usando os widgets e gráficos de tendências para cada aplicação. Essas estatísticas apresentam uma pontuação de integridade abrangente detalhando o estado da configuração e a eficácia da correção nas aplicações SIR. O painel de Integridade do Security Incident Response é compatível com as quatro guias a seguir:

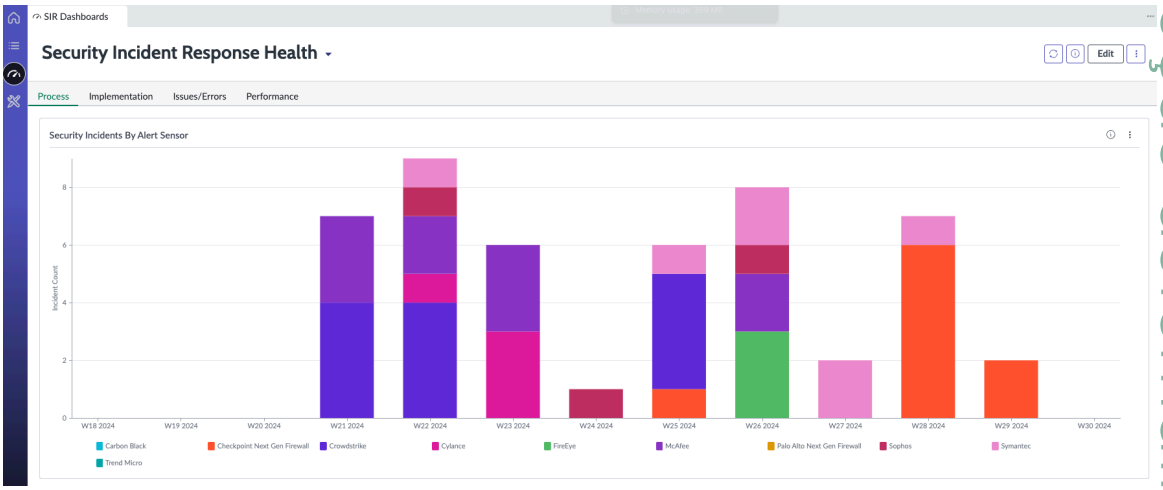
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Processo**: a guia exibe um resumo de todos os incidentes de vários sensores de alerta agrupados semanalmente.
- **Implementação**: esta guia exibe as personalizações que os clientes executam em suas instâncias, abrangendo inclusões de script, regras de negócio, fluxos e upgrades.
- **Problemas/erros**: a guia exibe widgets que destacam erros em processos de integração, discrepâncias durante a ingestão de dados brutos de incidentes, erros de HTTP de saída em aplicações SIR e quaisquer problemas que surgem durante a execução de playbooks.
- **Desempenho**: esta guia exibe os problemas de desempenho nas aplicações SIR, incluindo lentidão em consultas de desempenho, regras de negócio e scripts.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione o ícone **Painéis de SIR** na página inicial do espaço de SIR.
3. Selecione **Painel de Integridade do Security Incident Response** na lista suspensa.
4. Selecione a guia **Processo** para exibir o número de incidentes de segurança que foram acionados semanalmente para cada sensor de alerta no gráfico.

Guia Processo



Você pode executar as seguintes tarefas:

a. Selecione um sensor de alerta no gráfico para exibir os detalhes de KPI do número de incidentes de segurança acionados por sensores de alerta em uma semana.

b. Para obter os detalhes de KPI de uma semana específica, use a opção **Calendário**.

c. Para comparar os incidentes de segurança acionados pelo sensor de alerta, selecione a opção **Comparar registros**.

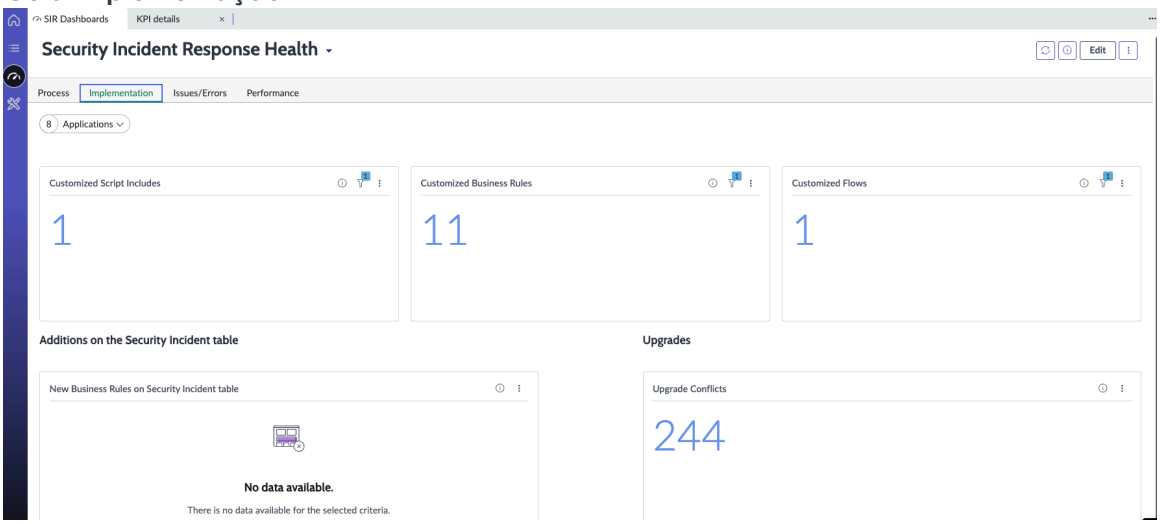
d. Para usar o tipo de gráfico, série temporal ou análise, selecione as **opções de gráfico**.

5. Selecione a guia **Implementação** para exibir o número de personalizações que foram criadas para os incidentes de segurança nas aplicações Security Incident Response.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Implementação



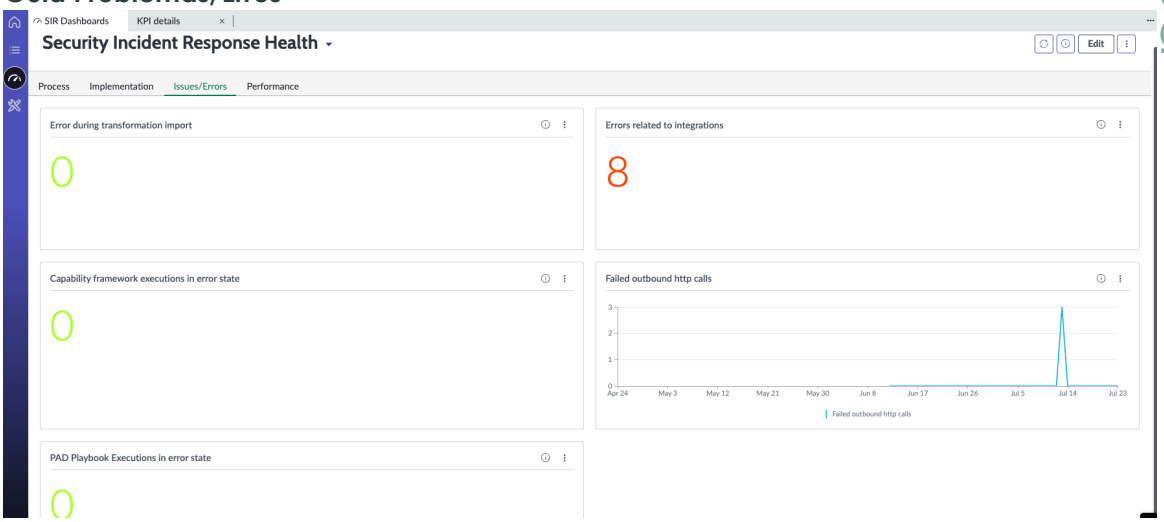
Guia**Implementação** :

Você pode exibir o painel agregado para o número de personalizações que foram criadas para cada aplicação Incident Response.

- Inclusões de**script personalizado**: este widget exibe o número de scripts personalizados que foram adicionados com base em seus requisitos nas aplicações SIR.
- **Regras de negócio personalizadas**: este widget exibe o número de regras de negócio personalizadas que foram adicionadas com base em seus requisitos nas aplicações SIR.
- **Fluxos personalizados**: este widget exibe o número de fluxos personalizados que foram adicionados com base em seus requisitos nas aplicações SIR.
- **Nova regra de negócio na tabela Incidente de segurança**: este widget exibe o número de regras de negócio que foram criadas na tabela Incidente de segurança.
- **Conflitos de upgrade**: este widget exibe o número de conflitos que foram acionados durante os upgrades nas aplicações SIR.

6. Selecione a guia **Problemas/Erros** para exibir o número de problemas ou erros que foram acionados nas aplicações do Security Incident Response.

Guia Problemas/Erros



Guia**Problemas/erros** :

Tradução automática

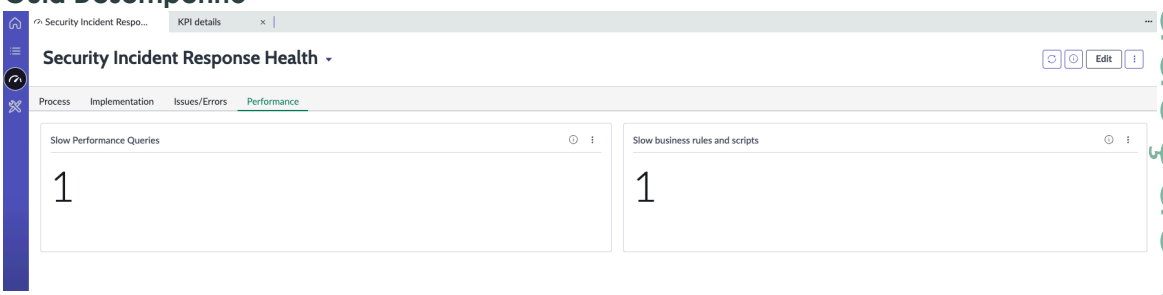
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir o painel agregado em busca de problemas ou erros nas aplicações do Security Incident Response.

- **Erros durante a importação de transformação**: este widget exibe o número de erros que foram acionados durante a importação de transformação em aplicações SIR.
- **Erros relacionados a integrações**: este widget exibe o número de erros que foram acionados durante as integrações de SIR.
- **Execuções da estrutura de capacidade em estado de erro**: este widget exibe o número de erros que foram acionados durante as execuções da estrutura de capacidade em aplicações SIR.
- **Chamadas HTTP de saída com falha**: este widget exibe o número de chamadas HTTP de saída com falha que foram acionadas nas aplicações SIR.
- **Execuções do Playbook de PAD em estado de erro**: este widget exibe o número de erros de execução do Playbook de PAD que foram acionados nas aplicações SIR.

7. Selecione a guia **Desempenho** para exibir o número de problemas de desempenho que foram acionados nas aplicações do Security Incident Response.

Guia Desempenho



Guia**Desempenho** :

Você pode exibir o painel agregado para problemas de desempenho nas aplicações do Security Incident Response.

- **Consultas de desempenho lento**: este widget exibe o número de consultas de desempenho nas aplicações SIR cujo tempo médio de execução é maior que 10 ms e calculado em 1000 ou mais execuções.
- **Regras de negócio e scripts lentos**: este widget exibe o número de regras de negócio e scripts nas aplicações SIR cujo tempo médio de execução é maior que 10 ms e calculado em 1000 ou mais execuções.

8. Você pode usar o ícone **Atualizar** para atualizar os dados no painel de Integridade do Security Incident Response.
9. Você pode usar o ícone **Exibir detalhes do painel** para exibir os detalhes do painel de Integridade do Security Incident Response.
10. Você pode usar a opção **Editar** para modificar os detalhes do painel de Integridade do Security Incident Response.
11. Você pode usar a opção **Mais** para executar ações adicionais no painel Integridade do Security Incident Response.

Criação de incidente de segurança

Os incidentes de segurança podem ser criados manualmente a partir do formulário ou automaticamente por meio de eventos de segurança recebidos de ferramentas integradas de monitoramento de alertas de terceiros, como Splunk.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Os recursos mais recentes em Security Incident Response estão disponíveis exclusivamente no Espaço de resposta a incidentes de segurança. Instale ou faça upgrade para a versão mais recente Security Incident Response ou Espaço de resposta a incidentes de segurança para acessar e aproveitar recursos como Transferência de turno, Calculadora de pontuação de risco etc.

Se você tiver uma função de segurança, poderá usar qualquer um dos métodos a seguir para criar incidentes de segurança manualmente.

Métodos para criar incidentes de segurança manualmente

Método	Descrição
Criado manualmente a partir da lista de incidentes de segurança	Na lista Incidente de segurança, clique em **Novo** para criar um novo incidente de segurança.
Criado manualmente a partir do Catálogo de incidentes de segurança	Você pode criar incidentes de segurança selecionando categorias de ameaças à segurança definidas no catálogo de incidentes de segurança.
Gestão de incidentes	No formulário Incidente na gestão de incidentes, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.
Convertido manualmente de uma solicitação de segurança	No formulário Solicitação de segurança, clique em **Converter em incidente de segurança** para criar um novo incidente de segurança.
Criado manualmente a partir de um alerta da Gestão de eventos	No formulário Alertas da Gestão de eventos, clique em **Criar incidente de segurança** para criar um novo incidente de segurança a partir de um alerta.
Criado manualmente a partir de um alerta	No formulário Alerta de gestão de eventos, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.
Convertido manualmente de um registro de vulnerabilidade (se o plug-in Resposta a vulnerabilidades estiver ativado)	No formulário Itens de vulnerabilidade, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.

Criação automática de incidentes de segurança

Geralmente, os administradores de segurança são responsáveis por configurar regras de alerta usadas para gerar automaticamente incidentes de segurança.

Método de administração de segurança para criar incidentes de segurança

Método	Descrição
Criado automaticamente usando regras de alerta	Os incidentes de segurança podem ser criados com base em regras de alerta definidas na Gestão de eventos na aplicação de datacenter .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação manual de incidente de segurança

Você pode criar um incidente de segurança a partir do formulário de Incidente de segurança, bem como de vários outros formulários.

Você pode criar incidentes de segurança com base em um registro existente nos seguintes formulários:

- A partir de qualquer lista de incidentes de segurança
- Formulário Incidente
- Gestão de eventos Formulário de alerta
- Formulário de Itens vulneráveis
- Formulário de solicitação de segurança

Criar um incidente de segurança a partir da lista de incidentes de segurança

Além dos métodos automáticos para criar incidentes de segurança, você pode criá-los manualmente, conforme necessário.

Este vídeo mostra uma visão geral de como você pode criar um incidente de segurança na lista de incidentes de segurança.

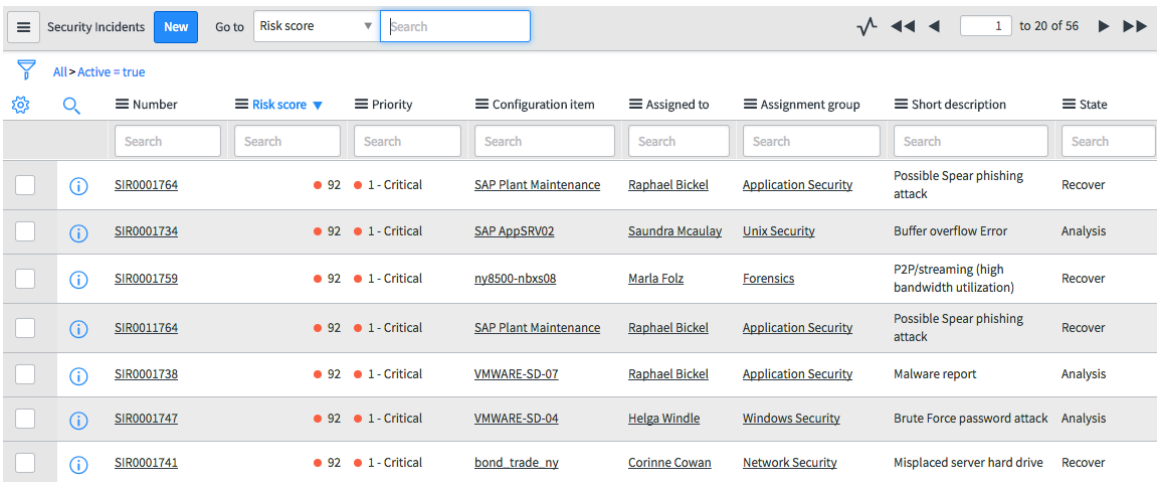
Criar um incidente de segurança a partir da lista de incidentes de segurança

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

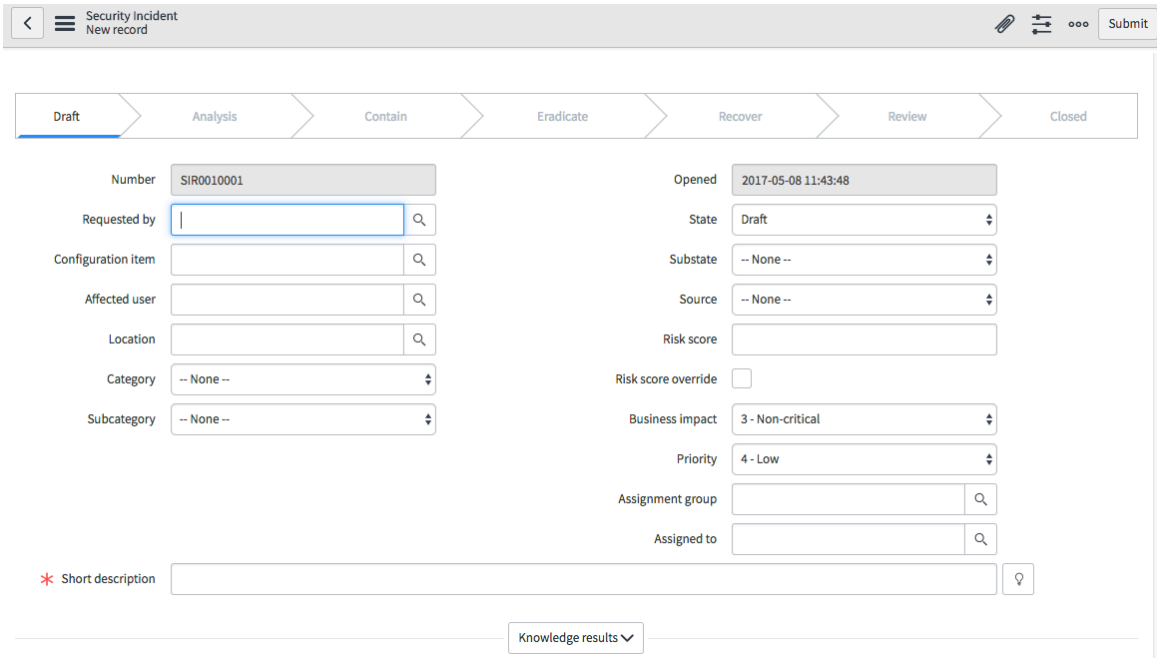
1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**).



2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. No formulário, preencha os campos.

Campo	Descrição
Selecione marcador de segurança	Se necessário, selecione um marcador de segurança para adicionar metadados ao registro ou identificar quem deve ter acesso a este registro de incidente de segurança. Este campo aparece somente depois que o incidente de segurança foi salvo.
Número	[Somente leitura] O número do incidente de segurança.
Solicitados por	A pessoa que está solicitando a execução do trabalho.
Item de Configuração	O servidor, computador, roteador ou outro item de configuração afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.
Local	O local do solicitante ou recurso. Se um **item de configuração** não estiver selecionado, este campo será preenchido previamente com o local do solicitante.
Categoria	A categoria que identifica o tipo de problema de segurança. Se uma categoria for selecionada, um fluxo de trabalho para analisar esse problema será executado quando o registro for salvo. Por exemplo, se você selecionar **Negação de serviço**, o fluxo de trabalho Incidente de segurança - Negação de serviço - Modelo será executado. Para obter mais informações, consulte Modelos de fluxo de trabalho do Security Incident Response.
Subcategoria	A subcategoria que define melhor o problema.
Aberto	[Somente leitura] Exibe a data e a hora em que o incidente foi aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	O estado atual do incidente de segurança. Na criação do incidente de segurança, o padrão deste campo é **Rascunho**.
Subestado	Identifica se o incidente de segurança inclui um problema ou mudança pendente.
Origem	Identifica a origem do incidente de segurança, como e-mail, chamada telefônica ou monitoramento de rede.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbon Black, CrowdStrike, McAfee e assim por diante.
Regra de Alerta	A regra no produto de segurança que acionou a criação deste incidente de segurança.
Pontuação de risco	Exibe a pontuação de risco calculada para este incidente de segurança. O valor é baseado na prioridade do incidente de segurança, no tipo de incidente de segurança (negação de serviço, Spear Phishing ou atividade de código malicioso) e no número de origens que acionaram uma pontuação de reputação com falha em um indicador. A pontuação de risco ajuda a priorizar o trabalho de incidente de segurança para os analistas. Três propriedades de incidente de segurança permitem que você designe um ponto codificado por cores para aparecer ao lado da pontuação de risco na exibição de lista para torná-los mais facilmente identificáveis. Se você fizer mudanças em determinados campos no incidente de segurança, como **Impacto nos negócios** ou **Prioridade**, e salvar o registro, a **Pontuação de risco** será automaticamente recalculada e exibida. A mudança também é refletida nas anotações de trabalho e na lista relacionada Auditorias de pontuação de risco. **Nota:** A pontuação de risco também é recalculada quando os usuários afetados são associados a um incidente de segurança, serviços afetados ou itens vulneráveis. Você também pode inserir manualmente uma nova **pontuação de risco**. Isso pode ser útil se você quiser manter um incidente de segurança específico no topo da lista de incidentes de segurança que está analisando. Se você inserir uma nova Pontuação de **risco**, a caixa de seleção **Substituição de pontuação de risco** será marcada automaticamente. Independentemente das mudanças feitas no incidente de segurança, uma pontuação de risco inserida manualmente não é recalculada automaticamente. **Nota:** Se você atualizou sua instância de uma versão anterior, as pontuações de risco foram calculadas para todos os incidentes de segurança em aberto. Para obter mais informações, consulte Noções básicas sobre calculadoras de incidentes de segurança.
Substituição de pontuação de risco	Marque esta caixa de seleção para substituir a atualização automática da pontuação de risco. A substituição será refletida nas anotações de trabalho.
Impacto nos negócios	Selecione a importância deste incidente de segurança para o seu negócio. O valor padrão é Não crítico. Se, depois que o registro do

Tradução automática

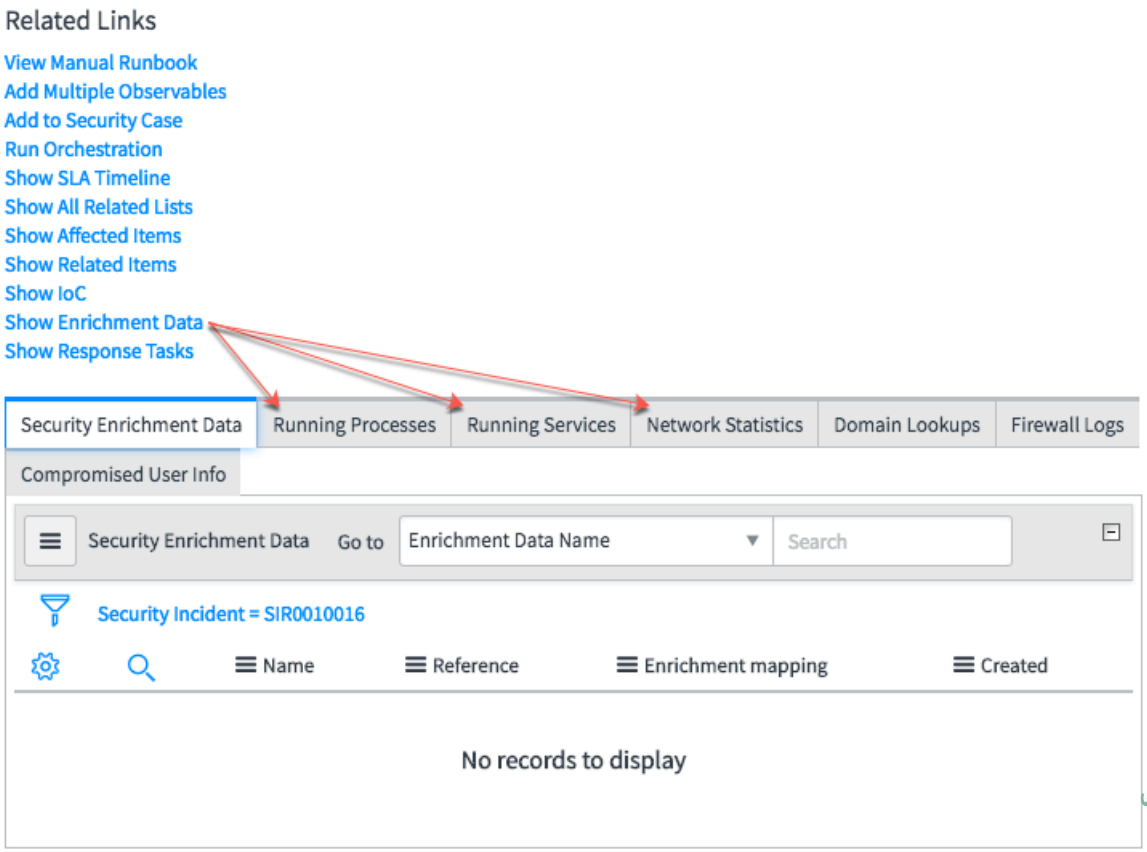
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	incidente de segurança for salvo, você alterar o valor nos campos **Prioridade** /ou **Risco**, o **Impacto nos negócios** será recalculado.
Prioridade	Selecione a ordem de abordagem deste incidente de segurança, com base na urgência. Se este valor for alterado depois que o registro for salvo, isso poderá afetar o cálculo **de impacto nos negócios**.
Grupo de atribuição	O grupo ao qual este incidente de segurança está atribuído.
Atribuído a	O indivíduo atribuído para analisar este incidente de segurança. As atribuições podem ser realizadas manual ou automaticamente. Para obter mais informações, consulte Atribuição de analistas de segurança.
Descrição resumida	Uma breve descrição do incidente de segurança.
Resultados de conhecimento	Conforme você digita a descrição resumida, são exibidos links para artigos relacionados da base de conhecimento. Verificar as informações pode resolver seu problema.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar**.
   Se você adicionou um novo IC ao incidente de segurança, os seguintes fluxos de trabalho de integração serão executados automaticamente:
   - Operações de segurança - Obter fluxo de trabalho de processos em execução. Este fluxo de trabalho recupera uma lista de processos em execução em um item de configuração (IC) de um host ou endpoint.
   - Fluxo de trabalho do Security Incident Response - Obter serviços em execução. Este fluxo de trabalho recupera uma lista de serviços em execução de ICs baseados no Windows.
   - Integrações de operações de segurança - Fluxo de trabalho Obter estatísticas de rede. Este fluxo de trabalho recupera uma lista de conexões de rede ativas de um host ou endpoint.
5. Para exibir as informações recuperadas por esses fluxos de trabalho, clique no link relacionado **Mostrar dados de aprimoramento** e clique em qualquer uma das guias indicadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Fluxos de trabalho adicionais são executados com base nas integrações de terceiros que você ativou da seguinte forma Integração do Carbon Black das Operações de segurança - Obter fluxo de trabalho dos processos em execução

Informações relacionadas

Configuração do Security Incident Response

Criar um incidente de segurança a partir do Catálogo de incidentes de segurança

Os usuários da sua empresa podem usar o Catálogo de incidentes de segurança para solicitar vários tipos de análises relacionadas à segurança.

Antes de Iniciar

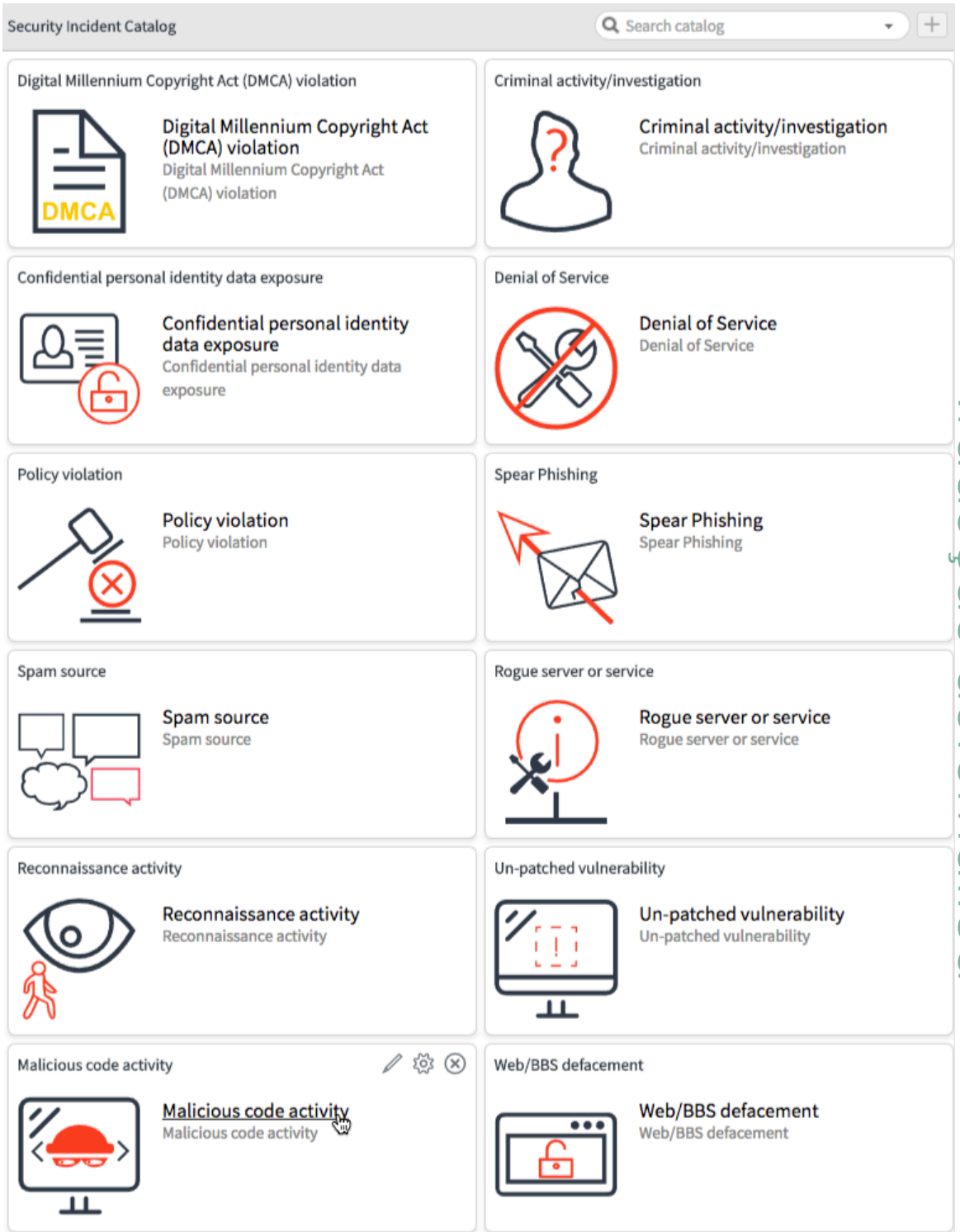
Função necessária: nenhuma

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

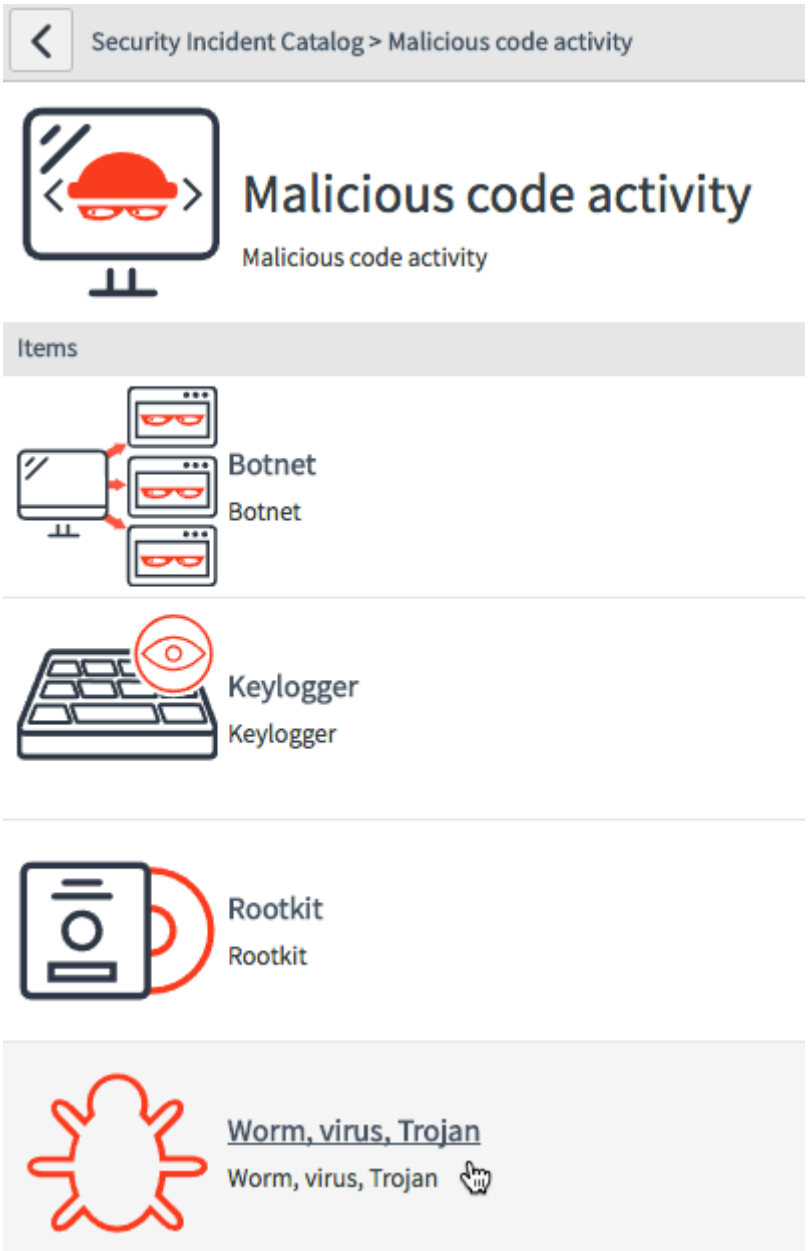
1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de incidente de segurança**.



2. Clique no item do catálogo para o qual você deseja fazer uma solicitação.
Se o item selecionado no catálogo principal contiver subcategorias, a lista será mostrada.
No exemplo a seguir, **a atividade de código malicioso** foi selecionada.

Tradução automática

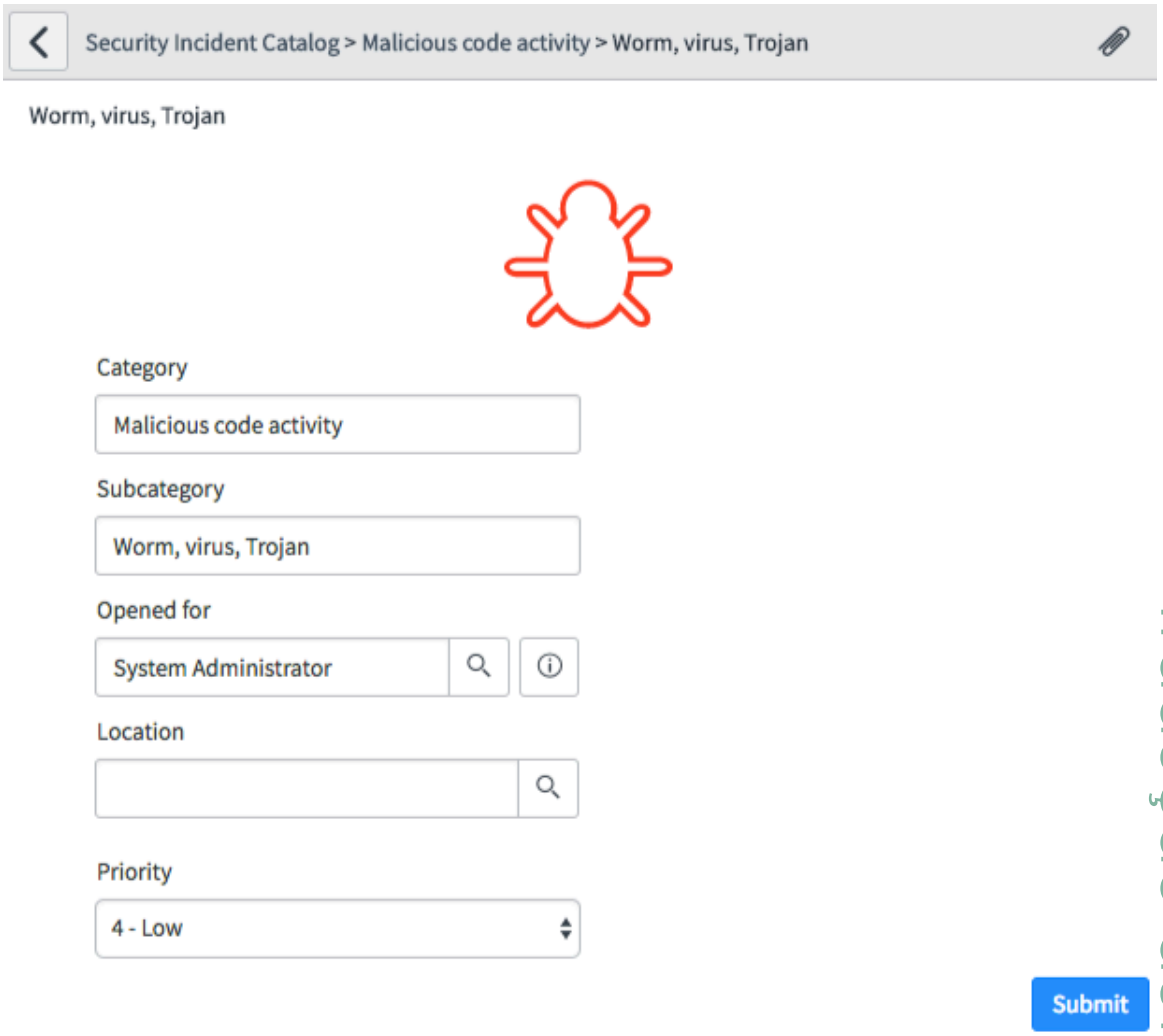
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique na subcategoria que melhor corresponde ao tipo de solicitação que você deseja fazer.
   Neste exemplo, a subcategoria **Verme, vírus e Cavalo de Tróia** foi selecionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira as informações da solicitação e clique em **Enviar**.
   A solicitação é enviada ao departamento de incidentes de segurança.
5. Depois de enviar a solicitação, você pode acompanhar o andamento navegando até **Autoatendimento** > **Minhas solicitações**e inserindo o número da solicitação.

Criar um incidente de segurança a partir de um alerta da Gestão de eventos

Quando a Gestão de eventos está ativada, você pode criar incidentes de segurança manualmente a partir do formulário Alerta.

Antes de Iniciar

O plug-in Gestão de eventos requer uma assinatura separada e deve ser ativado pela equipe da ServiceNow. Este plug-in inclui dados de demonstração e ativa plug-ins relacionados, caso ainda não estejam ativos. A Análise de Serviço é ativada automaticamente quando a Gestão de eventos é ativada.
Função necessária: evt_mgmt_admin, evt_mgmt_operator ou evt_mgmt_user

Procedimento

1. Navegar até **Todos** > **Gestão de eventos** > **Todos os Alertas**.
2. Clique no **Número**do alerta .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique **em Criar incidente de segurança**.
4. Clique em **Atualizar**.

Criação automática de incidente de segurança

Ferramentas de monitoramento de terceiros, como Splunk, podem ser integradas a Security Incident Response para que os eventos de segurança importados dessas ferramentas gerem automaticamente incidentes de segurança. Você também pode importar dados de ferramentas de terceiros para alertas de segurança.

Para integrar ferramentas de monitoramento de alertas ao Security Incident Response, você deve usar a REST API para gravar na tabela Importação de incidentes de segurança [sn_si_incident_import]. Em seguida, usando os mapas de transformação **de Transformação de incidente de segurança**, a tabela de origem do conjunto de importação é mapeada para campos na tabela Incidente de segurança [sn_si.incident] de destino.

Se você tentar importar registros de IC que não são reconhecidos pelo mapa de transformação, o script do mapa de transformação verificará o registro para o seguinte (nesta ordem) em uma tentativa de fazer uma correspondência:

- sys_id
- Nome do IC
- nome de domínio totalmente qualificado
- Endereço IP

Nota: Se você descobrir que o mapa de transformação **de transformação de incidente de segurança** não é adequado para a ferramenta de monitoramento de alertas de terceiros que você está usando, duplique o mapa de transformação, crie um novo e edite os campos, conforme necessário.

Incidentes de segurança criados a partir de eventos e alertas

Conforme os eventos são importados das ferramentas de monitoramento de alertas, eles são processados primeiro por Gestão de eventos e agrupados em alertas. Esses alertas podem ser usados para criar incidentes de segurança com base em regras de alerta personalizáveis ou revisados manualmente para selecionar esses alertas a serem investigados como um incidente de segurança.

Você pode encontrar um exemplo de regra de alerta chamada **Criar incidentes de segurança a partir de alertas críticos** no módulo Regras de AlertaGestão de eventos da aplicação []. Esta regra de alerta cria automaticamente incidentes de segurança quando eventos críticos relacionados à segurança são recebidos de dentro de ServiceNow ou de aplicações de monitoramento de terceiros. Depois que o incidente de segurança for criado, ele será atualizado conforme novos eventos forem recebidos. Você pode modificar o modelo de tarefa na regra de alerta para alterar os valores iniciais do incidente de segurança criado por esta regra de alerta. Para lidar com cada variedade distinta de incidente de segurança que você deseja criar, você pode definir outras regras de alerta com condições diferentes.

Como alternativa, se você for um usuário com a função de Administrador de segurança, poderá criar manualmente um incidente de segurança clicando no botão **Criar incidente de segurança** em qualquer alerta suspeito.

É importante que os eventos recebidos de ferramentas externas incluam as seguintes informações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O nó definido para o nome, endereço IP ou sys_id do IC que se torna o recurso afetado.
- A classificação de eventos é definida como Segurança para diferenciá-los de outros eventos de TI.
- A descrição do evento, que preenche a descrição do incidente de segurança.
- As informações adicionais podem incluir qualquer informação extra que não se encaixe nos campos listados anteriormente ou em outros campos de evento, como categoria, vetores de ataque, URL de retorno ou ID de correlação. O formato é uma cadeia de caracteres que lista os nomes de campo junto com seus valores, usando o seguinte formato JSON:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Nota: Para cada par de campo e valor, se o campo no incidente de segurança em que o nome da coluna corresponder ao fieldName estiver vazio, ele será definido como fieldValue. Se o campo no incidente de segurança não estiver vazio, ele não será alterado. Em qualquer um dos casos, o evento e todos os campos e valores codificados nas informações adicionais são registrados em uma entrada de anotações de trabalho que descreve o evento. Se nada mudar no incidente de segurança, uma entrada de anotação de trabalho não será criada. Todos os campos em um incidente de segurança, incluindo campos personalizados adicionados à tabela, podem ser definidos.

Dados importados para alertas de segurança

Quando um evento é criado com mais dados codificados por JSON, esses dados são importados para qualquer campo com um nome que corresponda ao fieldName desse valor nos dados JSON.

Se você tiver dados no software de monitoramento de terceiros (por exemplo, Splunk) que não sejam comuns ao sistema base, poderá adicionar novos campos à tabela Alerta para acomodar a importação de dados. O formato JSON para importar dados para alertas é o mesmo formato usado para criar incidentes de segurança a partir de eventos e alertas:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

A única diferença é que os dados no campo são sempre substituídos pelo fieldValue.

Quando os dados do evento de segurança são importados, eles preenchem os campos na tabela Alerta com nomes de campo correspondentes. Se o alerta for posteriormente transformado em um incidente de segurança, os mesmos dados de informações adicionais preencherão os campos correspondentes no incidente de segurança.

Criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário

Use esse recurso para criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário.

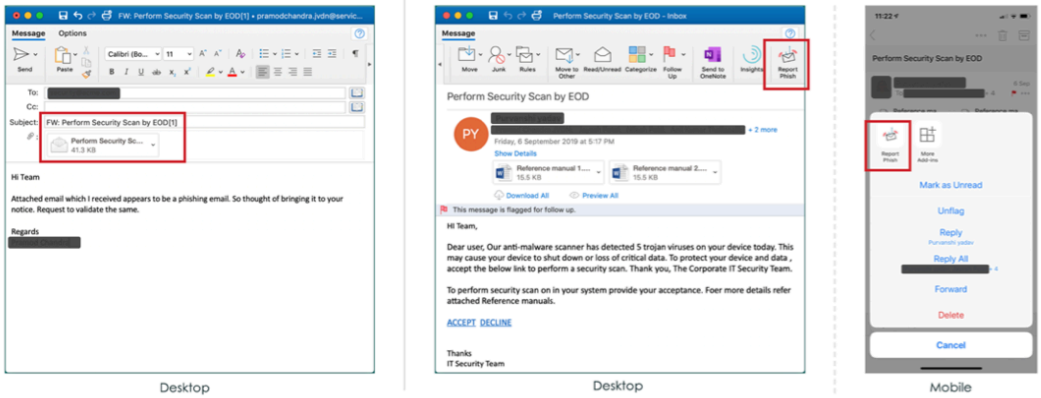
A funcionalidade aprimorada de Phishing relatado pelo usuário inclui recursos de agregação, extração de cabeçalho de e-mail e configuração.

- Os usuários podem relatar e-mails de phishing de várias maneiras:
  - Os e-mails podem ser encaminhados como anexos.
  - Se o plug-in **PhishAlarm** (anteriormente conhecido como Wombat) tiver sido configurado com o cliente Microsoft Outlook, os usuários poderão:

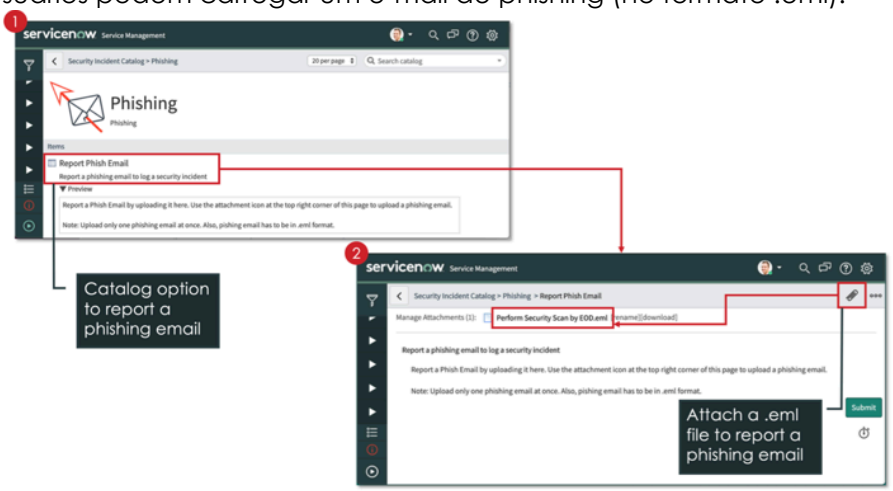
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Clicar no botão **Relatar phishing**.
- Encaminhar e-mails de phishing de um dispositivo móvel usando a opção **Relatar phishing**.



  - Os usuários podem carregar um e-mail de phishing (no formato .eml).



- O phishing relatado pelo usuário inclui **lógica de negócios de agregação** que identifica e-mails de phishing duplicados relatados por usuários em uma organização. Os usuários podem usar este recurso para:
  - Agregar incidentes de phishing relatados pelo usuário duplicados ou semelhantes (campanhas de phishing iniciadas pela empresa).
  - Evite fazer a triagem de incidentes de phishing relatados pelo usuário duplicados e reduza o esforço manual envolvido na consolidação de incidentes.
  - Permita que os analistas de segurança trabalhem em um único incidente de phishing relatado pelo usuário.
- Fornece cabeçalhos de e-mail de phishing no incidente de phishing relatado pelo usuário.
  - Os analistas de segurança podem verificar as principais informações do cabeçalho de e-mail no incidente.
  - O esforço manual na coleta de informações de cabeçalho de outras fontes não é mais necessário.
- O e-mail de phishing original enviado é armazenado como um **Registro de e-mail de phishing** em uma nova tabela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os analistas de segurança podem exibir detalhes do e-mail de phishing original, como conteúdo do e-mail de phishing, cabeçalhos e origem.
- Os administradores de segurança podem configurar e fazer algumas melhorias que incluem:
  - Configurações para extrair cabeçalhos de e-mail do corpo do e-mail (envios de **relatório de phishing**).
  - Filtros para capturar cabeçalhos selecionados.
  - Configurações para lidar com a associação de incidentes primários-secundários quando registros de e-mail de phishing duplicados são identificados.
  - Configurações do Flow Designer para modificar a lógica de negócios de agregação com base nos requisitos.

Configurar regras de ingestão para phishing relatado pelo usuário

Como usuário com a função `sn_si.admin`, você pode definir regras de correspondência de e-mail para filtrar e-mails de phishing relatados pelo usuário com base em critérios específicos. Por exemplo, você pode definir uma regra em que todos os e-mails enviados diretamente ou por meio do botão Denunciar phishing para *`security@acme.com`* sejam categorizados como e-mails de phishing relatados pelo usuário. Para obter mais informações, consulte Configurar regras de ingestão para phishing relatado pelo usuário.

Definir propriedades de phishing relatadas pelo usuário

Defina as informações do cabeçalho que precisam ser capturadas dos e-mails de phishing relatados pelo usuário. Para obter mais informações, consulte Definir propriedades de phishing relatadas pelo usuário.

Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário

Os e-mails de phishing relatados pelo usuário são convertidos em incidentes de segurança com base nas regras de correspondência de e-mail que foram definidas. Para obter mais informações, consulte Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário.

Transformar e-mail de phishing em incidente de segurança

O fluxo Transformar e-mail de phishing em incidente de segurança converte ou transforma registros de e-mail de phishing em incidentes de segurança. Para obter mais informações, consulte Transformar e-mails de phishing relatados por usuários em incidentes de segurança.

Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Exiba os detalhes do registro do incidente de segurança, incluindo as Listas relacionadas, anotações de trabalho e outras informações importantes. Para obter mais informações, consulte Registros de incidentes de segurança criados a partir de registros de e-mail de phishing.

Componentes e plug-ins necessários

O recurso de phishing relatado pelo usuário disponível nesta versão é uma versão aprimorada da funcionalidade de phishing relatada pelo usuário existente disponível na

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

versão London. Consulte o tópico **Criar regras para validar ataques de phishing relatados pelo usuário** na documentação de London para obter detalhes.

Instruções importantes de instalação

Esta melhoria substitui o design de phishing relatado pelo usuário existente. O novo design inclui as seguintes atualizações:

- As ações de entrada de e-mail de **phishing relatadas pelo usuário** (Tipo = Encaminhar e Tipo = Novo) foram desabilitadas.
- Uma nova ação de entrada **Criar e-mail de phishing** agora está disponível.
- O Transformar e-mails de phishing relatados por usuários em incidentes de segurança é um novo fluxo que contém a lógica de negócios de criação e agregação de incidentes de segurança para o novo design. Você deve ativar este fluxo para que o novo design tenha efeito.
- As regras de phishing relatadas pelo usuário existentes foram preservadas durante o upgrade.

Nota: Se você usar ações de entrada de e-mail personalizadas e fluxos de trabalho personalizados para envios de phishing relatados pelo usuário, deverá revisar os designs antigos e novos quanto a funcionalidades conflitantes ou sobrepostas.

Detalhes da melhoria de phishing relatada pelo usuário: a seguir estão os detalhes da melhoria:

- Relatando o e-mail de phishing de várias maneiras: consulte Criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário para obter detalhes. O e-mail de phishing é movido para a tabela *sn_si_phishing_email*.
- Criação de registros de e-mail de phishing: se as regras de correspondência de e-mail forem atendidas (Consulte Configurar regras de ingestão para phishing relatado pelo usuário), a ação de entrada **Criar e-mail** de phishing criará um registro de e-mail de phishing. Os cabeçalhos de e-mail analisados são armazenados na tabela cm*sn_si_phishing_email_header* e associados ao e-mail de phishing como uma lista relacionada.
- Agregar registros de phishing semelhantes em um único incidente de segurança: o fluxo Transformar e-mails de phishing relatados por usuários em incidentes de segurança cria incidentes de segurança a partir dos registros de e-mail de phishing e agrega registros semelhantes em um único incidente. As condições de agregação podem ser modificadas conforme necessário neste fluxo.

Nota:

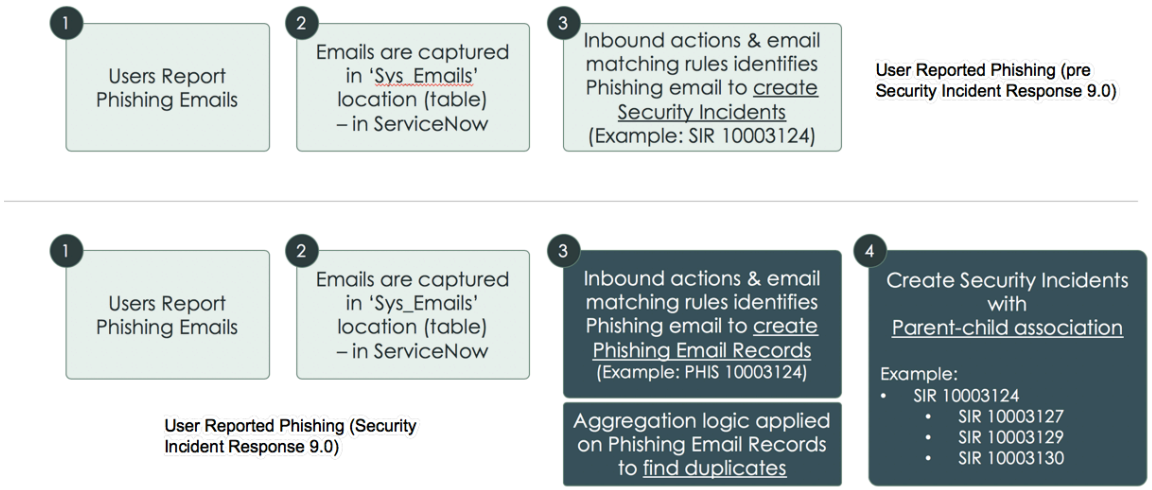
- As ações de entrada de **phishing relatadas pelo usuário** disponíveis antes da versão 9.0 do Security Incident Response agora estão desabilitadas. Os incidentes de segurança não são mais criados por meio de ações de entrada desabilitadas.
- A aplicação de spoke das Operações de segurança deve ser instalada para que o novo design tenha efeito. Isso inclui o fluxo Transformar e-mails de phishing relatados por usuários em incidentes de segurança, que está disponível em um estado inativo por padrão. Ative este fluxo para criar incidentes de segurança a partir dos registros de e-mail de phishing.

A imagem a seguir mostra as diferenças entre os designs antigos e os novos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

What Happens When User Reports A Phishing Email?



Para usar o recurso aprimorado de phishing relatado pelo usuário, os seguintes plug-ins e componentes são necessários:

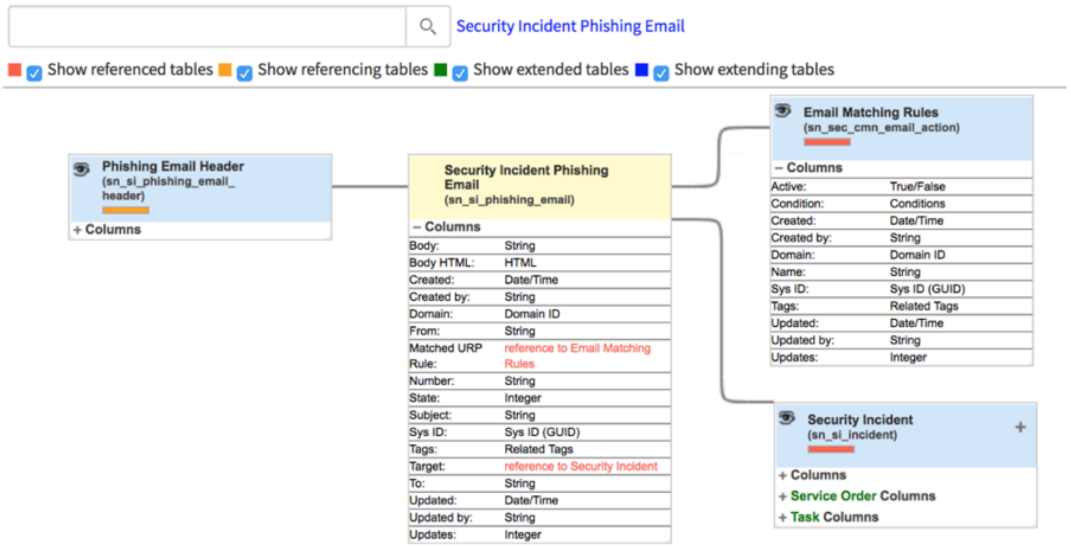
- Suporte de segurança comum (*sn_sec_cmn*): Inclui:
  - Ação de entrada
  - Novo script EmailUserReportedPhishing
  - Tabela de regras de ingestão
- Security Incident Response (sn_si): Inclui:
  - Tabela de incidentes de segurança (sn_si_incident)
  - Tabela de e-mails de phishing de segurança (sn_si_phishing_email)
  - Tabela de cabeçalhos de e-mail de phishing de segurança (sn_si_phishing_email_header)
  - Produtor de registro de carregamento de EML
- Spoke das Operações de segurança

  Fluxos e subfluxos para agregar e-mails e transformar e-mails de phishing em incidentes de segurança.

A figura a seguir mostra a tabela de novos e-mails de phishing com referências à regra de URP correspondente e ao registro de incidente de segurança de destino (sn_si_incident).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurar regras de ingestão para phishing relatado pelo usuário

Como usuário com a função `sn_si.admin`, você pode definir regras de correspondência de e-mail para filtrar e-mails de phishing relatados pelo usuário com base em critérios específicos. Por exemplo, você pode definir uma regra em que todos os e-mails enviados diretamente ou por meio do botão Denunciar phishing para *`security@acme.com`* sejam categorizados como e-mails de phishing relatados pelo usuário.

Antes de Iniciar

Função necessária: sn_si.admin

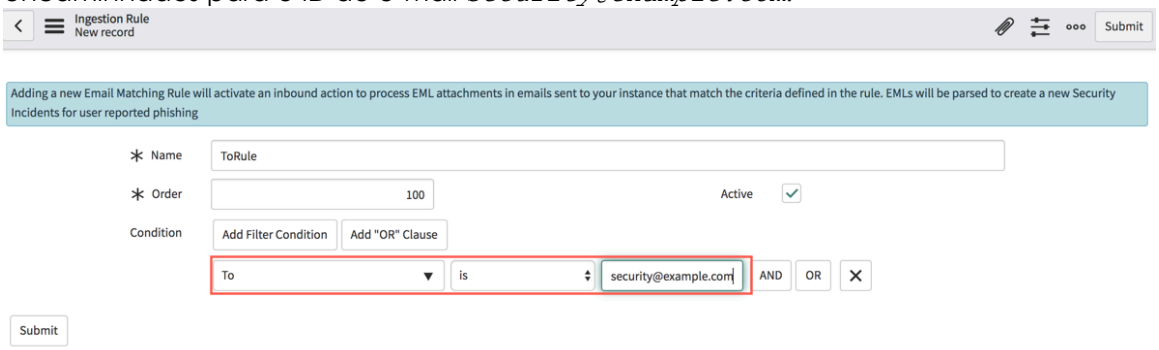
Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Processamento de E-mails** > **Regras de ingestão - Phishing reportado pelo usuário**.
2. Clique em **Novo** para criar uma nova Regra de correspondência de e-mail.
3. Insira um nome e defina uma ou mais condições para a regra.
4. Clique em **Enviar** para salvar a regra.
   A seguir estão alguns exemplos de regras:

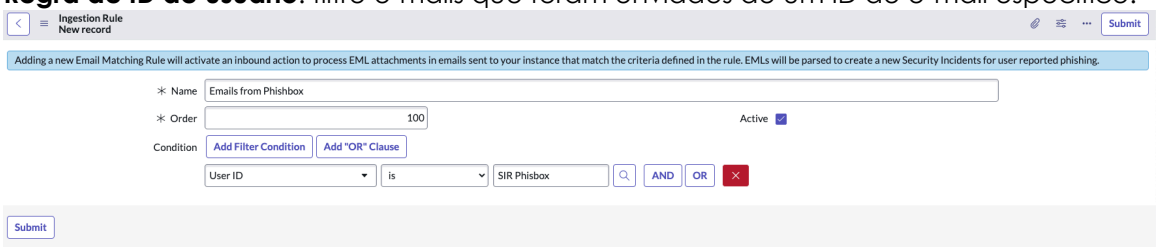
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **ToRule**: filtra e-mails que foram enviados diretamente ou encaminhados para o ID de e-mail *security@example.com*.



- **Regra de ID de usuário**: filtre e-mails que foram enviados de um ID de e-mail específico.



Definir propriedades de phishing relatadas pelo usuário

Defina as informações de cabeçalho que devem ser capturadas dos e-mails de phishing relatados pelo usuário.

Antes de Iniciar

Função necessária: sn_si.admin

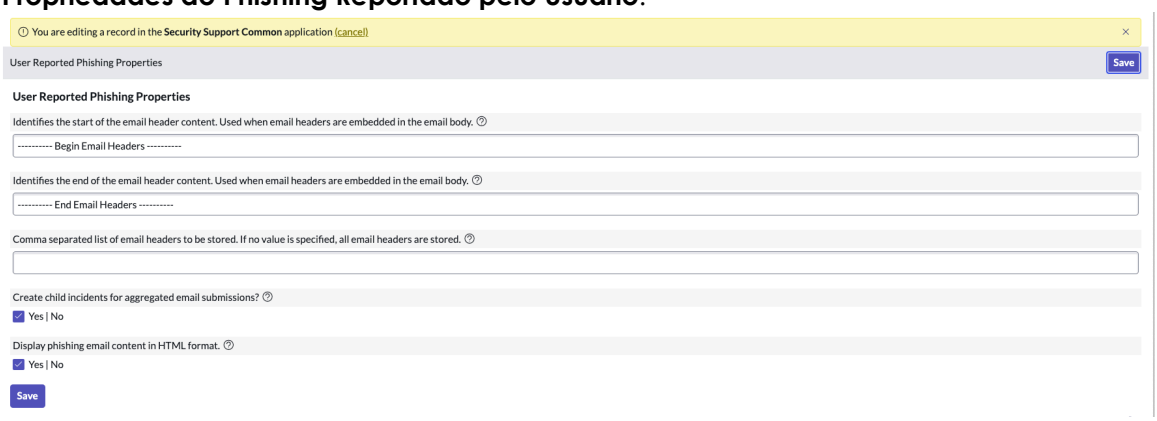
Por Que e Quando Desempenhar Esta Tarefa

Use essas opções para definir as seguintes configurações de phishing relatadas pelo usuário.

- Configuração para extrair cabeçalhos de e-mail do corpo do e-mail. (**Relatar** envios de phishing.)
- Filtrar para selecionar cabeçalhos.
- Habilite ou desabilite a associação primária-secundária.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Processamento de E-mails** > **Propriedades do Phishing Reportado pelo Usuário**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Especifique a configuração para extrair cabeçalhos de e-mail do corpo do e-mail:
   - Insira uma cadeia de caracteres que identifique o início do cabeçalho do e-mail.
   - Insira uma cadeia de caracteres que identifique o final do cabeçalho do e-mail.

   Nota: Aplique essas configurações somente a cabeçalhos capturados como parte do corpo do e-mail de phishing. Por exemplo, se o plug-in **PhishAlarm** (anteriormente conhecido como Wombat) tiver sido configurado com o cliente Microsoft Outlook, quando o usuário clicar no botão **Denunciar phishing**, os cabeçalhos de e-mail serão capturados de acordo com a configuração definida aqui. As informações do cabeçalho não serão capturadas se o e-mail de phishing for encaminhado como um anexo.

3. Especifique filtros para eliminar cabeçalhos que não são necessários para investigar o incidente de segurança.

   Insira uma lista separada por vírgulas de cabeçalhos de e-mail que devem ser capturados do e-mail de phishing relatado pelo usuário. Se você não especificar nenhum valor aqui, todas as informações do cabeçalho serão capturadas.

4. Habilite ou desabilite a associação primária-secundária.
   Por padrão, a opção **Sim** está habilitada. Selecione **Sim** para indicar que os incidentes de segurança secundários devem ser criados quando os e-mails de phishing relatados pelo usuário forem agregados. Se você selecionar **Não**, os incidentes de segurança secundários não serão criados, mas os e-mails de phishing relatados pelo usuário serão associados ao incidente de segurança e o registro do incidente de segurança será atualizado. Consulte Transformar e-mails de phishing relatados por usuários em incidentes de segurança para obter mais informações sobre como os incidentes de segurança secundários são criados.
5. Habilite ou desabilite a opção para exibir o conteúdo de e-mail de phishing no formato HTML.
   Por padrão, a opção **Sim** está habilitada. Selecione **Sim** para exibir o conteúdo do e-mail de phishing no formato HTML. Se você selecionar **Não**, o conteúdo do e-mail no formato HTML não ficará visível em um registro de phishing.

Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário

Os e-mails de phishing relatados pelo usuário são convertidos em incidentes de segurança com base nas regras de correspondência de e-mail que foram definidas.

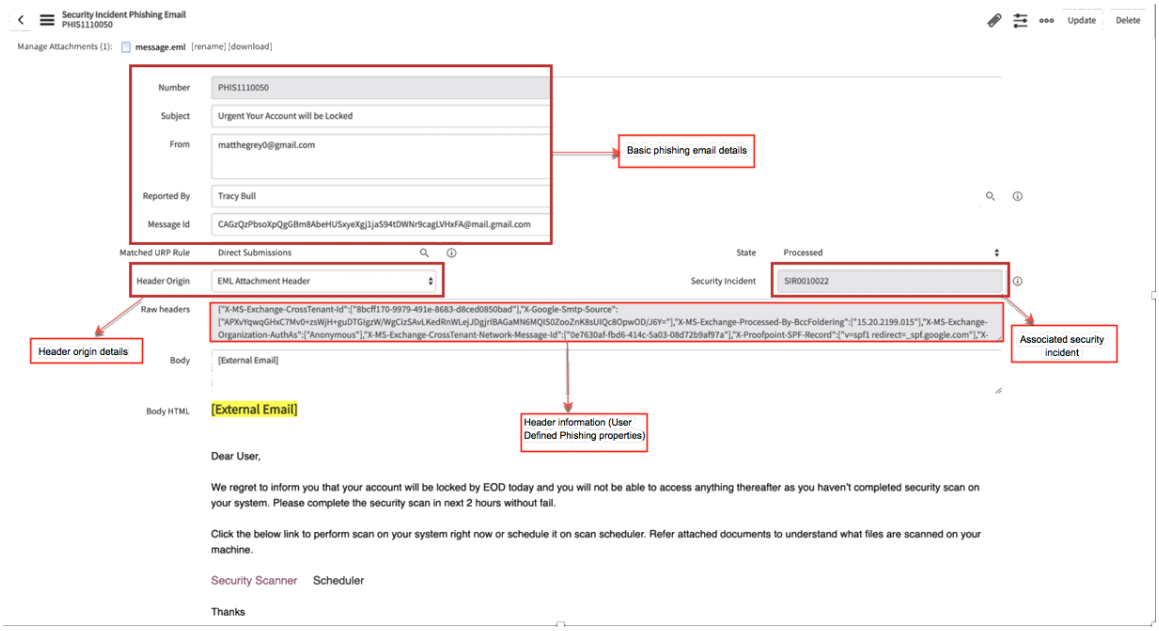
Quando um novo e-mail de phishing é relatado, as seguintes ações ocorrem:

- Um registro de e-mail é criado na tabela *sys_email*.
- A ação de entrada **Criar e-mail de phishing** é executada no registro de e-mail e usa as Regras de correspondência de e-mail (consulte Configurar regras de ingestão para phishing relatado pelo usuário) para determinar se é um e-mail de phishing.
- Quando é identificado como um e-mail de phishing, um registro de e-mail de phishing é criado na tabela `sn_si_phishing_email`.
- Por fim, o fluxo Transformar e-mails de phishing relatados por usuários em incidentes de segurança é aplicado para converter o registro de e-mail de phishing em um incidente de segurança.

Para exibir os detalhes do e-mail, navegue até **Incidente de segurança** > **Mostrar todos os e-mails de phishing**. Uma lista de registros de e-mail de phishing é exibida. Clique no link de data na coluna Criado para exibir o registro de e-mail.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



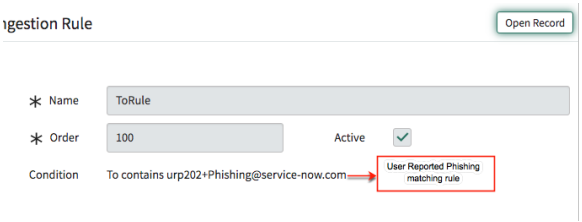
Detalhes do e-mail de phishing do incidente de segurança

Nome do Campo	Descrição
Número	O número atribuído ao e-mail de phishing relatado pelo usuário.
Assunto	O assunto do e-mail. A regra de assunto é útil em campanhas ou testes de phishing simulados. Nesse caso, as organizações enviam e-mails fraudulentos para sua própria equipe para testar sua resposta a phishing e ataques de e-mail semelhantes. Em testes de e-mail de phishing simulados, se o cliente de e-mail do Microsoft Outlook com o plug-in **PhishAlarm** (anteriormente conhecido como Wombat) estiver sendo usado, o usuário poderá clicar no botão **Denunciar** phishing para denunciar o e-mail de phishing. O e-mail é enviado para a equipe de Operações de segurança com o **phishing simulado** anexado ao assunto do e-mail. Isso é usado para identificar o e-mail como um e-mail de phishing simulado.
De	O endereço de e-mail de origem deste e-mail de phishing. Essas informações estarão disponíveis se o e-mail de phishing for encaminhado como anexo de arquivo .EML ou se os cabeçalhos originais estiverem incorporados ao e-mail. Se o usuário encaminhou o e-mail de phishing diretamente, o endereço De pode não estar disponível.
Relatado por	O ID de e-mail do usuário que denunciou este e-mail de phishing. Clique no ícone **Informações** para exibir detalhes adicionais.
ID da mensagem	O ID atribuído à mensagem.
Regra de URP correspondente	A regra de phishing relatada pelo usuário que será aplicada neste e-mail. Clique no ícone Informações para exibir detalhes adicionais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

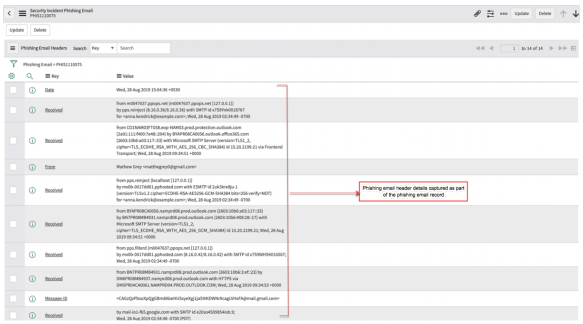
Detalhes do e-mail de phishing do incidente de segurança

Nome do Campo	Descrição
	Como você pode ver, neste exemplo, o campo **Condição** mostra que o ToRule foi aplicado neste e-mail e um incidente de segurança foi criado. Consulte Configurar regras de ingestão para phishing relatado pelo usuário para obter mais informações sobre como definir regras de correspondência de e-mail.
Estado	Quando um novo registro de e-mail de phishing é criado na tabela `sn_si_phishing_email`, o campo Estado é definido como **Novo**. Quando este registro de e-mail é convertido em um incidente de segurança (consulte Transformar e-mails de phishing relatados por usuários em incidentes de segurança), o campo Estado é atualizado para **Processado**.
Origem do cabeçalho	Este campo indica como os cabeçalhos de e-mail foram originados ou como o usuário denunciou o e-mail de phishing: • **Cabeçalho do e-mail**: o usuário encaminhou o e-mail de phishing para a equipe de operações de segurança. • **Corpo do texto do e-mail:** ◦ O usuário clicou na opção **Denunciar** phishing (se o plug-in **PhishAlarm** (anteriormente conhecido como Wombat) tiver sido configurado com o cliente de e-mail). ◦ Com base na regra de phishing relatada pelo usuário definida, o e-mail de phishing é encaminhado para a equipe de operações de segurança. • **Cabeçalho do anexo EML**: ◦ Anexo: o usuário encaminhou o e-mail como um anexo (arquivo .EML). ◦ Envio do catálogo de serviços: o usuário baixou o e-mail como um arquivo .EML para a área de trabalho e o carregou para um local especificado. O incidente de segurança é criado a partir do e-mail. • **Corpo do anexo EML**: ◦ O usuário clicou na opção **Denunciar** phishing (se o plug-in **PhishAlarm** (anteriormente conhecido como Wombat) tiver sido configurado com o cliente de e-mail). ◦ Com base na regra de phishing relatada pelo usuário definida, o e-mail de phishing é encaminhado como um anexo para a equipe de operações de segurança.
Incidente de segurança	Este campo fica em branco quando o e-mail de phishing relatado pelo usuário é relatado pela primeira vez. Quando o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes do e-mail de phishing do incidente de segurança

Nome do Campo	Descrição
	fluxo Transformar e-mails de phishing relatados por usuários em incidentes de segurança tiver sido executado, este e-mail será convertido em um registro de incidente de segurança e o número deste registro será exibido aqui.
Cabeçalhos brutos	Este campo mostra as informações completas do cabeçalho extraídas do e-mail, conforme definido na página Definir propriedades de phishing relatadas pelo usuário. Os cabeçalhos são analisados em pares de chave-valor e exibidos na lista Cabeçalhos de e-mail de phishing.
	
Corpo	Este é o corpo do e-mail de phishing relatado pelo usuário.

Transformar e-mails de phishing relatados por usuários em incidentes de segurança

O fluxo **Transformar e-mail de phishing em incidente de segurança** é um novo fluxo que converte ou transforma registros de e-mail de phishing em incidentes de segurança.

Antes de Iniciar

Nota: Para habilitar a funcionalidade de phishing relatado pelo usuário, você deve fazer uma cópia do fluxo e ativá -lo. Se você criou ações de entrada personalizadas e fluxos personalizados para lidar com envios de phishing relatados pelo usuário, as modificações de fluxo sugeridas aqui não são necessárias.

- Função necessária: sn_si.admin
- O spoke do Flow Designer deve ser instalado.

Por Que e Quando Desempenhar Esta Tarefa

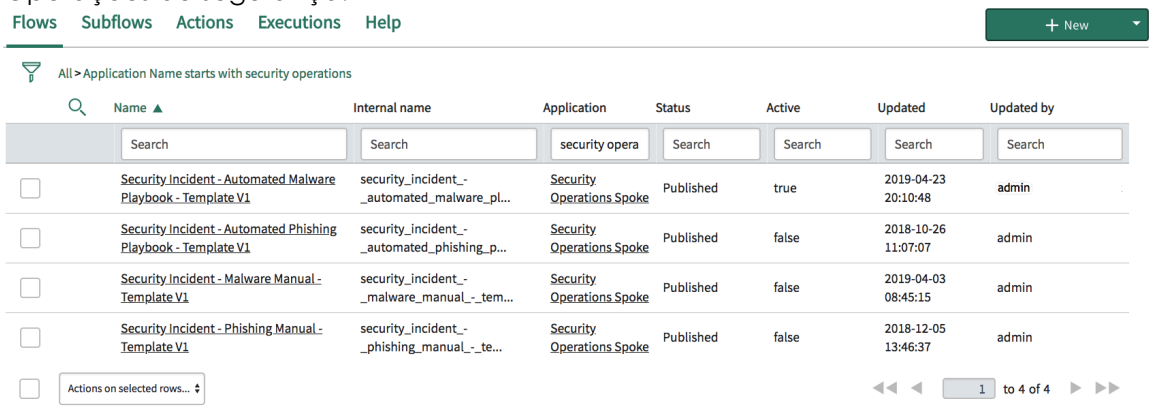
Este fluxo é iniciado automaticamente quando um registro de e-mail de phishing relatado pelo usuário com o Estado definido como **Novo** é criado. Este fluxo contém a lógica para:

- Incidentes de segurança agregados.
- Atualize os incidentes de segurança com anotações relevantes.
- Adicione dados de cabeçalho.
- Crie incidentes secundários conforme necessário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

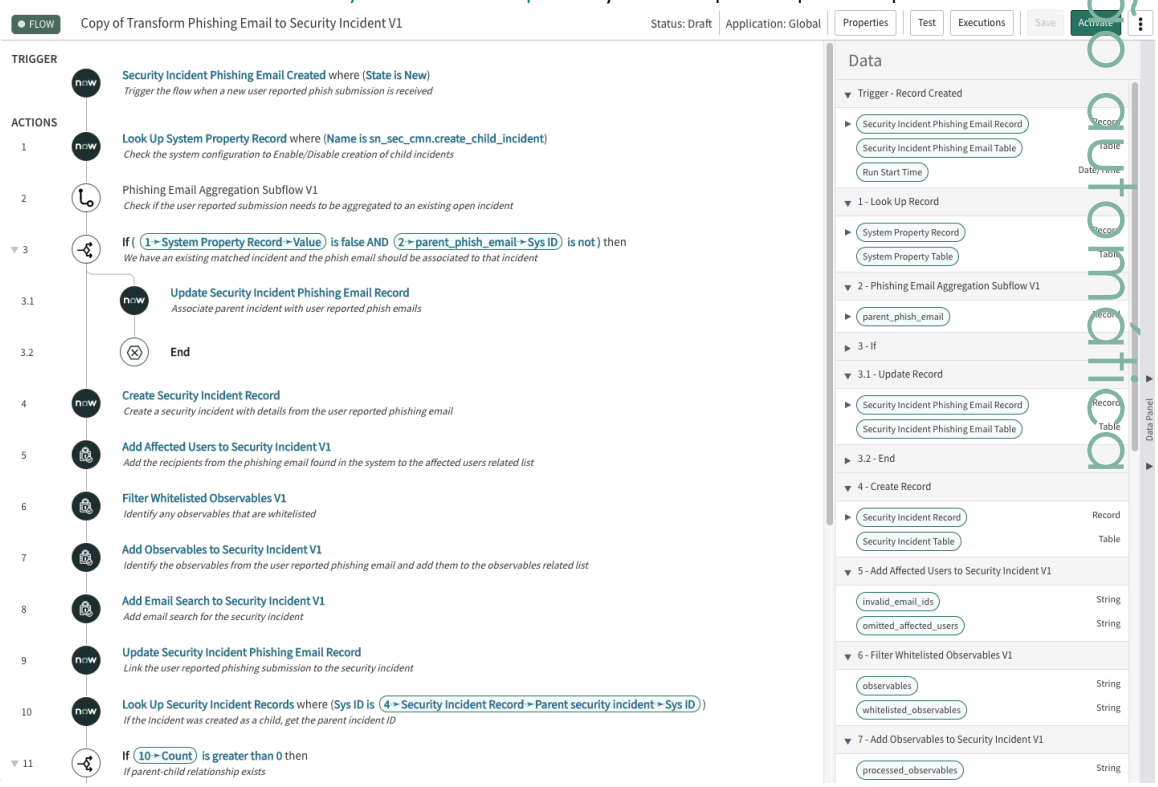
Procedimento

- Navegar até **Flow Designer** > **Designer** para exibir os fluxos disponíveis com o spoke das Operações de segurança.



- Clique no link **Transformar e-mail de phishing em incidentes de segurança** para exibir o fluxo.
- Este fluxo é fornecido com o sistema de base e está no modo **Somente leitura** e não pode ser usado.

  Clique no ícone mais ícone , faça uma cópia do fluxo e abra-o para uso. Agora você pode fazer mudanças no fluxo, como modificar condições ou ações do gatilho, ou adicionar e remover ações. Depois de fazer as mudanças necessárias, você deve ativar (Consulte Ativar um fluxo Security Incident Response) o fluxo para que ele possa ser executado.



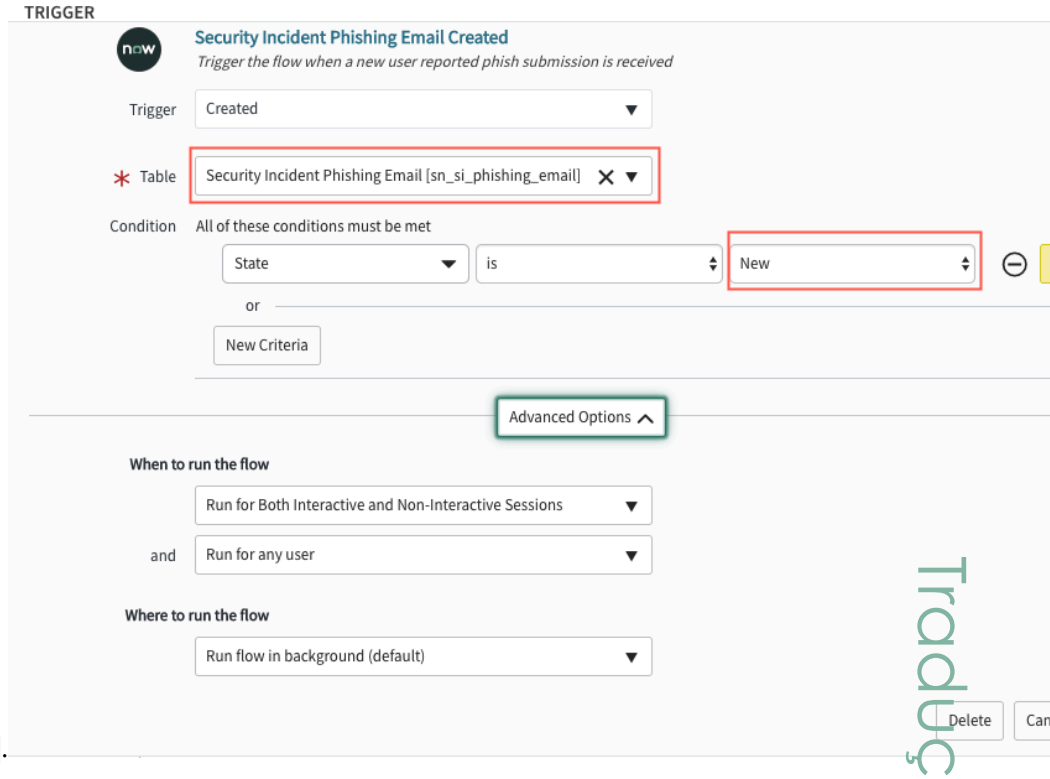
  Esta figura mostra o gatilho e as etapas executadas com o fluxo. O painel direito mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

- Clique no ícone do **gatilho**.
  Na primeira etapa, você define ou define o gatilho do fluxo. Especifique as condições para o gatilho e a tarefa a serem executadas quando as condições forem

Tradução automática

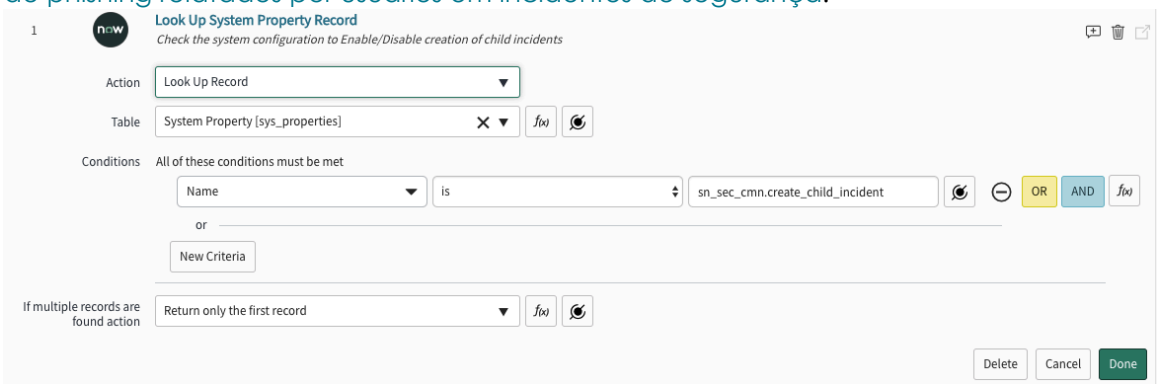
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atendidas. Este fluxo é iniciado quando um **novo** registro é carregado na tabela

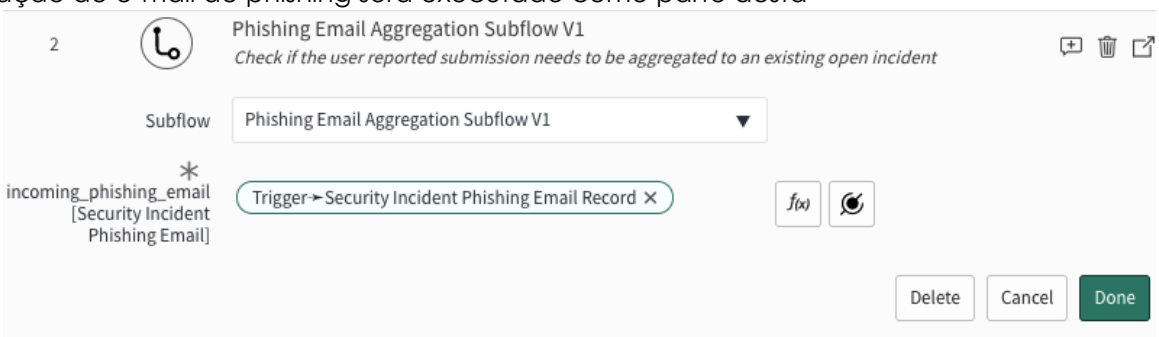


`sn_si_phishing_email`.

- Na etapa 1, o fluxo verifica se a opção **Criar incidentes secundários para envios de e-mail agregados?** O sinalizador está habilitado ou desabilitado na página Transformar e-mails de phishing relatados por usuários em incidentes de segurança.



- Na etapa 2, o incidente de segurança primário mais antigo é identificado. Observe o ícone na etapa 2. Isso indica que o subfluxo de agregação de e-mail de phishing será executado como parte desta

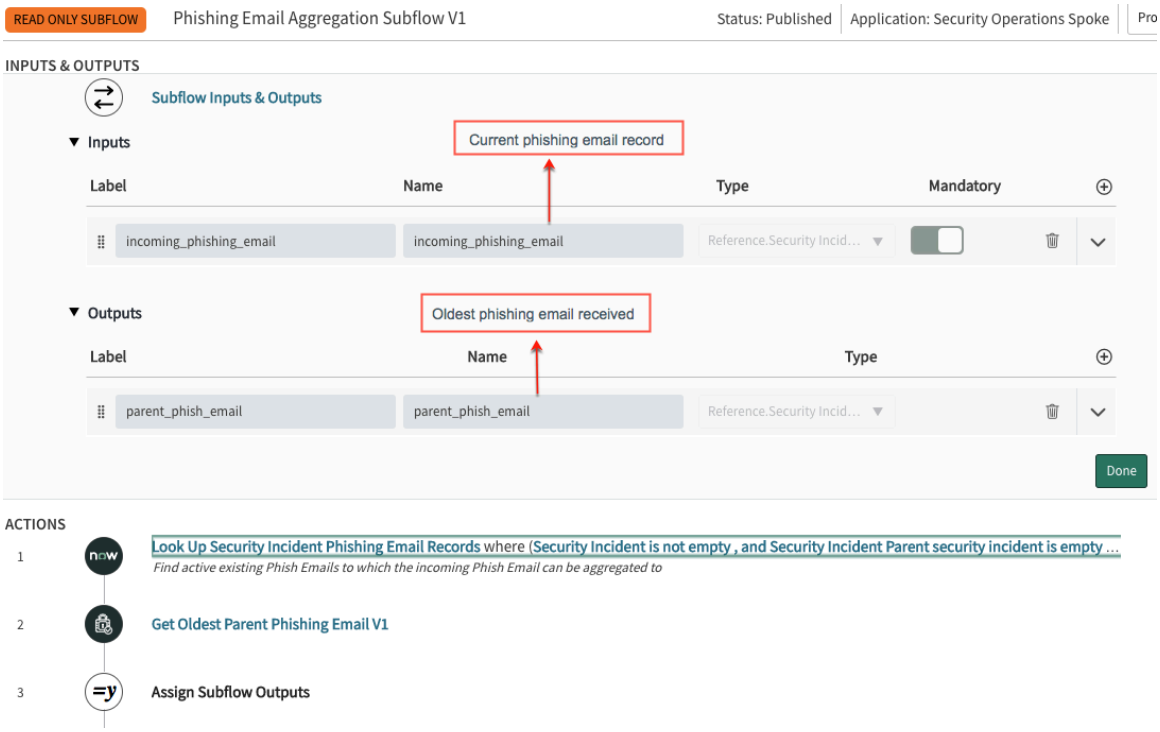


etapa.

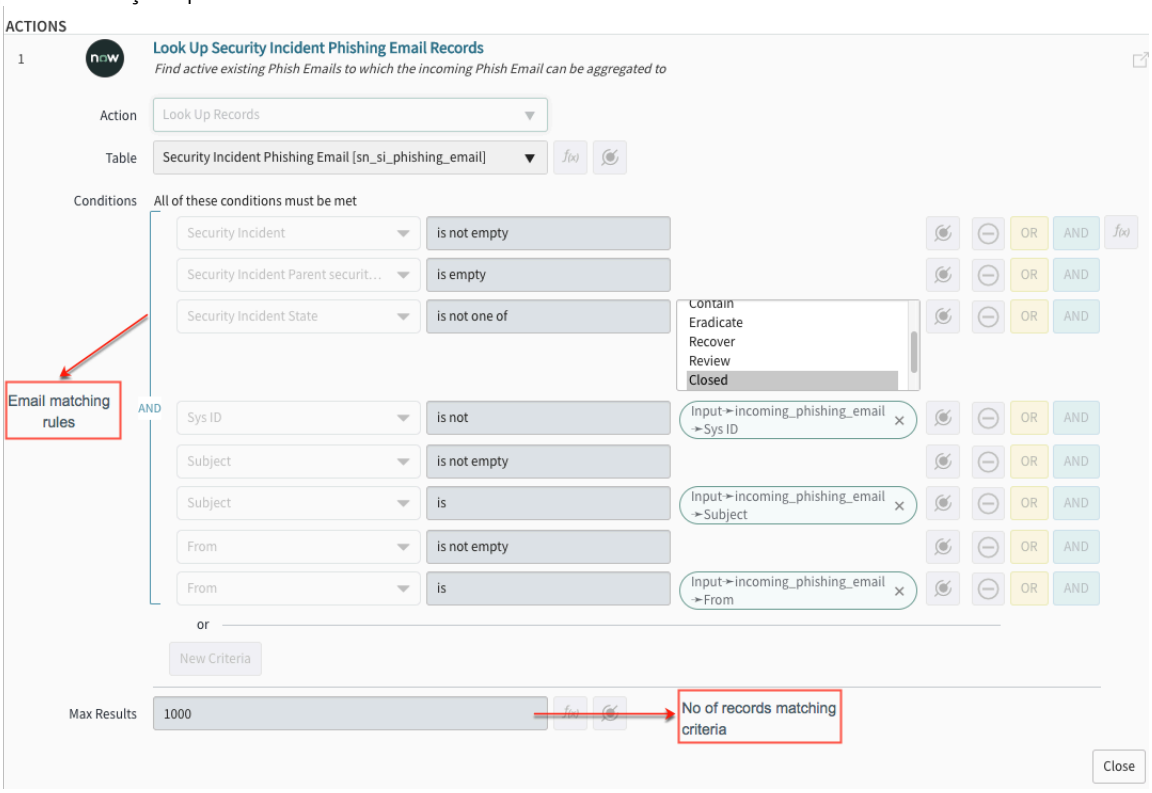
Clique no ícone do designer de ações para ter uma exibição detalhada da ação. Este subfluxo verifica o e-mail de phishing e o corresponde a um incidente de segurança existente com base nos critérios especificados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Essas duas ações são executadas quando este subfluxo é executado. Clique no link da primeira ação para exibir detalhes adicionais.



Esta ação verifica os e-mails que correspondem aos critérios do novo e-mail de entrada com base em condições como:

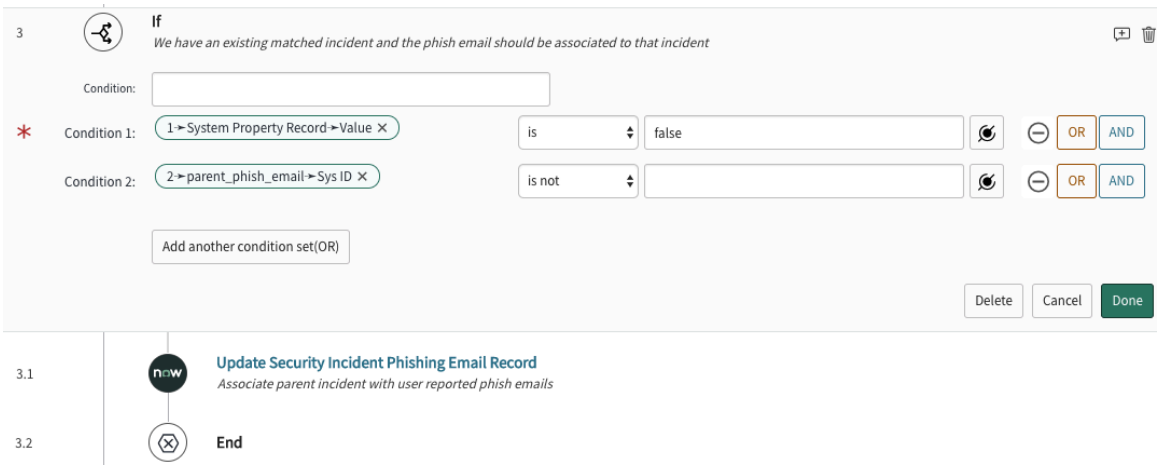
- O estado do incidente de segurança não é **Encerrado**.
- O valor de Assunto ou De corresponde às condições da regra de correspondência de e-mail definidas (consulte Configurar regras de ingestão para phishing relatado pelo usuário).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se essas condições forem atendidas, você poderá ver o número de registros que correspondem aos critérios no campo Máximo de resultados. O registro mais antigo ou o primeiro na lista é designado como o registro primário em relação ao qual os incidentes de segurança serão agregados.

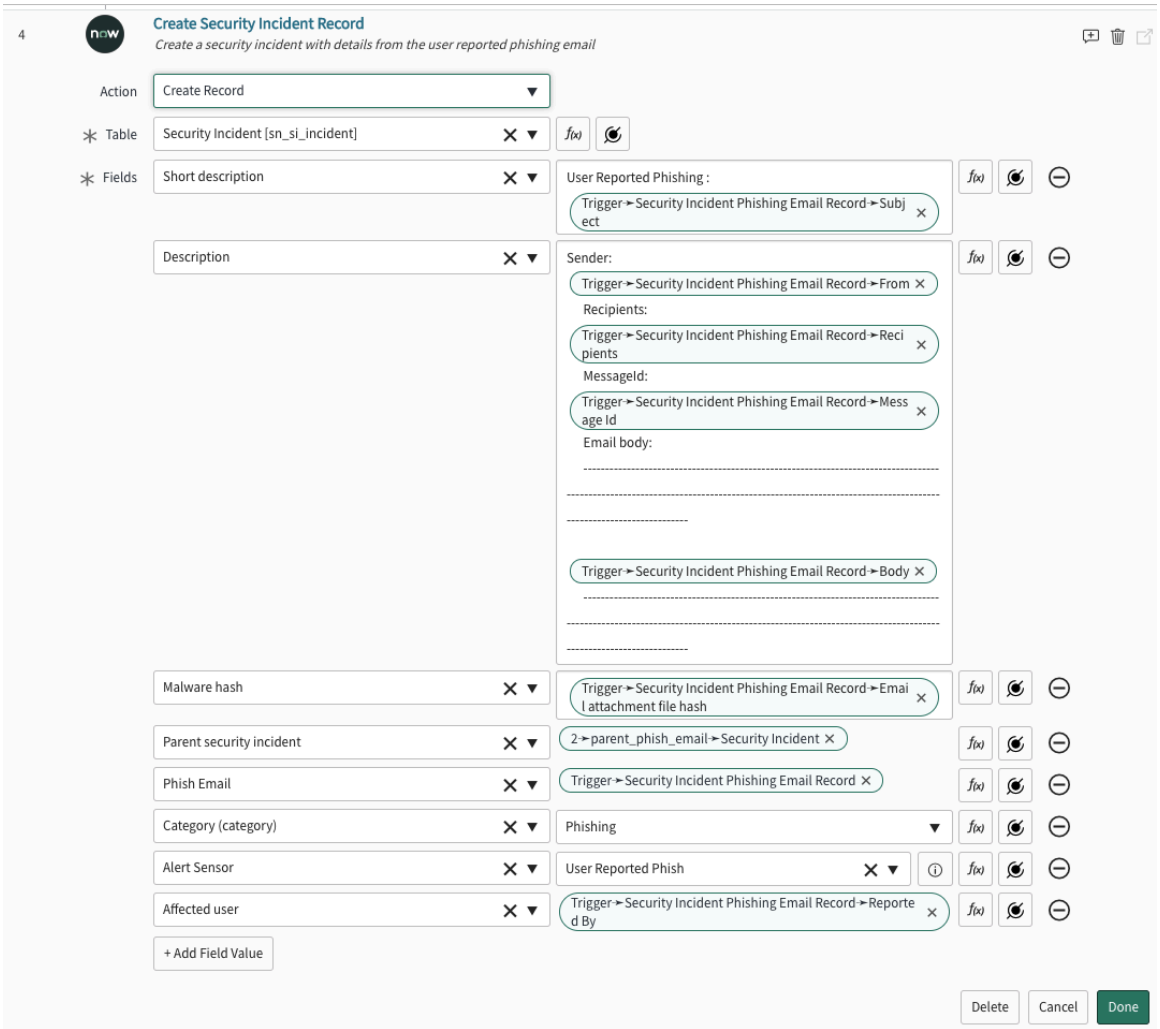
- A etapa 3 é aplicável somente se a **opção Criar incidentes secundários para envios de e-mail agregados?** O sinalizador foi definido como **Não** na página Transformar e-mails de phishing relatados por usuários em incidentes de segurança.
  Nesse caso, o e-mail de phishing é associado ao registro do incidente de segurança e o fluxo termina.



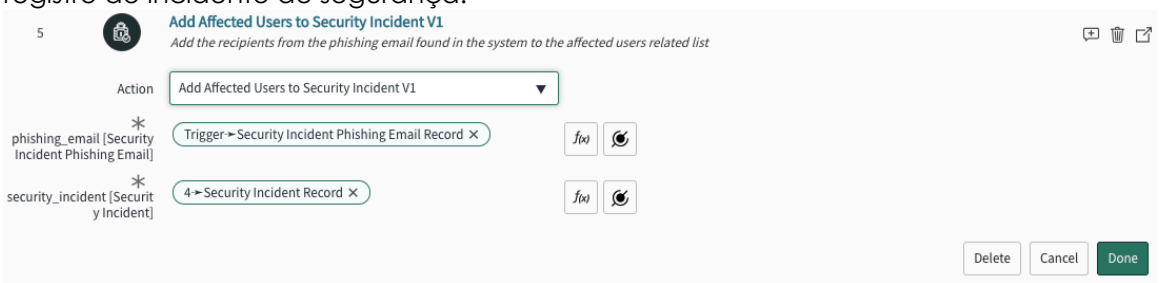
- Se a **opção Criar incidentes secundários para envios de e-mail agregados?** foi definido como **Sim**, o fluxo continuará a ser executado e um novo incidente de segurança será criado com base no e-mail de phishing relatado pelo usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



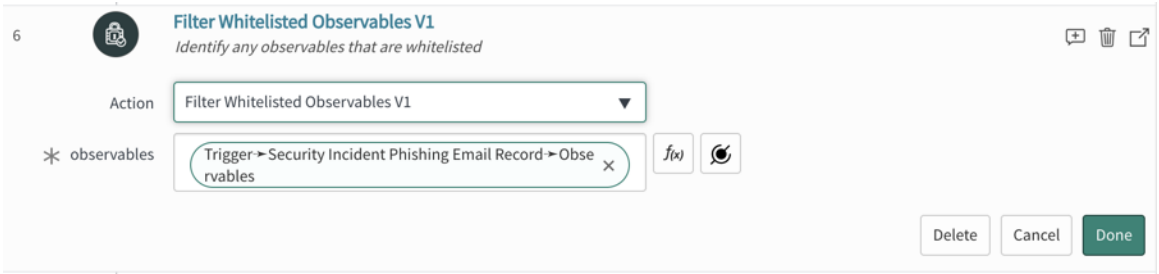
- Na etapa 5, os usuários que receberam o e-mail de phishing (funcionários nas listas Para e CC do e-mail de phishing) são adicionados à lista relacionada Usuários afetados no registro de incidente de segurança.



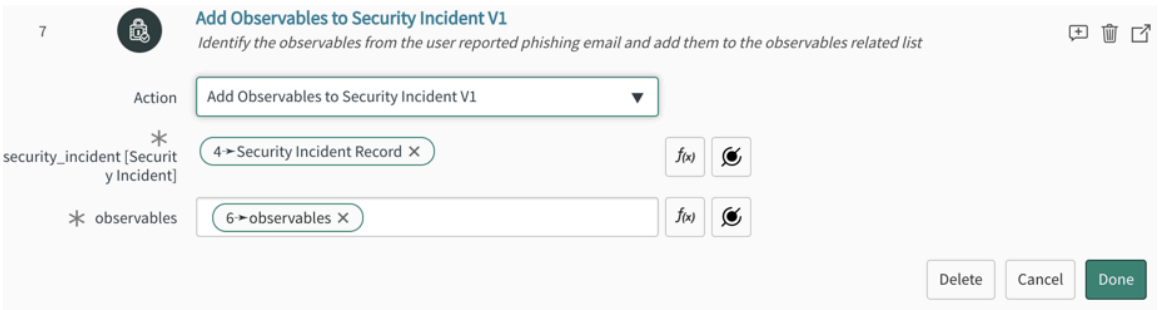
- Na etapa 6, permita que os observáveis listados sejam filtrados da lista de observáveis no incidente de segurança.
  Esses observáveis da lista de permissões não serão adicionados ao incidente de segurança.

Tradução automática

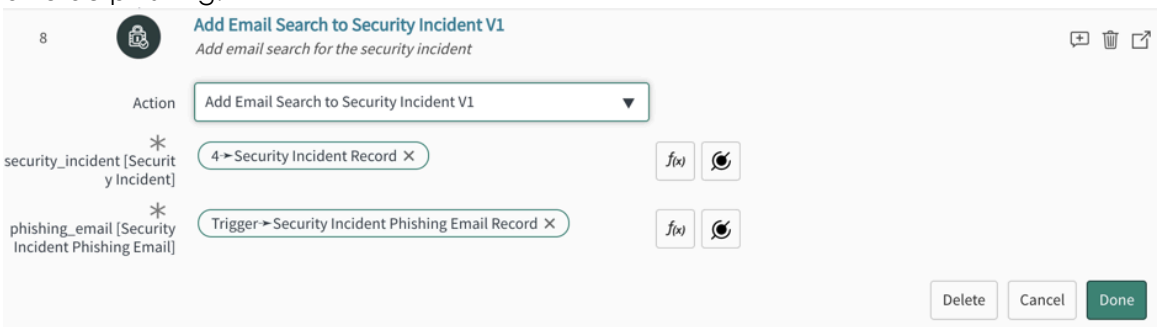
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



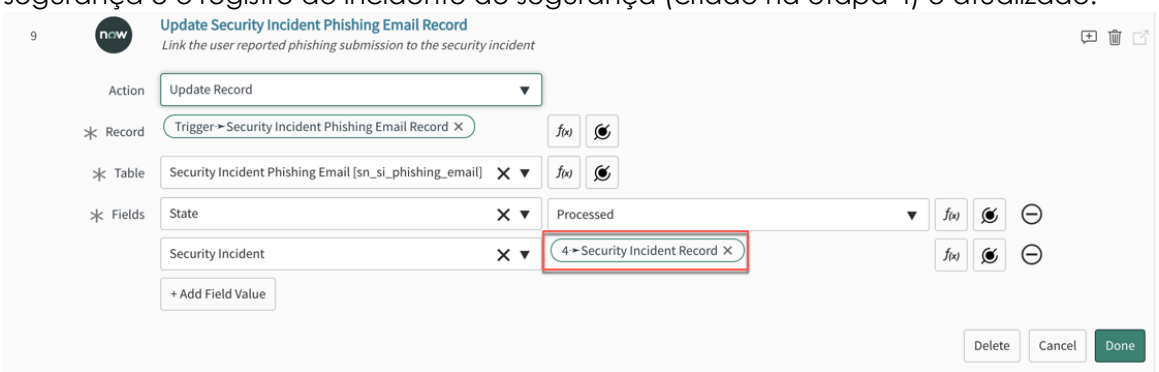
- Na etapa 7, observáveis desconhecidos do e-mail de phishing relatado pelo usuário são identificados e adicionados à lista relacionada de observáveis.



- Na etapa 8, é gerada uma consulta de pesquisa de e-mail que é uma combinação do Assunto e do endereço De do e-mail.
  Essas informações são úteis para identificar os funcionários da organização que foram alvo de phishing.



- Na etapa 9, o e-mail de phishing relatado pelo usuário é associado ao incidente de segurança e o registro do incidente de segurança (criado na etapa 4) é atualizado.

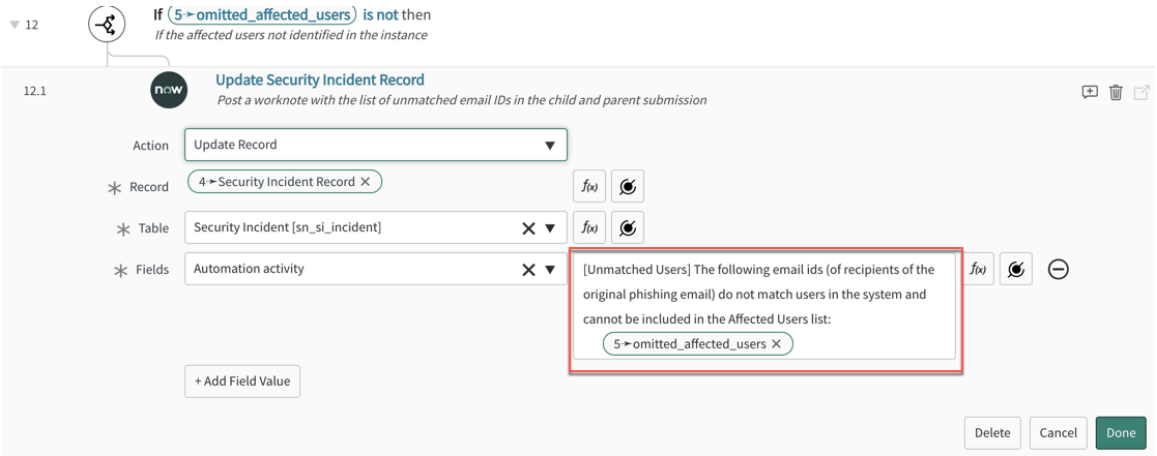


- Na etapa 10, o incidente de segurança primário é identificado e uma verificação é feita para ver se é um registro de incidente de segurança aberto.

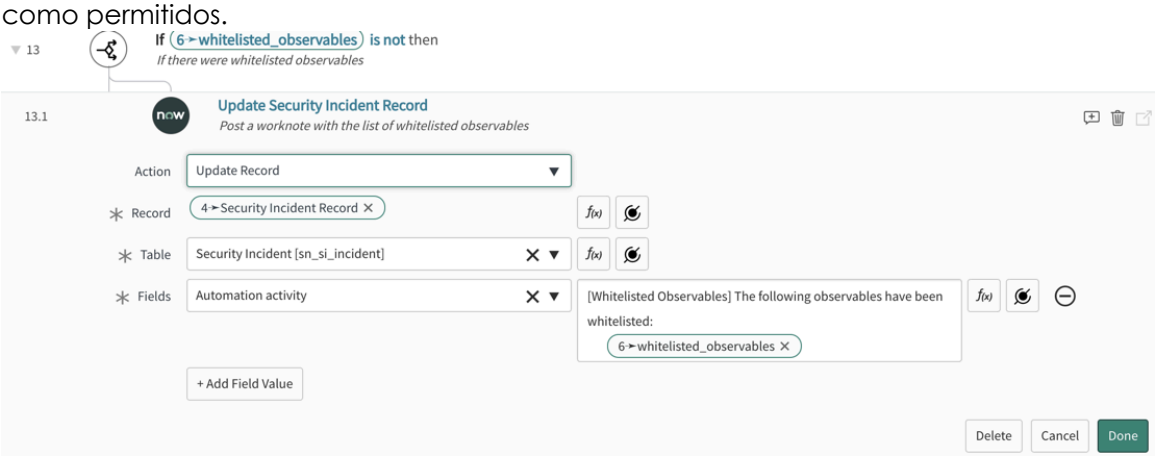
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se a segurança primária estiver ativa, anotações serão adicionadas aos registros de incidentes de segurança secundários e primários indicando como eles estão associados entre si.
- Na etapa 12, se nenhum usuário afetado for encontrado (na etapa 5 do fluxo), uma anotação de trabalho será adicionada e o registro do incidente de segurança será atualizado.



- Na etapa 13, uma anotação de trabalho é adicionada com a lista de observáveis listados como permitidos.



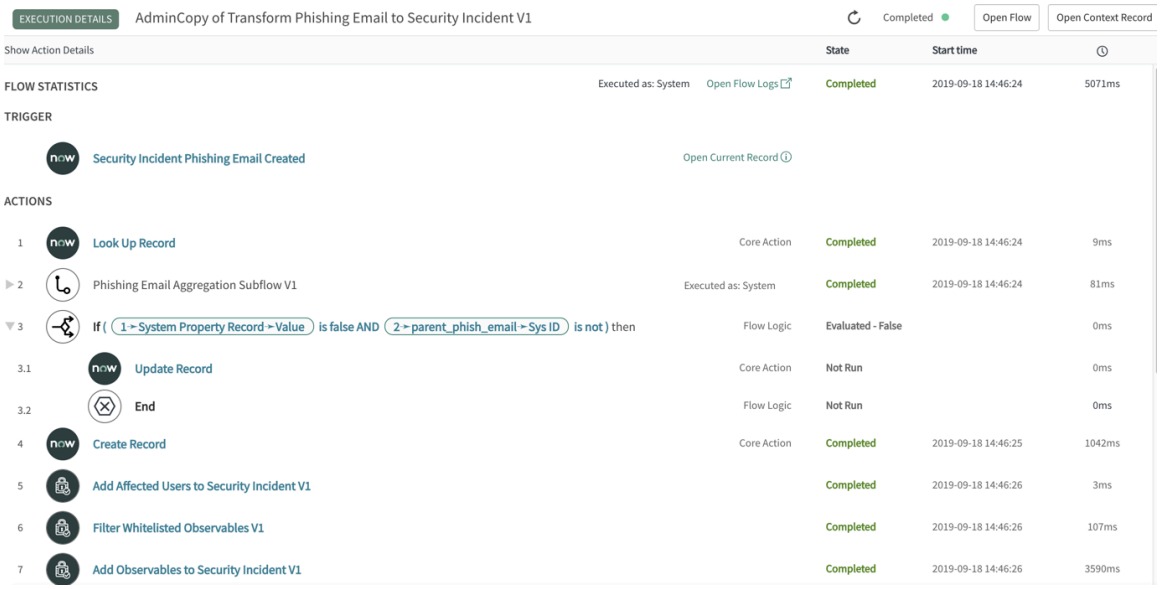
O que Fazer Depois

Você pode clicar em **Testar** para simular as ações no fluxo antes que ele seja publicado. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo para que ele possa ser executado.

Clique em **Execuções** para exibir os detalhes de execução do fluxo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

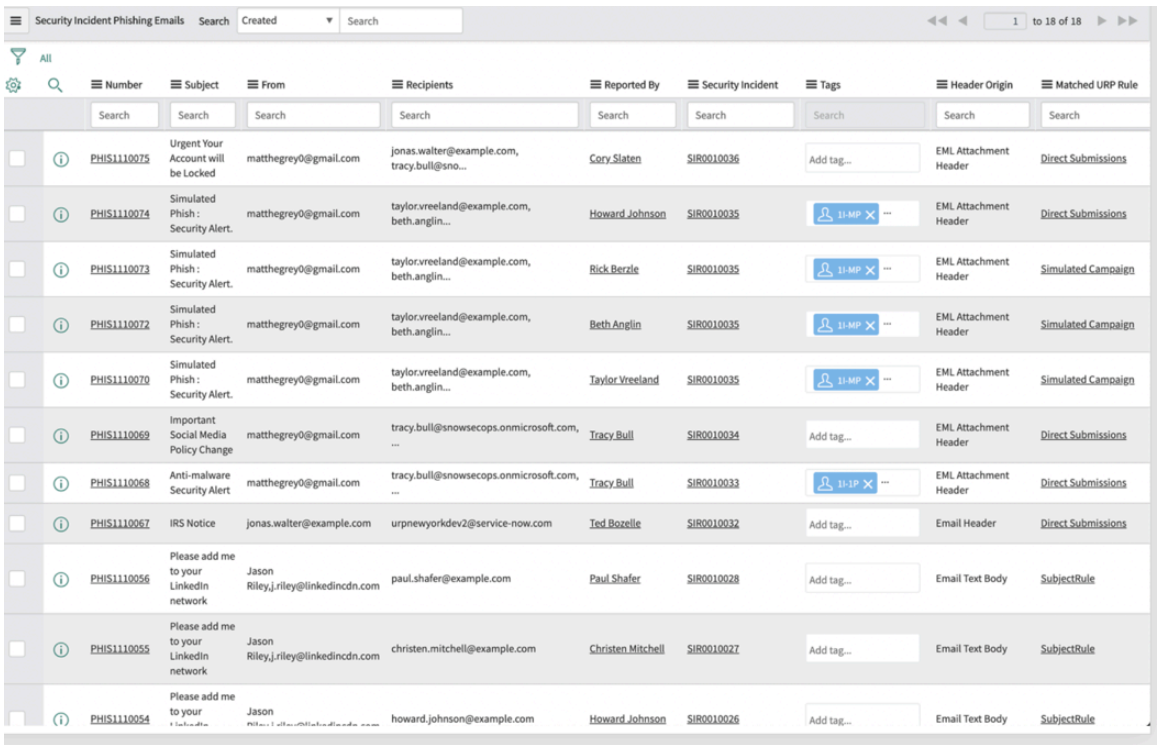


Quando o fluxo é executado, o registro de e-mail de phishing é convertido em um incidente de segurança. Veja Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Registros de e-mail de phishing armazenados na tabela *sn_si_phishing_email* são convertidos em registros de incidentes de segurança.

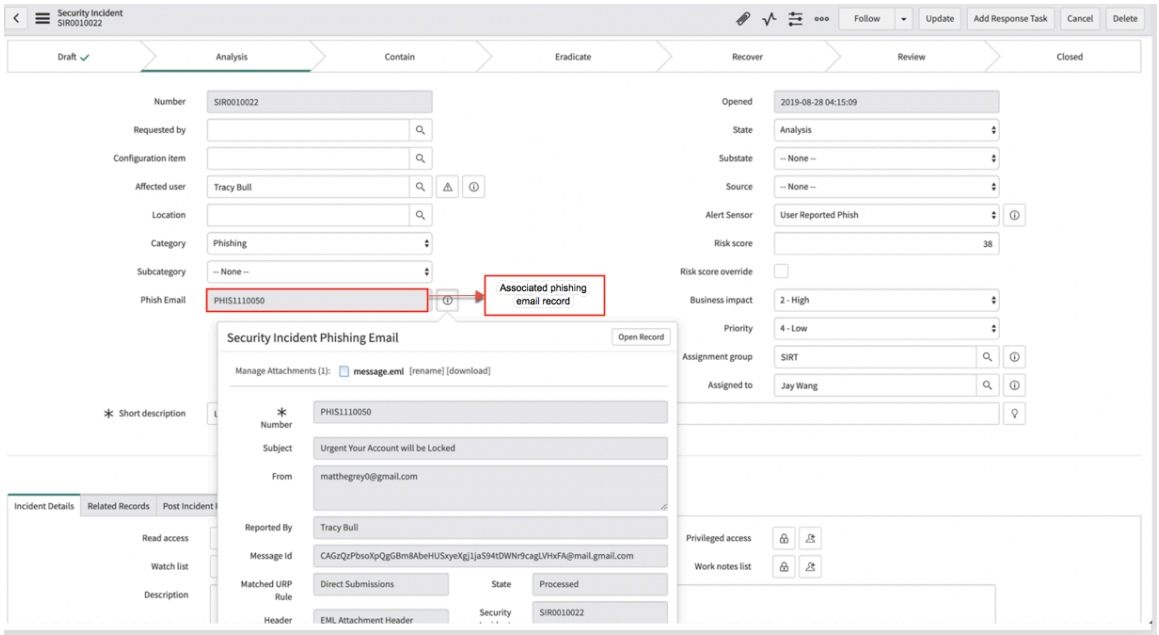
Para exibir o incidente de segurança associado ao registro de e-mail de phishing, clique em **Incidente de segurança** > **E-mail de Phishing** > **Mostrar todos os e-mails de phishing**.



Clique no link na coluna Incidente de segurança associada ao registro de e-mail de phishing. Os detalhes do incidente de segurança são exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



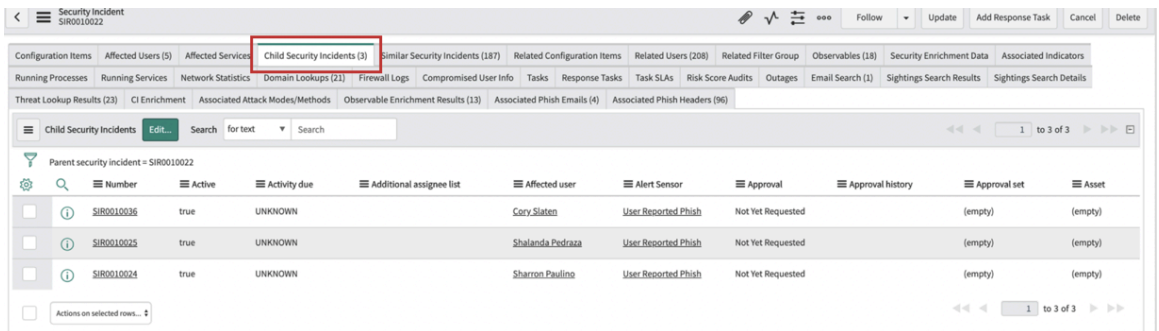
Listas relacionadas

Role para baixo até a seção Links relacionados do incidente de segurança e clique em **Mostrar tudo lista relacionada**. Exiba detalhes como incidentes de segurança secundários, usuários afetados, e-mails de phishing associados.

Incidentes de segurança secundários

Clique na guia **Incidentes de segurança secundários**. Você pode ver uma lista de incidentes de segurança secundários associados ao incidente de segurança primário com base na lógica de agregação que foi aplicada. Para cada registro secundário adicionado, uma atividade do sistema automatizada é adicionada (na seção Anotação de trabalho) ao registro primário. Isso notifica o analista de segurança sobre o registro secundário agregado.

Nota: Você pode ver os incidentes de segurança secundários aqui somente se o sinalizador **Criar incidentes secundários para envios de e-mails agregados** estiver definido como **Sim** na página Propriedades de phishing relatadas pelo usuário. Consulte Definir propriedades de phishing relatadas pelo usuário para obter detalhes.

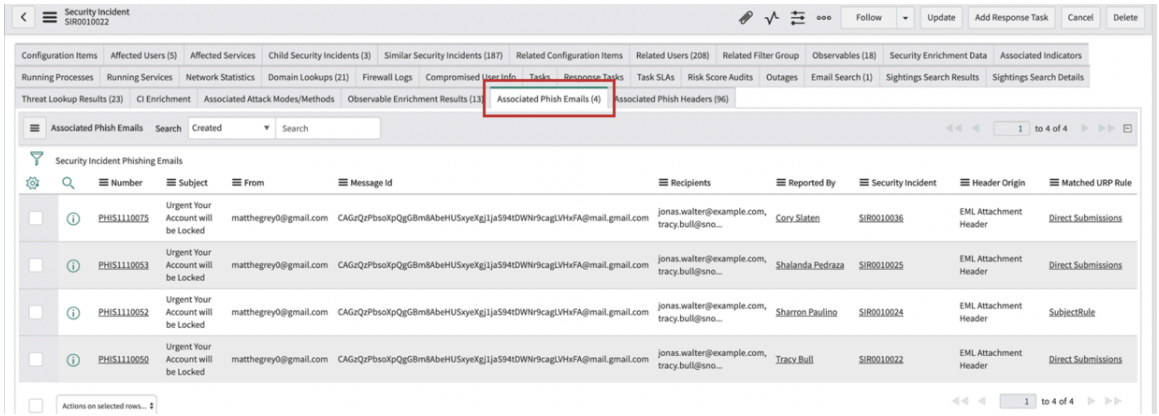


E-mails de phishing associados

Clique na guia E- **mails de phishing associados**. Você verá uma lista de registros de e-mail de phishing (registros duplicados) associados ao registro de e-mail de phishing primário.

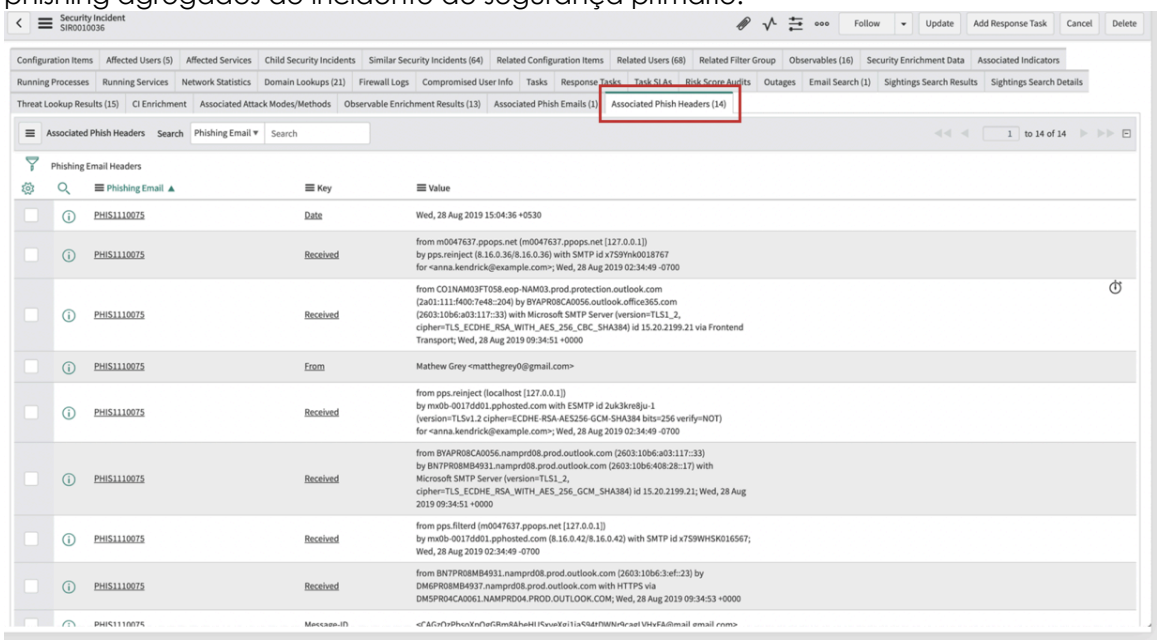
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cabeçalhos de e-mail de phishing associados

Clique na guia E- **mails de phishing associados**. Você verá os detalhes do cabeçalho do e-mail de phishing que foram capturados como parte do incidente de segurança. Você pode exibir os cabeçalhos acumulados de todos os registros secundários e registros de e-mail de phishing agregados ao incidente de segurança primário.



Observáveis da lista permitida

Enquanto o fluxo Transformar e-mails de phishing relatados por usuários em incidentes de segurança está sendo executado, você pode monitorar o status do incidente de segurança. Quando determinados observáveis são marcados como observáveis da lista de permitidos, eles não são adicionados à lista relacionada de observáveis. Ao marcar os observáveis para a lista de permissões, você pode garantir que somente os detalhes importantes sejam exibidos. Por exemplo, se www.google.com for um dos URLs que foram marcados como lista de permitidos, a seguinte mensagem do sistema será exibida. A lista de observáveis permitidos garante que somente os observáveis importantes sejam monitorados.

Capturando usuários incompatíveis

Algumas IDs de e-mail nas listas Para e CC do e-mail de phishing podem não pertencer a usuários na organização. Esses IDs de e-mail são categorizados como usuários incompatíveis e não estão incluídos na lista relacionada de usuários afetados. Uma anotação de trabalho indicando que esses são usuários incompatíveis é exibida.

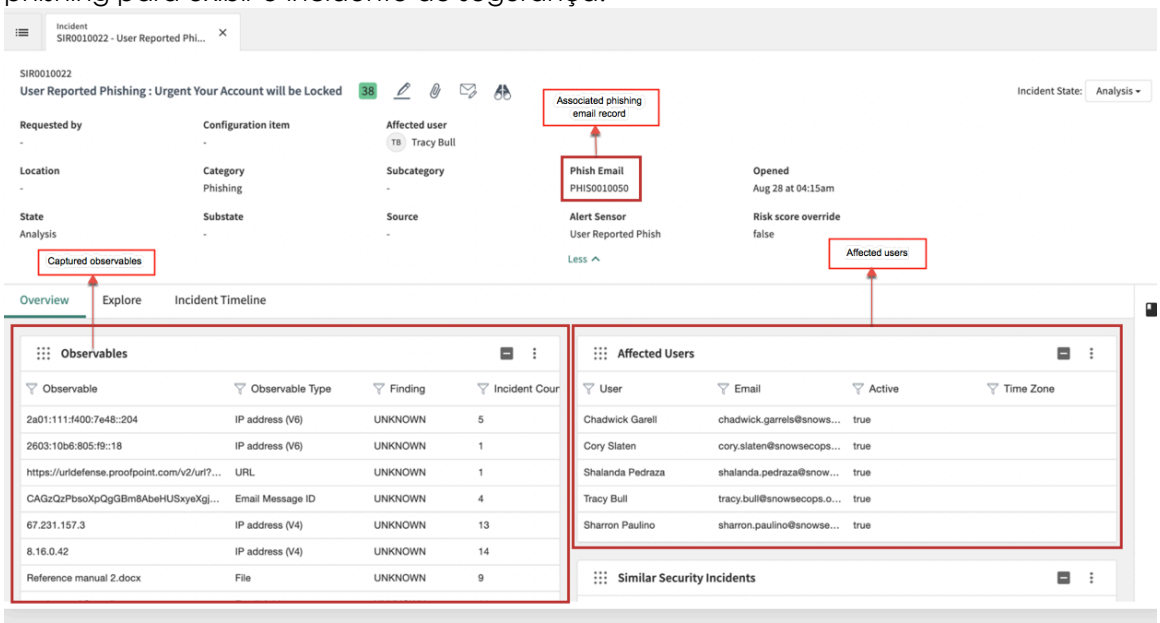
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

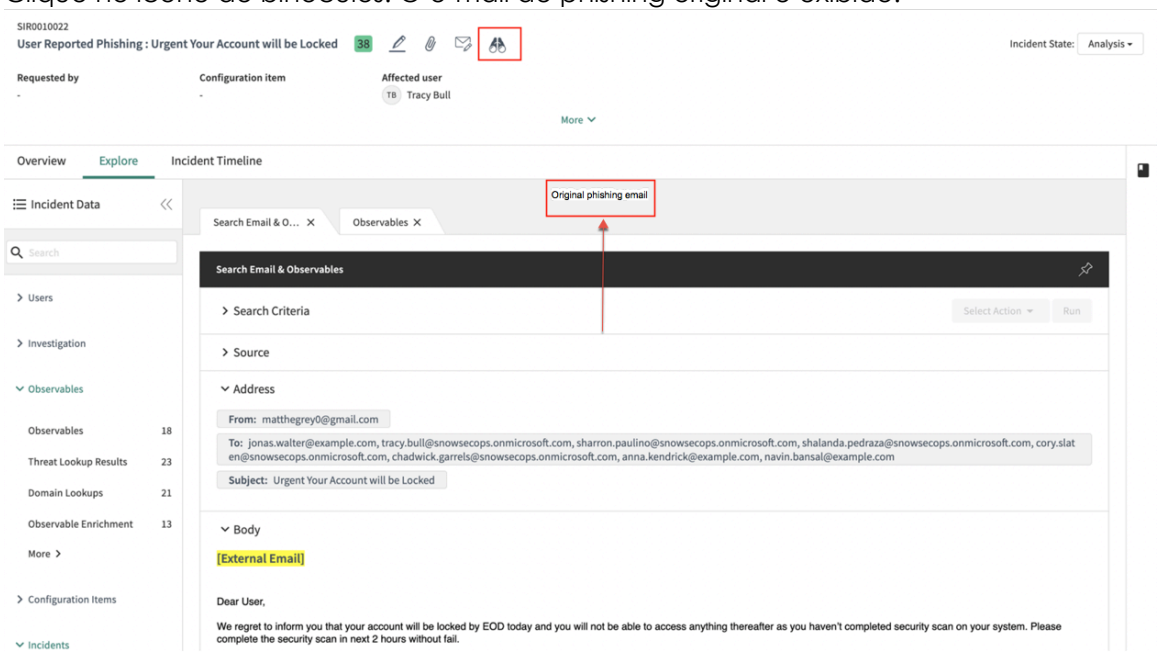
Phishing relatado pelo usuário no espaço do analista de segurança

Você pode exibir incidentes de segurança associados aos registros de e-mail de phishing no Espaço do analista de segurança.

Navegar até **Incidente de segurança** > **Nova IU**. O espaço é aberto em uma guia separada do navegador. Clique no incidente de segurança associado ao registro de e-mail de phishing para exibir o incidente de segurança.



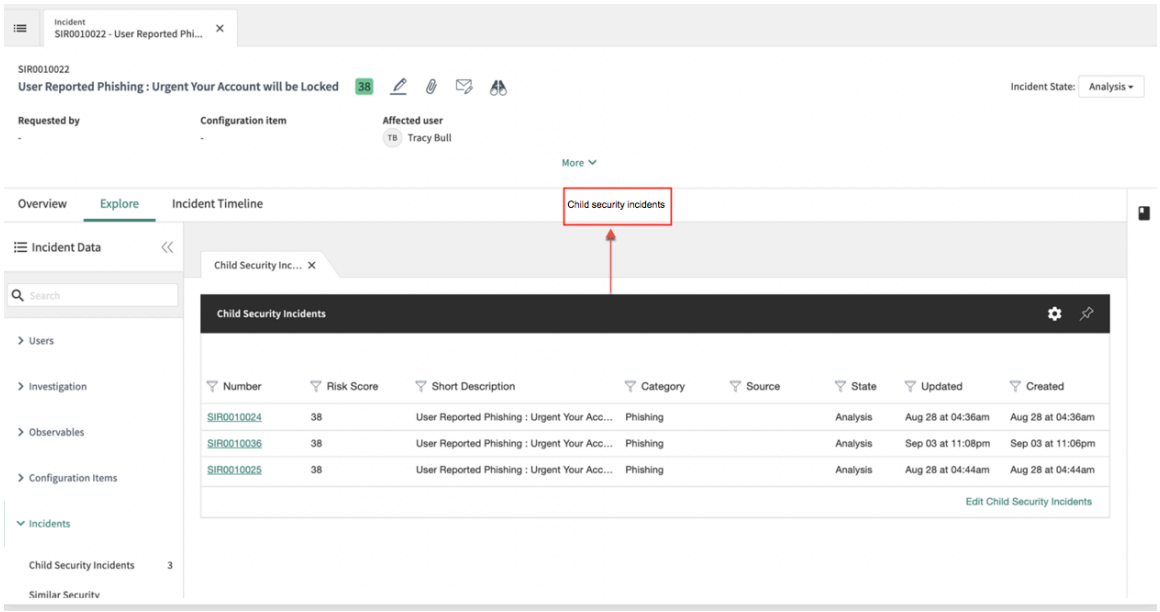
Clique no ícone de binóculos. O e-mail de phishing original é exibido.



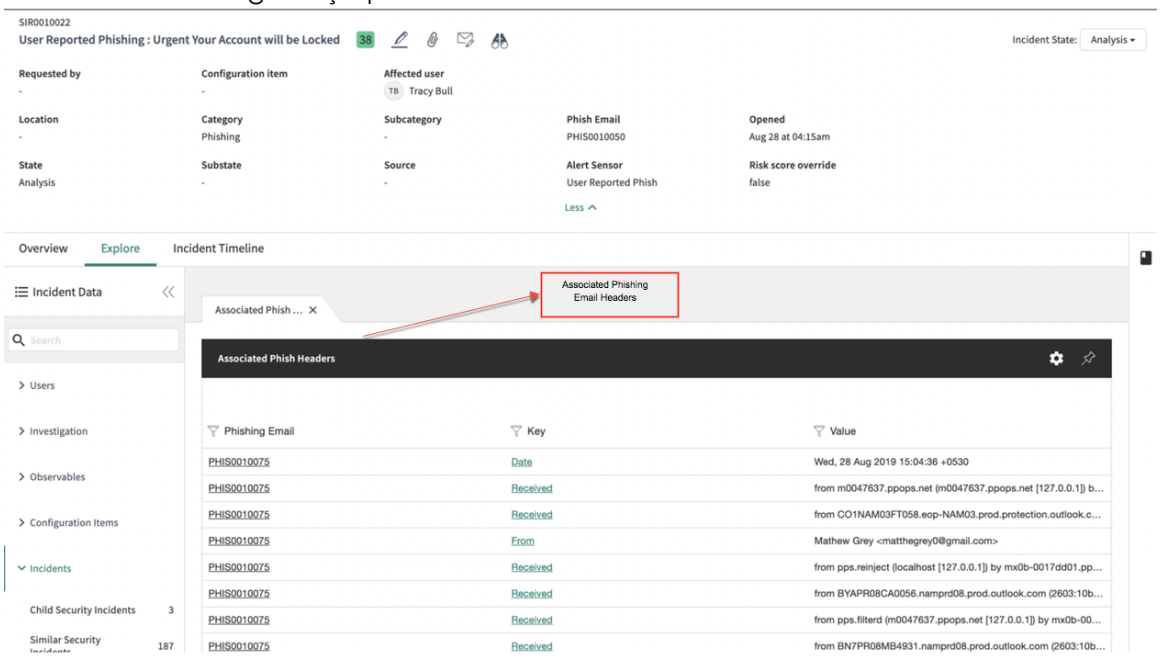
Na guia **Explorar**, clique em **Incidentes** > **Incidentes de segurança secundário**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



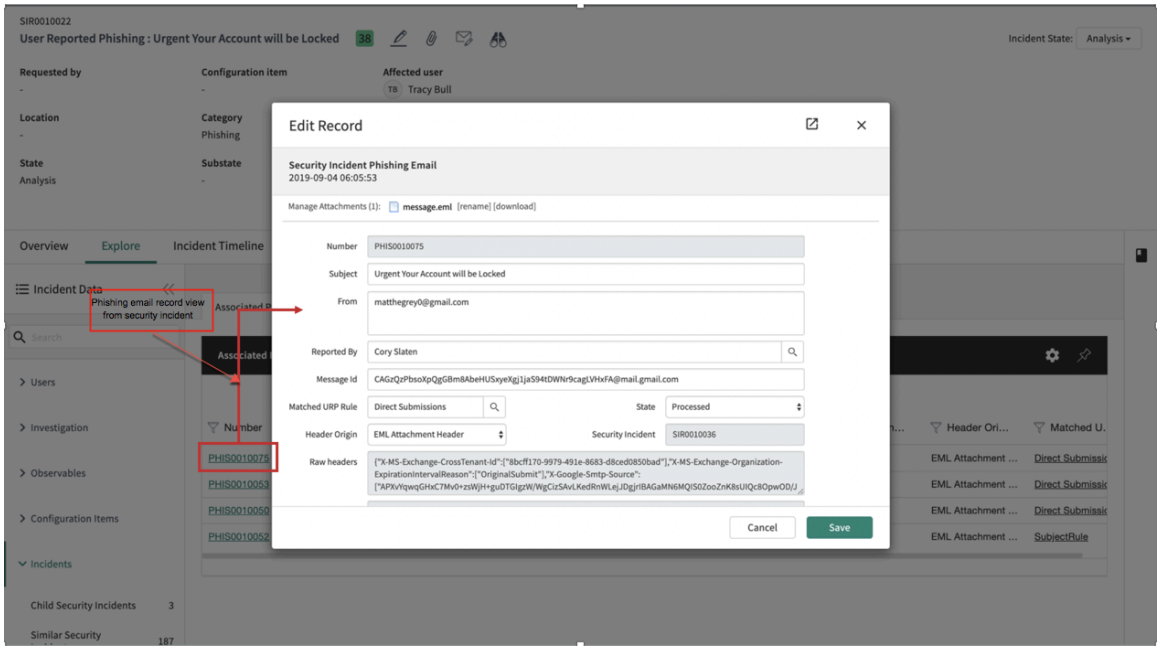
Clicar **Incidentes** > **Cabeçalhos de phishing associados** > . Você pode exibir os cabeçalhos acumulados de todos os registros secundários e registros de e-mail de phishing agregados ao incidente de segurança primário.



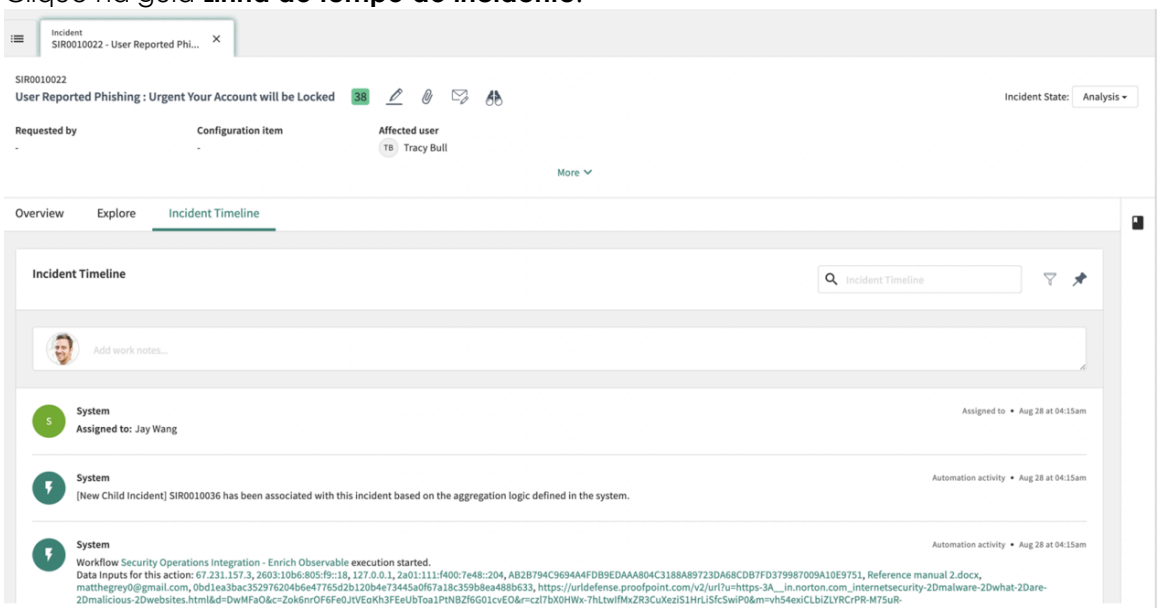
Clique no link do e-mail de phishing para exibir o registro de e-mail de phishing associado ao incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique na guia **Linha do tempo do incidente**.



Você pode exibir as atualizações do sistema que destacam:

- Registros secundários duplicados identificados.
- Observáveis da lista permitida.
- Usuários incompatíveis que receberam o e-mail de phishing, mas não pertencem à lista de Usuários afetados.

Perguntas frequentes

Esta seção aborda algumas das perguntas frequentes sobre o recurso aprimorado de Phishing relatado pelo usuário.

1. Instalei o novo spoke do Security Incident Response, mas não consigo exibir nenhum incidente de phishing relatado pelo usuário.

Por padrão, a funcionalidade de phishing relatado pelo usuário foi desabilitada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para habilitar este recurso, você deve fazer uma cópia do fluxo somente leitura Transformar e-mails de phishing relatados por usuários em incidentes de segurança e ativá-lo antes de usar.

2. Ao ingerir e-mails de phishing e convertê-los em incidentes de segurança, quais medidas de precaução são usadas para lidar com links e anexos mal-intencionados nos e-mails de phishing?

   O ServiceNow scanner antivírus verifica esses anexos e links mal-intencionados. No entanto, para garantir que os analistas de segurança possam investigar os incidentes com precisão, a aplicação Security Incident Response captura todos os artefatos que fazem parte de um e-mail de phishing. Mas a funcionalidade de phishing relatado pelo usuário silencia os links maliciosos no e-mail de phishing para que os analistas de segurança não cliquem acidentalmente nesses links. Em relação a anexos mal-intencionados, os analistas de segurança devem ter cuidado ao baixá-los.

3. Capturamos todos os arquivos mal-intencionados que fazem parte dos e-mails de phishing para aprimoramento do incidente de segurança?

   Sim, capturamos todos os arquivos dos e-mails de phishing. Você pode exibir esses detalhes que estão disponíveis como parte dos observáveis de incidentes de segurança na forma de um hash de arquivo.

4. Enviamos arquivos e links maliciosos de e-mails de phishing para uma instância de área restrita para investigação?

   Atualmente, não oferecemos suporte a integrações de área restrita prontas para uso para investigar arquivos e links mal-intencionados.

5. Há uma janela de tempo ou um gatilho que define a duração em que os registros de e-mail de phishing duplicados de entrada são associados a um incidente de segurança primário?

   Registros de e-mail de phishing duplicados são agregados somente a um incidente de segurança primário ativo. Se o incidente primário for encerrado ou cancelado, o novo e-mail de phishing duplicado de entrada será criado como um novo incidente de segurança. No entanto, neste cenário, no novo incidente de segurança, você pode exibir o incidente de segurança primário encerrado ou cancelado na lista relacionada **Incidentes de segurança semelhantes**.

   Nota: Esse comportamento pode ser configurado usando o Flow Designer.

6. O recurso de phishing de relatório de usuário oferece suporte ao uso somente do plug-in **PhishAlarm** do Microsoft Outlook (anteriormente conhecido como Wombat) para capturar detalhes do cabeçalho de e-mail?

   A funcionalidade Relatada pelo usuário foi criada para analisar cabeçalhos de e-mail e está em conformidade com os padrões RFC822. Portanto, semelhante ao plug-in **PhishAlarm** (anteriormente conhecido como Wombat), todos os outros plug-ins do Microsoft Outlook que capturam cabeçalhos de e-mail com base nos padrões RFC822 são compatíveis.

Criação de registro a partir de incidentes de segurança

Depois de criar e salvar um incidente de segurança, você pode criar um registro de solicitação de mudança (CHG), incidente (INC) ou problema (PRB) a partir dele. Você também pode criar um caso de atendimento ao cliente a partir de qualquer incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma mudança, incidente ou problema a partir de um incidente de segurança

Depois de criar e salvar um incidente de segurança, você pode criar um registro de solicitação de mudança (CHG), incidente (INC) ou problema (PRB) a partir dele.

Antes de Iniciar

Função necessária: sn.si_basic ou superior

Procedimento

1. Abra um incidente de segurança usando um desses métodos.
   - Abra um incidente de segurança existente navegando até **Incidente de segurança** > **Não atribuído** > **Incidentes**e clicando em um incidente de segurança.
   - Crie um incidente de segurança navegando até **Incidente de segurança** > **Não atribuído** > **Incidentes**, clique em **Novo**, preencha o formulário e salve o registro.
2. Clique com o botão direito do mouse na barra de cabeçalho do incidente de segurança e clique em uma das seguintes opções:
   - **Criar Mudança**
   - **Criar incidente**
   - **Criar problema**

   Nota: Esta opção se aplica somente se a propriedade pop-up (sn_vul.popup) estiver habilitada. Quando você clica em um desses botões, uma janela de visualização é aberta para mostrar as informações do incidente de segurança que são usadas para criar a mudança, o incidente ou o problema. Ou seja, o item de configuração, sua localização, sua prioridade e as descrições curta e longa. Se você estiver criando uma solicitação de mudança, poderá editar os campos **Prioridade**, **Descrição resumida**e **Descrição**. Se você estiver criando um incidente, poderá editar os campos **Impacto**, **Urgência**, **Descrição resumida** e **Descrição**. Os campos na tela do incidente de segurança associado não são afetados.
3. Clique em **Enviar** para criar a mudança, o incidente ou o problema.

Criar um caso de Atendimento ao cliente a partir de um incidente de segurança

Security Incident Response é enviado com um mapeamento de campo padrão que mapeia um incidente de segurança para um caso Atendimento ao cliente (CS). Você pode criar um caso de CS a partir de qualquer incidente de segurança, editar a **Prioridade**e também adicionar **Anotações opcionais**.

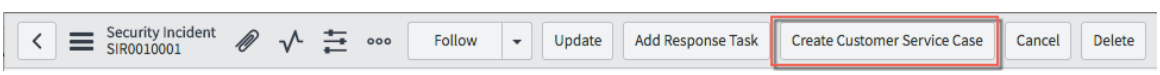
Antes de Iniciar

Função necessária: sn_si.basic e sn_customerservice_agent

Nota: O plug-in Atendimento ao cliente deve ser ativado para executar esta tarefa.

Procedimento

1. Navegue até **Incidente de segurança**.
2. Abra o incidente de segurança ao qual você deseja adicionar um caso de CS.
3. Clique em **Criar caso de atendimento ao cliente** no cabeçalho superior.



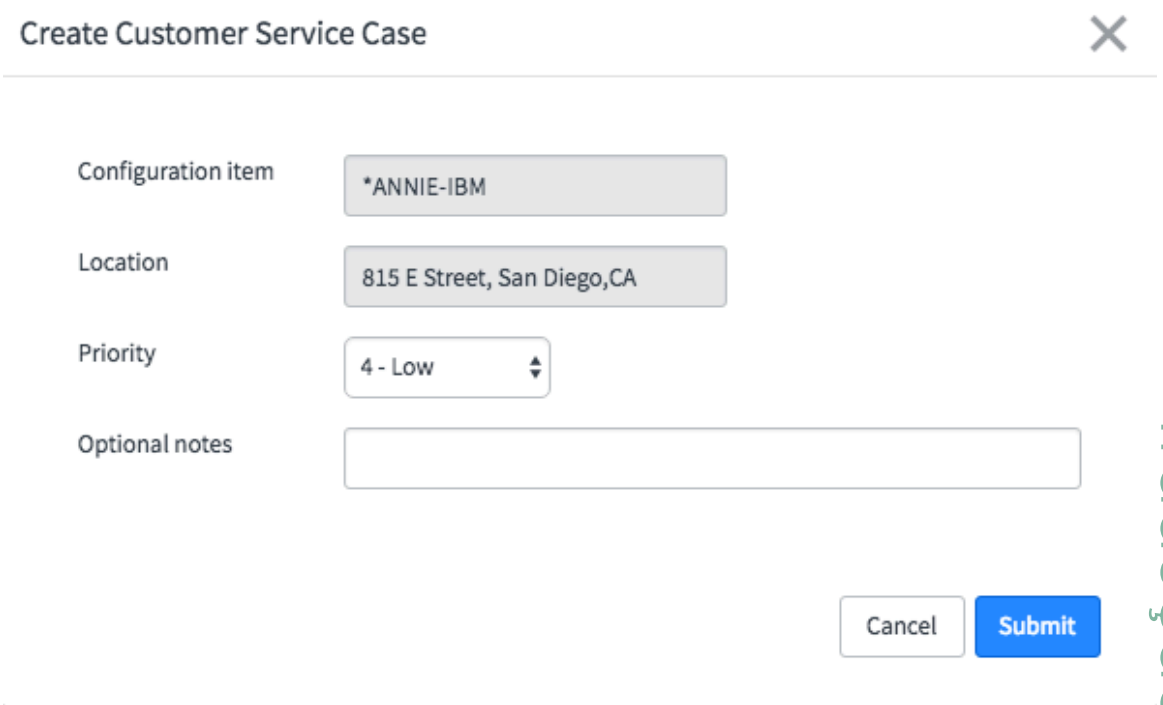
A janela pop-up é preenchida previamente com informações do incidente de segurança com base no mapeamento de campo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Você pode selecionar uma nova **Prioridade** e adicionar **Anotações opcionais**.

   Nota: O campo **Prioridade** substitui a configuração padrão. As **Anotações opcionais** são anexadas ao incidente.



5. Clique em **Enviar**.
   Um caso de CS é criado e exibido na lista relacionada Casos do Atendimento ao cliente no incidente de segurança.
6. Você pode clicar no link do caso de CS para acompanhar o caso.

Informações relacionadas

Gestão de casos de atendimento ao cliente

Adicionar um incidente de segurança a um caso de segurança

Se você determinar que um incidente de segurança requer um nível superior de análise, adicione-o a um caso novo ou existente.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

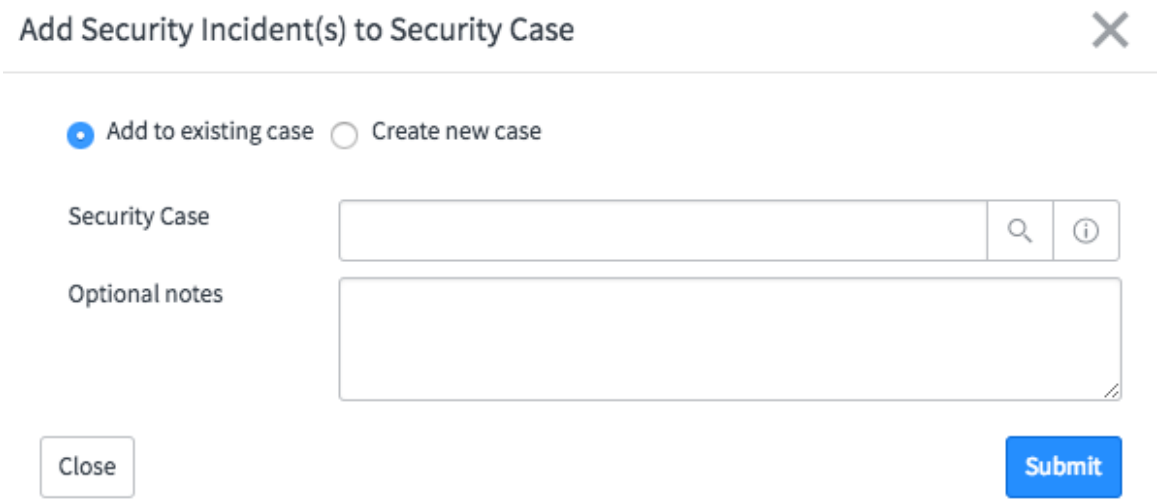
Função necessária: sn_si.admin, sn_ti.case_user_write

Procedimento

1. Navegue até o incidente de segurança que requer escalação clicando em **Incidente de segurança** > **Incidentes** > **Atribuídos a Mim**e abra o incidente de segurança.
2. Clique no link relacionado **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar incidente(s) de segurança ao caso de segurança** é aberta.

Tradução automática

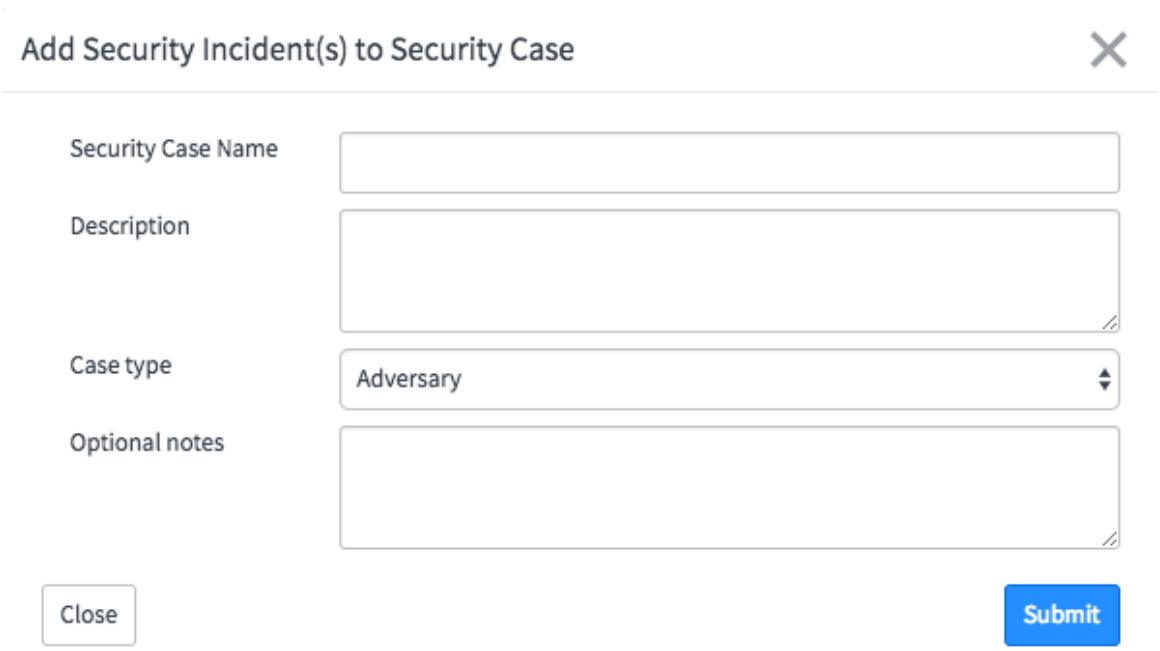
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Se você tiver um caso atribuído a você ao qual deseja adicionar este incidente de segurança, preencha os campos conforme apropriado e clique em **Enviar**.

Campo	Descrição
Caso de segurança	Selecione o caso de segurança.
Anotações opcionais	Conforme necessário, insira anotações adicionais que seriam valiosas para o analista de caso.

4. Se você tiver um ou mais casos atribuídos a você, mas quiser criar um novo caso e atribuir o incidente de segurança a ele, clique em **Criar novo caso** para mostrar os campos adicionais.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você não tiver nenhum caso atribuído a você, a tela acima será aberta primeiro.

5. Preencha os campos, se for o caso.

Campo	Descrição
Nome do caso de segurança	Insira o nome do novo caso de segurança.
Descrição	Insira uma descrição para o caso.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado.
Anotações opcionais	Conforme necessário, insira anotações adicionais que seriam valiosas para o analista de caso.

6. Clique em **Enviar**.
Uma mensagem aparece na parte superior do incidente de segurança, junto com um link para o novo caso.

Informações relacionadas

Security Case Management

Criar tarefas de resposta

Depois que um incidente de segurança foi criado, você pode criar tarefas de resposta para rastrear ações separadas a serem executadas para responder ao problema de segurança.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento

1. Navegue até o local apropriado para abrir o incidente de segurança para o qual você deseja criar tarefas.
Por exemplo:
   - Para criar uma tarefa de resposta com base em um incidente de segurança atribuído a você, selecione **Incidente de segurança** > **Incidentes** > **Atribuídos a Mim**.
   - Para criar uma tarefa de resposta com base em um incidente de segurança atribuído à sua equipe, selecione **Incidente de segurança** > **Incidentes** > **Atribuído à Equipe** > **Incidentes**.
   - Para criar uma tarefa de resposta com base em um incidente de segurança não atribuído, selecione **Incidente de segurança** > **Incidentes** > **Incidentes não atribuídos**.
2. Abra o incidente de segurança ao qual você deseja adicionar tarefas de resposta.
3. Clique no botão **Adicionar tarefa de resposta** no cabeçalho do formulário.

Nota: Para criar qualquer outra tarefa, clique na guia **Tarefas** na Lista relacionada de incidentes. Para obter mais informações sobre como criar outros tipos de tarefas, consulte Crie uma tarefa .

4. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança

Campo	Descrição
Selecione marcador de segurança	Se você configurou e ativou marcadores de segurança, poderá selecionar um ou mais marcadores para adicionar metadados ao registro ou especificar o grau de confidencialidade da tarefa de resposta. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Número	[Somente leitura] O número Security Incident Response gerado automaticamente.
Primário	[Somente leitura] O número do incidente de segurança relacionado.
Item de Configuração	O item de configuração (recurso) afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.
Prioridade	A prioridade usada para determinar quando esta tarefa é executada.
Estado	O estado atual da tarefa de resposta de segurança. Na criação da tarefa, o padrão deste campo é **Rascunho**.
Habilidades	A habilidade necessária para executar esta tarefa. Clique no ícone de cadeado e selecione a habilidade necessária. Depois de concluir suas seleções, clique no ícone de cadeado novamente.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuído a	O indivíduo atribuído para executar a tarefa.
Descrição resumida	Uma descrição da tarefa Security Incident Response.
Descrição	Uma descrição para a tarefa selecionada.
Notas de segurança	As anotações de trabalho criptografadas e não visíveis para o cliente.
Anotações de trabalho	As anotações de trabalho que não estão visíveis para o cliente.
Comentários adicionais	Comentários que você deseja que fiquem visíveis para o cliente.

5. Ao concluir suas entradas, clique em **Enviar**.

Nota: Depois de criar Security Incident Response tarefas, você pode exibi-las usando qualquer uma das aplicações a seguir no módulo **Tarefas de resposta** :

- **Atribuído a mim**.
- **Atribuído à Equipe**.
- **Mostrar tarefas em aberto**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Mostrar todas as tarefas**
- **Tarefas não atribuídas**.

Gerenciar Inteligência preditiva para phishing relatado pelo usuário

O recurso Inteligência preditiva para phishing relatado pelo usuário fornece uma solução significativa na triagem e priorização de e-mails de phishing relatados pelo usuário.

Esta seção descreve o seguinte:

- Inteligência preditiva para phishing denunciado por usuários
- Componentes e plug-ins necessários
- Geração de veredicto final para phishing relatado pelo usuário
- Solução de problemas da Inteligência preditiva para phishing relatado pelo usuário

Inteligência preditiva para phishing denunciado por usuários

Este recurso ajuda os analistas de segurança a triar e priorizar e-mails de phishing relatados pelo usuário.

A estrutura da Inteligência preditiva fornece soluções para treinar o sistema a prever, recomendar e organizar os resultados de dados. Para obter mais detalhes sobre inteligência preditiva, consulte Inteligência preditiva . Usando esta estrutura, você pode criar modelos para prever automaticamente se um e-mail de phishing relatado por um usuário é suspeito ou legítimo.

Usando dados históricos de incidentes de segurança de phishing relatados pelo usuário (cabeçalhos de e-mail, corpo de e-mail e resultados de triagem capturados por meio dos códigos de fechamento de incidentes de segurança), os analistas de segurança podem treinar o sistema para classificar os envios de phishing relatados pelo usuário de entrada como aqueles que precisam ser triados (prováveis suspeitos) e aqueles que são envios legítimos.

Ao triar e-mails de entrada automaticamente, os analistas de segurança podem priorizar facilmente a fila de incidentes e se concentrar nos incidentes que provavelmente representam um risco para a organização em primeiro lugar e gastar menos esforço em e-mails com grande probabilidade de serem falso-positivos. O resultado da previsão também fornece uma pontuação de confiança na classificação para habilitar a priorização granular.

Componentes e plug-ins necessários

Para usar a Inteligência preditiva para phishing denunciado pelo usuário, você deve instalar as seguintes aplicações

Nome do plug-in	Versão mínima
Resposta a incidentes de segurança	9.0.1 ou 10.0.2
Inteligência preditiva	Versão do Orlando
Inteligência preditiva para phishing denunciado por usuários	10.0.2

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Os novos aprimoramentos a seguir estão disponíveis com o Security Incident Response 10.4:

- A capacidade de escolher códigos de fechamento de campos personalizados para treinamento do modelo.
- A capacidade de ativar explicitamente as previsões após a criação do modelo.
- A capacidade de gerar um veredicto final sobre o envio de phishing relatado pelo usuário usando uma tabela de decisão. (requer o Spoke 10.3.0 das Operações de segurança)

Para usar os novos aprimoramentos, você deve fazer upgrade das seguintes aplicações:

Nome do plug-in	Fazer upgrade para
Resposta a incidentes de segurança	10.0.4
Inteligência preditiva para phishing denunciado por usuários	10.3.1

Tabelas novas e atualizadas

- sn_sir_ml_urp_config (Novo): contém a configuração da aplicação URP ML.
- sn_sir_ml_urp_feature (Novo): registros extraídos da tabela de e-mail sn_si_phishing.
- sn_sir_ml_urp_feature_import (Novo): usado para carregar dados históricos de e-mail de phishing.
- sn_si_incident (atualizado): os seguintes novos campos foram adicionados:
  - Previsão aceita
  - Resultado da previsão
  - Pontuação de confiança
- **Inclusões de script**
  - URPMLUtil: recupera a configuração, executa o trabalho de previsão e rastreia o processo de previsão.
  - URPMLProcessor: extrai e processa dados da tabela sn_si_phishing_email.
  - UPMLAction: executa o fluxo para aceitar o resultado da previsão.

Geração de veredicto final para phishing relatado pelo usuário

As equipes do Security Incident Response agora podem conduzir o veredicto finalizado para um registro de phishing relatado pelo usuário com base nos resultados da inteligência preditiva e integrações de enriquecimento de ameaças.

Essa geração de veredicto final é habilitada por meio de uma construção de tabela de decisão e aproveitada em um fluxo.

Pré-requisitos

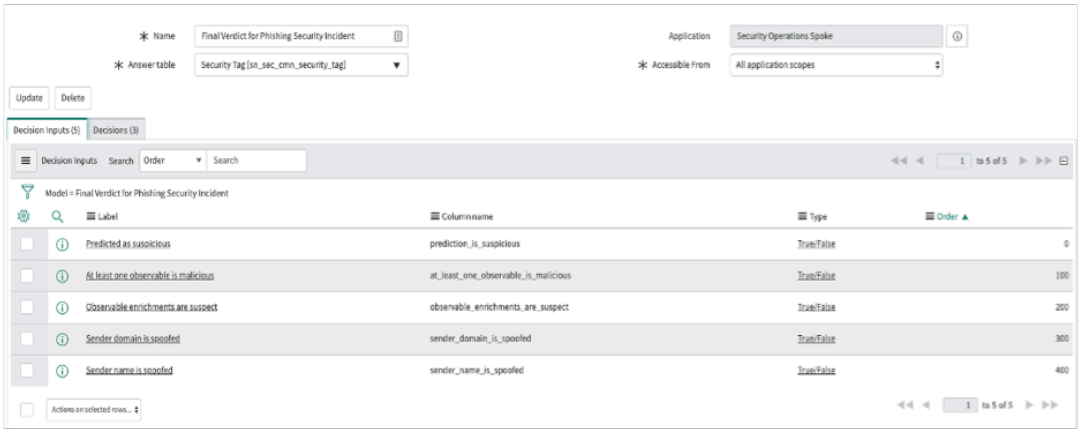
Certifique-se de que todos os plug-ins listados em Componentes e plug-ins necessários tenham sido instalados.

Navegar até **Inteligência preditiva para phishing** > **Veredito final** > **Veredicto final para incidente de segurança de phishing**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

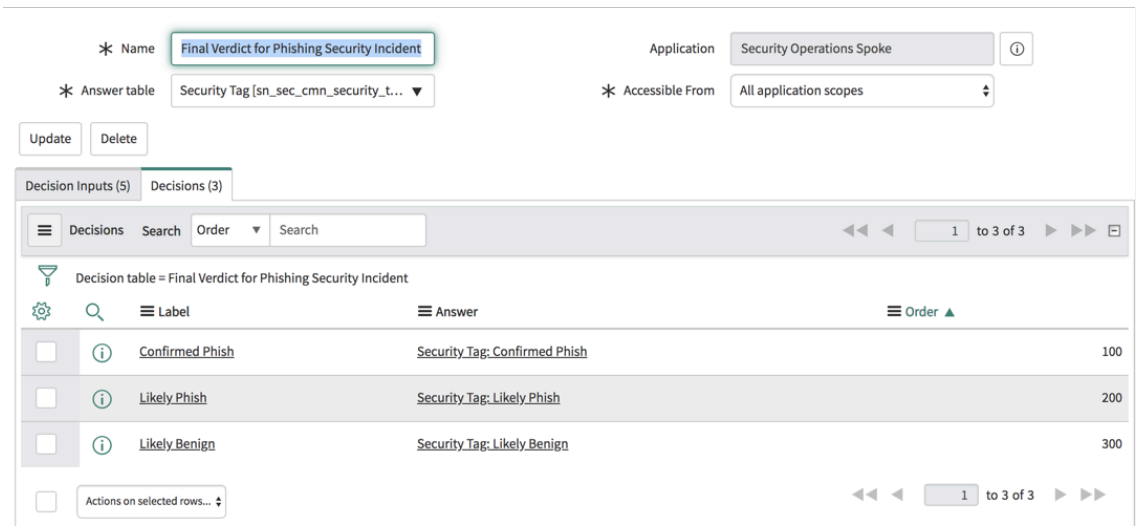
A guia **Entradas de decisão** mostra as diferentes condições que foram avaliadas para chegar ao veredicto final.



As seguintes condições estão disponíveis com o sistema de base:

- Previsto como suspeito: quando a inteligência preditiva tiver classificado o e-mail de phishing relatado pelo usuário como **suspeito**.
- Pelo menos um observável é mal-intencionado: quando um observável envolvido no incidente de segurança (por exemplo, URL, domínio, IP, hash) foi classificado como mal-**intencionado** por fontes de inteligência contra ameaças.
- O enriquecimento de observáveis é suspeito: quando o enriquecimento em observáveis (por exemplo, recência de registro de domínio de phishing, país de registro de domínio de phishing) é considerado suspeito.
- O domínio do remetente é falsificado: quando o domínio de e-mail do phisher é suspeito de falsificar um domínio confiável.
- O nome do remetente é falsificado: quando o endereço de e-mail do phisher é suspeito de falsificar um funcionário confiável de uma organização.

A guia **Decisões** mostra as opções de veredicto final que podem ser obtidas para um determinado incidente de segurança.

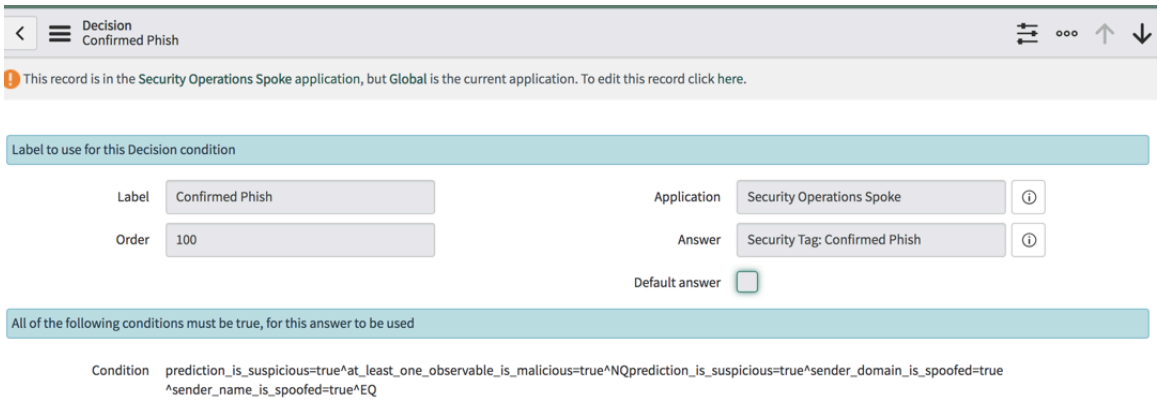


© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As seguintes decisões estão disponíveis com o sistema de base:

- Phish confirmado: quando as condições levam ao veredicto final como sendo um e-mail de phishing confirmado.
- Provável phishing: quando as condições levam ao veredicto final como uma possível tentativa de phishing.
- Provavelmente benigno: quando as condições levam ao veredicto final como um envio benigno.

Você pode ver as condições que foram avaliadas para cada uma das opções de veredicto final. Clique no link Rótulo para ver as condições.



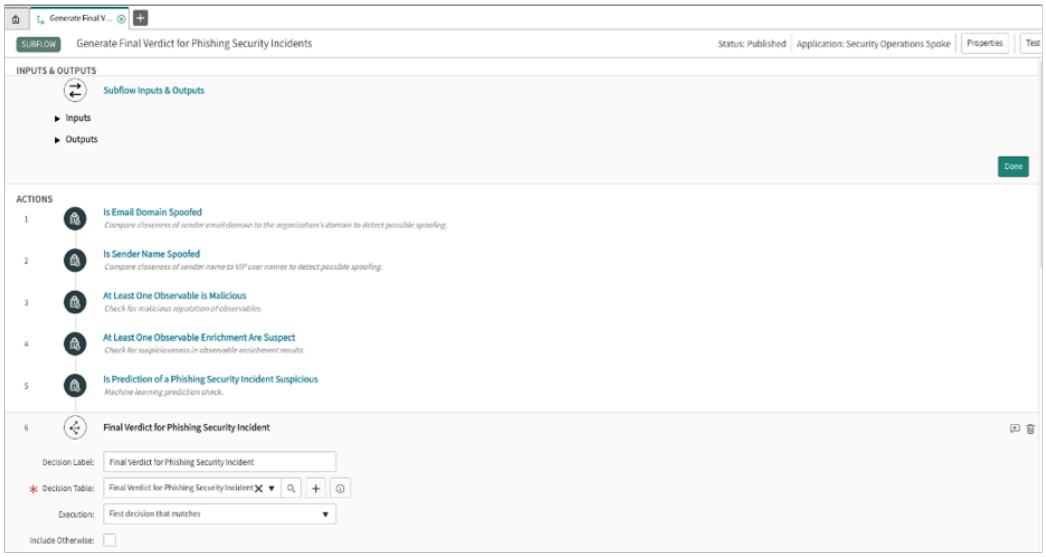
Você pode personalizar a tabela de decisão fornecida com o sistema de base ou criar sua própria tabela de decisão. Esta tabela de decisão pode ser aproveitada em playbooks de resposta a incidentes de segurança. O subfluxo **Gerar veredicto final para incidentes de segurança de phishing** está disponível com o sistema de base. Este subfluxo gera automaticamente o veredito final para um incidente de segurança de phishing e aplica um marcador de segurança com base nessa decisão. Você pode incluir este subfluxo como parte do playbook de **phishing automatizado**.

As entradas para este subfluxo são:

- incident_id: o SYS ID do incidente de segurança de phishing.
- c_level_names: lista separada por vírgulas de nomes (por exemplo, nomes de executivos da organização) que provavelmente serão falsificados no ataque de phishing.
- Trusted_domains: lista separada por vírgulas de domínios de e-mail confiáveis.
- richment_keywords: lista separada por vírgulas de palavras-chave que indicam a mal-intendência do observável a partir dos resultados de aprimoramento.
- sender_email (opcional): o endereço de e-mail do remetente do e-mail de phishing.

A saída deste fluxo pode ser **Phish confirmado**, **Provável phishing**ou **Provavelmente benigno**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Solução de problemas da Inteligência preditiva para phishing relatado pelo usuário

Esta seção cobre alguns cenários de problemas comuns.

- Problema: não consigo modificar a configuração da Inteligência preditiva.

  Solução: verifique se você tem permissões para fazer isso. Você deve fazer login como um usuário com a função ml_admin para modificar limites. Alguns cenários podem exigir privilégios ainda mais altos, como, por exemplo, você precisa modificar o limite de dados de treinamento. Para esses cenários, você deve entrar em contato com o Suporte ao cliente para obter assistência.

- Problema: falha no treinamento do modelo.

  Solução: verifique se os URLs do programador de ML foram configurados. Navegar até **Propriedades do sistema** > **Todas as Propriedades** e verifique se a propriedade *glide.shared_service_scheduler.url* foi configurada.

- Problema: os resultados da previsão não estão disponíveis em um incidente de segurança.

  Solução:

  - Verifique se a URL do preditor foi configurada na propriedade do sistema *glide.prediction_service.url* e certifique-se de que o datacenter corresponda à URL.
  - Verifique se o trabalho agendado Prever e-mail de phishing relatado pelo usuário está ativo.

Configurar a Inteligência preditiva para phishing relatado pelo usuário

Configure e prepare o modelo para identificar e-mails de phishing relatados pelo usuário.

Antes de Iniciar

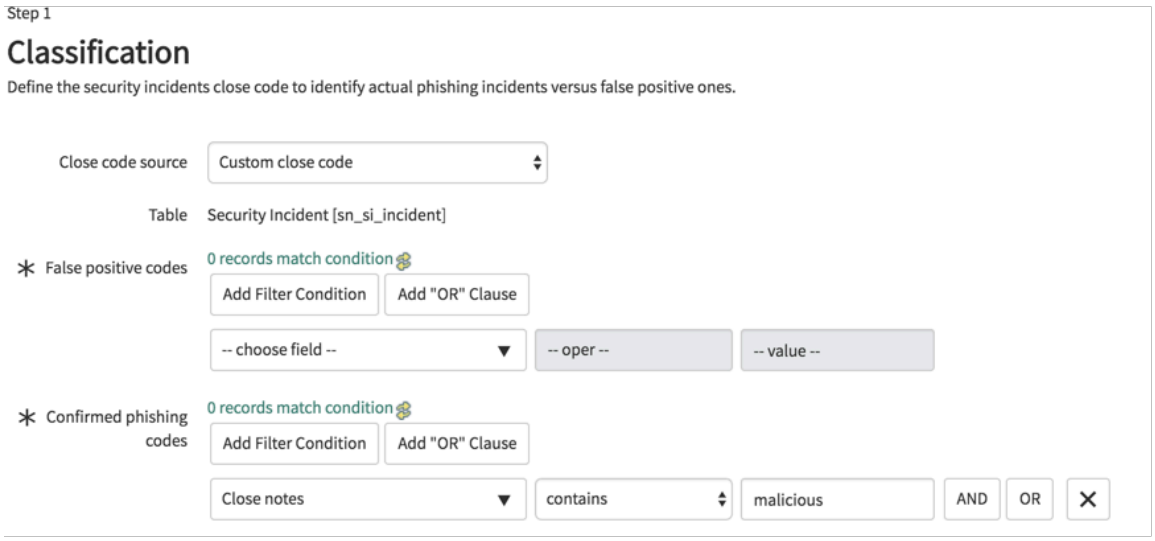
Função necessária: ml_admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência preditiva para phishing** > **Configuração**.
2. Na Etapa 1 da configuração, selecione uma das seguintes opções na lista de origem do código de fechamento:
   - Código de fechamento padrão: selecione esta opção para especificar os códigos de fechamento de incidentes de segurança padrão que devem ser usados pelo modelo de treinamento para identificar e-mails maliciosos e legítimos. Clique no ícone de cadeado e selecione um ou mais códigos falso-positivos ou códigos de phishing confirmados.
   - Código de fechamento personalizado: selecione a opção Código de fechamento personalizado se quiser definir códigos de fechamento de campos personalizados que podem ser usados como parte dos procedimentos de resposta a incidentes existentes. Para definir um código de fechamento, selecione um campo na tabela de incidentes de segurança e especifique uma ou mais condições de filtro.



3. Na Etapa 2, importe dados históricos que podem ser usados para treinar o modelo. Selecione a fonte de dados para importar os dados históricos. Pode ser:
   - Tabela de e-mail de phishing relatada pelo usuário: você pode ver o número de registros que podem ser importados como dados históricos. Selecione esta opção e clique em **Importar**.
   - Fonte de dados personalizada: você pode anexar um único arquivo CSV formatado que contenha registros de dados históricos. Selecione o arquivo e clique em **Importar**.

   Nota: O arquivo CSV importado deve conter os seguintes cabeçalhos:
   - Rótulo
   - Cabeçalho
   - Texto do corpo

   Cada registro deve conter um marcador malicioso ou legítimo na coluna Rótulo no arquivo CSV.

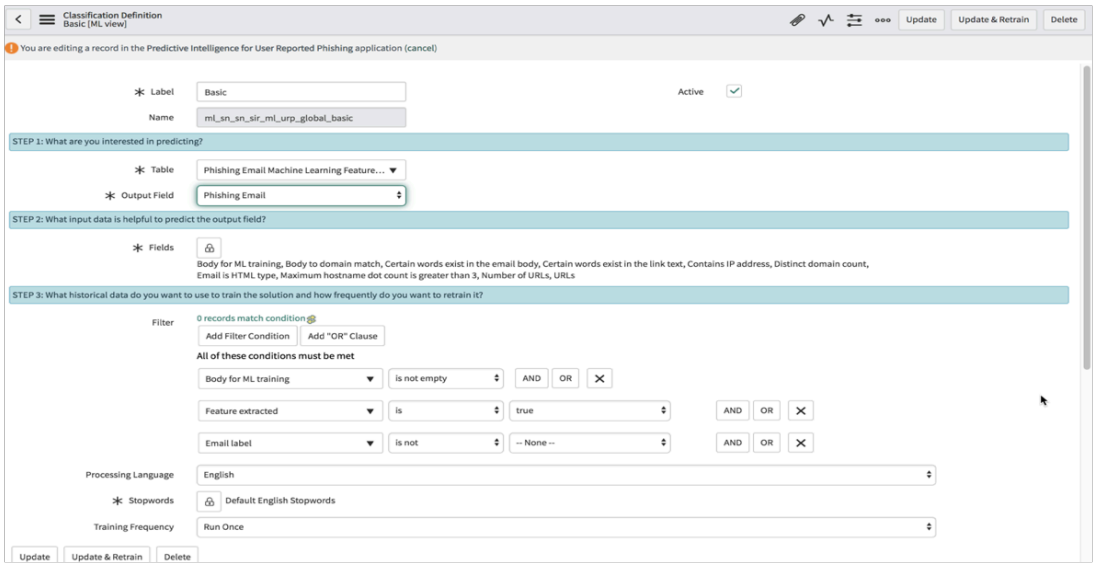
   Clique em **Cancelar importação** para interromper a importação dos dados. O processo de importação é cancelado e todos os registros importados até o momento são excluídos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Depois de importar os dados históricos, clique no link para atualizar a página.
   Você pode importar mais dados de treinamento ou continuar com a próxima etapa.
5. Na Etapa 3, verifique se o número de registros disponíveis para treinamento atende aos requisitos de limite mínimo.

> **Nota:** Os valores padrão para o número máximo e mínimo de registros de treinamento são exibidos. Esses limites podem ser modificados na página Propriedades do aprendizado de máquina da plataforma. Entre em contato com o Suporte ao cliente para obter assistência.

6. Se os dados de treinamento forem suficientes, clique em **Treinar modelo**.
   Você pode atualizar as entradas para treinamento na tela abaixo.



7. As entradas de previsão que você pode modificar incluem:
   - O que você está interessado em prever?
   - Quais dados de entrada são úteis para prever o campo de saída?
   - Quais dados históricos você deseja usar para treinar a solução e com que frequência deseja treiná-la novamente?

   Os valores padrão para essas entradas são exibidos. Você pode modificá-los e clicar em um dos seguintes:
   - **Atualizar**: atualiza a definição do modelo de treinamento.
   - **Atualizar e**treinar novamente: atualiza a definição do modelo de treinamento e treina novamente o modelo (aciona a função **Treinar modelo**).
8. Por fim, quando você concluir o treinamento do modelo, clique na caixa de seleção **Ativar previsão**.
   As previsões agora são fornecidas em todos os registros de phishing relatados por usuários usando esse modelo. Se você quiser parar de fornecer previsões sobre os registros de phishing relatados pelo usuário, desmarque a caixa de seleção **Ativar previsão** e clique em **Desativar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuição de analistas de segurança

Dependendo das suas configurações na tela SIR Configuração de administração, você pode atribuir analistas de segurança a incidentes de segurança manualmente; automaticamente usando um fluxo de trabalho; ou automaticamente usando a atribuição automática.

Atribuição manual de analista

Você pode configurar a tela Security Incident Response de configuração de administração para exigir que os analistas de segurança sejam atribuídos manualmente sempre que alguém ou a aplicação SIR criar um incidente de segurança ou gerar uma tarefa de resposta de segurança.

Se um incidente de segurança ou tarefa de resposta não puder ser atribuído automaticamente, você poderá definir a tela SIR Configuração de administração para exigir a atribuição manual de analistas de segurança. Esta é uma boa opção se você tiver um número limitado de analistas de segurança para concluir solicitações ou se simplesmente não quiser atribuí-los automaticamente.

Atribuição de analista de segurança baseada em fluxo de trabalho

Você pode configurar a tela Security Incident Response de configuração de administração para usar um fluxo de trabalho selecionado para atribuir o analista de segurança sempre que alguém ou a aplicação SIR criar um incidente de segurança ou tarefa de resposta de segurança.

Na tela de configuração Administração de incidentes de segurança, você pode optar por usar um fluxo de trabalho para atribuir um analista a cada incidente de segurança ou tarefa de resposta de segurança. Essa opção é ideal para organizações que usam um processo personalizado para resolver problemas de segurança ou têm um processo que pode ser automatizado.

Atribuição automática de analista de segurança

Você pode configurar a tela Security Incident Response de configuração de administração para atribuir automaticamente o analista de segurança sempre que alguém ou a aplicação SIR criar um incidente de segurança ou uma tarefa de resposta de segurança. A atribuição automática permite que você defina, com base nas necessidades da sua organização, os critérios pelos quais os analistas são atribuídos automaticamente a incidentes de segurança.

Atribuição automática de agente com base nas classificações do agente

Se a atribuição automática estiver habilitada e um incidente de segurança ou uma tarefa de resposta for criada, ocorrerão as seguintes ações:

- Os analistas de segurança disponíveis são avaliados com base nos critérios definidos na configuração.
- Um analista de segurança apropriado é atribuído automaticamente à tarefa.
- A tarefa é movida para o estado **Atribuído**.

Se a configuração estiver definida para considerar mais de um conjunto de condições, como habilidades, local, fuso horário ou área de cobertura do grupo, os analistas de segurança serão avaliados com base nas configurações da propriedade de ponderação e outros critérios. Essas definições de configuração ajudam a atribuir agentes automaticamente com base em propriedades opcionais. As classificações calculadas são usadas para determinar o melhor agente para o incidente de segurança ou a tarefa

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de resposta. Qualquer combinação de métodos baseados em classificação pode ser habilitada na tela de configuração da aplicação.

Quando uma tarefa é criada, uma classificação para cada tipo de critério de seleção habilitado é calculada para cada agente disponível. O agente cuja classificação total é mais alta é considerado para atribuição automática.

As configurações das propriedades de ponderação de atribuição automática, encontradas em **Incidente de segurança** > **Administração** > **Propriedades**, estão incluídos nos cálculos de classificação.

Esses valores ajudam a priorizar quais critérios de seleção de atribuição automática são mais importantes para sua organização. Defina os valores de prioridade entre 1 (menos importante) e 10 (importante).

Para obter um exemplo de como as propriedades de ponderação afetam as classificações do agente, consulte Atribuição automática de agente usando vários critérios de seleção.

Atribuição automática de agente usando local

Os agentes podem ser atribuídos automaticamente com base no local inicial no registro de usuário e no local das tarefas.

A atribuição automática por local é realizada quando a opção **de configuração A seleção automática de agentes considerará o local dos agentes** está habilitada.

Quando uma tarefa (incidente de segurança ou tarefa de resposta) é criada, o agente mais próximo do local da tarefa é considerado para a tarefa. Se a aplicação estiver configurada para que somente o local seja considerado, a tarefa será atribuída automaticamente ao agente mais próximo.

Quando uma tarefa é criada, os locais dos agentes são comparados aos seguintes intervalos para determinar a classificação de local de cada agente.

Cálculo de classificação de local

Distância (milhas) do agente até a tarefa	Classificação
0 a 0,1	1
0,11 a 0,5	0,9
0,51 a 5	0,7
5,1 a 10	0,5
10,1 a 20	0,4
20,1 a 30	0,3
30,1 a 40	0,2
40,1 a 100	0.1
> 100	0

Se a aplicação estiver configurada para usar outros critérios de seleção, como habilidades, fuso horário ou programação, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é atribuído automaticamente para a tarefa. Consulte Atribuição automática de agente usando vários critérios de seleção para obter detalhes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuição automática de agente usando habilidades

Os agentes podem ser atribuídos automaticamente com base em suas habilidades e nas habilidades necessárias para executar a tarefa. Atribuir habilidades aos registros de usuário usando **Habilidades** > **Usuários**.

A atribuição automática por habilidades pode ser realizada quando a opção Seleção **automática de agentes para tarefas requer que eles tenham habilidades** está definida como **todos** ou **alguns**.

Quando uma tarefa que inclui habilidades é atribuída automaticamente, as habilidades de um agente são comparadas com as habilidades necessárias para executar a tarefa. Uma classificação é calculada com base na opção de configuração de habilidades. Se a opção estiver definida como **some**, o agente com a correspondência de habilidades mais próxima será atribuído automaticamente à tarefa. Se a opção estiver definida como **todos**, somente os agentes que possuem todas as habilidades necessárias serão considerados. Se nenhum agente tiver todas as habilidades necessárias para executar a tarefa, ninguém será atribuído automaticamente.

Uma classificação de habilidades é calculada como:

Skills_agent/Skills_task

Em que:

- Skills_agent é o número de habilidades possuídas pelo agente que correspondem às habilidades necessárias para a tarefa.
- Skills_task é o número total de habilidades necessárias para a tarefa.

Por exemplo, se uma tarefa requer quatro habilidades e o Agente A possui três delas e o Agente B possui duas delas:

- Classificação de habilidade do agente A = 3/4 ou 0,75
- Classificação de habilidade do agente B = 2/4 ou 0,5

Se a aplicação estiver configurada para usar outros critérios de seleção, como local ou fuso horário, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é selecionado para a tarefa. Consulte Atribuição automática de agente usando vários critérios de seleção para obter detalhes.

Atribuição automática de agentes usando fusos horários

Os agentes podem ser atribuídos automaticamente com base no fuso horário definido em seus registros de usuário e no fuso horário das tarefas.

Se a opção Seleção **automática de agentes considerará o fuso horário para a configuração da tarefa** estiver habilitada, a atribuição automática por fuso horário poderá ser realizada.

Quando uma tarefa é criada, os agentes no fuso horário mais próximo do fuso horário da tarefa são considerados para a tarefa. Se a aplicação estiver configurada para que somente o fuso horário seja considerado, somente um agente no mesmo fuso horário poderá ser atribuído automaticamente à tarefa.

Nota: É importante que os fusos horários do agente e da tarefa sejam definidos corretamente.

Quando uma tarefa é criada, os agentes são classificados com base no fuso horário da tarefa e no fuso horário do agente usando a seguinte fórmula:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1 - [abs(Task_tz – Agent_tz) ÷ 12]

em que:

- abs é a função matemática para calcular o valor absoluto.
- Task_tz é a diferença entre o fuso horário da tarefa e o GMT.
- Agent_tz é a diferença entre o fuso horário do agente e o GMT.

Por exemplo, uma tarefa é criada na cidade de Nova York (GMT-4) e dois agentes estão disponíveis para executar a tarefa, um em Los Angeles (GMT-7) e um em Paris, França (GMT +1).

A classificação do agente em Los Angeles é calculada como:

1 - abs((-4) - (-7)) ÷ 12 ou 0,75

A classificação do agente em Paris é calculada como:

1 - abs((-4) - (+1)) ÷ 12 ou 0,58

Portanto, se a atribuição automática da tarefa for baseada somente no fuso horário, ela será atribuída ao agente de Los Angeles.

Se a aplicação estiver configurada para usar outros critérios de seleção, como habilidades ou localização, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é selecionado para a tarefa. Consulte Atribuição automática de agente usando vários critérios de seleção para obter detalhes.

Atribuição automática de agentes usando áreas de cobertura de grupo

Os agentes podem ser atribuídos automaticamente com base na área de cobertura do grupo definida em seus registros de usuário.

Atribuição automática de agente usando vários critérios de seleção

Quando uma tarefa é criada, as classificações dos agentes são calculadas. Para obter mais informações, consulte:

- Atribuição automática de agente usando local
- Atribuição automática de agente usando habilidades
- Atribuição automática de agentes usando fusos horários

A atribuição automática é baseada no seguinte cálculo:

(Classificação de Critérios_1 x peso de Critérios_1) + (classificação de Critérios_2 x peso de Critérios_2) + (classificação de Critérios_3 x peso de Critérios_3) / Número de tipos de critérios usados em que:

Número de tipos de critérios usados = 1, 2 ou 3, dependendo das configurações de local, habilidade e fuso horário usadas.

Este exemplo calcula a atribuição automática de agentes com base na localização e nas habilidades. O exemplo se baseia nas seguintes suposições.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A opção de configuração A **seleção automática de agentes considerará a localização dos agentes** está habilitada para a aplicação.
- A **seleção automática de agentes exige que eles tenham algumas das habilidades necessárias para que a opção de configuração de tarefa** esteja habilitada para a aplicação.
- A propriedade **Peso das habilidades** está definida como 10 para a aplicação.
- A propriedade **Peso** do local está definida como 5 para a aplicação.
- Os agentes A e B estão disponíveis para executar uma tarefa e a tarefa requer quatro habilidades específicas.
- O local do Agente A está a 8 km do local da tarefa e possui três das quatro habilidades necessárias.
- O local do Agente B fica a um quarto de milha do local e possui duas das habilidades necessárias.

A atribuição automática para os agentes usa este cálculo: `[(Classificação do local x Peso do local) + (Classificação de habilidades x Peso das habilidades)]/ 2`

- O cálculo de atribuição automática para o Agente A é: `[(0,7 x 0,5) + (0,75 x 1)]/ 2 = 0,55`
- O cálculo de atribuição automática para o Agente B é: `[(0,9 x 0,5) + (0,5 x 1)]/ 2 = 0,475`

Neste exemplo, a tarefa é atribuída automaticamente ao Agente A.

Gerenciamento de incidentes de segurança e solicitações de entrada

Depois que um incidente de segurança é criado, vários tipos de informações podem ser adicionados e exibidos conforme sua análise do problema avança em direção à resolução.

Importante: Os recursos mais recentes em Security Incident Response estão disponíveis exclusivamente no Espaço de resposta a incidentes de segurança. Instale ou faça upgrade para a versão mais recente Security Incident Response ou Espaço de resposta a incidentes de segurança para acessar e aproveitar recursos como Transferência de turno, Calculadora de pontuação de risco etc.

Esta seção descreve o seguinte:

- Criar uma solicitação de entrada
- Gerenciar observáveis
- Gerenciar pesquisas e verificações
- Gerenciar oorquestração de n-demand
- Calcular a gravidade de um incidente de segurança
- Gerenciar atividades pós-incidente
- Fechar incidentes de segurança

Criar uma solicitação de entrada

Ao contrário dos incidentes de segurança, as solicitações de entrada geralmente têm uma prioridade mais baixa. Solicitações de pesquisa, verificação ou um novo crachá são exemplos de solicitações de entrada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Funções necessárias: função sn_si.basic ou superior

Procedimento

1. Navegue até um dos formulários de Solicitações.
   Por exemplo, **Todos** > **Incidente de segurança** > **Solicitações de Entrada** > **Atribuídos a Mim**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Solicitação de segurança

Campo	Descrição
Número	[Somente leitura] O número da solicitação de segurança gerado automaticamente.
Empresa	A empresa do solicitante.
Local	O local do IC, se aplicável. Este campo é preenchido previamente quando o IC é selecionado.
Item de Configuração	O item de configuração afetado pela solicitação.
Prioridade	A prioridade da solicitação.
Aberto	[Somente leitura] A data e hora em que a solicitação foi aberta.
Estado	O estado atual da solicitação de segurança. Na criação da solicitação de segurança, o padrão deste campo é **Rascunho**.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuído a	O indivíduo atribuído para executar o trabalho.
Descrição resumida	Uma breve descrição da solicitação de segurança, que está visível para o solicitante.
Descrição	A descrição completa da solicitação, que está visível para o solicitante.
Anotações de trabalho	Anotações de trabalho, que ficam visíveis para o solicitante.

4. Ao concluir suas entradas, clique em **Enviar**.
5. Se você precisar escalar a solicitação para um incidente de segurança, clique em **Converter em incidente de segurança**.

Gerenciar observáveis

Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicam uma invasão. Os observáveis típicos são endereços IP, hashes MD5 de arquivos de malware ou URLs ou nomes de domínio. Inteligência contra ameaças dados da tabela de observáveis estão disponíveis em um incidente de segurança.

As informações de observáveis incluem valor, tipo, contexto e carimbo de data/hora.

Você pode criar ou excluir observáveis manualmente ou automaticamente por meio de solicitações de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma nova coluna de **descoberta** foi adicionada à guia **Resultados da pesquisa de ameaças**. Os valores possíveis são: malicioso e desconhecido.

Se uma solicitação de pesquisa de IoC não encontrar um observável de incidente de segurança, ele será rotulado como Desconhecido.

Se uma solicitação de pesquisa de IoC encontrar um observável de incidente de segurança, ele será rotulado como Mal-intencionado.

Durante um upgrade, os itens existentes têm a coluna **Descoberta** definida como Mal-intencionado.

Nota: Embora os dados da tabela de observáveis Inteligência contra ameaças façam parte de um incidente de segurança, nenhuma outra interação com o módulo Inteligência contra ameaças está incluída. Para a funcionalidade completa de ameaça, o plug-in Inteligência contra ameaças está disponível por assinatura.

Informações relacionadas

Criar um observável de incidente de segurança

Mostrar informações de IoC para um incidente de segurança

Você pode exibir informações de IoC, como resultados de pesquisa de observáveis e detecções associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir informações relacionadas ao IoC.
2. Clique no link relacionado **Mostrar IoC**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações ao incidente de segurança.

Guia	Descrição
Observáveis	Exiba ou adicione ou edite manualmente observáveis associados ao incidente de segurança. Para obter mais informações, consulte Gerenciar observáveis.
Indicadores associados	Se Inteligência contra ameaças estiver ativado, você poderá exibir outros indicadores associados a qualquer um dos mesmos registros de ameaça.
Resultados da pesquisa de detecções	Contém resultados da Pesquisa de detecções.
Detalhes de Pesquisa de detecções	Contém detalhes do registro da Pesquisa de detecções.
Pesquisas de ameaças	Armazena dados de aprimoramento de sistemas de detecção de malware. Esta guia só aparece quando o plug-in Inteligência contra ameaças está instalado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia	Descrição
Modos/métodos de ataque associados	Se Inteligência contra ameaças estiver ativado, você poderá exibir outros tipos de ataque associados a qualquer um dos mesmos registros de ameaça.
Solicitações de Verificação de Segurança	Se Inteligência contra ameaças estiver ativado, você poderá exibir as solicitações de verificação e pesquisa anexadas ao incidente de segurança.
Recursos com IoC Semelhante	Se Inteligência contra ameaças estiver ativado, você poderá exibir outros recursos com indicadores semelhantes.
Usuários com IOC Semelhante	Se Inteligência contra ameaças estiver ativado, você poderá exibir outros usuários com indicadores semelhantes.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar dados de enriquecimento
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar**.

Criar um observável de incidente de segurança

Você pode criar e exibir um observável em um incidente de segurança e tomar as medidas apropriadas. Ter observáveis disponíveis no incidente de segurança é escalonável e reduz o tempo de resposta.

Antes de Iniciar

Função necessária:

- sn_ti_observable.write (gravação)
- sn_ti_observable.read (leitura)
- sn_ti_observable.admin (excluir)

Procedimento

1. Navegue até **Incidente de segurança**.
2. Escolha um incidente.
3. Clique na guia da lista relacionada **de observáveis de incidente de segurança**.
4. Clique em **Nova**.
5. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do observável. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável. **Nota:** Se uma verificação de ameaças em um endereço IP ou hash retornar malware ou alguma outra falha, o endereço IP ou o valor de hash será adicionado automaticamente à tabela Observável [sn_ti_observable]. Como tal, ele pode ser pesquisado no formulário Observáveis.
Tipo de observável	Selecione a classificação de observável, como um endereço IP ou hash de arquivo. Esses tipos de observável são definidos no módulo **Tipos de observável**.
Contagem de incidentes	O número de vezes que o valor do observável foi encontrado.
É composição	Este campo é exibido somente depois que o registro do observável foi salvo. Se o **tipo de observável** estiver definido como qualquer outra coisa que não seja **composição de observável**e este novo observável for uma composição, marque esta caixa de seleção. Se o **Tipo de observável** já estiver definido como **Composição de observável**, a caixa de seleção será marcada e será somente leitura. Uma composição de observável é um observável que contém observáveis secundários.
Descoberta	Selecione uma das seguintes propriedades: ◦ **Mal**-intencionado : indica que o observável é prejudicial à organização. ◦ **Suspeito**: indica que o observável pode ser prejudicial à organização. ◦ **Limpar**: indica que o observável não é prejudicial à organização. ◦ **Desconhecido**: indica que ainda não determinamos a descoberta do observável. ◦ Valor padrão: desconhecido. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças. **Nota:** Após um upgrade, os observáveis existentes são marcados como Mal-intencionados.
Operador	Este campo aparece somente quando a caixa de seleção **É composição** está marcada. Dependendo da sua configuração neste campo, os observáveis e seus secundários são considerados ao decidir se um indicador associado está presente. Defina este campo como **E** se todos os observáveis secundários precisarem estar presentes para que um indicador associado seja considerado presente. Defina como **OU** se algum dos observáveis secundários estiver presente para que um indicador associado seja considerado presente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

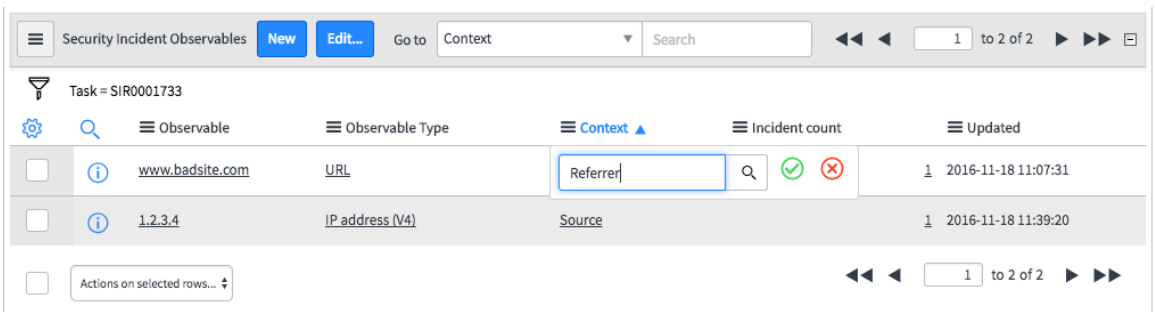
Campo	Descrição
Não deve estar presente	Este campo é exibido somente depois que o registro do observável foi salvo. Se selecionado, este campo significa que a ausência do observável é o possível problema (por exemplo, uma chave de registro ausente).
Local	Usando as configurações em duas propriedades e uma definição de inclusão de script, você pode carregar Carregar mais dados de IoC neste campo.
Anotações	Insira anotações adicionais sobre o observável.

6. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**. Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores que foram identificados pela origem da ameaça.
Tarefas Associadas	Lista as mudanças associadas ao observável.
Observáveis secundários	Lista os observáveis relacionados que foram identificados pela origem da ameaça.
Recursos correspondentes para IP	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.
Origens observáveis	Lista as origens deste observável, junto com o nível de confiança da origem.
Anotações de segurança	Lista as anotações de segurança adicionadas a este observável.

7. Retornando ao incidente de segurança, as seguintes informações estão disponíveis.

Nota: Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. As guias da lista relacionada **Itens de configuraçãorelacionados e Usuários** relacionados são atualizadas de acordo.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Definição
Observável	O valor (por exemplo, endereço IP ou hash) associado ao observável.
Tipo de Observável	O tipo específico de observável.
Contexto	Selecionado pelo usuário. As opções são: ◦ IP - Origem ou Destino **Nota:** Se Inteligência contra ameaças e Palo Alto Networks - Firewall estiverem ativados, alterar ou adicionar um valor a este campo fará com que o fluxo de trabalho Fluxo de trabalho Obter dados de log Palo Alto Networks - Obter dados de log das Operações de segurança seja executado. O fluxo de trabalho recupera dados de log de ameaças aprimorados do firewall e os anexa ao incidente de segurança. As informações também são analisadas e exibidas na seção Logs do firewall na guia **Dados** de aprimoramento. ◦ URL - Referenciador **Nota:** Quando o usuário clica em um link em um e-mail de phishing, um referenciador é o URL do salto final antes que o URL do malware seja acessado.
Contagem de Incidentes	O número de incidentes em que este observável aparece. Este valor é atualizado automaticamente quando o observável é adicionado a outro incidente manualmente ou por meio de um fluxo de trabalho.
Atualizado	Data e hora em que a lista foi atualizada pela última vez.

Nota: Se o plug-in Inteligência contra ameaças estiver instalado, você também poderá exibir o observável na lista **Observáveis** no **Repositório de IoC**.

Informações relacionadas

Editar uma lista de observáveis de incidente de segurança

Adicionar vários observáveis de incidentes de seguranças

Gerenciar observáveis de arquivo

Gerenciar observáveis de arquivo fornece medidas de segurança rígidas para armazenar os arquivos suspeitos e habilita os observáveis do tipo de arquivo para integração na área restrita.

Antes de Iniciar

Função necessária: sn_ti_maliciosa_attachment_access (upload)

Carregar os observáveis de tipo de arquivo:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Automaticamente: quando os incidentes de segurança são criados para os e-mails de phishing, os anexos no e-mail de phishing são criados como observáveis do tipo de arquivo.

- Manualmente: um analista de segurança também pode carregar os arquivos suspeitos para criar observáveis de tipo de arquivo.

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar e exibir observáveis de tipo de arquivo para um incidente de segurança. Os arquivos suspeitos que fazem parte dos observáveis são armazenados em um local específico, que pode ser acessado pelo analista de segurança para baixar o arquivo somente com uma função específica.

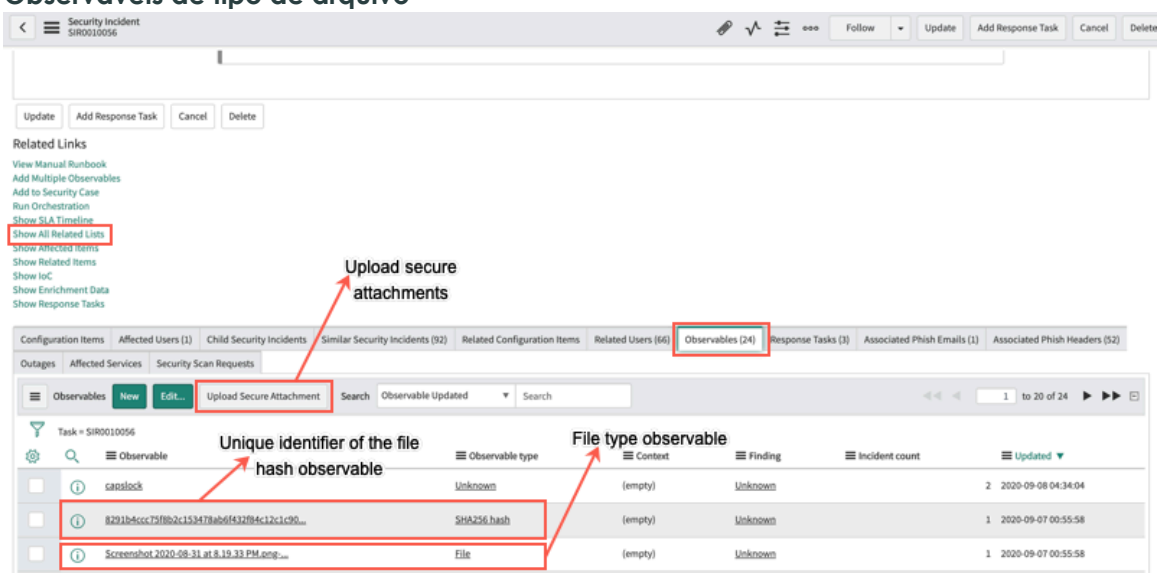
Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** na guia **Mostrar todas as listas relacionadas**.

   Se houver anexos no e-mail de phishing, por padrão, esses anexos serão criados como observáveis do tipo de arquivo no incidente de segurança correspondente. Cada anexo é criado como dois observáveis, como tipo de arquivo e observável de hash de arquivo.

3. Para carregar os anexos seguros manualmente:
   - Clique **em Carregar anexo seguro**.
   - Em Carregar anexos seguros, clique em **Escolher arquivo** para carregar um ou mais arquivos. Cada arquivo é considerado como um único registro de observável.
   - Clique em **Criar observáveis de arquivo** para criar os observáveis de tipo de arquivo, como um é o tipo de arquivo e o outro é o hash do arquivo, que é um identificador exclusivo.

Observáveis de tipo de arquivo



Selecione o tipo de arquivo observável a ser processado para futuras integrações, como área restrita, pesquisa de ameaças. Além disso, você também pode baixar os anexos do observável tipo de arquivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A pesquisa de ameaças (VirusTotal) recupera o arquivo dos anexos protegidos para os novos observáveis de tipo de arquivo e as propriedades do sistema abaixo não são aplicáveis aos novos observáveis de tipo de arquivo.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Para uma referência rápida, o observável de tipo de arquivo é mapeado como secundário para o observável de hash e o observável de hash é mapeado como secundário para o observável de arquivo.

Se os anexos de e-mail de phishing excederem o tamanho definido, os observáveis não serão criados. Você deve modificar as propriedades do sistema para oferecer suporte a arquivos de tamanho maior.

Propriedades do sistema de tamanho de arquivo

Propriedade do sistema	Descrição
glide.email.inbound.max_total_attachment_size_bytes	Se você estiver encaminhando o e-mail de phishing diretamente, use este valor de propriedades do sistema para aumentar o tamanho do arquivo de 18 MB para o tamanho desejado.
com.glide.attachment.max_get_size	Se você estiver encaminhando o e-mail de phishing como um anexo, use este valor de propriedade do sistema para criar as propriedades do sistema abaixo no escopo global para aumentar o tamanho do arquivo de 5 MB para o tamanho desejado.

Você também pode criar um novo observável de tipo de arquivo da seguinte forma:

a. Clique em **Nova**.

b. Selecione a **categoria do tipo de observável: arquivo**

c. Clique em **Carregar** para anexar um arquivo.

Editar uma lista de observáveis de incidente de segurança

Você pode editar quais observáveis na lista associada a um incidente de segurança serão exibidos.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Navegue até **Incidente de segurança**.

2. Escolha um incidente.

3. Clique na guia da lista relacionada **de observáveis de incidente de segurança**.

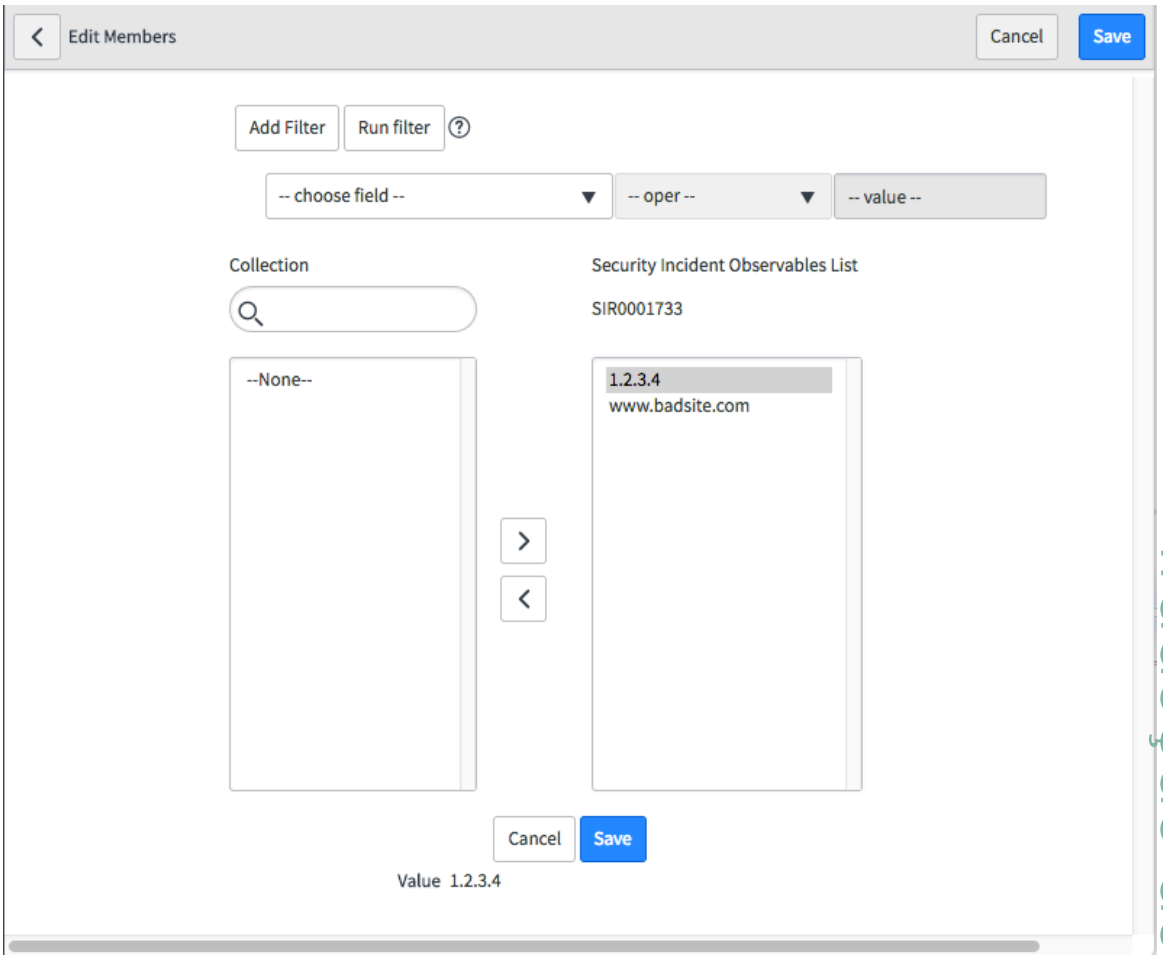
4. Clique em **Editar**.

5. Adicione ou remova observáveis da lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie um filtro para listas longas.



6. Clique em **Salvar**.

Nota: Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. As guias da lista relacionada **Itens de configuraçãorelacionados e Usuários** relacionados são atualizadas de acordo. Além disso, se o plug-in Inteligência contra ameaças estiver ativado e você tiver pelo menos uma implementação de integraçãoIntegrações do Security Incident Response ativada, o Integração de Operações de segurança - Capacidade de pesquisa de ameaças executará um ou mais fluxos de trabalho e as pesquisas de segurança contra ameaças serão realizadas nos observáveis adicionados. Os resultados aparecem na guia **Resultados da pesquisa de ameaças**.

Informações relacionadas

Adicionar vários observáveis de incidentes de seguranças

Criar um observável de incidente de segurança

Adicionar vários observáveis de incidentes de seguranças

Para economizar tempo, você pode adicionar vários observáveis de incidentes de segurança à lista de observáveis de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_ti_write

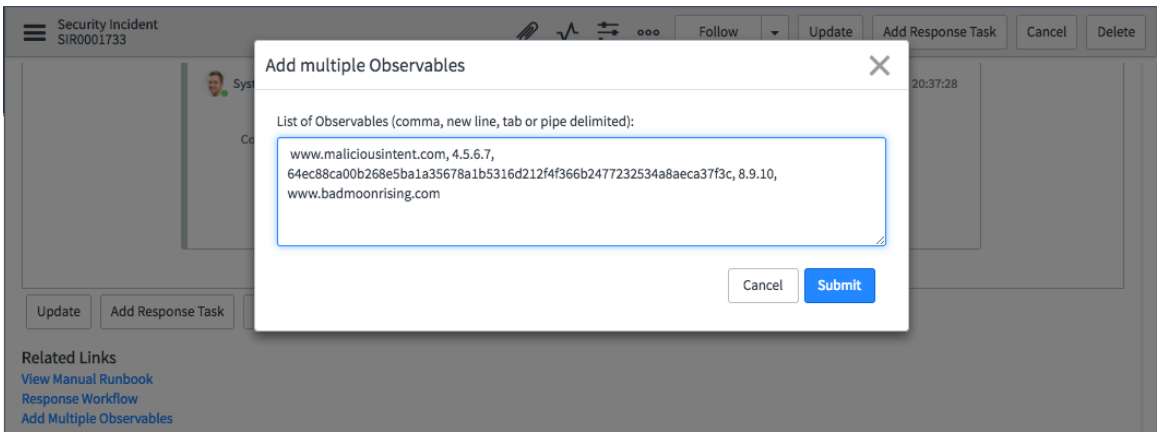
Nota: Ao adicionar vários observáveis de incidentes de segurança, as duplicatas são ignoradas durante o processamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Incidente de segurança**.
2. Escolha um incidente.
3. Clique no link relacionado **Adicionar vários observáveis**.
4. Insira ou cole vários observáveis.
   As entradas podem ser de qualquer tipo de observável. Os formatos aceitos são: separadores de vírgula, nova linha, guia ou pipe.



> **Nota:** Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. As guias da lista relacionada **Itens de configuraçãorelacionados e Usuários** relacionados são atualizadas de acordo.

Observação: os valores de observável não detectados automaticamente são atribuídos ao tipo Desconhecido.

5. Clique **em Enviar.**.

Aprimoramento automático de dados do log do observável incidente de segurança

Quando determinadas aplicações e integrações são configuradas, incluindo Inteligência contra ameaças e a integração Palo Alto Networks - Firewall, as informações de observáveis em um incidente de segurança podem ser aprimoradas automaticamente com dados de log de ameaças sempre que o IP de origem de seus observáveis é modificado.

Quando ocorre uma modificação, uma regra de negócio inicia um fluxo de trabalho que recupera dados de logs de ameaças no firewall e aprimora as informações de observáveis no incidente de segurança.

Antes que os observáveis possam ser aprimorados, as etapas a seguir devem ser executadas.

- A Inteligência contra ameaças deve ser ativada.
- A integração do firewall da Palo Alto Networks deve ser ativada e configurada. Isso também pode incluir Configurar credenciais SSH para o MID Server.

Depois que essa configuração for concluída, o ato de alterar o IP de origem de observáveis associados a um incidente de segurança faz com que uma regra de negócio execute o fluxo de trabalho **Operações de segurança Palo Alto Networks - Obter dados de log**. As atividades de fluxo de trabalho enfileiram uma consulta de pesquisa no firewall e retornam um ID de trabalho que é usado para recuperar dados de logs de ameaças do firewall e anexá-los como um arquivo XML ao incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

- Obter fluxo de trabalho de aprimoramento de informações da sessão do AutoFocus
- Integração de Operações de segurança Palo Alto Networks Fluxo de trabalho do inicializador de firewall
- Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor
- Fluxo de trabalho Obter dados de log
- Obter fluxo de trabalho de aprimoramento de dados do WildFire

Publicar observáveis em uma lista de observação de terceiros

Você pode publicar um ou mais observáveis ou indicadores associados em uma lista de observação de terceiros. Atualmente, a única implementação compatível com essa funcionalidade é o CrowdStrike Falcon Host.

Antes de Iniciar

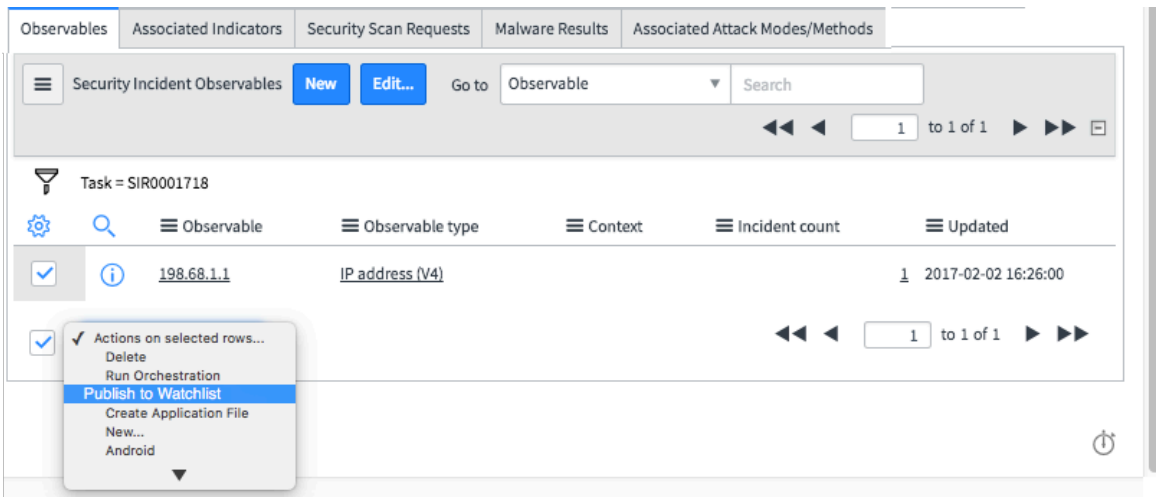
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Procedimento

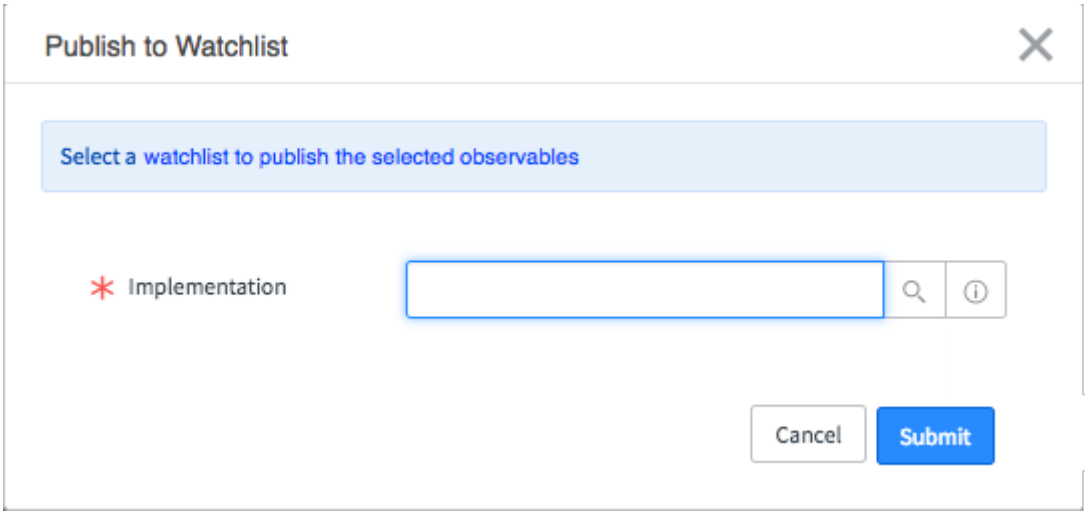
1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** na guia **Lista relacionada**.
3. Clique **em Publicar na lista de observação** no menu suspenso **Ações nas linhas selecionadas....**



A caixa de diálogo é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira ou escolha a implementação.

   Nota: Um fluxo de trabalho é acionado pelo Integração de Operações de segurança - Capacidade de publicar na lista de observação quando você seleciona a implementação do CrowdStrike Falcon Host.

5. Clique em **Enviar**.

Gerenciar pesquisas e verificações

Você pode executar pesquisas e verificações de vulnerabilidade a partir de incidentes de segurança e do catálogo de incidentes de segurança para identificar possíveis ameaças e vulnerabilidades.

Como enviar uma solicitação de pesquisa de IoC a partir de um incidente de segurança

Uma pesquisa de IoC é executada automaticamente sempre que observáveis são adicionados a um incidente de segurança. Além disso, se o seu incidente de segurança tiver anexos, eles poderão ser encontrados facilmente com o toque de um botão.

Antes de Iniciar

Para pesquisas automáticas de IoC, o plug-in Inteligência contra ameaças deve ser ativado.

Função necessária: sn_si.basic

Nota: Por padrão, o **tipo de pesquisa** de **arquivo** está inativo.

Procedimento

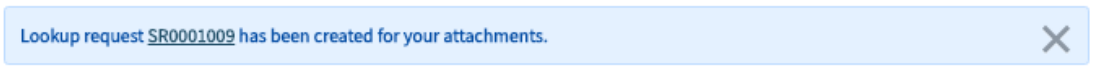
1. Crie um novo incidente de segurança ou abra um existente se você pretender anexar novos arquivos a ele.
2. Clique no ícone de clipe de papel no cabeçalho do formulário e anexe um ou mais arquivos.
3. Quando tiver concluído suas entradas no formulário, clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
   Depois que o registro for salvo, um botão **Pesquisar anexos** será exibido.
4. Clique **em Pesquisar anexos**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As anotações de trabalho em **Detalhes do incidente** relatam o andamento do processo de pesquisa.

5. Você pode clicar no número de pesquisa no final da mensagem para exibir o registro de pesquisa.
   Você pode clicar no link de referência de pesquisa para exibir resultados detalhados.



Envie uma solicitação de pesquisa de IoC do Catálogo de incidentes de segurança

Se o plug-in Security Incident Response estiver ativado, você poderá enviar pesquisas de ameaças para arquivos, valores de hash, URLs e endereços IP do Catálogo de incidentes de segurança. As solicitações são enviadas e você pode exibir os resultados no módulo **Minhas solicitações**.

Antes de Iniciar
Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa
As pesquisas são realizadas automaticamente para o tipo de pesquisa padrão para cada origem de pesquisa listada no registro de pesquisa. Os resultados da solicitação de pesquisa estão disponíveis no módulo **Minhas solicitações**.

Procedimento

1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de incidente de segurança**.
2. Clique **em Pesquisa de IoC**.
3. Clique **em Pesquisar arquivos, valores de hash, URLs ou endereços IP**.
4. Insira um ou mais dos seguintes:

Solicitação de pesquisa de IoC

Item a ser pesquisado	Descrição
Arquivos	Clique no ícone de clipe de papel e localize e anexe os arquivos que deseja pesquisar. **Nota:** Por padrão, o **tipo de pesquisa** de **arquivo**está inativo. Os arquivos são convertidos e enviados como um valor de hash.
URLs	No campo **URLs**, insira os URLs que você deseja pesquisar, separados por vírgulas. Por exemplo: www.abc.com,www.xyz.net.
Endereços IP	No campo **Endereços IP**, insira os endereços IP que você deseja pesquisar, separados por vírgulas.
Valores de hash	No campo **Valores de hash**, insira os valores de hash que você deseja pesquisar, separados por vírgulas. **Nota:** Quando o **tipo de pesquisa** de **arquivo** está inativo, este valor é a ação padrão para os valores de **arquivo** e **hash**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Depois de fazer suas seleções, clique em **Enviar**.
6. Para exibir o status e/ou os resultados das pesquisas, navegue até **Autoatendimento** > **Minhas solicitações**.
7. Clique no número de SR da solicitação.
   As anotações de trabalho em **Atividade** listam as tarefas realizadas durante a pesquisa, incluindo a criação de pesquisas individuais para cada arquivo, valor de hash, URL ou endereço IP e os resultados da pesquisa.

Como enviar uma solicitação de verificação de vulnerabilidade a partir de um incidente de segurança

Se o seu incidente de segurança tiver um ou mais itens de configuração (servidores, computadores e assim por diante), eles poderão ser verificados quanto a vulnerabilidades no formulário Security Incident Response.

Antes de Iniciar

O plug-in Resposta a vulnerabilidades deve ser ativado.

Função necessária: sn_si.write

Procedimento

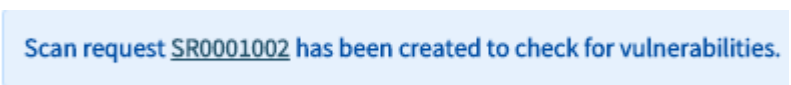
1. Crie um incidente de segurança e inclua pelo menos um recurso.
   Você também pode abrir um incidente existente que tenha itens de configuração.
2. Quando tiver concluído suas entradas no formulário, clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
   Depois que o registro for salvo, um link relacionado a **Verificar vulnerabilidades** será exibido.

   Nota: Se a lista relacionada **Verificar vulnerabilidades** não for mostrada, você deverá navegar até **Vulnerabilidade** > **Scanners**, configure pelo menos um scanner e defina o padrão como **verdadeiro**.

3. Clique **em Verificar vulnerabilidades**.

   Nota:

   Uma mensagem aparece na parte superior do formulário de incidente de segurança, junto com um link para o registro de verificação.

4. Você pode clicar no número da solicitação de verificação para exibir o registro da verificação.
   Os detalhes do incidente mostram os resultados da verificação no registro de solicitação de verificação de segurança.

Enviar uma solicitação de verificação de vulnerabilidades do catálogo do Security Incident Response

Você pode enviar verificações de vulnerabilidade para ICs e endereços IP do catálogo Security Incident Response. As solicitações são enviadas e você pode exibir os resultados no módulo **Minhas solicitações**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: nenhuma

Procedimento
1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de incidente de segurança**.
2. Clique em Verificação de **vulnerabilidade**.
3. Clique **em Verificar item de configuração e endereços IP**.
4. Insira um ou mais dos seguintes itens a serem verificados.

Verificadores de vulnerabilidade

Item a ser verificado	Descrição
Item de configuração	No campo **Item de configuração a ser verificado**, selecione o IC a ser verificado.
Endereços IP	No campo **Endereços IP a serem verificados**, insira os endereços IP, separados por vírgulas.

5. Depois de fazer suas seleções, clique em **Enviar**.
   Se um observável for encontrado, um indicador será criado, de acordo com os padrões STIXX.
6. Para exibir o status e/ou os resultados das verificações, navegue até **Autoatendimento** > **Minhas solicitações**.
7. Clique no número de SR da solicitação.
   As anotações de trabalho em **Atividades** listam as tarefas realizadas durante a verificação, incluindo a criação de verificações individuais para cada IC ou endereço IP e os resultados das verificações.

Gerenciar oorquestração de n-demand

Durante a Security Incident Response análise, um analista de segurança pode executar uma tarefa que é orientada por um fluxo de trabalho de incidente de segurança. Por exemplo, execute um despejo de processo em um IC específico. Isso pode ser realizado com a orquestração sob demanda.

Cada aplicação de Operações de segurança registrada inclui várias orquestrações sob demanda no sistema de base. Você pode definir orquestrações personalizadas sob demanda, conforme necessário.

A orquestração sob demanda pode ser invocada a partir de uma lista de seleção na parte inferior das seguintes listas e formulários em Security Incident Response:

- Formulário Incidente de segurança
- Lista de incidentes de segurança
- Lista relacionada de observáveis de incidente de segurança
- Lista relacionada de itens de configuração

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Uma propriedade em Common de suporte de segurança chamada **sn_sec_cmn.use_on_demand_tbl_as_allowed** define quais fluxos de trabalho estão disponíveis para execução sob demanda.
- Se a propriedade estiver definida como **verdadeira**, somente os fluxos de trabalho especificados na tabela Orquestração sob demanda [sn_sec_cmn_on_demand_orchestration] estarão disponíveis.
- Se a propriedade estiver definida como **falsa** (padrão), todos os fluxos de trabalho das aplicações configuradas no Registro de aplicações SecOps estarão disponíveis.
- Dependendo da configuração da propriedade, a lista de fluxos de trabalho disponíveis é personalizada para o tipo de informação que está sendo analisada.

Executar orquestração sob demanda a partir do formulário de Incidente de segurança

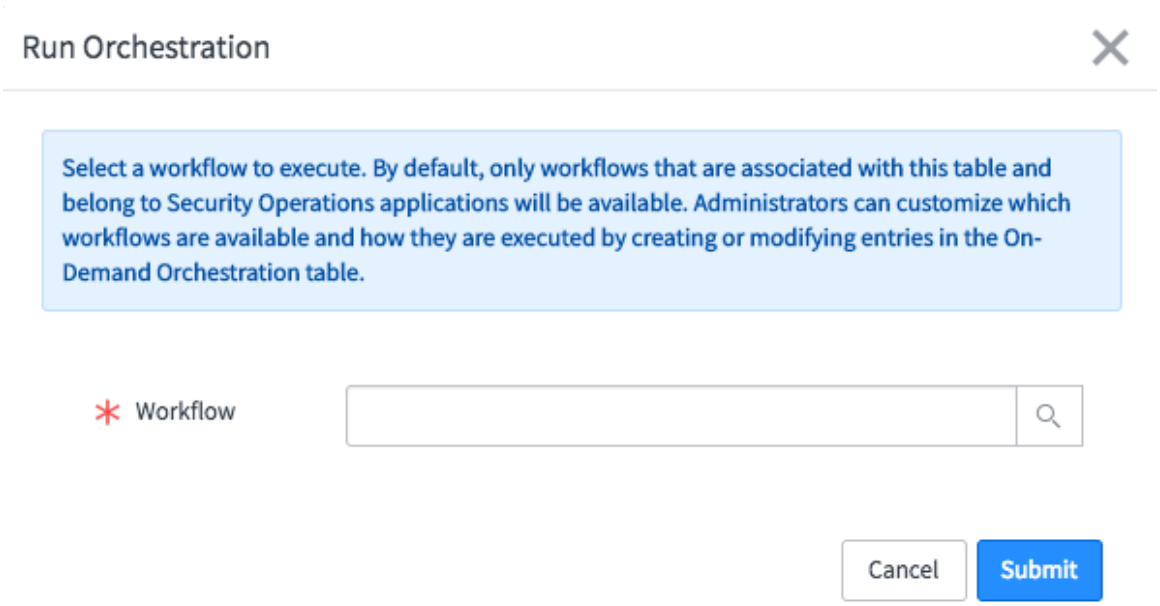
A orquestração sob demanda pode ser invocada em uma lista de seleção na parte inferior do formulário de Incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
2. Selecione o registro (incidente de segurança, observável ou IC) para o qual você deseja executar um fluxo de trabalho.
3. Clique no link relacionado **Executar Orquestração**.
   A caixa de diálogo **Executar Orquestração** é aberta. A aparência da caixa de diálogo depende da configuração da propriedade sn_sec_cmn.use_on_demand_tbl_as_whitelist em Security Support Common.



4. Clique no ícone de pesquisa e selecione o fluxo de trabalho que você deseja executar.
   O fluxo de trabalho selecionado é executado. Para obter detalhes, consulte Orquestração do Security Incident Response fluxos de trabalho e atividades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar orquestração sob demanda da lista de incidentes de segurança

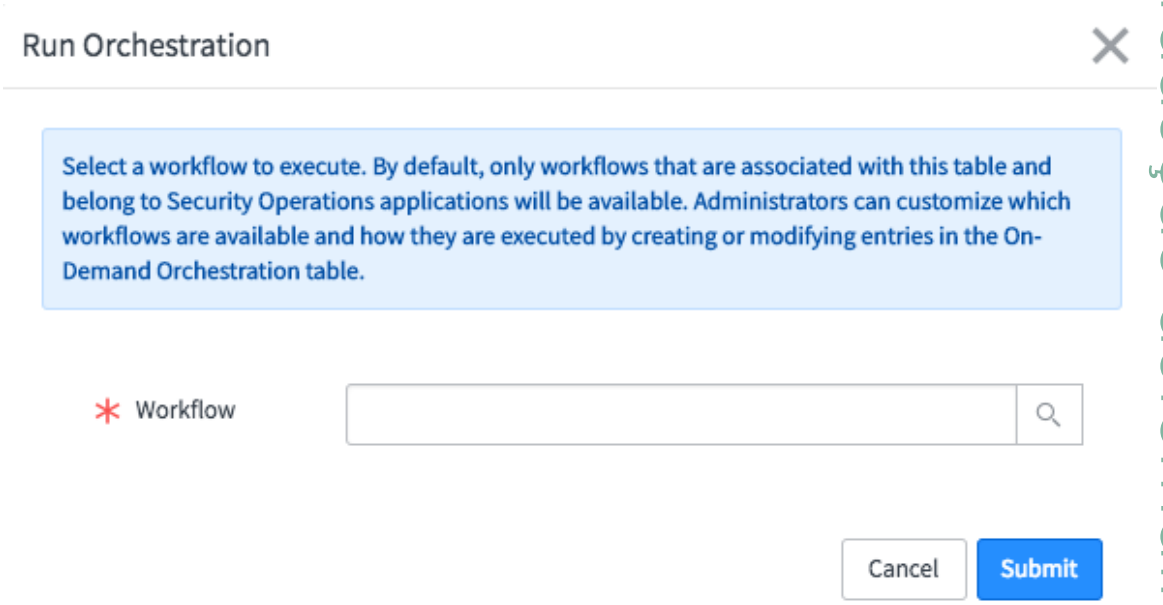
A orquestração sob demanda pode ser invocada na lista de Incidentes de segurança, bem como nas listas relacionadas em Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
2. Marque a caixa de seleção ao lado do incidente de segurança para o qual você deseja executar um fluxo de trabalho.
3. Clique na lista de seleção **Ações nas linhas selecionadas** na parte inferior da tela e clique em **Executar Orquestração**.
   A caixa de diálogo **Executar Orquestração** é aberta. A aparência da caixa de diálogo depende da configuração da propriedade sn_sec_cmn.use_on_demand_tbl_as_whitelist em Security Support Common.



4. Clique no ícone de pesquisa e selecione o fluxo de trabalho que você deseja executar.
   O fluxo de trabalho selecionado é executado. Para obter detalhes, consulte Orquestração do Security Incident Response fluxos de trabalho e atividades.

Definir novas orquestrações sob demanda

No sistema de base, você pode selecionar orquestrações sob demanda que executam fluxos de trabalho predefinidos. Você pode definir novas orquestrações sob demanda para personalizar como os fluxos de trabalho são invocados nas listas de seleção **Executar Orquestração**.

Antes de Iniciar

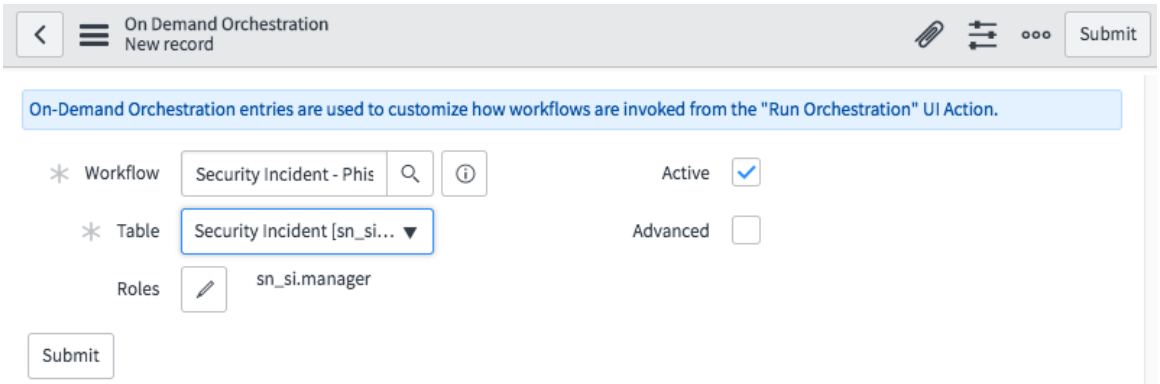
Função necessária: sn_si.write

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Orquestração sob Demanda**
2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Preencha os campos, se for o caso.

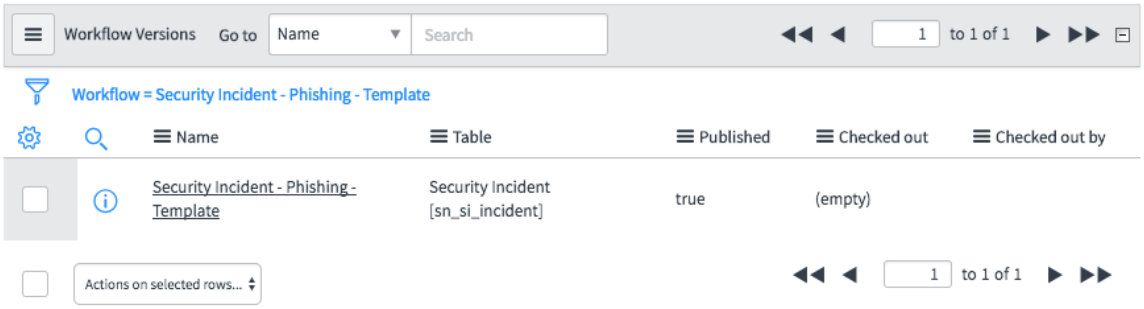
Orquestração sob Demanda

Campo	Descrição
Fluxo de trabalho	Selecione o fluxo de trabalho a ser incluído na lista de seleção **Executar Orquestração**.
Tabela	Selecione a tabela na qual o fluxo de trabalho selecionado será executado. Se a tabela não corresponder à tabela configurada para o fluxo de trabalho selecionado, você deverá marcar a caixa de seleção **Avançado** e modificar o **script de execução** para passar o registro correto para o fluxo de trabalho em execução.
Funções	Conforme necessário, selecione funções adicionais para restringir quem pode ver este fluxo de trabalho na lista de seleção **Executar Orquestração**.
Ativo	Marque esta caixa de seleção para ativar este registro de orquestração sob demanda.
Avançado	Marque esta caixa de seleção para modificar o script de execução para que ele passe o registro correto para a tabela selecionada para este fluxo de trabalho.
Script de execução	Modifique o script de execução para que ele passe o registro correto para a tabela selecionada para este fluxo de trabalho. Este campo aparece apenas se a caixa de seleção **Avançado** estiver marcada.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar**.
A lista relacionada **Versões de fluxo** de trabalho é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Se você precisar fazer modificações adicionais no fluxo de trabalho, será necessário fazer check-out.

Informações relacionadas

Como trabalhar com versões de fluxo de trabalho

Registrar novas aplicações de Operações de segurança para orquestração sob demanda

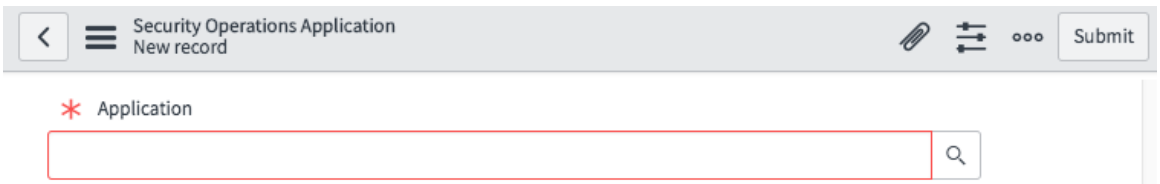
No sistema base, as aplicações Operações de segurança são registradas automaticamente quando são ativadas. O registro permite que os fluxos de trabalho associados às aplicações estejam disponíveis para solicitações de orquestração sob demanda. Se necessário, você pode definir novas aplicações e associar fluxos de trabalho a elas para orquestração sob demanda.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

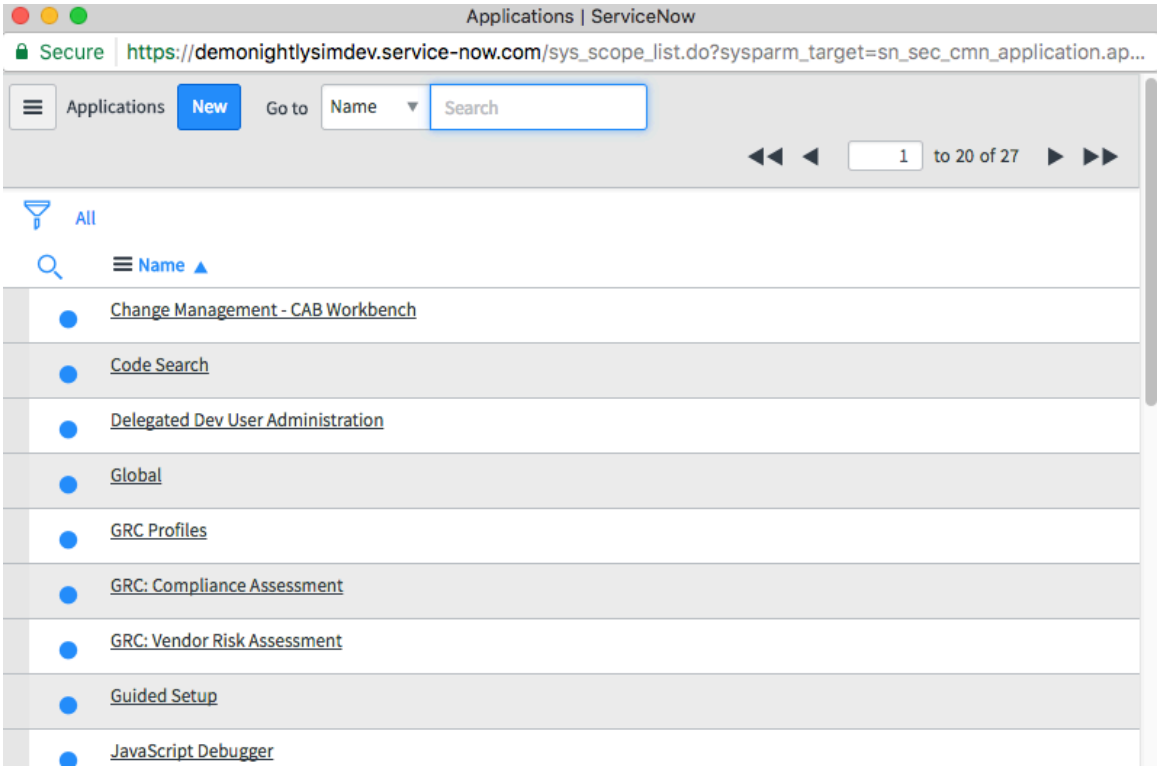
1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Registro da aplicação SecOps**e clique em **Registrar aplicação**.
   A tela da aplicação Operações de segurança é exibida.



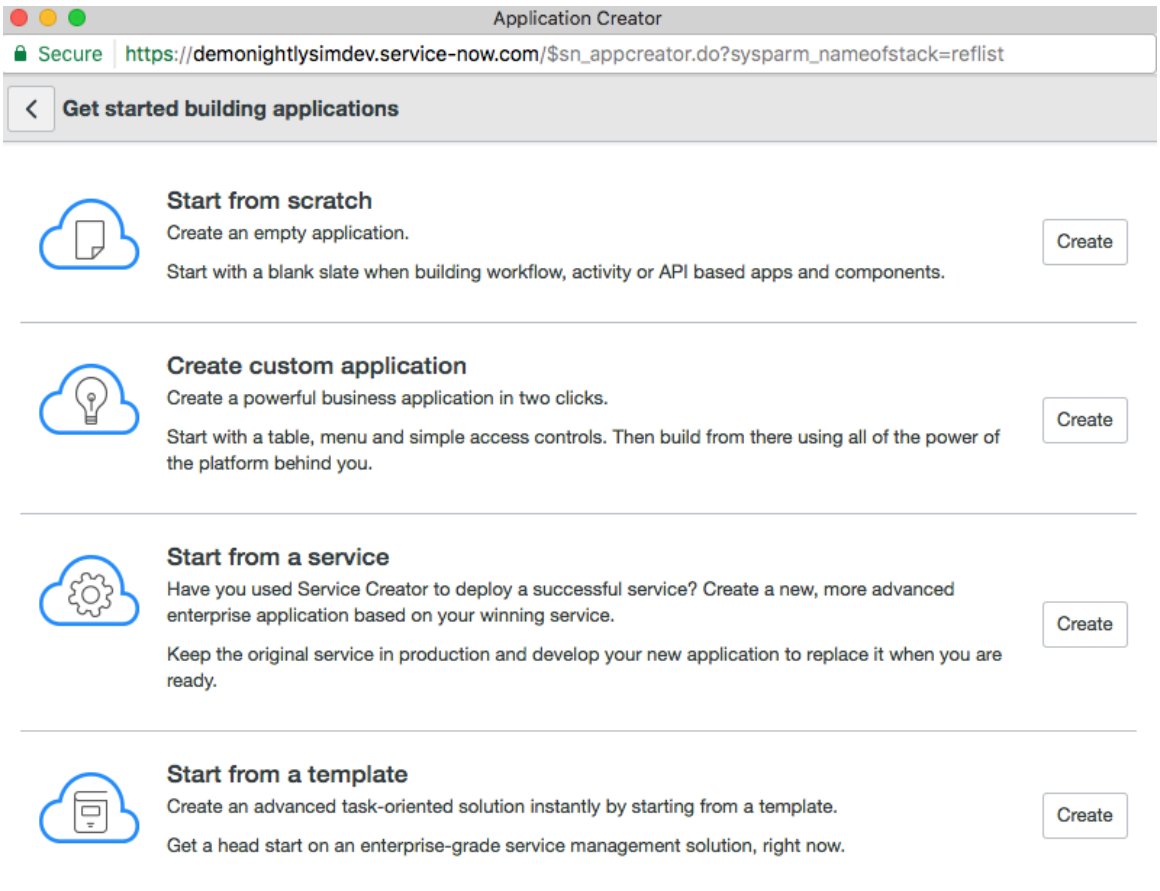
2. No campo **Aplicação**, clique no ícone de pesquisas (lupa).
   A tela Aplicações é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Nova**.
A tela do Criador de aplicações é exibida.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As opções exibidas dependem das aplicações que você ativou. Para obter informações detalhadas sobre como criar novas aplicações, consulte Como criar aplicações .

4. Depois que a aplicação tiver sido gerada, você poderá criar scripts para configurar a orquestração sob demanda.

Nota: Configurar a orquestração sob demanda para novas aplicações requer conhecimento técnico avançado de script e criação de gatilhos para os scripts (regras de negócio, ação de IU, fluxos de trabalho e assim por diante). Para obter mais informações, entre em contato com ServiceNow Serviços profissionais.

Adicionar informações a um incidente de segurança

Depois que um incidente de segurança é criado, você pode adicionar mais detalhes para ajudar na análise, como funções de acesso e diferentes tipos de anotações.

Antes de Iniciar

Função necessária: sn_si.basic

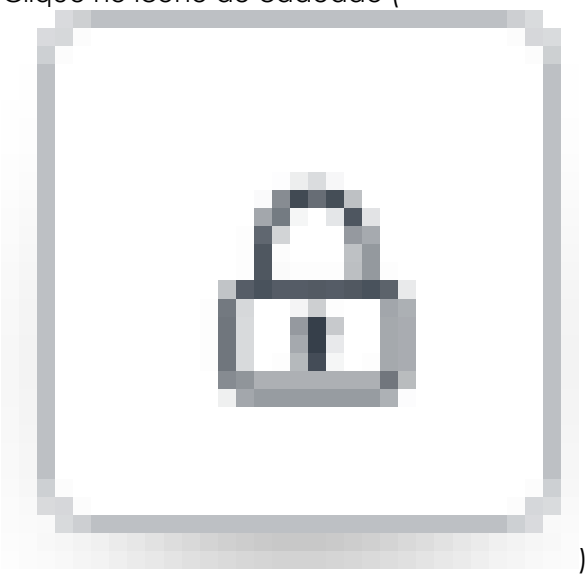
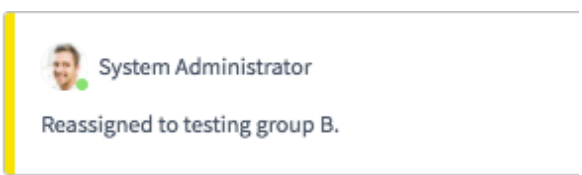
Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique na guia **Detalhes do incidente**.
3. Preencha os campos conforme necessário.

Campo	Descrição
Acesso de leitura	Concede a um usuário com a função **de acesso especial acesso** de leitura ao incidente de segurança. O usuário é capaz de ler e escrever anotações de trabalho. **Nota:** ◦ Se um usuário for adicionado às listas de acesso de **leitura e de acessoprivilegiado**, somente as permissões de **acesso privilegiado** persistirão. ◦ O usuário com a função sn_si.admin só pode modificar o acesso de leitura e o acesso privilegiado.
Lista de observação	Clique no ícone de cadeado para adicionar usuários que serão notificados quando ocorrerem mudanças no incidente de segurança. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários ou inserir endereços de e-mail do usuário. Ao concluir suas entradas, clique no ícone de cadeado para bloquear o campo.
Acesso privilegiado	Concede a um usuário com a função **de acesso especial acesso de** leitura e gravação a todos os campos do incidente de segurança, exceto **Atribuído a**. Usuários com funções de acesso especiais têm seu próprio módulo que contém todos os incidentes de segurança atribuídos a eles. Nenhum outro módulo está disponível para eles. Ninguém mais pode ver o módulo **Visível para mim**.

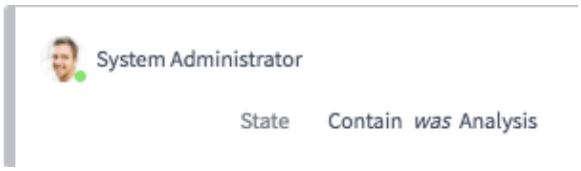
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

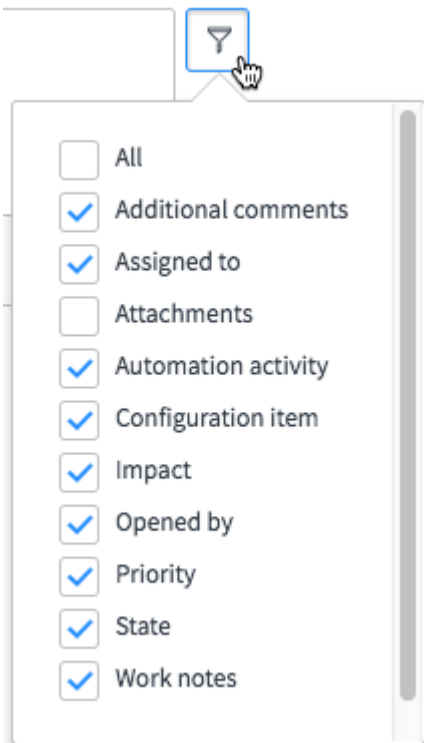
Campo	Descrição
	Nota: Somente um usuário atribuído ou alguém com uma função de segurança (por exemplo, sn_si_analyst ou sn_si.admin) pode alterar o campo **Atribuído a**. Se um usuário for adicionado às listas de acesso de **leitura e de acessoprivilegiado**, somente as permissões de **acesso privilegiado** persistirão.
Lista de Anotações de trabalho	Clique no ícone de cadeado () para adicionar usuários que serão notificados quando novas anotações de trabalho forem adicionadas. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários ou inserir endereços de e-mail do usuário. Ao concluir suas entradas, clique no ícone de cadeado para bloquear o campo.
Descrição	Insira uma descrição completa do incidente de segurança, junto com todas as informações que possam ajudar a encontrar a causa ou resolver o problema.
Notas de segurança	Somente as funções de usuário com sn_si.admin e sn_si.analyst podem exibir ou editar as anotações seguras.
Anotações de trabalho	Digite anotações de trabalho que não estão visíveis para o cliente. As anotações de trabalho aparecem na área **Atividade**.
Atividade	Exibe informações inseridas manualmente em Anotações de trabalho e todas as atividades de tarefa atualizadas dinamicamente (ações, comentários, anotações de trabalho e assim por diante) em registros relacionados a este incidente de segurança. As anotações de trabalho aparecem com uma faixa amarela. 

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	As anotações geradas automaticamente aparecem com uma faixa de cor cinza. 

4. Você pode limitar os tipos de informações exibidas no campo **Atividade** clicando no ícone de filtro ( ).



Nota: A caixa de seleção **Atividade de automação** permite incluir qualquer enriquecimento realizado por este incidente de segurança, incluindo atividades de fluxo de trabalho, atualizações de pontuação de risco e assim por diante.

5. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Registros relacionados
   - Análise pós-incidente
   - Informações de Fechamento
6. Ao concluir suas entradas, clique em **Enviar**.

Adicionar problemas, mudanças e incidentes relacionados a um incidente de segurança

Você pode adicionar registros relacionados, como problemas, mudanças e incidentes a incidentes de segurança existentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento
1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique na guia **Registros relacionados**.
3. Preencha os campos conforme necessário.

Campo	Descrição
Problema	Selecione um registro de Problema (PRB) que resolva o problema subjacente que causou a criação deste incidente de segurança. Os PRBs para este incidente são normalmente criados clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar problema**.
Primário	Selecione um registro de tarefa relacionado ao problema subjacente que causou a criação deste incidente de segurança.
Incidente de segurança primário	Selecione um registro de incidente de segurança relacionado ao problema subjacente que causou a criação deste incidente de segurança. Consulte Relacionamentos entre incidentes de segurança primários e secundários.
Incidente	Selecione um registro de Incidente (INC) que resolva o problema subjacente que causou a criação deste incidente de segurança. O incidente é normalmente criado clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar incidente**.
Solicitação de mudança	Selecione um registro de Solicitação de Mudança (CHG) que resolva o problema subjacente que causou a criação deste incidente de segurança. A solicitação de mudança normalmente é criada clicando com o botão direito do mouse no cabeçalho do formulário do incidente de segurança e selecionando **Criar mudança**.

4. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Detalhes de Incidentes
   - Análise pós-incidente
   - Informações de Fechamento
5. Ao concluir suas entradas, clique em **Enviar**.

Invocar um despejo de processo para um processo aprimorado no Windows

Um analista de segurança pode executar um despejo de processo em um processo específico, despejá-lo em um arquivo e publicá-lo em um site compartilhado em uma rede interna. Um analista pode exibir um processo da lista de proibições, destacado em vermelho em um incidente de segurança, e executar análises adicionais.

Antes de Iniciar
Os itens a seguir são necessários:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um cliente executando o Windows Vista ou superior ou um servidor executando o Windows Server 2008 ou superior.
- O utilitário de linha de comando ProcDump instalado, com uma variável de ambiente do sistema que aponta para o caminho do arquivo executável do procdump. O nome da variável deve ser PROCDUMP. Este nome é usado em um script do PowerShell.

Função necessária: sn_si.analyst

Procedimento

1. Navegue até o incidente de segurança com o processo aprimorado no qual você deseja invocar um procdump clicando em **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**e abrir um incidente de segurança.
2. Clique na guia **Dados** de aprimoramento.
3. Clique no registro de aprimoramento **Recuperar processos em execução**.
4. Marque as caixas de seleção dos processos em execução para os quais você deseja executar um procdump, clique na lista suspensa Ações nas linhas selecionadas na parte inferior da lista e clique em **Executar procdump**.
   Uma **mensagem de Fluxo de trabalho de produção iniciado para o processo selecionado** aparece na parte superior da lista e o fluxo de trabalho **Resposta a incidentes de segurança - Executar procdump** é executado.

Exibir informações em um incidente de segurança

Você pode executar várias outras ações em um incidente de segurança existente usando os links relacionados.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Em **Links relacionados**, você pode executar as seguintes tarefas,

Opção	Descrição
Exibir runbook manual	Exiba uma lista de runbooks disponíveis para este incidente de segurança.
Fluxo de trabalho de resposta	Exibir qualquer fluxo de trabalho associado a este incidente.
Adicionar Vários Observáveis	Adiciona uma lista de observáveis nos formatos delimitados por vírgula, nova linha, guia ou pipe.
Adicionar ao Caso de Segurança	Adiciona o incidente de segurança a um ou mais casos de segurança. Você também pode criar um novo caso de segurança e adicionar este incidente de segurança a ele.
Obter resumos de IP do QRadar	Se uma integração do QRadar estiver disponível e contiver ICs válidos e endereços IP de origem e de destino, ela acionará os

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	fluxos de trabalho do QRadar e exibirá os resultados em anotações de trabalho.
Executar Orquestração	Escolha e execute um fluxo de trabalho das Operações de segurança.
Exibição da linha do tempo do ANS	Você pode exibir uma linha do tempo de ANS de um registro de ANS de tarefa ou de uma definição do ANS.
Mostrar todas as listas relacionadas	Exibe todas as listas relacionadas padrão e todas as listas adicionadas manualmente. **Nota:** Itens adicionados manualmente estão disponíveis somente nesta exibição.
Mostrar itens afetados	Exibe as listas de ICs, usuários e serviços diretamente afetados por este incidente
Mostrar itens relacionados	Exibe as listas de incidentes relacionados, ICs, usuários e grupos afetados por este incidente.
Mostrar IoC	Exibe as listas de observáveis, indicadores, malware, modos e métodos e solicitações de verificação de segurança associadas a este incidente.
Mostrar dados de enriquecimento	Exibe as listas de dados de aprimoramento, processos, serviços, estatísticas, pesquisas, logs de firewall e informações de usuários comprometidos associados a este incidente.
Mostrar tarefas de resposta	Exibe as listas de tarefas, ANS, auditorias de pontuação de risco, indisponibilidades e pesquisas do Exchange associadas a este incidente.
Exibir detalhes no sistema externo	Se este incidente de segurança tiver sido gerado a partir de uma aplicação externa, diretamente ou por eventos, e um link para os dados de origem tiver sido fornecido, a ação **Exibir detalhes no sistema externo** abrirá o URL. Você pode exibir e pesquisar os logs que geraram este incidente.
Verificar vulnerabilidades	Se Resposta a vulnerabilidades estiver ativado e você tiver selecionado pelo menos um IC afetado para o incidente de segurança, poderá enviar uma solicitação de verificação para determinar quais vulnerabilidades existem no IC.

Tradução automática

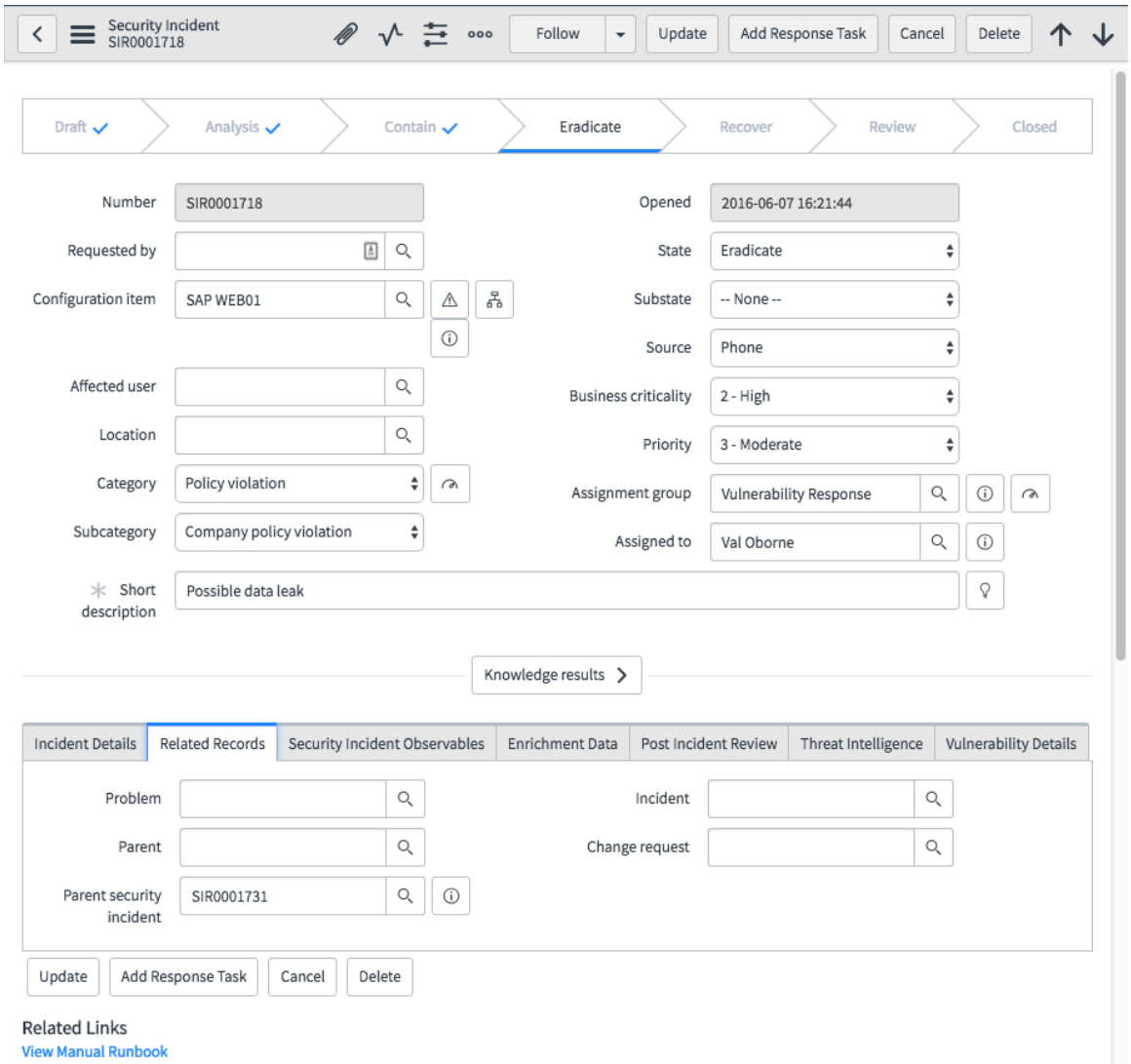
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos entre incidentes de segurança primários e secundários

Você pode associar e rastrear o impacto de qualquer problema usando relacionamentos de incidentes de segurança primários e secundários em Security Incident Response.

Usando a guia **Registros relacionados**, você pode adicionar um problema de **incidente de segurança primário** a qualquer formulário Security Incident Response. Este recurso torna automaticamente o incidente um secundário que aparece na guia **Listas relacionadas - Incidentes de segurança secundários** do problema primário.

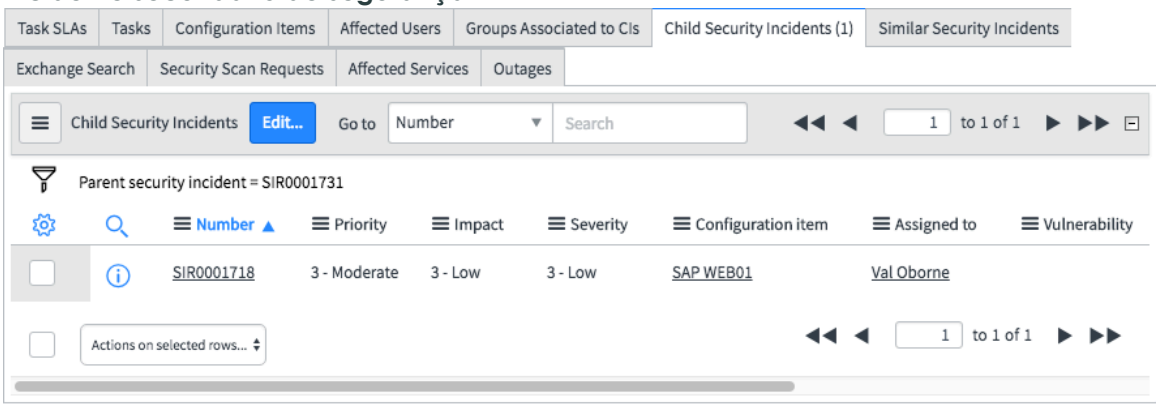
Nota: Você não pode tornar um incidente de segurança primário existente seu próprio secundário usando o mesmo número para ambos os incidentes.



Tradução automática

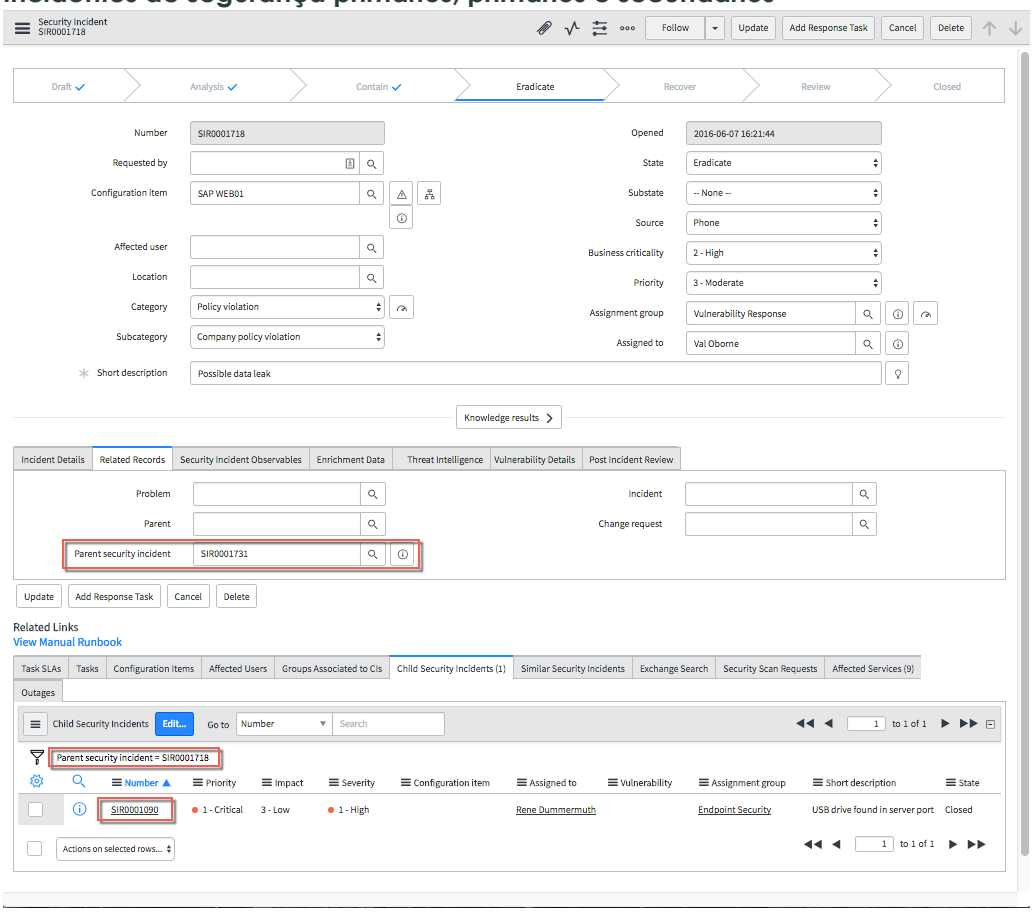
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente secundário de segurança



Você também pode adicionar um ou mais **incidentes de segurança secundários** a qualquer registro de incidente de segurança, usando o botão **Editar** na guia **Incidentes de segurança secundários**. No exemplo a seguir, todos os três registros estão conectados.

Incidentes de segurança primários, primários e secundários



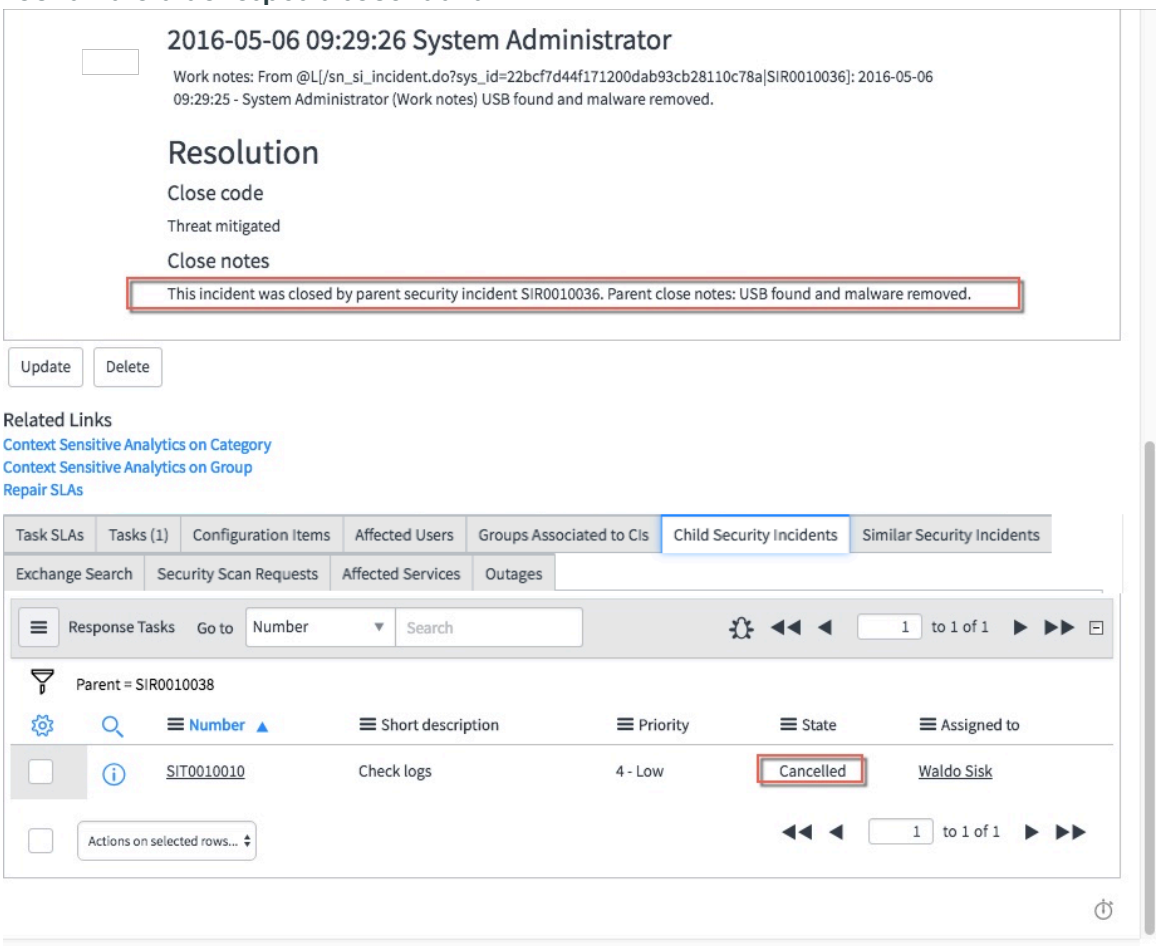
Observação: todas as anotações de trabalho registradas no primário são propagadas para todos os secundários ativos em **Atividades** na guia **Detalhes do incidente**.

Quando um primário é fechado ou cancelado, todos os secundários ativos também são fechados ou cancelados. Todas as **tarefas de resposta** ativas nos incidentes secundários são canceladas. Se não houver outras **tarefas**em aberto, o incidente secundário será encerrado. Quando fechada, a **Entrevista pós-incidente** registra o fechamento e as informações encontradas na guia **Informações de fechamento** são propagadas do primário para os secundários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fechar tarefa de resposta secundária



Exibir itens afetados por um incidente de segurança

Você pode exibir itens afetados, como ICs, usuários afetados e serviços afetados associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir os itens afetados.
2. Clique no link relacionado **Mostrar itens afetados**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações ao incidente de segurança.

Guia	Descrição
Itens de configuração	Itens de configuração (IC) afetados. Depois que os ICs afetados forem identificados, você poderá adicionar manualmente os recursos afetados dessa lista relacionada.
Usuários afetados	Depois que os usuários afetados forem identificados, você poderá adicionar manualmente os usuários afetados dessa lista relacionada.
Serviços afetados	Exiba ou adicione serviços de negócio associados ao incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia	Descrição
	Nota: Se um IC afetado for adicionado após a abertura do incidente de segurança, convém clicar com o botão direito do mouse no cabeçalho do formulário e selecionar **Atualizar serviços afetados**.

Nota: Se a capacidade de integração de Operações de segurança - Obter processos em execução estiver ativa e você adicionar um IC a um incidente de segurança, o fluxo de trabalho Obter processos em execução será executado e recuperará uma lista de processos em execução no IC.

Se a capacidade de integração do Security Operations Integration - Isolar host estiver ativa, você poderá selecionar um ou mais ICs e restringir suas conexões do sistema a outros dispositivos. Para fazer isso, marque as caixas de seleção dos ICs e clique em **Isolar host** na lista de seleção **Ações nas linhas selecionadas**.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar dados de enriquecimento
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar**.

Exibir itens relacionados a um incidente de segurança

Você pode exibir itens relacionados, como incidentes de segurança semelhantes e secundários, usuários relacionados, grupos de vulnerabilidades e itens vulneráveis associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir itens relacionados.
2. Clique no link relacionado **Mostrar itens** relacionados.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações ao incidente de segurança.

Guia	Descrição
Incidentes de segurança secundário	Selecione um registro de tarefa relacionado ao problema que causou a criação deste incidente de segurança.
Incidentes de segurança semelhantes	Exibir quaisquer outros incidentes de segurança associados a qualquer um dos mesmos registros observáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia	Descrição
Itens de Configuração Relacionados	Exibe uma lista de incidentes de segurança que contêm itens de configuração com o mesmo observável que este incidente de segurança. Esta lista pode ser filtrada usando o grupo de filtros de **exclusões de IC**. Quando um observável é adicionado a um incidente de segurança, essa lista é atualizada automaticamente. Por padrão, os observáveis com um tipo de contexto de destino são excluídos.
Usuários relacionados	Exibe uma lista de incidentes de segurança que contêm usuários com os mesmos observáveis que este incidente de segurança. Esta lista pode ser filtrada usando o grupo de filtros **de exclusão de usuário**. Quando um observável é adicionado a um incidente de segurança, essa lista é atualizada automaticamente. Por padrão, os observáveis com um tipo de contexto de destino são excluídos.
Grupo de filtros relacionados	Depois que os itens de configuração são identificados, todos os ICs ou grupos de filtros correspondentes são adicionados automaticamente.
Grupos de vulnerabilidade	Se Resposta a vulnerabilidades estiver ativado, você poderá exibir grupos de vulnerabilidades associados a este incidente de segurança.
Itens vulneráveis	Se Resposta a vulnerabilidades estiver ativado, você poderá exibir itens de vulnerabilidade associados a este incidente de segurança.
Riscos	Se qualquer um dos principais plug-ins da Gestão de riscos (Policy and Compliance Management, Audit, Management ou Risk Management) estiver ativado, você poderá exibir ou adicionar riscos associados ao incidente de segurança. Você pode adicionar esta lista relacionada a partir do menu de contexto do cabeçalho do formulário em **Configurar** > **Listas relacionadas**.
Eventos de item de configuração	Se Gestão de eventos estiver ativado, você poderá exibir eventos.
Alertas de item de configuração	Se Gestão de eventos estiver ativado, você poderá exibir alertas.
Casos de atendimento ao cliente	Se Atendimento ao cliente estiver ativado, você poderá exibir Atendimento ao cliente informações do caso.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar IoC
   - Mostrar dados de enriquecimento
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir dados de aprimoramento de um incidente de segurança

Você pode exibir dados de aprimoramento, como processos em execução, serviços em execução e estatísticas de rede associadas a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir os dados de aprimoramento.
2. Clique no link relacionado **Mostrar dados de aprimoramento**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações ao incidente de segurança.

   Nota: Os detalhes dos dados brutos são armazenados em um anexo no registro de dados de aprimoramento. Se excederem o limite do campo, os detalhes exibidos serão truncados.

Guia	Descrição
Processos em execução	Armazena os registros criados pelo fluxo de trabalho Security Incident Response **Obter processos em execução**.
Serviços em execução	Armazena os registros criados pelo fluxo de trabalho Security Incident Response **Obter serviços em execução**.
Estatísticas de Rede	Armazena os registros criados pelo fluxo de trabalho Security Incident Response **Obter estatísticas de rede**.
Pesquisas de domínio	Se o plug-in WhoisXML API Integration estiver ativado, armazenará os registros criados por uma pesquisa Whois.
Logs do Firewall	Armazena dados de aprimoramento de logs de firewall, como os logs de firewall da Palo Alto Network.
Informações do usuário comprometido	Armazena contas identificadas como comprometidas por meio de Have I Been Pwned? pesquisa.

   Observação: a guia **Dados de aprimoramento da segurança** mostra dados brutos de aprimoramento de fluxos de trabalho Security Incident Response, como recuperação de estatísticas de rede ou processos em execução. Esta guia pode ser exibida clicando no link relacionado **Mostrar todas as listas** relacionadas.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar tarefas de resposta
5. Ao concluir suas entradas, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir informações da tarefa de resposta para um incidente de segurança

Você pode exibir informações da tarefa de resposta, como SLAs de tarefa e auditorias de pontuação de risco. e indisponibilidades associadas a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir as tarefas de resposta.
2. Clique no link relacionado **Mostrar tarefas de resposta**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações ao incidente de segurança.

Guia	Descrição
Tarefas	Exibe as tarefas já definidas para o incidente de segurança. Você pode criar manualmente uma tarefa de resposta ou e Criar uma tarefa a partir desta lista relacionada.
Tarefas de Resposta	Exibe ações a serem executadas em resposta ao incidente de segurança.
ANS de tarefas	Exiba ou adicione SLAs de tarefa ativa que foram definidos para o incidente de segurança.
Auditorias de Pontuação de Risco	Um registro de auditoria para cada instância de uma pontuação de risco que está sendo alterada.
Indisponibilidades	Exiba ou adicione manualmente novos registros de indisponibilidade associados ao incidente de segurança.
Pesquisa de E-mail	Uma lista de registros que contém critérios de pesquisa para executar consultas em um servidor de e-mail, como um Microsoft® Exchange Server (com base na implementação instalada) e armazena os resultados recebidos. **Nota:** se o Integração de Operações de segurança - Capacidade de pesquisa e exclusão de e-mail não estiver ativo, o link relacionado à **Pesquisa de e-mail** não será exibido.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar dados de enriquecimento
5. Ao concluir suas entradas, clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir eventos e alertas relacionados em incidentes de segurança

Enquanto um incidente de segurança está sendo trabalhado, você pode exibir os detalhes dos eventos. Para alertas, você pode exibir e confirmar esses alertas e criar incidentes ou incidentes de segurança a partir deles, conforme necessário.

Antes de Iniciar

Você deve ter o plug-in de suporte da Gestão de eventos de resposta a incidentes de segurança ativado.

Função necessária: si.sn_agent

Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Todos** > **Incidente de segurança** > **Incidentes** > **Incidentes não atribuídos**).
2. Se os recursos afetados pelo incidente de segurança que você está exibindo tiverem recebido alertas ou eventos nas últimas 24 horas, uma ou ambas as listas relacionadas a seguir serão exibidas.
   - Alertas de IC de incidente de segurança
   - Eventos de IC de incidente de segurança
3. Clique na lista relacionada que você deseja exibir.

Lista relacionada	Descrição
Alertas de IC de incidente de segurança	Você pode exibir detalhes de alertas recebidos nas últimas 24 horas. Você tem a opção de clicar em **Confirmar** para indicar que está ciente do alerta e que ele está sendo tratado. Use **Fechar** para indicar que o alerta não é importante.
Eventos de IC de incidente de segurança	Você pode exibir detalhes do evento recebido nas últimas 24 horas.

Exibir incidente de segurança para mapeamento de caso de atendimento ao cliente

Security Incident Response é enviado com um mapeamento de campo padrão que mapeia um incidente de segurança para um caso Atendimento ao cliente. Você pode exibir o incidente de segurança para o mapa padrão de caso de CS.

Antes de Iniciar

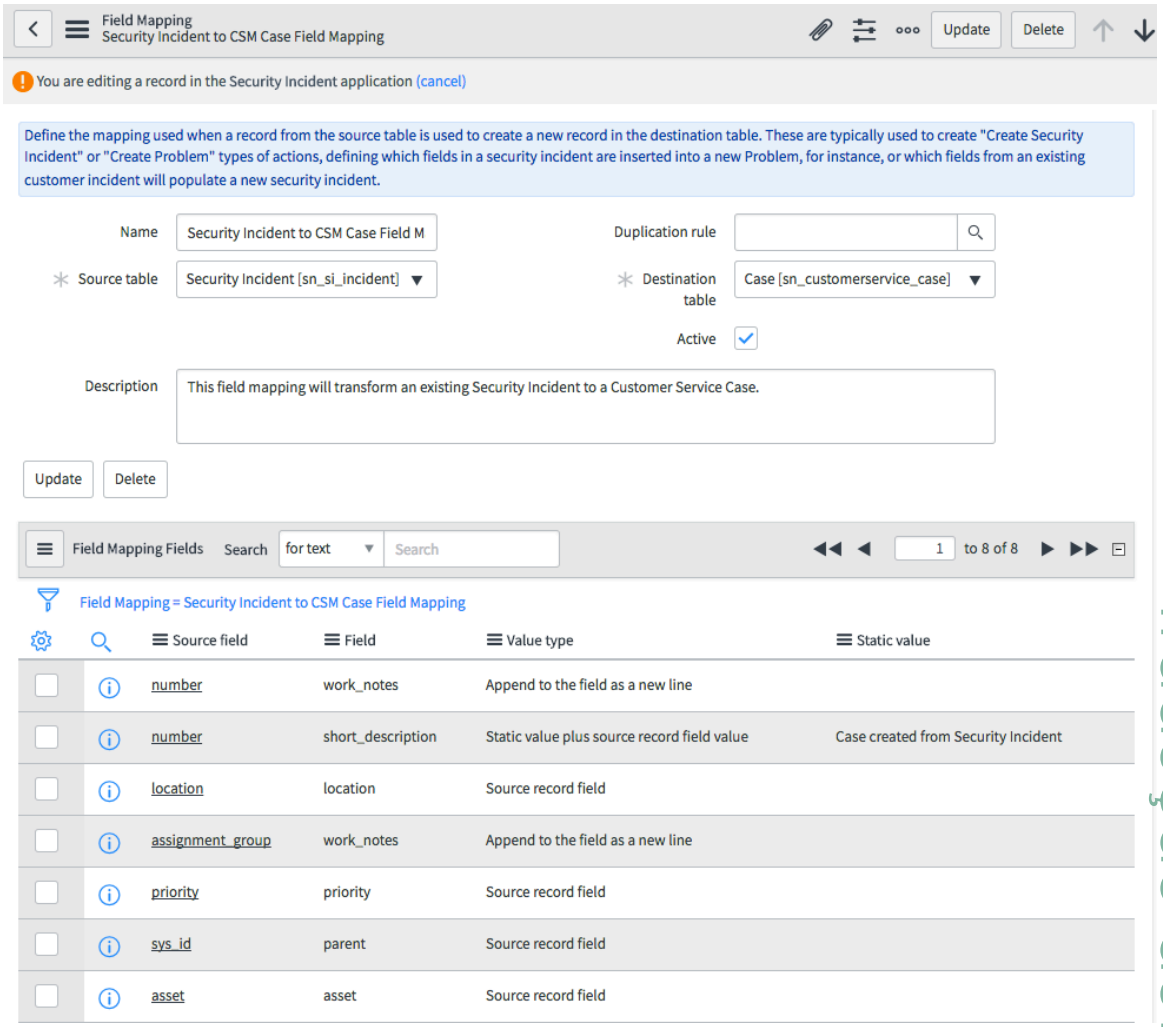
Função necessária: sec_cmn.read

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Mapeamento de Campos**.
2. Clique **em Incidente de segurança para mapeamento de campo de caso de CSM** para exibir o mapa padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Você pode editar o mapeamento, conforme necessário.

4. Ao concluir as mudanças, clique em **Atualizar**.

Exibir um runbook do Security Incident Response

Os runbooks concedem acesso a procedimentos relacionados às tarefas nas quais você está trabalhando.

Antes de Iniciar

Função necessária: sn.si.knowledge_admin

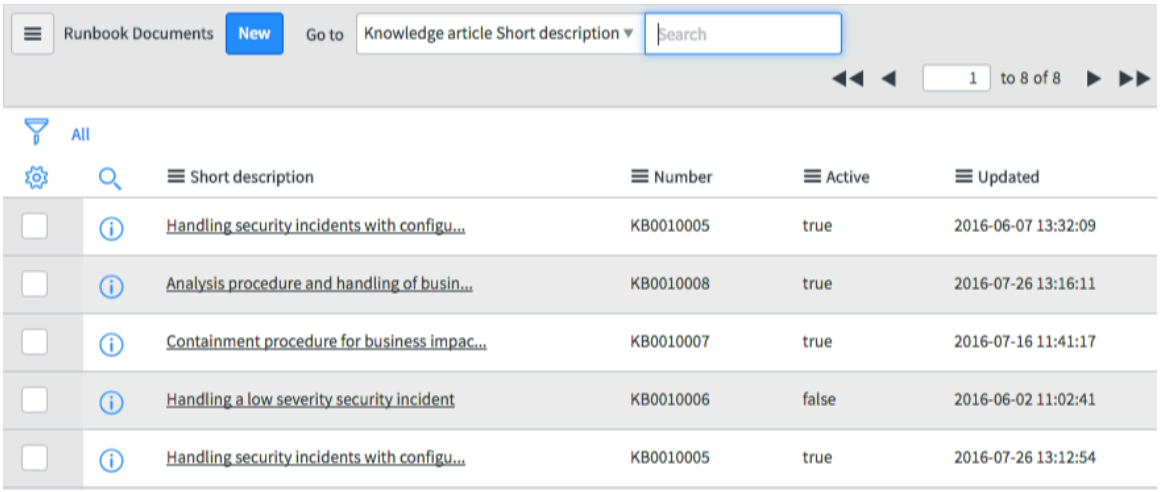
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Runbook manual** > **Exibir documentos do runbook**.

2. Selecione um runbook na lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para criar um runbook, clique em **Novo**.
   Para obter mais informações, consulte Criação de um runbook.

Identificar todos os itens de configuração afetados por um incidente de segurança

Se você souber qual recurso (servidor, desktop ou outro item de configuração) está por trás de um incidente de segurança e quiser identificar recursos relacionados e serviços de negócio que podem ser afetados, você pode usar o mapa de Gestão de serviços de negócio (BSM).

Antes de Iniciar

Função necessária: administrador ou sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

O mapa BSM exibe as dependências ascendentes e descendentes de um IC raiz selecionado.

Existem dois métodos que você pode usar para exibir o mapa BSM de um IC:

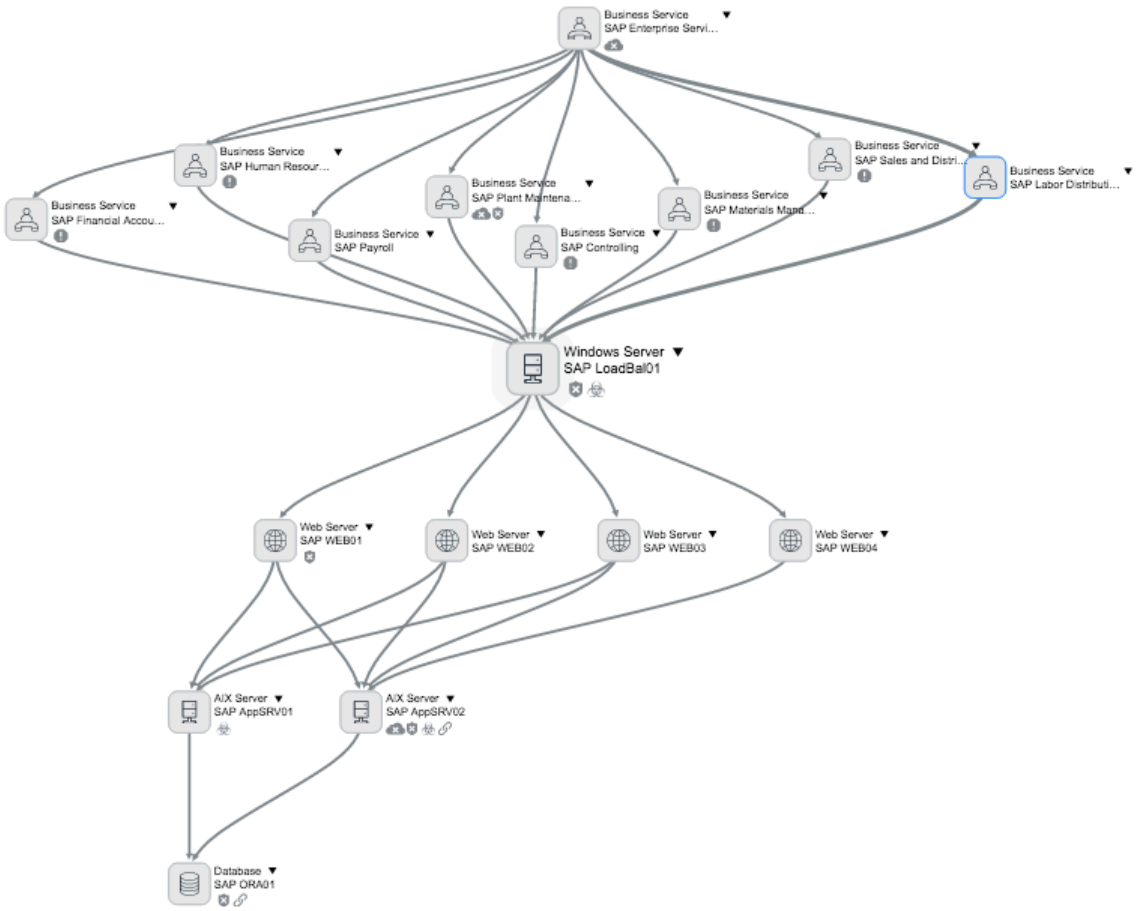
- Se você quiser exibir ICs no contexto de uma tarefa, exiba no formulário de incidente de segurança.
- Se você não quiser exibir ICs do ponto de vista de uma tarefa, exiba na barra de navegação.

Procedimento

1. No formulário Incidente de segurança, preencha o campo **Item de configuração** e clique no ícone de mapa BSM ( ).
   A tela do mapa BSM exibe o mapa do último incidente acessado na Gestão de incidentes ou o último incidente de segurança acessado na Gestão de incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique nos ícones ao lado de um item de configuração para exibir diferentes tipos de detalhes sobre o recurso (servidor, desktop ou outro IC).
   Por exemplo, clique em (⚠) para exibir alertas associados ao IC.

   Nota: Para exibir uma lista de todos os ícones disponíveis, clique em **Filtros** acima do mapa BSM e expanda **Tipos de tarefa**de filtro .

3. Para organizar o mapa em diferentes configurações, selecione qualquer um dos formatos listados acima do mapa (**Vertical**, **Horizontal**, **Radial**) ou clique em **Filtros** para filtrar o mapa e facilitar a exibição.
4. Se você abriu o mapa BSM a partir do formulário de incidente de segurança, poderá adicionar um IC dependente ao incidente de segurança clicando com o botão direito do mouse no IC e selecionando **Adicionar ICs afetados**.
   Você também pode adicionar vários ICs por vez. Arraste uma caixa ao redor dos ICs que deseja adicionar, clique com o botão direito do mouse na caixa e selecione **Adicionar ICs afetados**.
   Os ICs são adicionados à lista relacionada de ICs afetados do incidente de segurança.

Calcular a gravidade de um incidente de segurança

Você pode calcular a gravidade de um incidente de segurança usando calculadoras predefinidas.

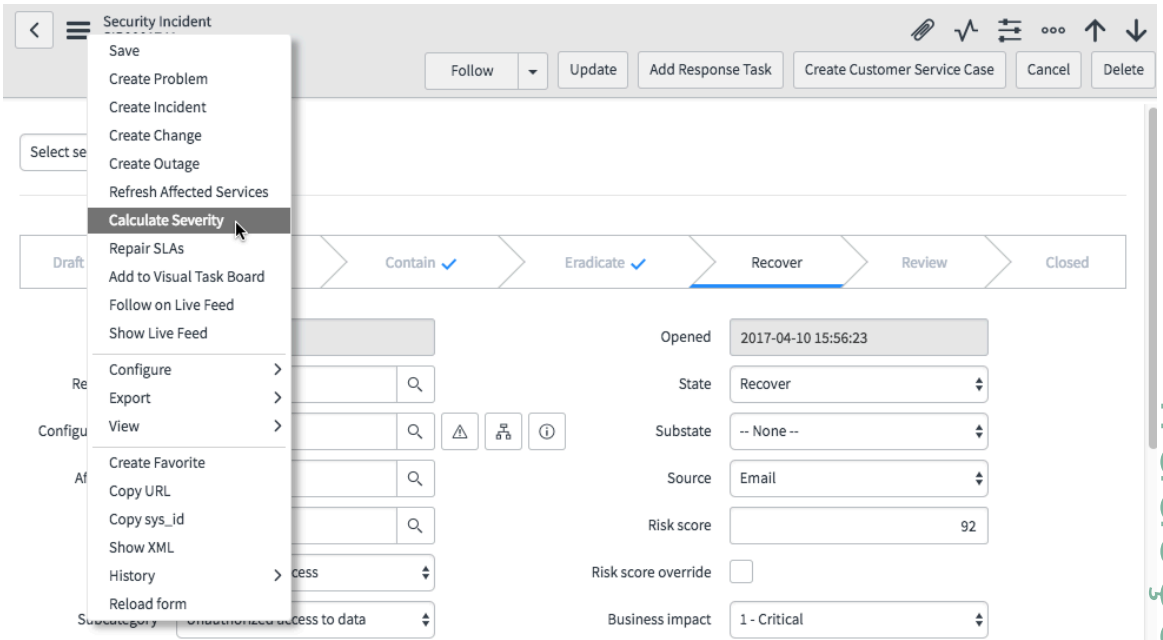
Antes de Iniciar
Função necessária: sn_si.basic

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja calcular a gravidade.
2. Clique no menu de contexto do cabeçalho do formulário e selecione **Calcular gravidade**:



A severidade é calculada com base nas regras predefinidas das calculadoras básicas. Para obter mais informações, consulte Noções básicas sobre calculadoras de incidentes de segurança.

Pesquisar e excluir e-mails de phishing

A exclusão de e-mails de phishing pode ajudar a reduzir a exposição a um ataque específico em uma organização. Você pode gerenciar e-mails de phishing no servidor de e-mail pesquisando, concedendo aprovações e excluindo-os.

Antes de Iniciar

Funções necessárias: sn_sec_cmn.cap_email_read

Você pode determinar quantos usuários foram alvo de um ataque de phishing consultando um registro de e-mail associado a um incidente de segurança.

Softwares compatíveis:

- Microsoft® Exchange Server 2010

Limitação: ao pesquisar o corpo dos e-mails, você pode pesquisar no máximo 1.500 caixas de correio.

Por Que e Quando Desempenhar Esta Tarefa

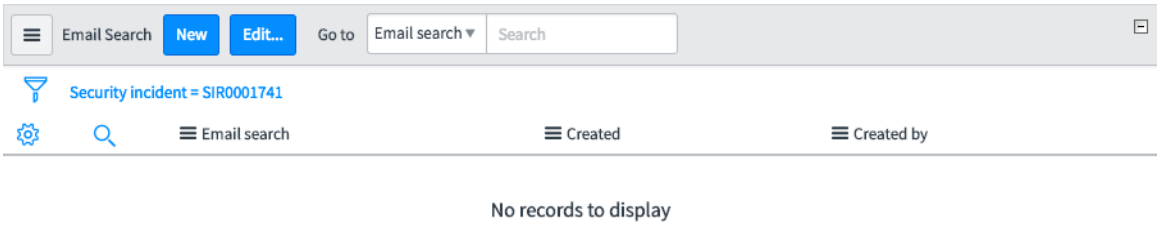
Este recurso é usado pelo Integração de Operações de segurança - Fluxo de trabalho de pesquisa e exclusão de e-mail para executar uma consulta no seu servidor de e-mail. Dependendo dos critérios de pesquisa selecionados, a pesquisa identifica todos os e-mails em um ataque de phishing e retorna o número total de e-mails afetados ou detalhes dos e-mails afetados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

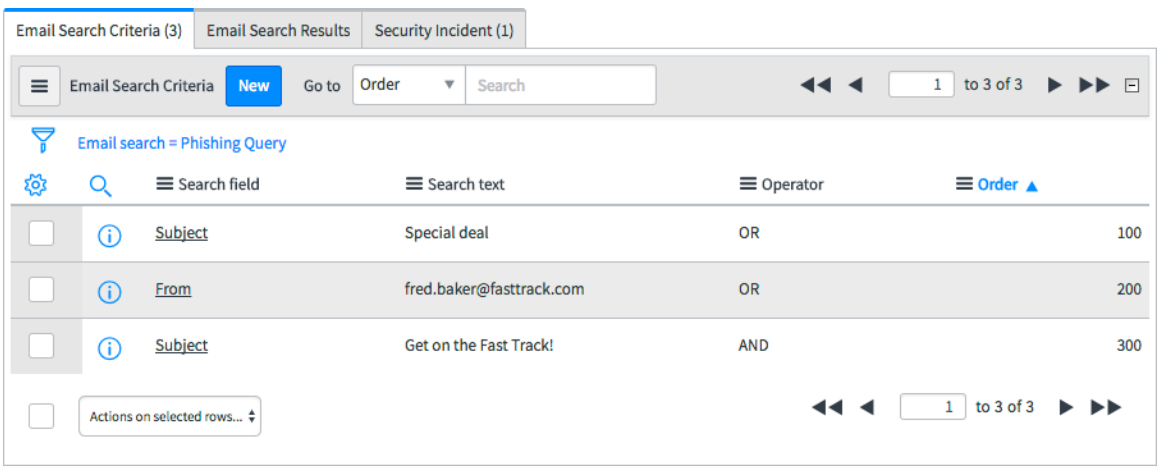
1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Escolha um incidente de segurança.
3. Se a lista relacionada **Pesquisa de e-mail** não estiver visível, clique no link relacionado **Mostrar todos os links** relacionados.
4. Clique na lista relacionada **Pesquisa de e-mail**.



5. Clique em **Nova**.
6. Preencha os campos, se for o caso.

Campo	Descrição
Nome	Nome da consulta de pesquisa
Consultar pelo critério	Uma visualização da consulta executada no servidor de e-mail. Gerado a partir de todos os registros de critérios de pesquisa ativa associados.
Descrição	Descreva o que a consulta de pesquisa está procurando.

7. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.



8. Clique na guia **Critérios de pesquisa de e-mail** e clique em **Novo**.
9. Preencha ou edite os campos, conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisa de e-mail	Exibe o nome da pesquisa de e-mail. Você pode alterá-lo, se necessário.
Campo de pesquisa	Campo para pesquisar no servidor de e-mail. O campo de pesquisa tem as seguintes opções: Assunto Esses critérios pesquisam e-mails que contenham o texto da linha de assunto especificado no campo **Texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem, são retornados. De Esses critérios pesquisam e-mails que contenham o endereço de e-mail completo do remetente (por exemplo, jane.doe@abc.com) especificado no campo de **texto Pesquisar**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem, são retornados. **Nota:** Você não pode usar os campos **De** e **Destinatário** na mesma consulta. Destinatário Esses critérios pesquisam e-mails que contenham o endereço de e-mail completo do destinatário (por exemplo, john.doe@abc.com)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	especificado no campo de **texto Pesquisar**. Ele também pesquisa e-mails nos campos Para, Cc e Cco. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem, são retornados. **Nota:** Você não pode usar os campos **De** e **Destinatário** na mesma consulta. Corpo Esses critérios pesquisam e-mails que contêm o texto do corpo especificado no campo **Texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Nota:** Ao pesquisar o corpo dos e-mails, você pode pesquisar no máximo 1.500 caixas de correio. Cc: Este critério pesquisa e-mails que contenham o endereço de e-mail completo Cc (por exemplo: jane.doe@abc.com) especificado no campo de **texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. Cco: Este critério pesquisa e-mails que contenham o endereço de e-mail completo Cco (por exemplo: jane.doe@abc.com) especificado no campo de **texto de pesquisa**. Para e-mails que atendem a esses

Tradução automática

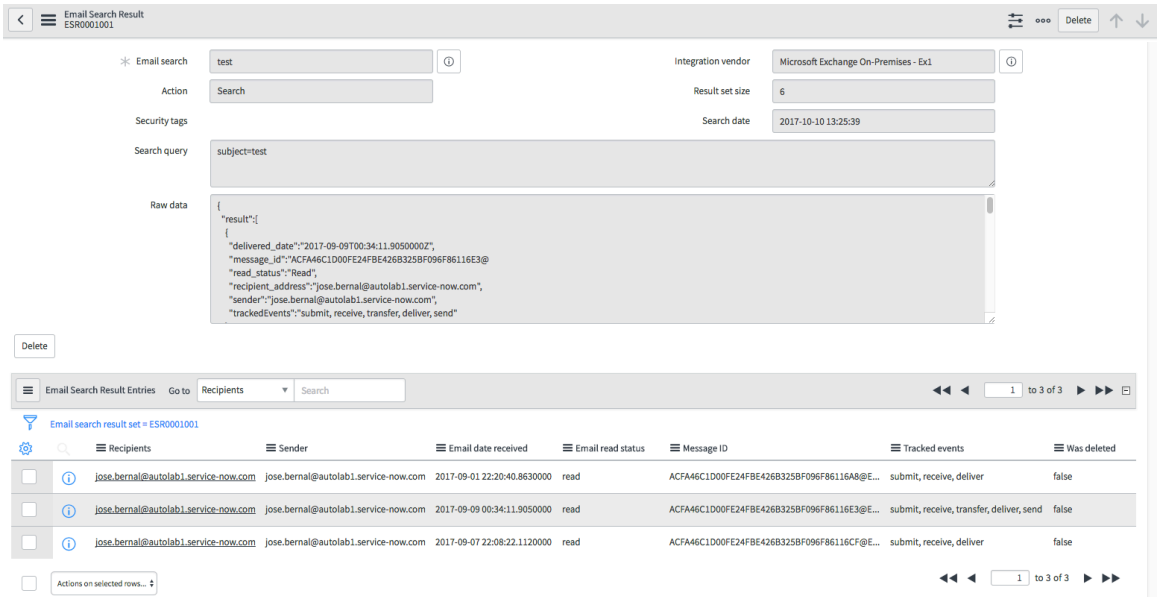
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	critérios de pesquisa, o número total de e-mails de phishing é retornado. Anexo Esses critérios pesquisam e-mails que contenham o nome do arquivo de anexo ou o conteúdo do anexo especificado no campo de **texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Nota:** Somente anexos de texto sem formatação são compatíveis com a pesquisa do conteúdo do anexo. Política de Retenção Esses critérios pesquisam e-mails que contêm números de política de retenção especificados no campo de **texto Pesquisar**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado.
Ativo	Marque esta caixa de seleção para ativar esta consulta de pesquisa de e-mail.
Operador	Os valores possíveis são E e OU. Você pode definir como os critérios de pesquisa são combinados para execução no servidor de e-mail.
Ordem	A ordem na qual a consulta de pesquisa é criada a partir dos critérios de pesquisa.
Pesquisar Texto	O texto a ser pesquisado. Aspas simples, aspas duplas e dois pontos não são compatíveis.

10. Clique em **Enviar**.
11. Repita conforme necessário para definir critérios de pesquisa adicionais.
12. Você pode exibir os resultados da pesquisa clicando na guia **Resultados da pesquisa de e-mail**.

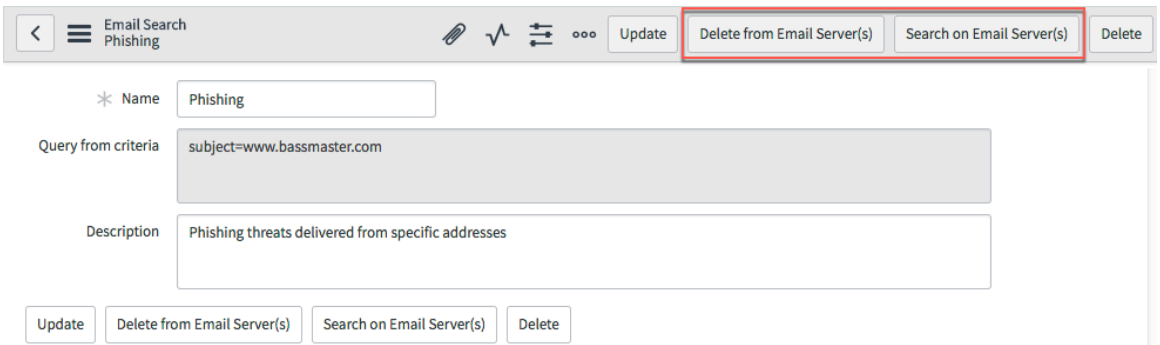
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cada linha do formulário Entradas de resultado da pesquisa de e-mail representa um e-mail separado.

13. Depois de criar um registro de critérios de pesquisa, dois botões serão exibidos no formulário Pesquisa de e-mail: **Excluir do(s) servidor(es)** de e **-mail e Pesquisar no(s)**servidor(es) de e-mail.



14. Para pesquisar e-mails no servidor selecionado que atendam aos critérios de pesquisa definidos, clique **em Pesquisar em servidor(es) de e-mail**.

Criar um artigo de conhecimento de incidente de segurança

Conforme você trabalha com incidentes de segurança e tarefas de resposta, os artigos de conhecimento são exibidos automaticamente para fornecer informações pertinentes sobre a tarefa que você está executando. Sua organização pode criar e manter artigos na base de conhecimento de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.knowledge_admin

Por Que e Quando Desempenhar Esta Tarefa

Artigos de conhecimento compartilham informações de segurança, documentam os tipos de ameaças cibernéticas que sua organização enfrenta e fornecem respostas e respostas a essas ameaças.

Se necessário, você pode organizar artigos de conhecimento em runbooks, que criam associações entre os artigos e tarefas específicas. Por exemplo, você pode configurar um runbook com condições que fazem com que um artigo da base de conhecimento sobre

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

phishing seja exibido ao criar um incidente de segurança para um ataque de phishing. Para obter mais informações, consulte Criar um runbook do Security Incident Response.

Artigos de conhecimento em runbooks também podem ser associados a tarefas específicas em um playbook. Para obter mais informações, consulte Como associar um artigo de conhecimento a uma tarefa do playbook.

Os benefícios dos artigos de conhecimento incluem o seguinte.

- Os funcionários têm uma fonte de informações fácil de pesquisar.
- As informações podem ser mantidas atualizadas, pois os artigos de conhecimento têm um ciclo de vida definido: criar, revisar e atualizar, publicar e desativar.
- Quando você cria manualmente uma solicitação de segurança, incidente ou tarefa de resposta, uma lista de artigos relevantes é apresentada conforme você digita a descrição resumida.

Nota: É importante atribuir um gerente de conhecimento a cada base de conhecimento de incidente de segurança.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Catálogo e Conhecimento** > **Conhecimento**.
2. Clique no ícone Criar um artigo (ícone).
3. Preencha os campos no formulário, conforme o apropriado.

Formulário de conhecimento

Campo	Descrição
Número	O número de KB gerado automaticamente.
Base de conhecimento	A base de conhecimento selecionada para este artigo.
Categoria	A categoria deste artigo.
Publicado	Quando este artigo de conhecimento foi publicado. Este valor é definido quando o artigo é criado e atualizado quando o artigo é publicado.
Válido até	Quando este artigo de conhecimento expira. Este artigo não aparecerá nos resultados da pesquisa após esta data ou se uma data não for selecionada.
Imagem	Uma imagem que aparece ao lado do artigo ao pesquisar no portal de conhecimento legado.
Fluxo de trabalho	[Somente leitura] O estado de publicação do artigo, como Rascunho ou Publicado. Quando inserir um novo artigo a partir de um artigo existente, o estado do novo artigo será redefinido para **Rascunho**.
Origem	A tarefa para a qual este artigo de conhecimento foi criado em resposta, se houver. Este campo é definido automaticamente quando você cria o artigo de conhecimento a partir de um registro de tarefa.
Link de anexo	Marque a caixa para baixar um arquivo anexado automaticamente quando um usuário acessar o artigo, em vez de abrir a exibição do artigo. Adicione um anexo ao artigo para usar esta opção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Exibir anexos	Caixa de seleção para exibir anexos para usuários que visualizam este artigo de conhecimento. Os anexos aparecem abaixo do texto do artigo. Adicione um ou mais anexos ao artigo para usar esta opção.
Descrição resumida	O título do artigo. Este título aparece ao navegar e pesquisar conhecimento e na parte superior do artigo.
Texto	Conteúdo do artigo. Use o editor de HTML WYSIWYG para criar conteúdo. Uma visualização do conteúdo aparece ao navegar e pesquisar conhecimento.

Nota: Se você estiver criando um artigo de conhecimento a ser associado a uma tarefa do playbook, defina o campo **Base de conhecimento** como **Runbook do Security Incident Response**.

4. Clique em **Enviar** para criar o artigo.

O que Fazer Depois

Todas as etapas adicionais necessárias para publicar o artigo, como aprovações, dependem do fluxo de trabalho de publicação da base de conhecimento.

Informações relacionadas

Criar um runbook do Security Incident Response

Escalar um incidente de segurança

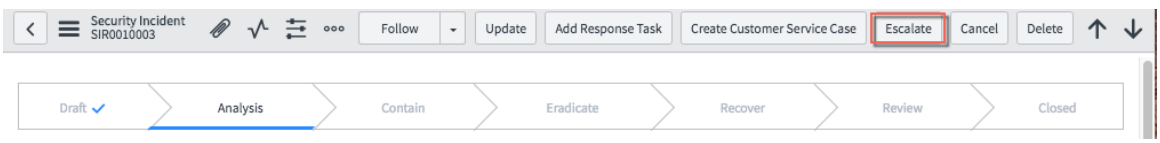
Se houver um caminho de escalação para um incidente de segurança, o botão Escalar estará disponível no cabeçalho do incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin
Você deve ter um grupo de escalação criado para ver este botão. Para obter mais informações, consulte Criar um Operações de segurança grupo de escalação definido pelo usuário.

Procedimento

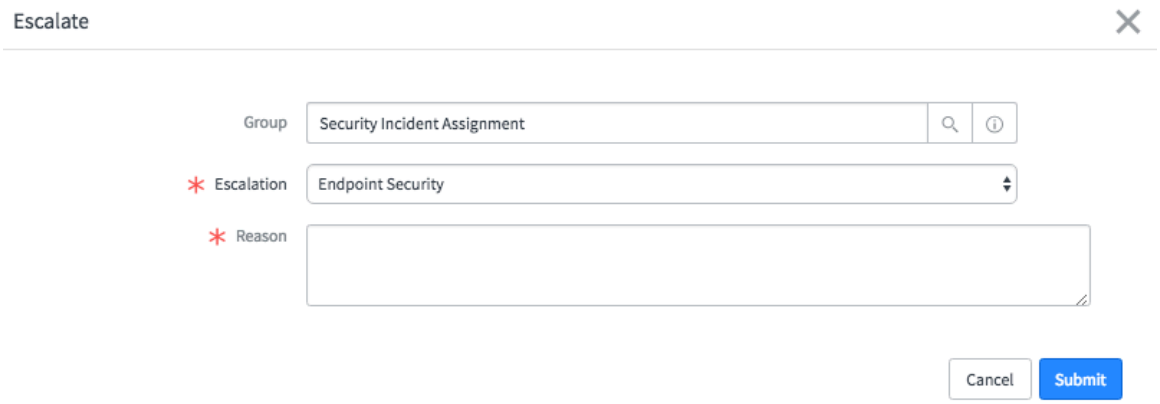
1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Abra o incidente que você deseja escalar.
3. Clique no botão **Escalar**.



4. Escolha um grupo de escalação.
5. Insira um motivo para a escalação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique em **Enviar**.
   Atualiza o **Grupo de atribuição** e **Atribuído a** no incidente de segurança.

Gerenciar atividades pós-incidente

Com base nos requisitos da sua empresa, uma revisão das origens e o tratamento de incidentes de segurança geralmente são necessários.

A funcionalidade Análise pós-incidente em ServiceNow fornece muitas ferramentas para automatizar, rastrear, auditar e simplificar esse processo.

Esta seção descreve o seguinte:

- Atribuir funções de análise pós-incidente
- Configurar uma condição do gatilho de avaliação
- Realizar uma análise pós-incidente baseada em questionário
- Criar regras de atribuição de PIR
- Relatório de análise pós-incidente

Atribuir funções de análise pós-incidente

Você pode direcionar perguntas para grupos predefinidos específicos atribuindo funções a categorias de Revisão pós-incidente (PIR).

Antes de Iniciar

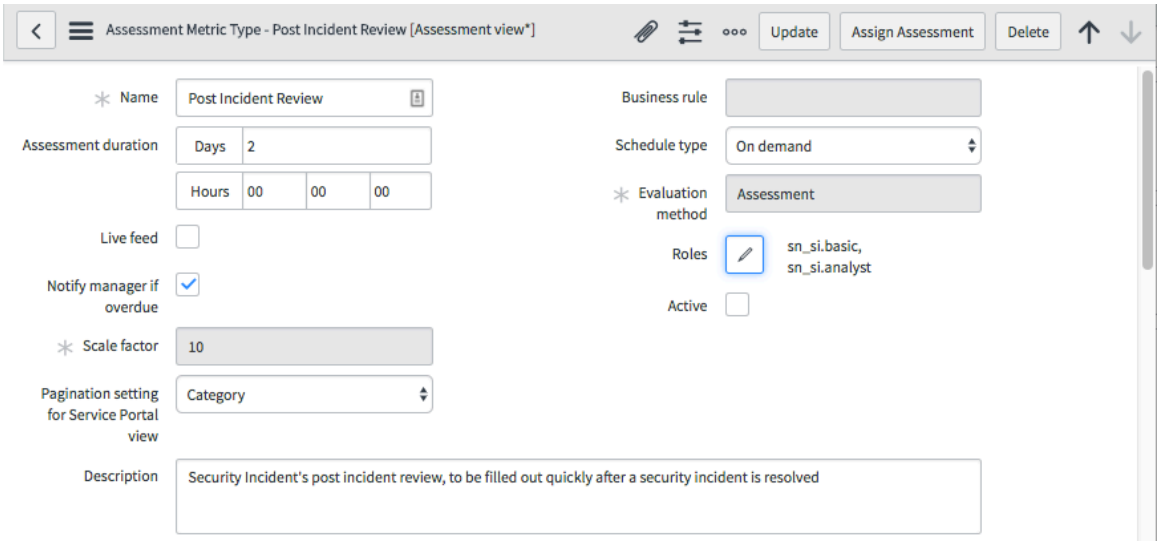
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Avaliações** > **Definição de métrica** > **Tipos**.
2. Na coluna **Tipos**, pesquise um registro **de Análise pós-incidente**.
3. Abra o registro.
4. Atribua uma ou mais funções para esta categoria de perguntas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Atualizar**.

6. Navegar até **Administração de usuários** > **Usuários**.

7. Escolha um usuário

8. Adicione uma ou mais funções de tipo de métrica ao registro do usuário.

> **Nota:** As funções devem corresponder às funções atribuídas na categoria Análise pós-incidente.

Relatório de análise pós-incidente

O recurso de relatórios de análise pós-incidente (PIR) permite que você configure e baixe os relatórios de análise pós-incidente usando a guia Análise pós-incidente.

O administrador de segurança pode criar e configurar os modelos de relatório e mapear esses modelos para o incidente de segurança usando a configuração de relatório.
Um analista de segurança pode exibir ou baixar o relatório depois que o incidente de segurança é resolvido e o status é atualizado para o estado Revisão.

Um relatório em PDF é gerado e anexado ao incidente de segurança quando o incidente é movido para o estado Encerrado após a configuração bem-sucedida.

> **Nota:** O recurso de relatórios é aplicável e compatível com o Orlando Patch9.

Para personalizar seus relatórios de análise pós-incidente, você deve fazer a configuração a seguir.

1. **Modelos de relatório**: personalize e configure os seguintes recursos de modelo de relatório para adicionar informações adicionais ao relatório:
   - **a.** Linha do tempo
   - **b.** Identidade visual
   - **c.** Scripts do Modelo
2. **Configuração de Relatório**

Esta seção descreve o procedimento de configuração:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelos de relatório

Use a seção Modelos de relatório para criar modelos de relatório primário e adicional que são aplicados aos incidentes de segurança para gerar o relatório de análise pós-incidente. Você pode formatar e configurar o relatório com base em seus requisitos. Os modelos também ajudam a incluir os detalhes da avaliação no modelo.

A seguir estão algumas etapas opcionais que podem ser executadas ao criar o modelo:

1. Configurando as informações de identidade visual.
2. Configurar o tamanho e a margem da página.
3. Adicionar campos relacionados a incidentes de segurança (personalizados e padrão).
4. Usando os seguintes tokens personalizados predefinidos:
   a. *$sessionUser*: retorna o nome de usuário conectado
   b. *$date*: retorna a data atual
   c. *$if_not_null_start* & *$if_not_null_end*: se esses marcadores forem usados em qualquer campo, os marcadores serão exibidos somente se o valor existir. Por exemplo:
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. Incluindo os dados da lista relacionada usando os scripts do modelo. Para obter mais informações, consulte a seção abaixo em **Scripts de modelo**.
6. Incluindo as informações da linha do tempo usando os Filtros de linha do tempo. Para obter mais informações, consulte a seção abaixo na **Linha**do tempo.
7. Gerenciar e formatar o conteúdo do modelo, como anexos, tabelas e imagens.

Nota: Os recursos aprimorados da barra de ferramentas do modelo de relatório estão disponíveis somente na versão de lançamento Paris.

Pontos principais dos modelos de relatório:

1. As imagens anexadas ao modelo de relatório são exibidas no relatório de análise pós-incidente somente quando estão incluídas na tabela sys_attachment.

   Nota: As imagens selecionadas na tabela db_image não serão exibidas no relatório de análise pós-incidente.

2. Os vídeos não são compatíveis com o relatório de análise pós-incidente.
3. Os URLs no PDF não são clicáveis. Para habilitar os URLs não clicáveis (.) é indicado como (ponto).
4. O relatório não será gerado se o tamanho do modelo de relatório exceder 50 MB.
5. A família de fontes selecionada para o conteúdo do modelo de relatório não será aplicada ao PDF se não for compatível com o gerador de PDF.

   Nota: Se a fonte correspondente não estiver lá, o gerador de PDF identificará a fonte alternativa mais próxima e gerará o PDF.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Se você fornecer valores de margem de página mais altos, haverá falha na geração do relatório de análise pós-incidente. Por exemplo, Margem superior e inferior > 450 e Margem esquerda e direita > 450.
7. Se um texto grande for incluído no modelo de relatório sem espaços, o texto poderá ficar truncado. Visualize o texto e modifique-o de acordo.

O administrador de segurança pode visualizar o relatório usando o botão **Visualizar relatório** disponível na página Modelo de relatório.

Nota:

Selecione um incidente de segurança para visualizar um relatório com esta opção de modelo e clique em **Visualizar relatório**.

Identidade visual

Você pode adicionar o nome do modelo de identidade visual, a imagem do cabeçalho e rodapé, o texto do cabeçalho e rodapé, gerar números de página e incluir o registro de identidade visual no modelo de relatório após sua criação.

A seguir está um exemplo de formato de relatório de identidade visual:

Pontos principais de identidade visual do modelo de relatório:

1. O tamanho máximo permitido para a imagem do cabeçalho e do rodapé é de 5 MB. Se o tamanho exceder o limite especificado, uma mensagem de erro "O formato da imagem não pode ser reconhecido" será exibida no incidente de segurança.
2. O tamanho do texto do rodapé está limitado a 100 caracteres.
   a. Se o texto da imagem do rodapé e o conteúdo do relatório forem sobrepostos durante a visualização, você deverá fazer mudanças no registro de identidade visual.
   b. Se o texto do rodapé contiver link de URL, ele poderá se sobrepor à imagem do rodapé. Visualize e corrija conforme necessário.

Linha do tempo

A configuração da linha do tempo permite criar e modificar os filtros da linha do tempo conforme necessário. Você pode filtrar os tipos de atividade que devem ser incluídos no relatório, configurar se as tarefas secundárias devem ser incluídas ou excluídas no relatório e configurar se as imagens devem ser incluídas ou excluídas do relatório.

Se você quiser utilizar e preencher qualquer configuração de linha do tempo, deverá adicionar o marcador conforme mencionado abaixo: *`${timeline:timeline name}`*. Duas configurações de linha do tempo de exemplo são fornecidas na configuração que são usadas no modelo de relatório de phishing e no modelo de relatório padrão. Você pode modificar e reutilizar as configurações.

Scripts do Modelo

Use os scripts de modelo para incluir os dados das listas relacionadas, o carimbo de data/hora e quaisquer outros dados que não sejam diretamente percorridos por pontos. A seguir está um exemplo:

Crie um script de modelo para exibir a lista relacionada no modelo de relatório:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Para preparar os dados da lista relacionada, chame o método PostIncidentReportUtils.fetchRelatedListDataForReport.
2. Para representar os dados da etapa 1 no formato e estilo da tabela, chame o método ReportTemplateUtil.constructTablefunction.

Se você quiser utilizar e preencher qualquer script de modelo, deverá adicionar o marcador de script do modelo de marcador como *`${template_script:script name}`*.

A seguir estão alguns exemplos de scripts de modelo fornecidos para configurar e modificar seus relatórios pós-incidente.

Nome do script	Descrição
data_atual_formatada	Retorna a data e hora locais atuais no formato DMMAAAA 00:00 AM ou PM. Por exemplo, 21 de janeiro de 2021 3:51 PM PST.
si_afetados_usuários	Retorna os usuários afetados da lista relacionada em um formulário tabular.
si_assessments	Retorna os resultados da avaliação pós-incidente em um formulário tabular.
si_associated_phish_e-mails	Retorna os e-mails de phishing associados da lista relacionada em um formulário tabular.
si_associated_phish_headers	Retorna os cabeçalhos de phishing associados da lista relacionada em um formulário tabular.
si_business_criticality	Retorna o valor de criticalidade dos negócios codificado por cores.
si_maliciosos_observáveis	Retorna os observáveis maliciosos da lista relacionada em um formulário tabular.
si_observáveis	Retorna os observáveis da lista relacionada em um formulário tabular.
si_priority	Retorna o valor de prioridade codificado por cores.
si_response_tasks	Retorna as tarefas de resposta da lista relacionada em um formulário tabular.
si_time_to_identify	Retorna a duração gasta no estado Rascunho e Análise.
si_time_to_resolver	Retorna o tempo para resolver o incidente.

Pontos principais dos scripts do modelo de relatório:

1. Se uma lista relacionada for adicionada com mais de 5 colunas, os dados da tabela serão truncados durante a geração do PDF. A largura mínima de cada coluna é definida como 124 px.
2. Se um script de modelo não puder carregar o conteúdo no modelo de relatório devido a problemas técnicos, uma mensagem de erro será exibida no relatório, "Erro ao avaliar o script do modelo", e o administrador de segurança deverá avaliar a exatidão do script para resolver o problema. problema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. si_assessments: por padrão, todas as categorias de avaliação são adicionadas ao relatório. O administrador de segurança pode filtrar os dados modificando o script do modelo conforme necessário. Adicione o parâmetro `categories: sys_id1,# sys_id2;` para filtrar os dados.
4. Tempo de resolução e tempo de identificação de scripts: use os registros de definição que fazem parte da lista relacionada à métrica. Se os registros de definição não estiverem disponíveis para o incidente de segurança, crie ou adicione esses registros de definição para preencher os valores dos dois campos.

Nota:

Por padrão, o administrador de segurança não tem acesso para exibir os registros de versão de qualquer tabela. Você deve adicionar a função de administrador para acessar os registros de versão e reverter para a versão anterior.

Configuração de Relatório

Use a seção Configuração de relatório para configurar as condições e aplicar os modelos de relatório aos incidentes de segurança. Você pode adicionar um relatório primário e um ou mais modelos de relatório adicionais à mesma condição.

A seguir está um exemplo de condição que é fornecido para aplicar o modelo de relatório de phishing aos incidentes da categoria de phishing e outro para aplicar o modelo de relatório padrão a todos os incidentes de segurança. O modelo de relatório padrão será aplicado aos incidentes de segurança se as condições não forem atendidas.

Procedimento para desativar a nova implementação

1. Desative as seguintes regras de negócio:
   a. Gerar PDF de PIR
   b. Criar novo conhecimento no fechamento
2. Ative as seguintes regras de negócio:
   a. Gerar PIR quando em Revisão e Fechamento
   b. Criar conhecimento no fechamento
   c. [Regenerar PIR no fechamento/cancelamento/exclusão]
3. Ative a regra de IU, `Hide PIR field when empty`.
4. Acesse o layout do formulário no formulário de incidente de segurança. Na seção **Análise pós-incidente** :
   a. Remover seletor de relatório PIR da seção PIR
   b. Adicionar campo de relatório pós-incidente à seção PIR

Configurar propriedades do relatório de análise pós-incidente (PIR) para incidentes de segurança secundários

Você tem a opção de configurar as duas propriedades de relatório PIR a seguir para incidentes de segurança secundários:

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Usuários com a função de administrador do sistema [admin] podem exibir as propriedades. Usuários com a função de administrador de segurança [sn_si.admin] podem modificá-las.

Configurar propriedades do relatório PIR para incidentes de segurança secundários

Propriedade	Uso
sn_si.generate_pir_report_for_child_si	Opção para habilitar a geração de relatórios de análise pós-incidente (PIR) para incidentes de segurança secundários. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: navegue até Todos > Propriedades do sistema > Todas as propriedades.
sn_si.include_child_si_timeline_in_pir	Opção para incluir a linha do tempo dos incidentes de segurança secundários no relatório PIR do incidente de segurança primário. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: navegue até Todos > Propriedades do sistema > Todas as propriedades.

Gerenciar relatório de análise pós-incidente

Gerenciar relatório de análise pós-incidente inclui as informações que foram configuradas e aplicadas pelo administrador de segurança, e os analistas de segurança podem modificar os filtros da linha do tempo em tempo de execução e baixá-los.

Antes de Iniciar

Função necessária: sn.si_analyst

Por Que e Quando Desempenhar Esta Tarefa

O Analista de segurança pode selecionar um dos modelos de relatório primários ou adicionais disponíveis e configurar os filtros da linha do tempo, visualizar e baixar o relatório. O analista de segurança também pode baixar diretamente o relatório com a configuração da linha do tempo que foi aplicada pela última vez.

O analista de segurança pode acessar os relatórios usando a guia Análise pós-incidente.

Procedimento

1. Navegue até o incidente de segurança no estado Revisão.
2. Clique na guia **Análise pós-incidente**.
3. Se o incidente de segurança estiver no estado **Revisão** :
   Modelo de relatório:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Por padrão, o modelo de relatório primário que foi configurado na página de configuração será aplicado ao incidente de segurança e estará disponível para download.

- O analista pode escolher outros relatórios na lista suspensa para configurar e baixar o relatório.

4. **Configurar/Visualizar:**

   Um analista de segurança pode visualizar e modificar a configuração do modelo de relatório. Na configuração atual, o analista de segurança só pode modificar os filtros da linha do tempo.

   Caso a configuração seja modificada para o relatório primário antes que o incidente de segurança seja encerrado, o relatório de análise pós-incidente anexado ao incidente de segurança será atualizado de acordo com as modificações feitas pelo analista de segurança. Após o fechamento, o analista poderá modificar a configuração e baixar o relatório em qualquer lugar. No entanto, o relatório anexado seguiria a última configuração antes do fechamento.

   Para Configurar/Visualizar o relatório, execute as seguintes etapas:

   a. Selecione o modelo de relatório desejado na lista suspensa **Modelo** de relatório na guia **Análise pós-incidente**.
   b. Clique na guia **Configurar/Visualizar**.
   c. **Atualize** ou configure os filtros da linha do tempo conforme necessário.
   d. Use a caixa de seleção **Mostrar imagens** para incluir ou excluir as imagens da linha do tempo. Se estiver desmarcada, somente os nomes das imagens serão incluídos na seção da linha do tempo.
   e. Use a caixa de seleção **Mostrar tarefas** secundárias para listar todas as tarefas secundárias associadas ao incidente de segurança.

5. **Salve** a configuração e clique na guia **Visualizar** para visualizar e baixar o relatório.
6. Clique em **Download** para baixar diretamente o relatório.

Configurar uma condição do gatilho de avaliação

Defina condições de regra e gere avaliações obrigatórias e opcionais para incidentes de segurança específicos.

Antes de Iniciar

Função necessária: sn_si.admin

Nota: Para usar o recurso Condições do gatilho da avaliação de análise pós-incidente, você deve fazer upgrade para Security Incident Response 11.0. Antes de atualizar, você deve reverter todas as personalizações feitas no tipo de métrica de análise pós-incidente e nas condições do gatilho. Além disso, talvez você também precise reverter as personalizações feitas nas regras de negócio específicas para a revisão pós-incidente.

- Exigir que as avaliações sejam concluídas
- Armazenar atribuído

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração** > **Análise pós-incidente – Configuração de avaliações**.
2. Na seção **Condições do gatilho de avaliação Configurar**, clique em **Configurar**.

Nota: No formulário Configurações de avaliação e na seção Configurações de avaliações, a caixa de seleção **Gerar avaliações** está marcada por padrão.

- Quando você marca a caixa de seleção, uma avaliação opcional é criada para cada incidente de segurança.
- Quando você desmarca a caixa de seleção, as avaliações não são geradas. As regras de avaliação não são exibidas e você não pode configurar condições para os incidentes de segurança.

3. No formulário Configurações de avaliação, na seção Condições, especifique as informações necessárias.

a. No campo **Nome**, especifique o nome da regra.

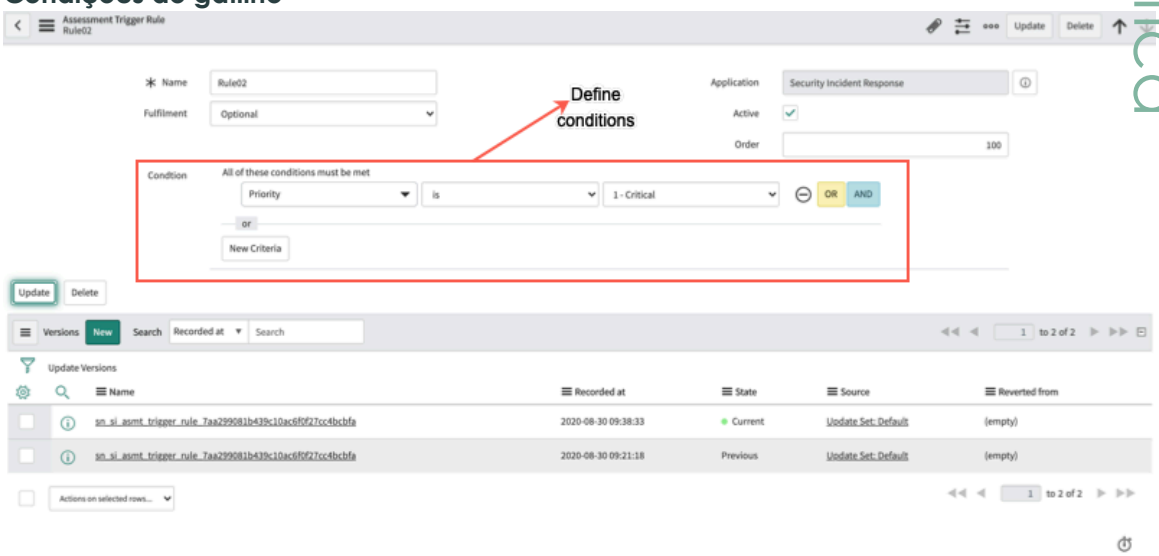
b. No campo **Execução**, especifique o tipo de execução.

c. Para configurar uma condição, clique no registro de regra e defina as condições no campo **Condição**.

Nota:

- Se você criar uma regra sem definir uma condição no campo **Condição**, a condição será avaliada como verdadeira e a regra será aplicável a todos os incidentes de segurança.
- Você pode definir uma regra específica para tornar as avaliações obrigatórias ou opcionais, e as avaliações não serão geradas para os incidentes de segurança restantes, que não correspondem às regras definidas.

Condições do gatilho



Tradução automática

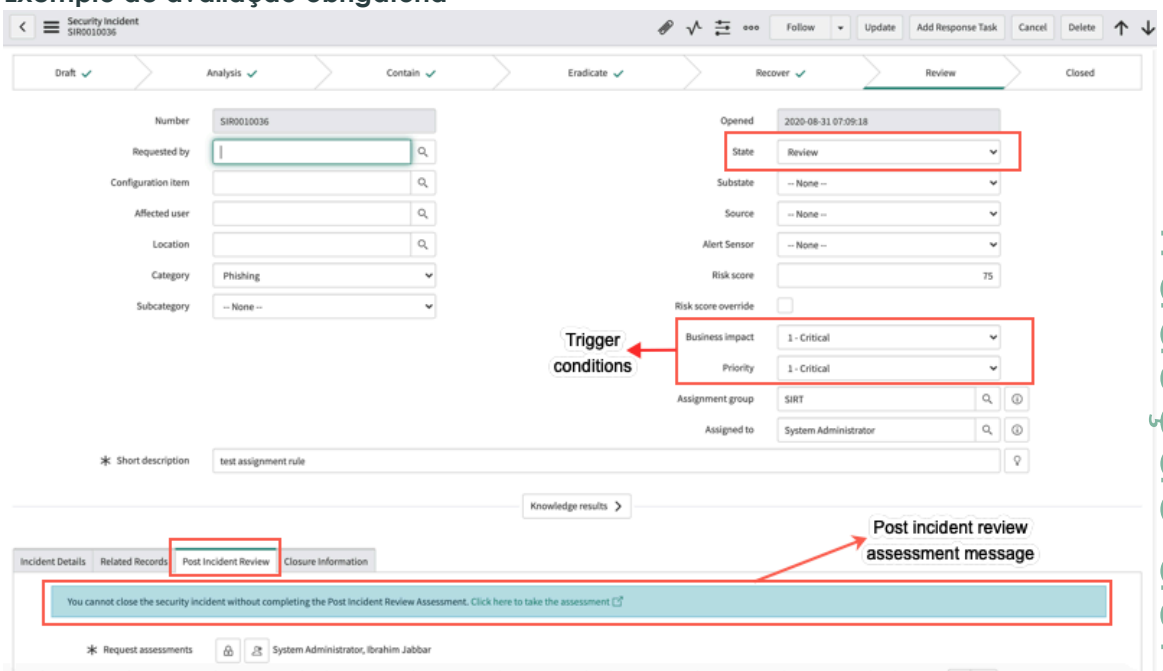
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplos de condições do gatilho de avaliação

Os exemplos a seguir fornecem diferentes cenários sobre como as condições do gatilho de avaliação obrigatória e opcional são geradas.

- No formulário Condição do gatilho de avaliação, gere avaliações obrigatórias quando a **Prioridade** e o **Impacto nos negócios** de um incidente de segurança estiverem definidos como **Crítico** na página **Regra do gatilho de avaliação**. Nesse cenário, os analistas de segurança não podem fechar o incidente até que as avaliações obrigatórias sejam concluídas.

Exemplo de avaliação obrigatória



- Como você pode ver, neste exemplo, se um incidente de segurança estiver em um estado de **revisão**, os analistas de segurança não poderão fechar o incidente de segurança sem concluir a **avaliação de análise pós-incidente**. Um link de avaliação está disponível para levar a avaliação aos analistas de segurança atribuídos (ou que solicitaram a avaliação) ao incidente.
- No formulário Condição do gatilho de avaliação, gere avaliações opcionais quando a **Prioridade** e o **Impacto nos negócios** de um incidente de segurança estiverem definidos como **Altos**. Neste exemplo, se os analistas de segurança não concluírem as avaliações e fecharem o incidente de segurança, as avaliações serão canceladas automaticamente.
- No caso, se as avaliações obrigatórias ou opcionais não corresponderem ao incidente de segurança, as avaliações não serão geradas para esses incidentes de segurança. Um analista de segurança pode fechar o incidente de segurança sem concluir a avaliação de análise pós-incidente.

Realizar uma análise pós-incidente baseada em questionário

Você pode decidir que uma revisão pós-incidente do incidente de segurança é garantida. Uma revisão pós-incidente descreve o que aconteceu, ajuda a determinar por que o incidente ocorreu e identifica como ele pode ser evitado ou tratado no futuro.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.manager, sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Qualquer usuário pode participar de um questionário de análise pós-incidente, independentemente da função. As funções podem ser atribuídas a uma revisão.

Por Que e Quando Desempenhar Esta Tarefa

A aplicação ServiceNow Security Incident Response pode automatizar a coleta de informações de análise pós-incidente de todos os envolvidos em um incidente de segurança usando questionários. Se você decidir usar um questionário como parte de uma revisão pós-incidente, uma lista de perguntas relevantes ao incidente de segurança será enviada para a lista de participantes definida pelo usuário. Conforme cada usuário conclui o questionário, o relatório pós-incidente é gerado automaticamente. O relatório compila todas as informações relacionadas ao incidente de segurança, bem como todas as respostas à revisão pós-incidente.

Embora uma lista inicial de perguntas seja fornecida com o sistema de base, ela é personalizável. Você pode criar categorias e adicionar novas perguntas a elas ou pode mudar perguntas individuais em categorias existentes. Você pode fazer perguntas com base em funções. Você pode definir quando determinadas perguntas são feitas. Pode haver perguntas que você faz somente para seus servidores UNIX, por exemplo, ou somente quando há atividade criminal. Você pode definir as perguntas que são feitas com base na resposta a outra pergunta ou no valor em um campo no formulário. Pode até haver perguntas que são preenchidas totalmente consultando o banco de dados.

Depois que o incidente de segurança é resolvido e movido para o estado **Revisão**, as avaliações são geradas para todos os usuários atribuídos e usuários que são adicionados diretamente da lista **Solicitar avaliações**.

O questionário pode ser uma ferramenta útil para coletar informações sobre o tratamento do incidente de segurança de várias fontes.

Durante a revisão, você pode adicionar mais usuários à lista ou remover usuários existentes da lista, a menos que eles já tenham começado a preencher o questionário. Se você adicionar novos usuários à lista, eles receberão as perguntas quando o registro for salvo. O incidente de segurança não pode ser encerrado até que todos os questionários tenham sido concluídos. Conforme os questionários são preenchidos por cada usuário, o relatório pós-incidente é gerado automaticamente (e gerado novamente) e exibido na guia **Análise pós-incidente**.

Para iniciar uma análise pós-incidente:

Procedimento

1. Crie um incidente de segurançaou abra um existente navegando até **Incidente de segurança** > **Incidentes** > **Atribuído a mim (ou Atribuído à equipe ou Incidentes não atribuídos)**.
2. Clique na guia **Análise pós-incidente**.
3. O campo **Solicitar avaliações** é padronizado para o indivíduo no campo **Atribuído a**. Clique no ícone de cadeado para adicionar outros usuários à lista de revisão. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários, funções ou inserir endereços de e-mail do usuário.
4. Ao concluir suas entradas, clique no ícone de cadeado para bloquear o campo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você também pode definir condições que, quando atendidas em um incidente de segurança, podem fazer com que usuários específicos sejam adicionados automaticamente ao campo **Solicitar avaliações** para esse incidente de segurança. Por exemplo, quando uma **categoria** de incidente de segurança é alterada para **Phishing**, indivíduos específicos com experiência em ameaças de phishing podem ser adicionados à lista de análise pós-incidente. Para obter mais informações, consulte Criar regras de atribuição de PIR.

5. Clique em **Atualizar**.
   Quando o incidente entra no estado **Revisão** (ou imediatamente, se já estiver no estado **Revisão**), cada um dos usuários na lista de revisão recebe uma notificação por e-mail inicial. Os lembretes são enviados conforme a data de vencimento se aproxima. Quando cada usuário acessa o questionário a partir do link de e-mail ou acessando **Análise pós-incidente** > **Minhas Revisões Pendentes**, as perguntas mostradas são extraídas de todas as categorias que se encaixam neste incidente de segurança. Se novos usuários forem adicionados à lista de revisão antes do prazo, eles receberão notificações quando o incidente de segurança for salvo.

   Conforme os usuários preenchem seus questionários, o relatório pós-incidente compila os dados e exibe o relatório na guia **Análise pós-incidente**. Os dados do questionário são exibidos na guia **Descobertas**.

Criar categorias de questionário de análise pós-incidente

Você pode usar as categorias de questionário que vêm com o sistema de base ou criar suas próprias categorias.

Antes de Iniciar
Função necessária: sn.si_admin

Por Que e Quando Desempenhar Esta Tarefa
Para criar uma nova categoria de perguntas:

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Análise pós-incidente**.
2. Clique **em Revisar perguntas**.
   Uma lista de categorias é exibida, junto com sua ordem e filtros que definem sob quais condições as perguntas são feitas (por exemplo, somente quando a categoria de incidente de segurança é `Atividade criminal`). Cada categoria é uma seção no questionário de análise pós-incidente e as perguntas em cada categoria são incluídas somente quando o incidente de segurança corresponde ao filtro Condição. Por exemplo, para uma categoria de perguntas que se aplica somente a servidores Linux, você configuraria um filtro que selecionasse incidentes de segurança em que o tipo de recurso afetado fosse Servidor Linux. Nessa categoria, você criaria todas as perguntas necessárias quando um incidente de segurança estivesse em um servidor Linux. Você usa uma das categorias fornecidas no sistema de base ou cria uma nova categoria. Este procedimento pressupõe que você deseja criar uma nova categoria antes de definir perguntas.
3. Clique em **Novo** na lista de categorias.
4. Preencha os campos no formulário, conforme o apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança

Campo	Descrição
Nome	Nome da categoria que aparece no questionário de incidentes de segurança.
Tipo	A análise pós-incidente é o padrão.
Criar Partes Interessadas	Não usado por Security Incident Response.
Tabela	Este campo é atribuído automaticamente quando o formulário é enviado.
Filtrar	Insira a condição que determina quando as perguntas nesta categoria são usadas. Se um registro de incidente de segurança corresponder a este filtro, as perguntas serão incluídas em uma revisão pós-incidente para esse incidente de segurança. Os filtros podem usar quaisquer dados no registro ou em outros registros vinculados a este registro. Por exemplo, o departamento do gerente do usuário solicitante.
Aplicação	Aplicação de escopo para o incidente.
Ponderação	Valor numérico que representa a importância dessa métrica relativa a outras métricas na mesma categoria. Por padrão, o peso é 10.
Métricas totais	Número de métricas usadas pela categoria.
Descrição	Descrição do questionário.

5. Clique em **Enviar** para salvar a categoria.

Redigir perguntas de análise pós-incidente

Você pode usar as perguntas que vêm com o sistema de base ou criar suas próprias perguntas.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Os métodos para coletar informações de análise pós-incidente podem estar na forma de perguntas ou como dados coletados automaticamente usando scripts.

As perguntas podem depender das respostas a outras perguntas. Por exemplo, você pode perguntar se todos os logs necessários estavam disponíveis. Se a resposta for Não, você faz uma pergunta de acompanhamento para verificar quais logs necessários não foram habilitados.

A coleta de dados com script, também chamada de métricas de script, reúne dados relacionados ao incidente de segurança por meio de scripts que você grava. Esta ação pode ir muito além dos dados no próprio registro de incidente de segurança. Por exemplo, uma métrica de script pode coletar o tempo de indisponibilidade recente de um servidor afetado por este incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por fim, você pode misturar os dois tipos. As perguntas podem ter valores padrão obtidos de um script ou simplesmente de um campo no registro de incidente de segurança. Ao usar um tipo de pergunta `Resposta padrão de...`, você pode escolher se deseja que o usuário sempre responda à pergunta - com o valor padrão fornecendo a ele um valor inicial - ou se deseja que a pergunta seja feita ao usuário somente se o O script ou o campo aparece em branco.

Para criar uma nova pergunta:

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Análise pós-incidente**.
2. Clique na categoria para a qual você deseja criar uma nova pergunta.
3. Clique na guia **Métricas de avaliação**.
4. Clique em **Nova**.
   Você também pode clicar em uma pergunta existente para modificá-la.
5. Preencha os campos no formulário, conforme o apropriado.

Formulário de métrica

Campo	Descrição
Nome	Nome da métrica (pergunta ou script). Se a métrica for uma coleta de dados com script, este nome aparecerá no relatório pós-incidente.
Categoria	A categoria à qual a métrica pertence. O sistema preencherá automaticamente essa categoria se você criar uma métrica a partir do formulário Categoria de métrica. **Nota:** Você não poderá mudar a categoria se o campo **Depende de** estiver definido ou se outra métrica depender dessa métrica
Método	Indica o tipo de métrica, da seguinte forma: ◦ *Assessment*: uma pergunta que não tem valor padrão. Existem vários tipos de dados que podem ser definidos no campo **Tipo de dados** na guia **Tipo** de campo, como caixas de seleção, listas de seleção e entrada de texto. ◦ *Script*: métrica com script. Obtenha valores gravando um script personalizado. O método *Script* é compatível com os tipos de dados **Duração**, **Número**e **Porcentagem**. ◦ *Default answer from field*: uma pergunta em que a resposta padrão vem de um campo selecionado no incidente de segurança. A seleção desta opção adiciona dois campos à guia **Geral** : ▪ *Default answer*: selecione o campo no incidente de segurança que contém a resposta padrão para a pergunta. Por exemplo, para a pergunta: "quem relatou este incidente inicialmente?", o campo **Solicitado por** seria uma escolha provável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	▪ *Ask question*: especifica quando fazer a pergunta: sempre ou somente se o campo **Resposta padrão** estiver vazio. Usando o exemplo acima, a pergunta seria feita se o campo **Solicitado por** estivesse vazio. ◦ *Default answer from script*: uma pergunta em que a resposta padrão vem de um script. A resposta pode ser um número, uma cadeia de caracteres ou uma porcentagem. A guia **Geral** adiciona um campo: *Ask question*: como o Especifica quando fazer a pergunta: sempre ou somente se o script não fornecer uma resposta padrão. O script é definido na guia **Tipo de campo**. **Nota:** Se você selecionar um **Tipo de dados** que seja incompatível com o **Método**selecionado, o sistema mudará automaticamente o **Método** para um valor compatível.
Ponderação	[Obrigatório] Valor numérico que representa a importância dessa métrica relativa a outras métricas na mesma categoria. Por padrão, o peso é 10. Esse campo ficará visível e será obrigatório somente se o **Tipo de dados** for **Data**, **Data/Hora** ou **Cadeia de caracteres**. Esses tipos de dados não são incluídos nos cálculos de resultados.
Ordem	[Obrigatório] Valor numérico que determina a ordem da pergunta de métrica em questionários de avaliação, em relação a outras perguntas de métrica na mesma categoria. A métrica com o menor valor de ordem aparece como a primeira pergunta na seção de categoria. Por padrão, a ordem é 100. **Nota:** Não importa qual valor de ordem você usa para métricas com o método de script, já que eles não aparecem em questionários.
Ativo	Caixa de seleção que determina se esta métrica é usada. Se a caixa de seleção não estiver marcada, é como se o registro da métrica não existisse.
Obrigatório	Marque a caixa que torna a pergunta de métrica obrigatória (selecionada) ou opcional (desmarcada) em questionários de avaliação. Os usuários não podem enviar questionários até que eles forneçam respostas válidas a todas as perguntas obrigatórias, que são indicadas por um indicador de status de campo vermelho. Este campo ficará visível somente se o campo **Depende de** estiver vazio e o tipo de dados não for **Caixa**de seleção .

6. Clique na guia **Geral** e preencha os campos, conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Geral

Campo	Descrição
Pergunta	Texto a ser usado como pergunta em questionários de análise de incidentes de segurança. Insira uma pergunta clara e direta que seja fácil de responder, como **Como contivemos o incidente**
Descrição	Informações sobre a métrica e o que ela avalia. Se o *Method* for **Avaliação**, inclua detalhes que ajudem os usuários a entender como responder à pergunta. Esse texto aparece como uma dica quando um usuário aponta para o texto da pergunta no questionário.
Depende de e Exibido quando	Selecione uma pergunta no campo **Depende de da** qual a pergunta atual depende. Por exemplo, a pergunta "Quais logs adicionais foram necessários?" depende da pergunta "Todos os logs necessários estavam disponíveis?" Em seguida, use o campo **Exibido quando** para identificar quando você deseja que a pergunta dependente apareça em questionários. Por exemplo, se você quiser que a pergunta dependente seja feita somente quando o usuário responder **Não** à pergunta "Todos os logs necessários estavam disponíveis?" pergunta, selecione **Não** no campo **Exibido quando**. **Nota:** O sistema evita a criação de dependências recursivas entre métricas. Por exemplo, se a Métrica A depender da Métrica B, a Métrica B não poderá depender da Métrica A.

7. Clique na guia **Tipo de campo** e preencha os campos, conforme apropriado.

Guia Tipo de campo

Campo	Descrição
Tipo de dados	O tipo de dados da resposta esperada da qual a lista de tipos disponíveis depende para o método selecionado. Se o método for **Avaliação**, o tipo de dados determinará como os usuários responderão à pergunta correspondente nos questionários. Se o método for **Script**, o tipo de dados determinará como o sistema calculará os resultados da avaliação. **Nota:** Se outra pergunta depender dessa métrica, você não poderá mudar o tipo de dados.
Respostas aleatórias	Caixa de seleção que determina se as opções de resposta para esta pergunta de métrica devem ser apresentadas em uma ordem aleatória sempre que um usuário abrir um questionário de avaliação que contém a pergunta. A preferência de resposta pode ser influenciada pela ordem em que as opções de resposta aparecem. Isso pode resultar em resultados tendenciosos. As opções de resposta de aleatoriedade podem ajudar a evitar essa tendência.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este campo ficará visível somente se você selecionar **Escala Likert** ou **Opção** no campo **Tipo de dados**.
Plug-in dependente	[Obrigatório se o *Method* for **Script**.] Plug-in que contém as tabelas consultadas no script. O sistema executará o script de métrica somente se o plug-in estiver ativo. Os valores padrão disponíveis são **Gestão de ativos**, **CMDB**, **Core**, **Gestão de custos**, **Compras** e **Software Asset Management**. Este campo ficará visível somente se o *Method* for **Script**. **Nota:** ◦ Se o valor padrão Core for usado, o script será sempre executado. ◦ Se você for um administrador, poderá adicionar mais opções de plug-ins ao campo.
Definição de escala	Configuração que determina se valores numéricos menores ou maiores são iguais a uma boa pontuação nos cálculos de resultados da avaliação. Selecione **Baixo** se valores numéricos menores forem melhores, como para uma métrica que mede o número de defeitos de um fornecedor. Selecione **Alto** se valores numéricos maiores forem melhores, como para uma métrica que mede a satisfação do usuário em uma escala de um a cinco. O valor padrão é **Alto**. Este campo é visível e obrigatório, a menos que *Data type* seja **Data**, **Data/Hora** ou **Cadeia de caracteres**. Os resultados para esses tipos de dados não são incluídos nos cálculos de resultados.
Mínimo(a)	O valor numérico mais baixo a ser usado como uma opção de resposta em avaliações ou como um valor com escala em uma métrica com script. Esse campo é visível e obrigatório somente quando determinados tipos de dados são selecionados. Se o tipo de dados for **Opção** ou **Escala Likert**, este campo será somente leitura e será definido automaticamente com base na menor definição de métrica *Value*.
Máximo(a)	Maior valor numérico a ser usado como opção de resposta ou valor com escala. Esse campo é visível e obrigatório somente quando determinados tipos de dados são selecionados. Se o tipo de dados for **Opção** ou **Escala Likert**, este campo será somente leitura e será definido automaticamente com base na maior definição de métrica *Value*.
Script	Script que obtém as informações do sistema desejadas. O script tem uma variável de entrada, definida com o ID do incidente de segurança (primário), e três variáveis de saída possíveis definidas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	pelo script, string_result, scaled_result e actual_result. Quando o tipo de dados é cadeia de caracteres, somente o string_result é necessário. Este campo é visível e obrigatório quando o *Method* é **Script** ou o valor padrão vem de um script.
Modelo	Um conjunto predefinido de respostas comuns a serem usadas para a pergunta. Por exemplo, um modelo de frequência provavelmente iniciaria com um valor de "Nunca" e chegaria ao valor máximo de "Sempre". Este campo será visível e obrigatório somente se o *Data type* for **Modelo**. **Nota:** Se outra métrica depender dessa métrica, você não poderá mudar o modelo.

8. Opcional: Ao concluir suas entradas, clique em **Atualizar**.

Criar regras de atribuição de PIR

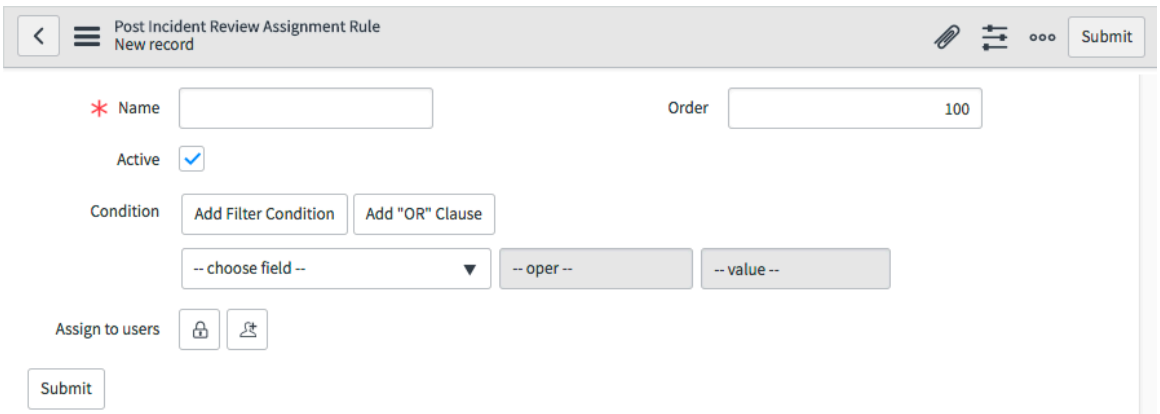
Além de adicionar manualmente a lista de avaliação de análise pós-incidente de usuários para um incidente de segurança, você pode definir regras de atribuição para adicionar usuários automaticamente à lista.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.manager, sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração** > **Análise pós-incidente – Configuração de avaliações**.
2. Faça o detalhamento ativo até a seção **Regras de atribuição de usuário**.
3. Clique em **Configurar**.
4. Clique em **Nova**.



5. Preencha os campos conforme necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

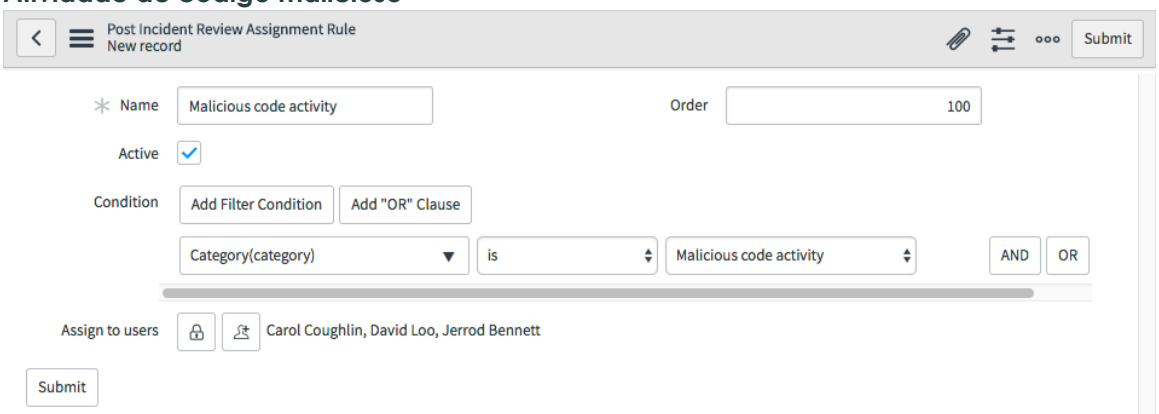
Campo	Descrição
Nome	O nome desta regra de atribuição.
Ativo	Marque esta caixa de seleção para ativar a regra.
Ordem	Insira um valor numérico para especificar onde na lista de regras de atribuição essa regra deve aparecer. Números menores aparecem na parte superior da lista. **Nota:** Somente a primeira regra de atribuição correspondente é executada e somente os usuários definidos nessa regra são adicionados à lista de avaliação.
Condição	Use o Construtor de condição para definir as condições que devem ser atendidas no incidente de segurança para que esta regra seja executada. Para obter mais informações, consulte o exemplo abaixo.
Atribuir a usuários	Clique no ícone de cadeado para adicionar usuários à lista de revisão. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários, funções ou inserir endereços de e-mail do usuário.

6. Clique em **Enviar**.

Example: Atividade de código malicioso

Na regra de atribuição de análise pós-incidente mostrada aqui, quando um incidente de segurança com o campo **Categoria** definido como **Atividade de código mal** -intencionado passa para o estado **Revisão**, os três usuários identificados (que são especialistas em lidar com atividade de código mal-intencionado) são adicionados à lista de usuários que receberão o questionário de análise pós-incidente para este incidente de segurança.

Atividade de código malicioso



Fechar incidentes de segurança

Quando um incidente de segurança faz a transição para o estado Revisão, é possível fechá-lo e inserir um código de fechamento apropriado. Os códigos de fechamento podem ser pesquisados posteriormente para facilitar a localização.

Antes de Iniciar

Função necessária: sn_si.write

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Nota: Nas versões anteriores do Security Incident Response, os usuários podiam fechar incidentes de segurança ou solicitações como spam. Na versão Istanbul, a opção de spam não está mais disponível. Incidentes ou solicitações de segurança de spam podem ser cancelados ou excluídos, conforme apropriado.

Procedimento

1. Se o incidente de segurança que você deseja fechar ainda não estiver aberto, navegue até **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**e localize o incidente de segurança que você deseja fechar.

   Nota: Se houver avaliações de análise pós-incidente que não tenham sido concluídas para este incidente de segurança, o incidente de segurança não poderá ser encerrado. Retornar a **Incidente de segurança** > **Análise pós-incidente** > **Todas as revisões incompletas**, localize as revisões que estão incompletas e peça aos revisores para concluir as revisões ou cancelar as avaliações restantes.

2. Clique na guia **Informações de fechamento** e preencha os campos, conforme apropriado.

Incidente de segurança

Campo	Descrição
Criar artigo de conhecimento	Selecione este campo para criar automaticamente um rascunho de artigo da base de conhecimento que contenha o conteúdo da revisão pós-incidente.
Código de fechamento	Selecione o código de encerramento que melhor descreve o motivo pelo qual você está encerrando este incidente de segurança. ◦ Investigação concluída ◦ Ameaça mitigada ◦ Vulnerabilidade corrigida ◦ Vulnerabilidade inválida ◦ Não resolvido ◦ Falso positivo
Encerrado por	Exibe o usuário que encerrou o incidente de segurança depois que o registro foi atualizado.
Encerrado	Exibe a data e a hora do fechamento depois que o registro é atualizado.
Anotações de encerramento	Insira anotações adicionais que descrevam o resultado do encerramento deste incidente de segurança.

3. Clique em **Atualizar**.
4. O usuário atribuído pode alterar manualmente o **Estado** para **Encerrado**.
   Quando um incidente primário é encerrado, todas as tarefas de resposta pertencentes ao incidente secundário são canceladas. Se não houver outros tipos de tarefas, o incidente secundário também será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar informações de fechamento a um incidente de segurança

Quando um incidente de segurança está no estado Revisão ou Encerrado, você pode inserir informações de fechamento.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique na guia **Registros relacionados**.
3. Preencha os campos conforme necessário.

Campo	Descrição
Criar artigo de conhecimento	Marque esta caixa de seleção para gerar um artigo de conhecimento usando o conteúdo do relatório pós-incidente.
Código de fechamento	Selecione o código de fechamento que melhor descreve o motivo para fechar o incidente de segurança.
Encerrado por	[Somente leitura] Exibe o usuário que encerrou o incidente de segurança.
Encerrado	[Somente leitura] Exibe a data e a hora em que o incidente de segurança foi encerrado.
Anotações de encerramento	Como o incidente de segurança foi encerrado, incluindo lições aprendidas, resolução e assim por diante.

4. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Detalhes de Incidentes
   - Análise pós-incidente
5. Ao concluir suas entradas, clique em **Enviar**.

Restringir o acesso a incidentes de segurança

Gerencie o acesso dos incidentes de segurança que contêm informações confidenciais. Você pode impor restrições de incidente de segurança para determinar quem pode acessar um determinado incidente e limitar o acesso somente a usuários ou grupos específicos.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
As restrições de incidente de segurança permitem que você oculte incidentes de segurança críticos para que não sejam acessados por outros usuários em uma organização específica. Essas restrições permitem que você forneça uma maneira mais granular de controlar os incidentes de segurança que um usuário pode acessar. Você pode impor uma restrição de incidente de segurança habilitando a caixa de seleção **Impor restrição** e selecionando os usuários ou grupos que têm permissão para acessar o incidente de segurança específico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

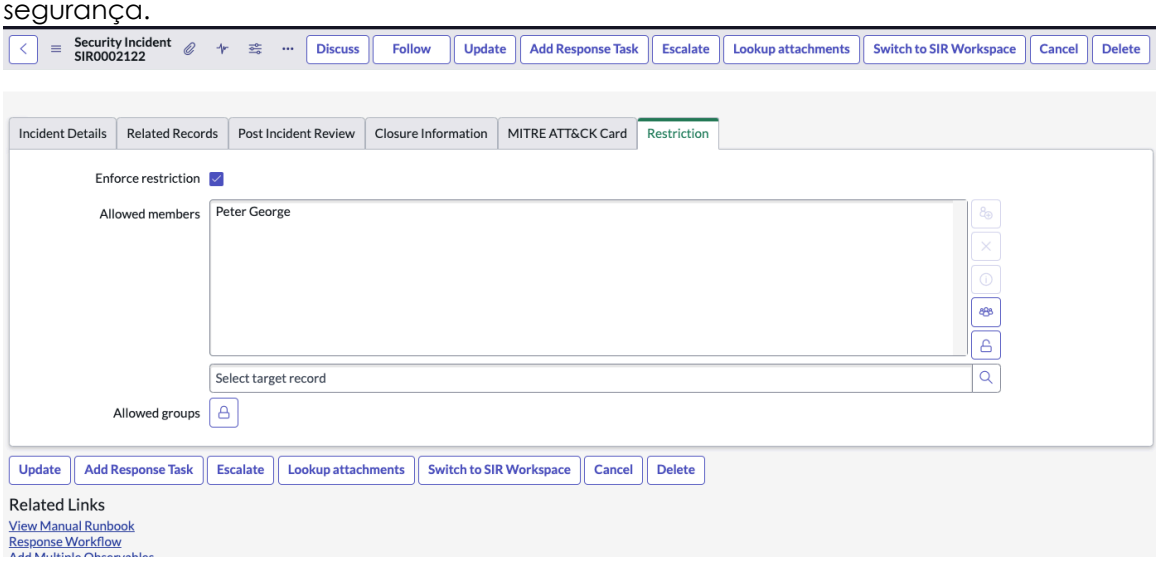
Depois de impor a restrição a incidentes de segurança específicos e limitar o acesso a determinados usuários ou grupos, todos os outros usuários restantes em sua organização não poderão acessar esses incidentes de segurança, mesmo que pesquisem um incidente de segurança restrito específico.

Procedimento

1. Abra um incidente de segurança que você deseja restringir.
2. Se você estiver usando a IU clássica, execute o seguinte:

   a. Clique na guia **Restrição**.

   b. Marque a caixa de seleção **Impor restrição** para habilitar a restrição do incidente de segurança.



   c. No campo Membros permitidos, clique no para selecionar os usuários que podem acessar o incidente de segurança.

   d. Selecione o para adicionar a si mesmo como o usuário permitido.

   e. Selecione o ícone para adicionar ou remover usuários.

   f. No campo Grupos permitidos, clique no para selecionar os grupos que podem acessar o incidente de segurança.

   g. Selecione o ícone para adicionar ou remover grupos.

   Nota: Depois que a caixa de seleção **Impor restrição** estiver habilitada para o incidente de segurança, somente o sn_si.admin e os membros ou grupos permitidos terão acesso ao incidente de segurança.

   h. Clique em **Atualizar**.

3. Se você estiver usando o Espaço SIR, execute o seguinte:

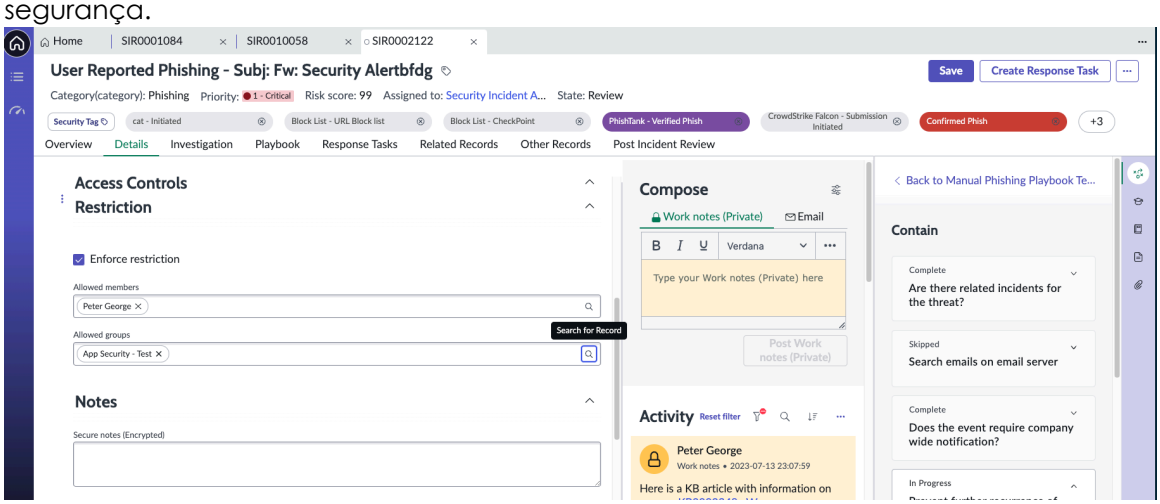
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. No incidente de segurança, clique na guia **Detalhes**.

b. Role para baixo e clique na seção **Restrição**.

c. Marque a caixa de seleção **Impor restrição** para habilitar a restrição do incidente de segurança.



d. No campo Membros permitidos, selecione os usuários que podem acessar o incidente de segurança usando a opção Pesquisar.

e. No campo Grupos permitidos, selecione os grupos que podem acessar o incidente de segurança usando a opção Pesquisar.

> **Nota:** Depois que a caixa de seleção **Impor restrição** estiver habilitada para o incidente de segurança, somente o sn_si.admin e os membros ou grupos permitidos terão acesso ao incidente de segurança.

f. Clique em **Salvar**.

Gerenciar ameaças à segurança usando o Espaço do analista de segurança

Security Incident Response inclui uma nova interface de usuário chamada Espaço do analista de segurança que apresenta ferramentas poderosas para auxiliar na análise, incluindo o playbook, a exibição de espreitadelas e as guias para trabalhar em vários incidentes de segurança.

Criadas especificamente para analistas de segurança, as ferramentas poderosas no Espaço do analista de segurança permitem que você analise o volume cada vez maior de dados associados a incidentes de segurança. E as ações automatizadas reduzem significativamente o tempo de investigação de incidentes de segurança, o que pode ser a diferença entre interromper um ataque e sofrer uma violação.

Antes de usar o Espaço do analista de segurança

Antes de começar a usar o Espaço do analista de segurança, você deve garantir que sua instância tenha pelo menos o London Patch 3 instalado, que você tenha as funções corretas definidas e tenha baixou a aplicação de IU do Security Incident Response do ServiceNow Store.

Tradução automática

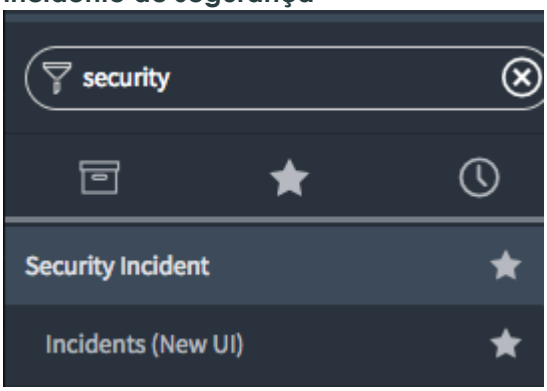
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se sua instância estiver executando uma versão anterior ao Patch 3 de London, você deverá solicitar o plug-in de IU de resposta a incidentes de segurança por meio do sistema de atendimento ao cliente HI.

Como acessar o Espaço do analista de segurança

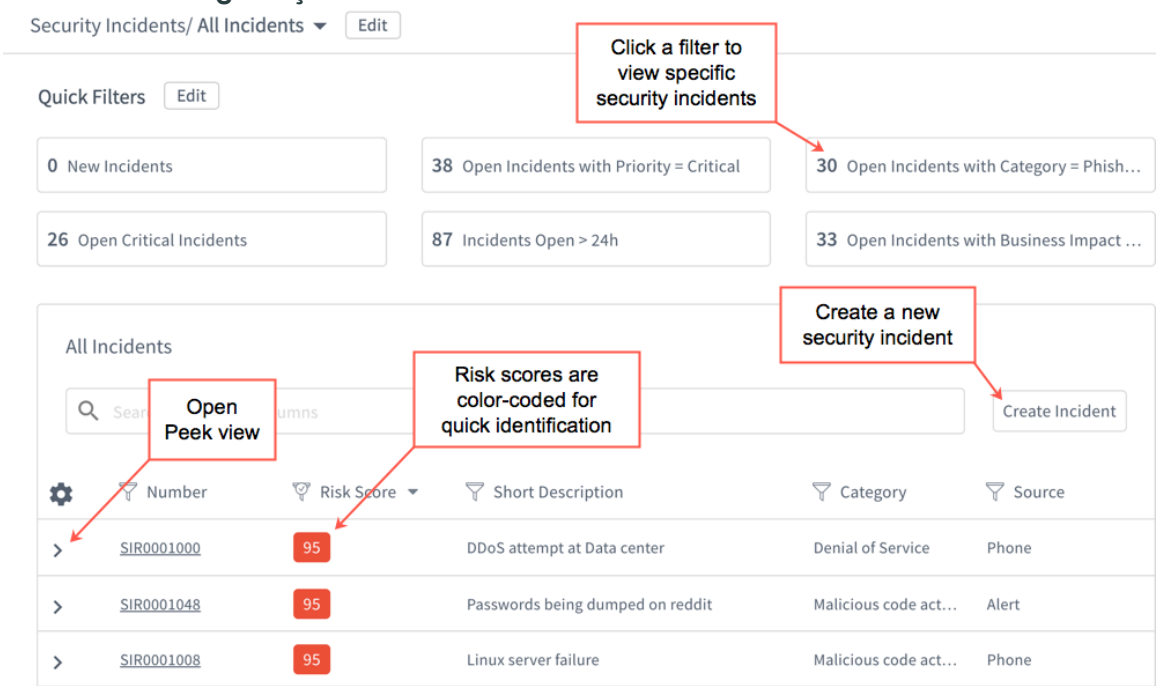
Para acessar este novo espaço, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.

Incidente de segurança



O espaço é aberto em uma guia separada do navegador.

Incidentes de segurança

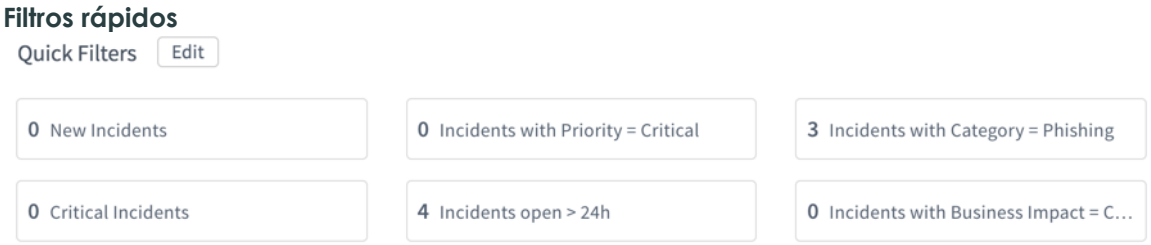


Localize os incidentes de segurança que você deseja analisar com Filtros rápidos

O Espaço do analista de segurança fornece várias ferramentas para filtrar a lista de incidentes de segurança para que você possa encontrar rapidamente os incidentes de segurança que deseja analisar. Os Filtros rápidos permitem selecionar um subconjunto dos incidentes de segurança com base nos critérios do filtro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Basta clicar no filtro rápido que você deseja usar.

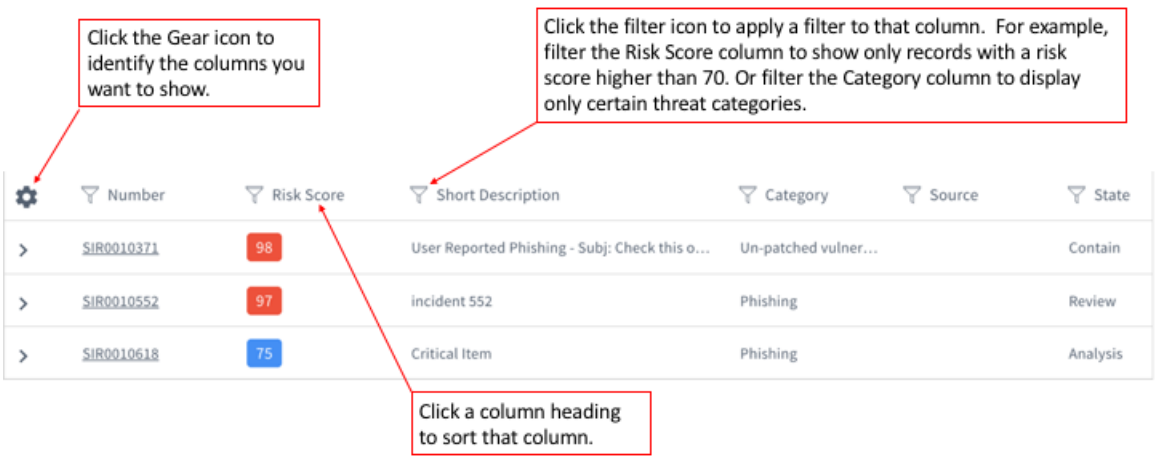
Nota: Você pode clicar em um botão **Editar** para identificar quais filtros rápidos deseja exibir na tela da lista. Um mínimo de um filtro deve ser selecionado, até um máximo de seis.

Você pode definir filtros rápidos adicionais, bem como filtros primários para Espaço do analista de segurança, usando o ambiente clássico. Para obter mais informações, consulte Configurar filtros primários e secundários para Espaço do analista de segurança.

Personalizar a lista de incidentes de segurança

Como acontece com todas as listas em sua instância, o Espaço do analista de segurança fornece ferramentas para personalizar a lista e classificar as informações exibidas para atender às suas necessidades de análise.

Personalizar a lista de incidentes de segurança



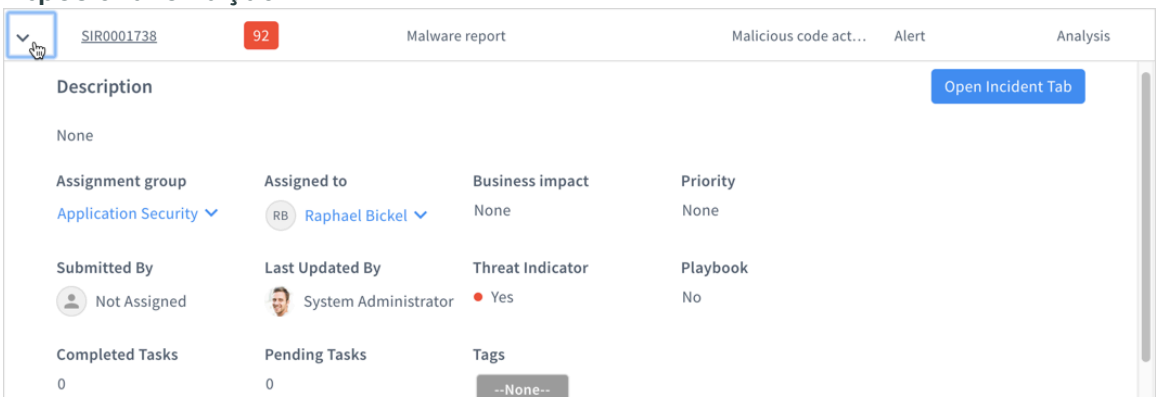
Economize tempo com a exibição de Inspeção

Antes de abrir um registro de incidente de segurança, você pode economizar tempo usando a exibição de Inspeção. Este recurso permite que você localize rapidamente artefatos de segurança vitais sem precisar recarregar a página inteira. Basta clicar no ícone **>** à esquerda de um número de incidente de segurança para dar uma olhada.

Tradução automática

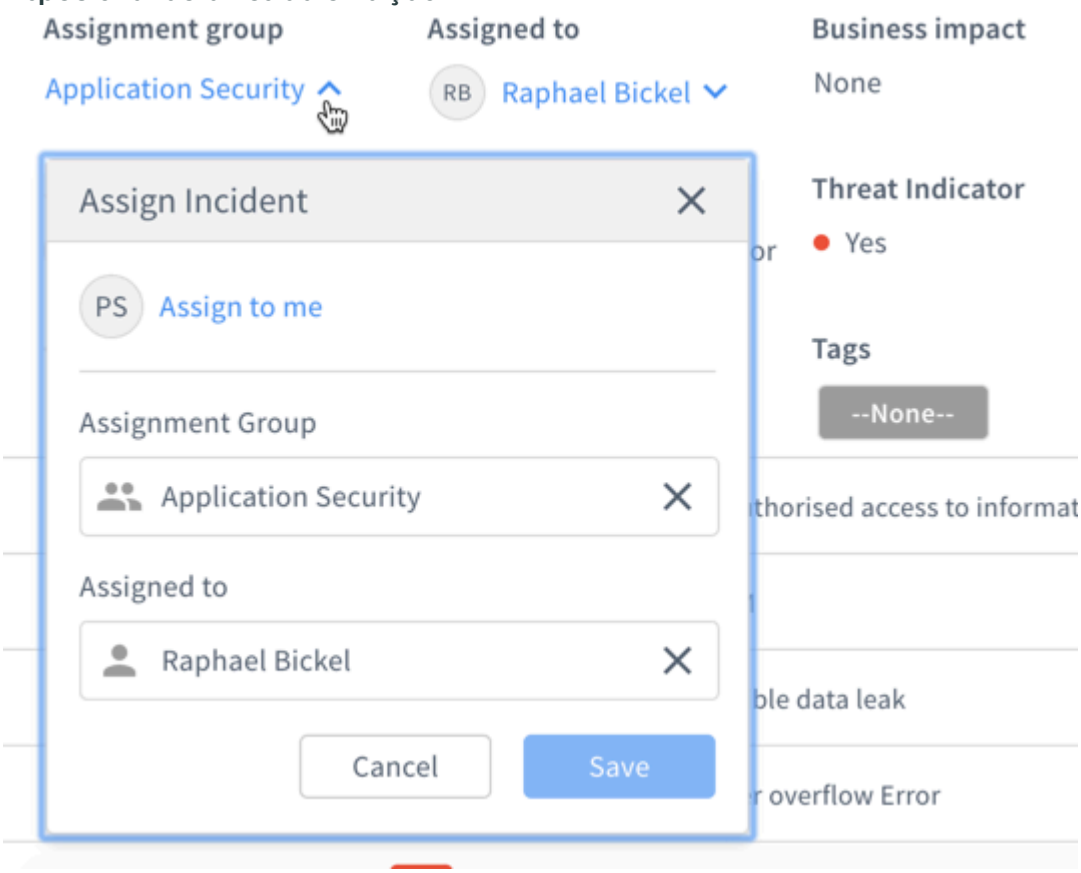
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inspecionar exibição



A exibição de espreitadela fornece um snapshot de informações vitais em uma única exibição. Esta exibição pode economizar um tempo valioso quando você está trabalhando com vários incidentes. Você pode clicar nas setas para baixo em determinados campos para fazer atualizações dinâmicas, como atribuir um grupo de atribuição ou um analista específico.

Inspecionar detalhes da exibição



Executar ações rápidas em um incidente de segurança

Depois de selecionar e abrir um incidente de segurança específico, você pode executar ações de economia de tempo no registro.

Tradução automática

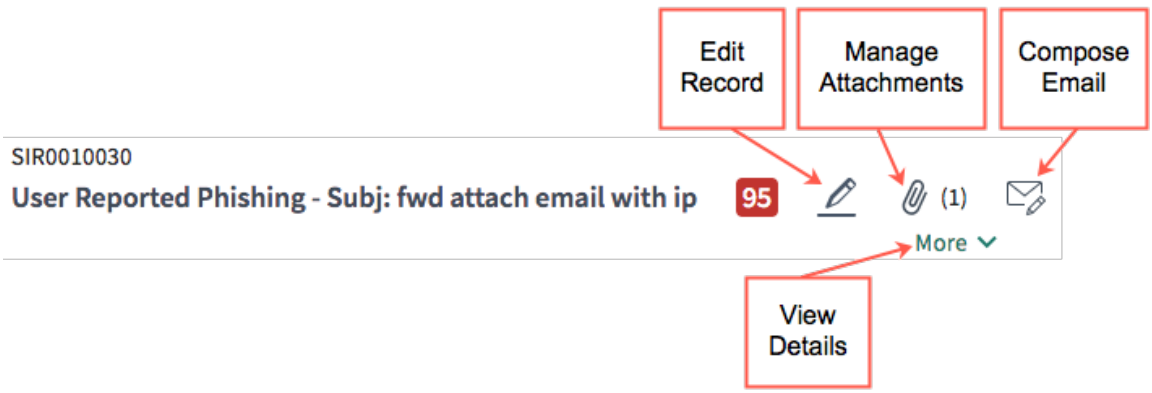
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o incidente de segurança estiver aberto, clique no ícone **Editar registro** para fazer mudanças rápidas em qualquer um dos campos. Se o registro estiver fechado, você poderá alterar somente seu marcador.
- Clique em **Gerenciar anexos** para anexar arquivos ao incidente de segurança. Você também pode baixar ou remover arquivos anexados e editar a criptografia aplicada aos anexos.
- Clique em **Compor e-mail** para enviar um e-mail rápido para um colega. Os e-mails podem ser de forma livre ou você pode enviar e-mails predefinidos selecionados em uma lista de modelos. Os e-mails enviados e as respostas recebidas são capturados na Linha do tempo do incidente.

  Nota: Você pode criar modelos personalizados que contêm conteúdo reutilizável para e-mails e notificações por e-mail. As variáveis podem ser usadas para inserir informações específicas para o incidente ou alerta de segurança, como a linha de assunto, a prioridade ou a categoria de ameaça. Use a tabela Incidente de segurança [sn_si_incident] para e-mails e notificações por e-mail relacionados a Security Incident Response. Para obter mais informações, consulte Modelos de e-mail

- Clique em **Mais** para exibir um snapshot rápido do incidente de segurança, como a descrição, o impacto nos negócios e a prioridade. Você também pode clicar na seta para baixo nos campos **Grupo de atribuição** e **Atribuído a** para fazer mudanças dinâmicas nesses campos.

Grupo de atribuição



Como trabalhar com vários incidentes de segurança

A interface com guias permite que você mantenha vários incidentes de segurança abertos simultaneamente para que você possa alternar entre eles com um único clique. Isso pode economizar tempo e permitir que você tenha uma visão geral quando ameaças de várias origens forem identificadas.

Como trabalhar com vários incidentes de segurança

Exibir informações de análise nas guias de incidentes de segurança

Quando você abre um registro de incidente de segurança, três guias são mostradas:

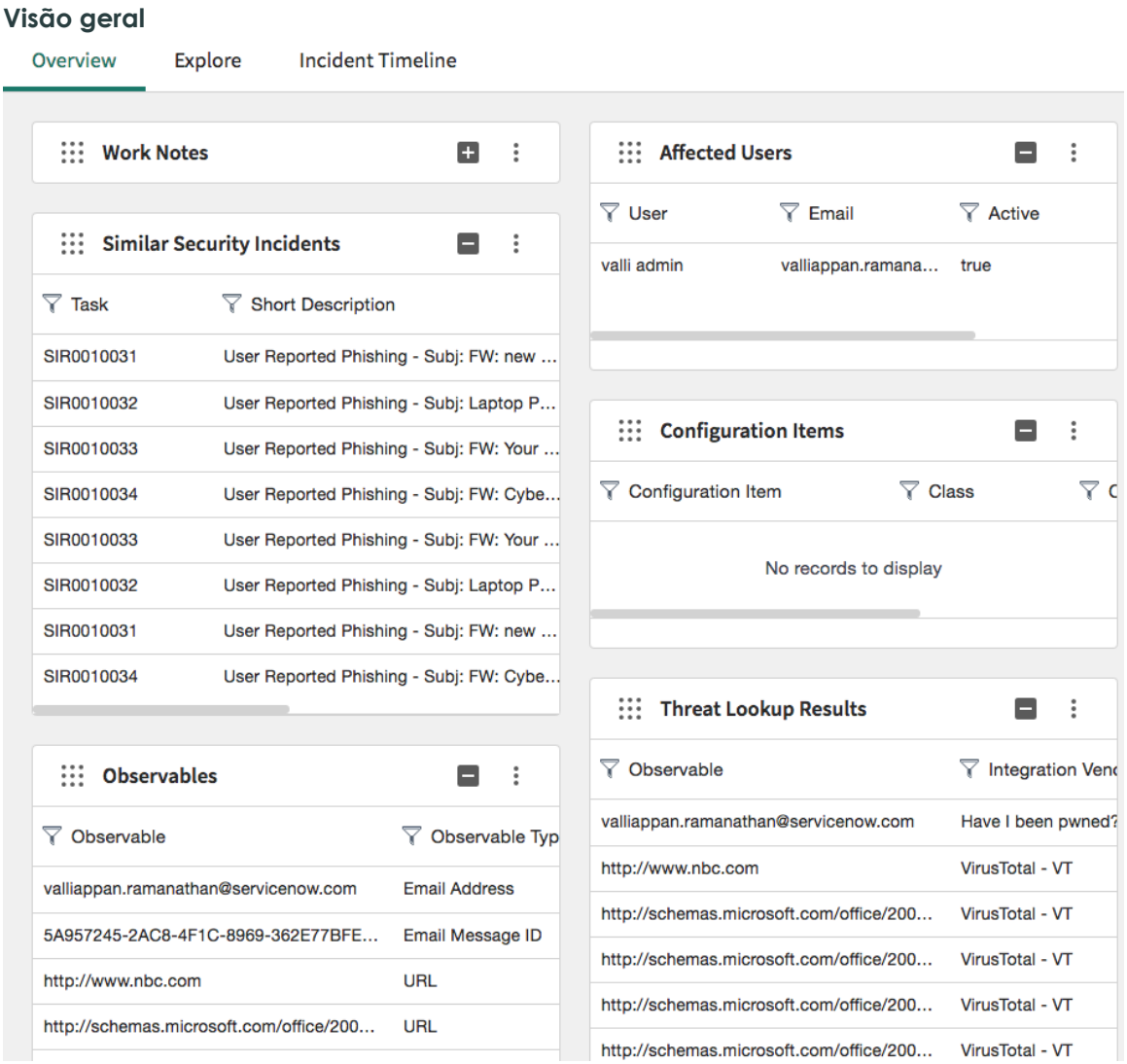
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Visão geral
- Explorar
- Linha do tempo do Incidente

Guia Visão Geral

Use a guia **Visão geral** para exibir informações em um incidente de segurança em um único local. Não é necessário abrir outra aplicação ou console.

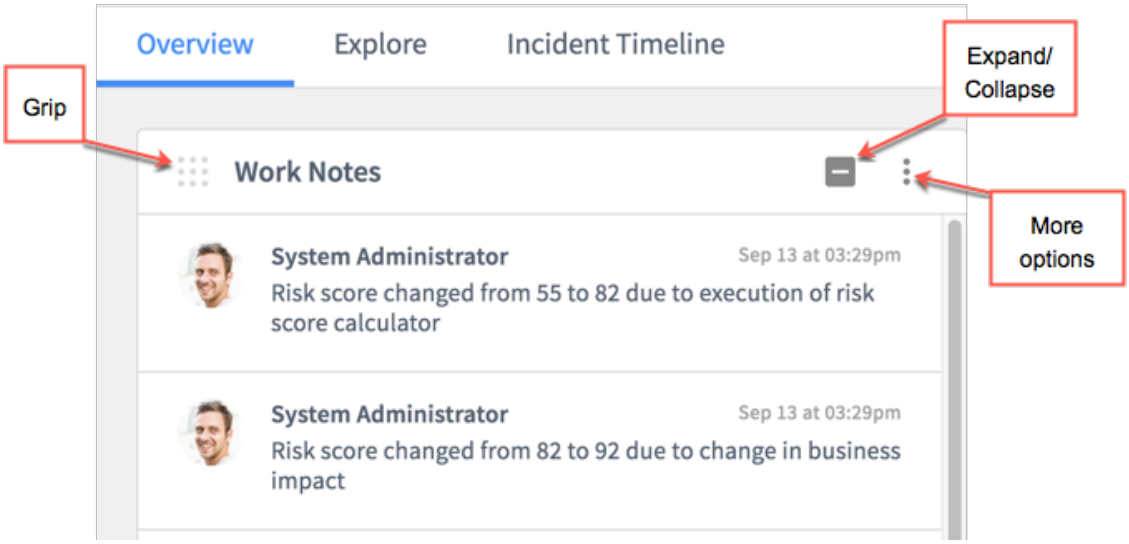


Os blocos exibidos na guia **Visão geral** são personalizáveis. Você pode recolhê-los e expandi-los conforme necessário e movê-los arrastando o ícone de **Punho**. Clique no ícone **Mais opções** para excluir um bloco ou alterar o texto do título.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

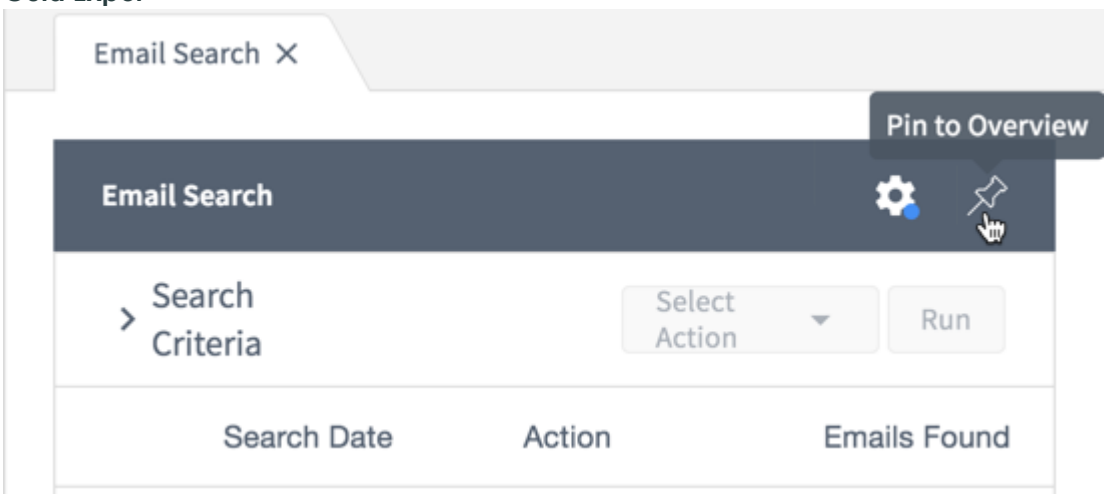
Guia Visão Geral



Guia Explorar

Configure os blocos exibidos na guia **Visão geral** usando a guia **Explorar**. Basta selecionar os blocos que você deseja exibir no painel esquerdo e clicar no ícone **Fixar**. Os blocos fixados aparecem automaticamente na guia **Visão geral**.

Guia Expor



O painel esquerdo da guia **Explorar** inclui uma ampla variedade de informações que você pode exibir na guia **Visão geral**. Por exemplo, expanda **Observáveis** para exibir essas listas relacionadas.

- Observáveis
- Resultados da Pesquisa de ameaças
- Resultados da verificação de segurança
- Pesquisas de domínio
- Aprimoramento de Observável

Listas relacionadas adicionais estão disponíveis em **Usuários**, **Itens de configuração**e **Incidentes**.

Tradução automática

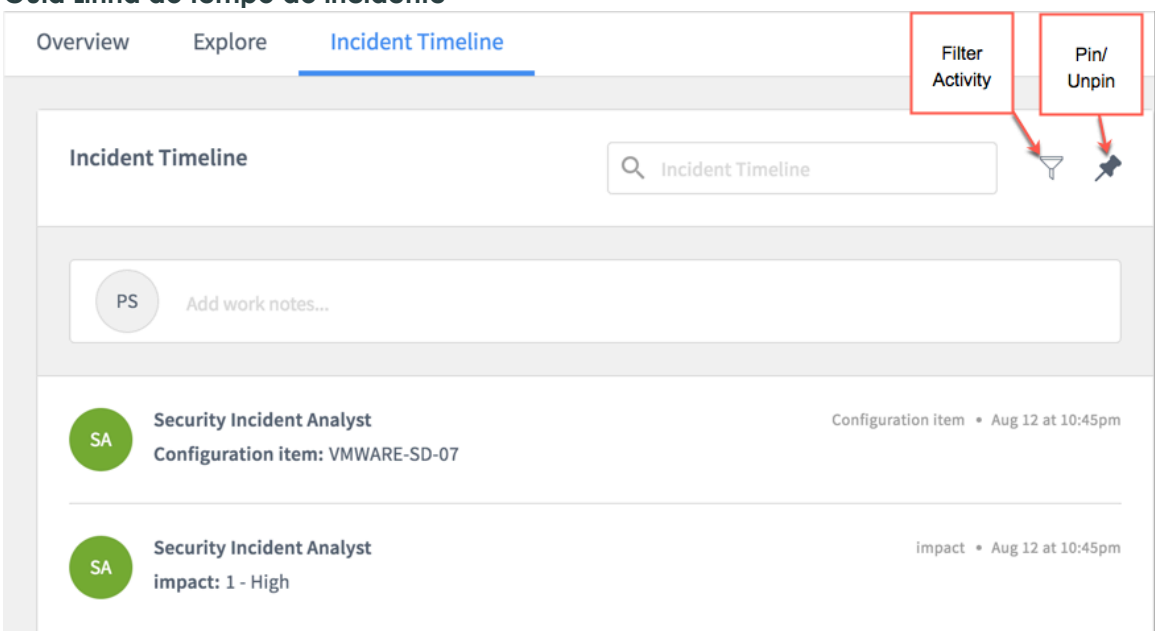
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Linha do tempo do incidente

Use a guia **Linha do tempo de incidentes** durante sua investigação para fins de acompanhamento. Cada vez que uma ação é realizada em um incidente de segurança, o sistema a registra na Linha do tempo de incidentes.

- Você também pode adicionar manualmente anotações de trabalho à linha do tempo digitando-as na caixa **Adicionar anotações de trabalho** e clicando em **Publicar**.
- Você pode pesquisar uma atividade de linha do tempo específica usando a caixa de pesquisa.
- O ícone **Filtrar atividade** permite exibir somente os tipos de atividade da linha do tempo que você deseja ver (por exemplo, somente incidentes criados por um analista específico).
- Você pode adicionar ou remover a Linha do tempo do incidente na guia **Visão geral** usando o ícone **Fixar/Desmarcar**.

Guia Linha do tempo do incidente



Lidar com incidentes de segurança usando o Playbook

Resolva determinados tipos de ameaças à segurança passo a passo usando os Playbooks do analista de segurança integrados. Por exemplo, um analista pode usar o playbook para resolver ataques de phishing e ameaças causados por atividades de código mal-intencionado. Para obter mais informações, consulte Resolver ameaças à segurança com o playbook.

Resolver ameaças à segurança com o playbook

Use o Playbook para resolver determinados tipos de ameaças à segurança passo a passo. Por exemplo, você pode resolver ataques de phishing e ameaças causados por atividade de código mal-intencionado usando playbooks.

Antes de Iniciar

Função necessária: sn_si.admin ou administrador

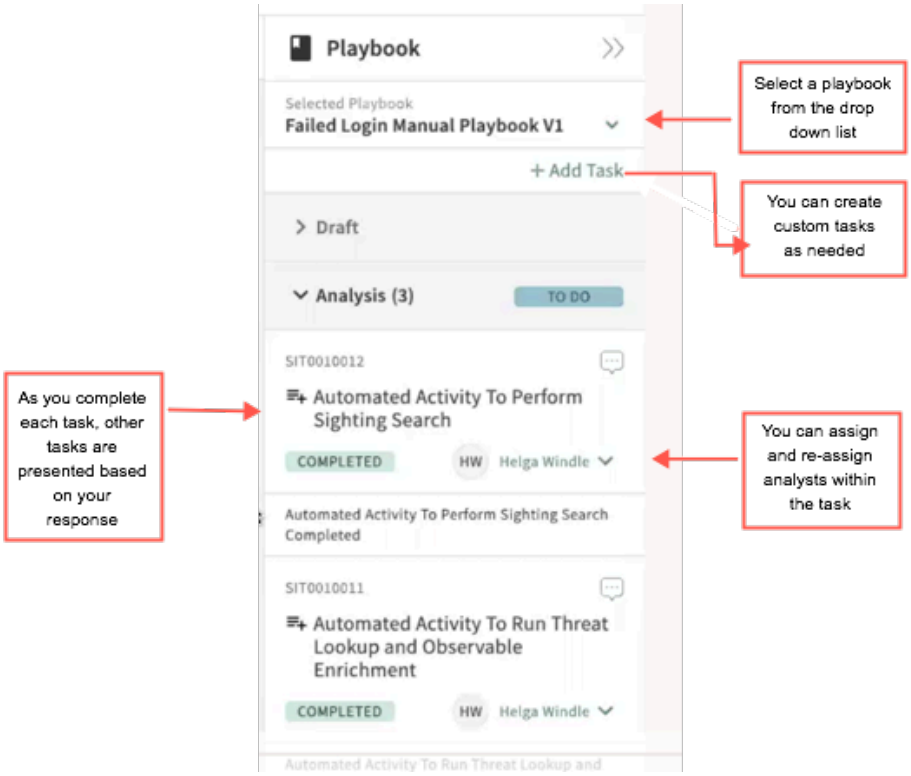
Por Que e Quando Desempenhar Esta Tarefa

Cada grupo de tarefas (Análise, Contenção e assim por diante) orienta você em uma série de perguntas e outras atividades para resolver a ameaça.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

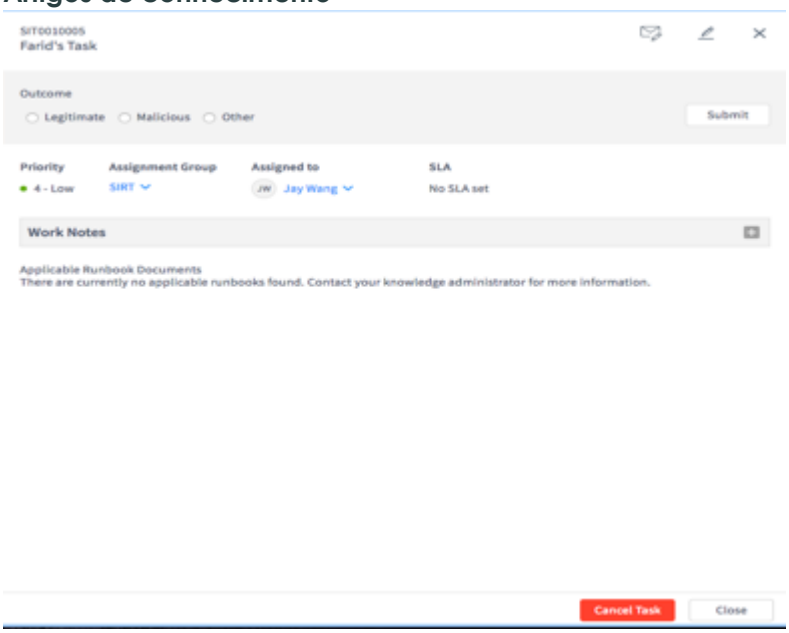
Playbook



Conforme você trabalha em cada tarefa, insira anotações de trabalho para ajudar a analisar ataques semelhantes no futuro. Depois que uma ameaça é identificada, você também pode usar as informações no playbook para colocar a ameaça em quarentena, isolar ativos afetados de forma semelhante e remover malware.

Os artigos de conhecimento, incluídos em cada tarefa, fornecem dicas e outras informações para ajudá-lo a executar as etapas necessárias.

Artigos de conhecimento



O sistema de base inclui artigos de conhecimento para cada uma das tarefas do playbook. Você pode, no entanto, escrever seus próprios artigos de conhecimento e associá-los a tarefas do playbook.

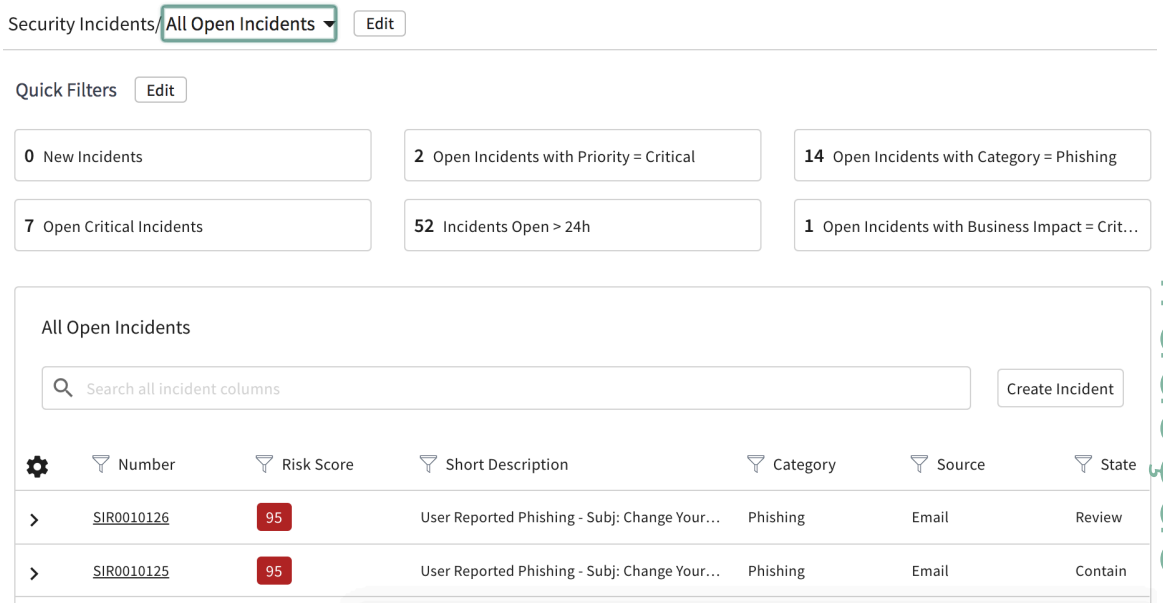
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

Nota: Para obter um exemplo de como usar o playbook para analisar e resolver uma ameaça específica, consulte Como resolver ataques de phishing relatados por usuários com o playbook.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes (Nova IU)**.
   A tela Incidentes de segurança mostra os incidentes de segurança que foram atribuídos a você.



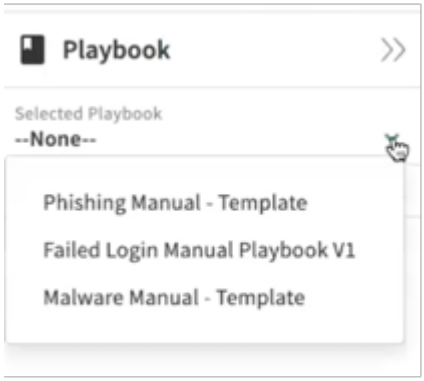
2. Você pode clicar na lista de seleção **Atribuído a mim** para selecionar um filtro diferente, como todos os incidentes em aberto ou todos os incidentes não atribuídos.
   Como alternativa, você pode clicar em um dos Filtros rápidos para exibir incidentes de segurança de um tipo específico, como somente Incidentes críticos.
3. Clique no incidente de segurança que você deseja analisar.

   Considere priorizar incidentes de segurança com pontuações de alto risco.

4. Se o painel do playbook na borda direita da tela estiver fechado, clique no ícone do playbook ( ) para abri-lo.
   Se nenhum playbook estiver atribuído ao incidente de segurança, você poderá selecionar um playbook na lista de seleção Playbook selecionado, conforme mostrado abaixo:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você também pode atribuir um playbook diferente ao incidente de segurança. Para incluir um playbook na lista de seleção Playbook selecionado ou para mudar o playbook de um incidente de segurança, consulte Habilitar playbooks para seleção de analista para obter detalhes.

O playbook específico para o tipo de ameaça à segurança é aberto. Ele é dividido em categorias de tarefas semelhantes. Por exemplo, você usa as tarefas no grupo **Análise** para determinar a validade e o escopo da ameaça. O grupo **Conter** inclui tarefas para isolar a ameaça a um usuário ou ativo específico. As tarefas no grupo **Erradicar** orientam você no processo de remoção do malware ou na recriação da imagem do host.

5. Clique no primeiro grupo (**Análise**) e, em seguida, clique na primeira tarefa no playbook.
6. Siga os avisos na tarefa.
   - Algumas tarefas fazem uma pergunta, como "O e-mail faz parte da campanha?" Execute a análise necessária para responder à pergunta e selecione **Sim** ou **Não**.
   - Se você definiu artigos de conhecimento e os associou a tarefas do playbook, os artigos serão exibidos quando você começar a trabalhar em uma tarefa.
   - Algumas tarefas são transitórias. Eles simplesmente instruem você a executar uma ação, como adicionar observáveis a um incidente de segurança. Depois de concluir a ação, clique em **Marcar como Concluída**.

   Conforme você conclui as tarefas, as tarefas subsequentes são apresentadas a você com base nas escolhas que você faz. Grupos esmaecidos (como **Recuperar**, **Revisar**e assim por diante) podem ser ativados por suas escolhas.
7. Continue trabalhando em cada tarefa apresentada até concluir todas as tarefas para resolver a ameaça e encerrar o incidente de segurança.

Informações relacionadas

Adicionar uma tarefa personalizada ao playbook

Como resolver ataques de phishing relatados por usuários com o playbook

O playbook de phishing orienta você nas tarefas necessárias para analisar e resolver um ataque de phishing relatado por um dos funcionários da sua empresa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

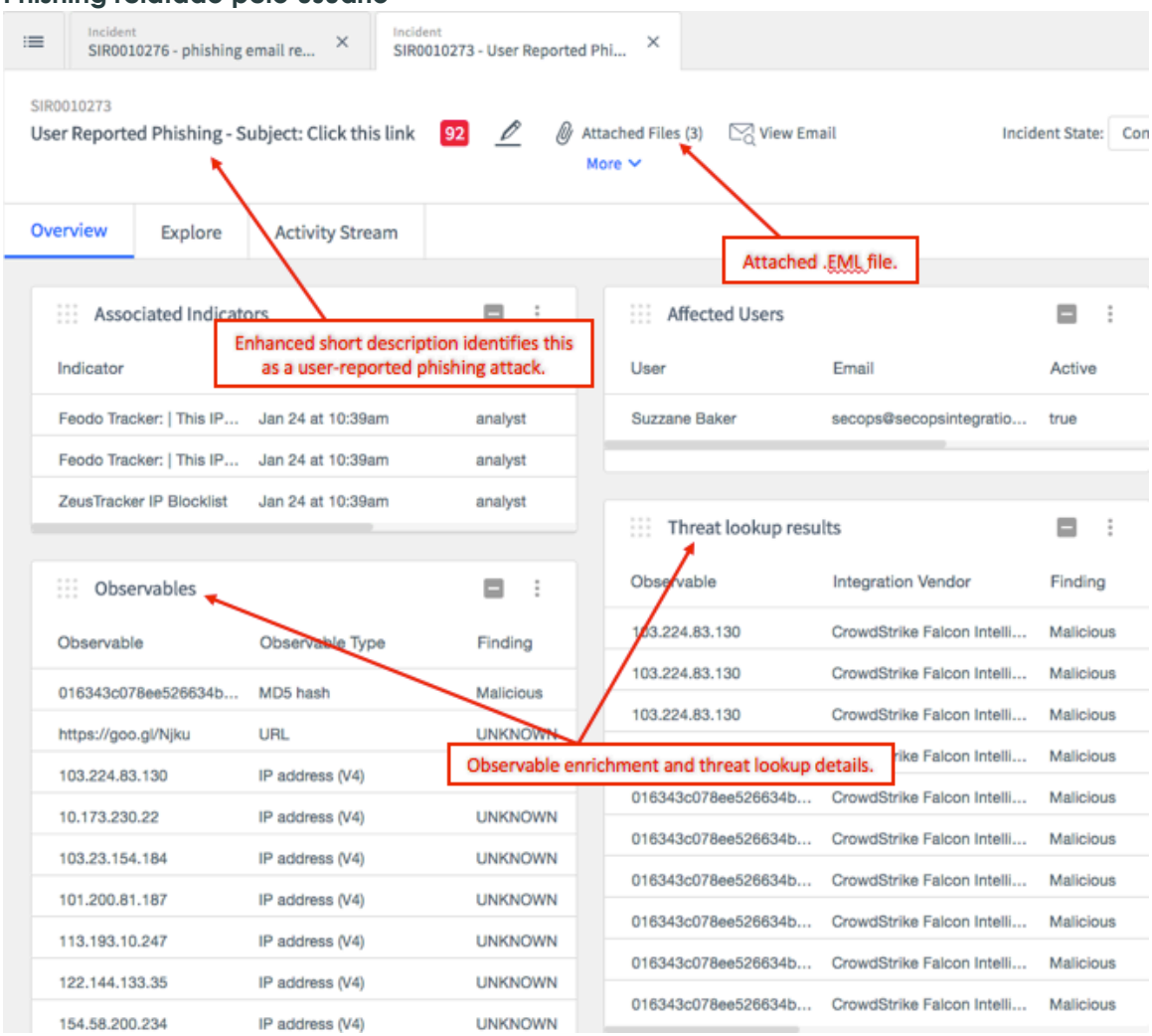
Como os incidentes de segurança são criados a partir de ataques de phishing relatados pelo usuário

Durante a configuração do Security Incident Response, o administrador do sistema cria uma série de regras de correspondência de e-mail que podem identificar e-mails que contêm sinais de um ataque de phishing. Quando os funcionários recebem um e-mail suspeito que contém os sinais comuns de um ataque de phishing (conforme definido por suas políticas de segurança), eles podem enviá-lo como um anexo .EML para o endereço de e-mail de phishing definido por sua organização.

Quando o e-mail é recebido no endereço de e-mail de phishing, o anexo .EML é analisado e suas informações são comparadas com as regras de correspondência de e-mail. Se uma correspondência for encontrada, um incidente de segurança contendo as seguintes informações será criado:

- A descrição resumida inclui o phishing relatado pelo usuário, seguido pelo assunto real do e-mail de origem.
- O arquivo .EML está anexado ao incidente de segurança.
- Se o .EML contiver observáveis, eles serão analisados e as pesquisas de aprimoramento e ameaça serão realizadas automaticamente.

Phishing relatado pelo usuário

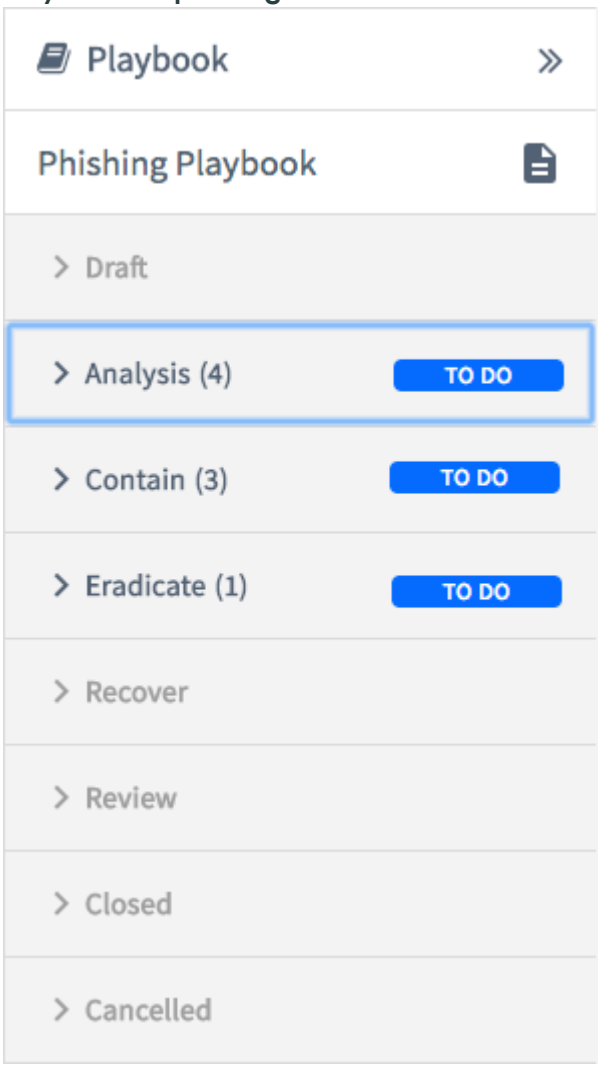


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando um incidente de segurança da categoria de phishing é aberto, o Playbook de phishing fica disponível automaticamente. Basta clicar no ícone do playbook ( ) para abrir o playbook.

Playbook de phishing



O playbook de phishing contém tarefas para ajudá-lo a analisar, conter e erradicar uma ameaça de phishing. As tarefas são organizadas em estados (por exemplo, **Análise**, **Conter**e assim por diante). Quando todas as tarefas de um estado forem concluídas, o playbook orientará você para o próximo estado.

Analisar detalhes do incidente de segurança

Quando o incidente de segurança está no estado Análise, você recebe tarefas para executar a investigação básica do incidente, incluindo:

- Determinar a validade do incidente.
- Estude o impacto da possível ameaça.
- Coordenar uma resposta eficaz ao incidente.

Conforme você trabalha nas tarefas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Familiarize-se com os artigos de conhecimento.
- Abra o anexo de e-mail e examine-o quanto a sinais de elementos de phishing comuns.
- Revise os resultados da pesquisa de ameaças.

Contendo o incidente de segurança

Quando o incidente de segurança está no estado **Conter**, você recebe tarefas para revisar os detalhes do e-mail. Para garantir que as ameaças não possam entrar na sua organização, atualize as defesas de rede, na forma de assinaturas e regras do Sistema de defesa contra intrusão (IDS) e do Sistema de prevenção de intrusão (IPS).

Conforme você trabalha nas tarefas:

- Tome medidas para limitar os impactos da ameaça, como isolar os dispositivos afetados.
- Examine os observáveis anexados ao e-mail.
- Determine se algum conteúdo de e-mail está associado a uma ameaça conhecida, incluindo:
  - URL
  - Remetente do e-mail
  - URL de phishing
  - Endereço IP do servidor SMTP do remetente

Como erradicar o malware

Depois de implantar assinaturas e regras atualizadas na solução antivírus, use as tarefas no estado **Erradicar** para determinar se há malware presente e trate-o de acordo.

Conforme você trabalha nas tarefas:

- Verifique os endpoints dos dispositivos afetados quanto à presença de malware.
- Remova qualquer malware encontrado.
- Como último recurso, limpe e crie novamente a imagem dos dispositivos host.

Revisão do incidente de segurança

Se você determinou que um ataque de phishing foi um alarme falso ao executar as tarefas de análise, o incidente de segurança será movido para o estado **Revisão** e você precisará notificar os usuários para que eles saibam que é seguro abrir o anexo de e-mail.

Fechando o incidente de segurança

Quando todas as tarefas no playbook forem concluídas, o incidente de segurança será movido para o estado **Encerrado**. Você deve inserir comentários de encerramento antes que o incidente possa ser encerrado.

Como cancelar um incidente de segurança

Quando um incidente de segurança está no estado **Revisão** e você informou com sucesso aos usuários que o e-mail não é uma ameaça, o estado **Cancelado** se torna ativo e você pode cancelar o incidente de segurança.

Nota: A tarefa de recuperação não é usada no playbook de phishing.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como associar um artigo de conhecimento a uma tarefa do playbook

Ao analisar as ameaças à segurança usando o playbook Security Incident Response, você pode exibir artigos de conhecimento para cada tarefa, se definida pela sua organização. Se os artigos de conhecimento não estiverem presentes, você poderá criá-los e associá-los a tarefas do playbook.

Antes de Iniciar

Ao usar o playbook em Security Incident Response, anote o texto associado a cada tarefa. Por exemplo, a primeira tarefa na categoria Phishing é **O alerta foi enviado pelo funcionário?** Esta é a descrição resumida da tarefa e você precisa deste texto (exatamente como aparece no playbook) para associar um artigo de conhecimento à tarefa.

Função necessária: sn_sir.knowledge_admin e sn_si.admin ou admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Catálogo e Conhecimento** > **Conhecimento**.
2. Crie e publique um artigo de conhecimento para uma tarefa específica do playbook.
3. Navegar até **Incidente de segurança** > **Runbook manual** > **Criar novo runbook**.
4. Crie um runbook, preenchendo as seguintes informações:

Campo	Descrição
Artigo de conhecimento	Selecione o artigo de conhecimento publicado que você deseja associar à tarefa do playbook.
Tabela	Selecione Security Incident Response Tarefa [sn_si_task].
Condição	Defina o Construtor de condições como: ◦ **Opção:** selecione **Descrição resumida**. ◦ **Operador:**selecione **é**. ◦ **Valor de entrada:** insira a descrição resumida da tarefa, exatamente como ela aparece no playbook.

5. Clique em **Enviar**.
   Na próxima vez que você executar o playbook e selecionar esta tarefa, o artigo de conhecimento associado será exibido.

Informações relacionadas

Criar um artigo de conhecimento de incidente de segurança

Criar um runbook do Security Incident Response

Adicionar uma tarefa personalizada ao playbook

O sistema de base Espaço do analista de segurança inclui uma série de tarefas para cada categoria de ameaça. Você pode criar tarefas personalizadas que atendam às necessidades exclusivas do seu sistema ou dos clientes.

Antes de Iniciar

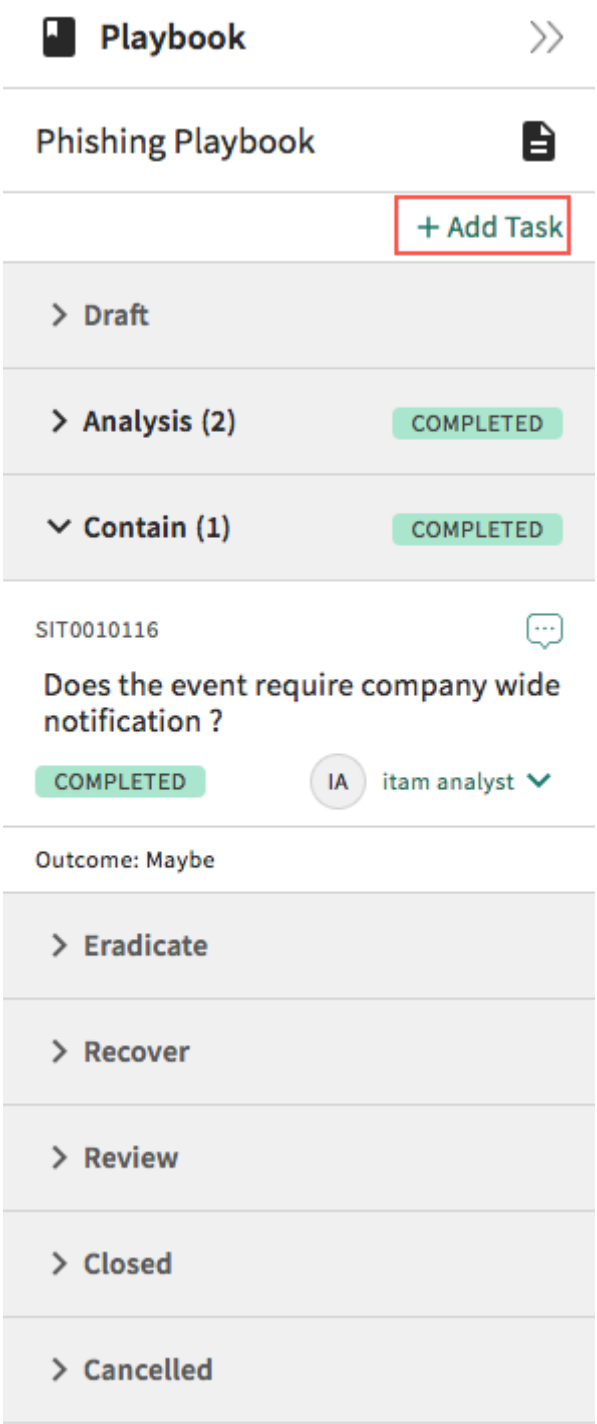
Função necessária: sn_si.basic ou security_admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

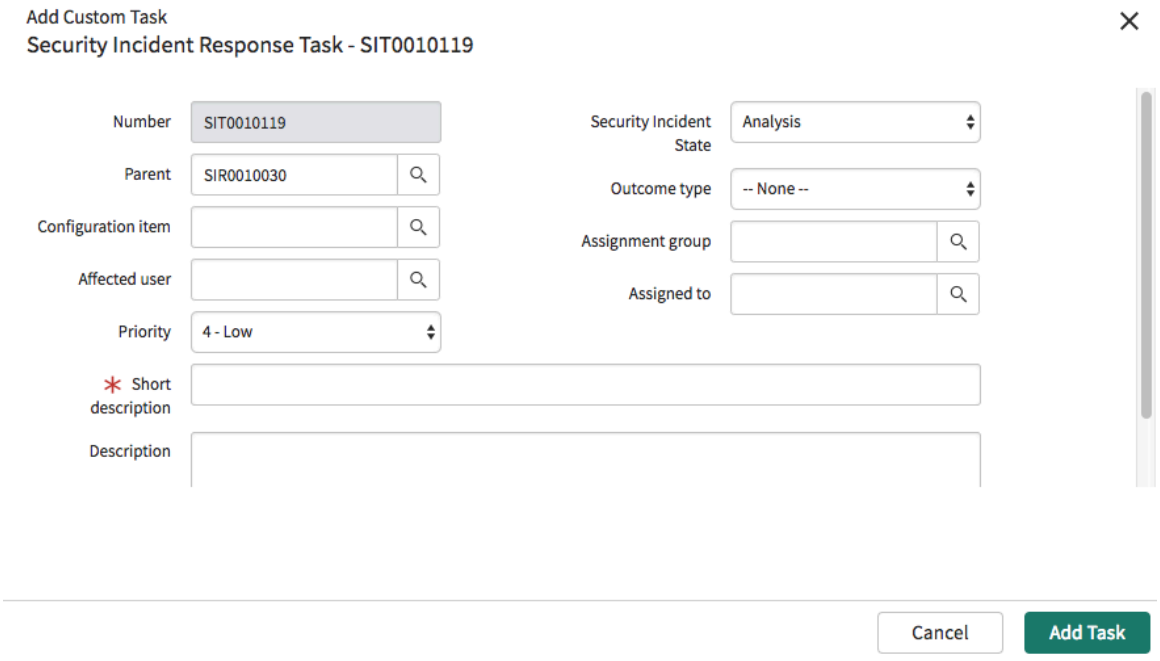
1. Com o playbook aberto, clique em **Adicionar tarefa**.



A tela Adicionar tarefa personalizada é aberta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Preencha os campos conforme necessário.

Campo	Descrição
Número	[Somente leitura] O número da tarefa de incidente de segurança gerado automaticamente.
Primário	O número do incidente de segurança relacionado.
Item de configuração	O item de configuração afetado pelo problema de segurança, se houver.
Usuário afetado	O usuário afetado pelo problema de segurança, se houver.
Prioridade	Selecione a prioridade usada para determinar quando esta tarefa deve ser executada.
Estado do Incidente de segurança	O estado atual da tarefa de resposta de segurança. Você pode selecionar um estado futuro, se necessário.
Tipo de resultado	Se você tiver a função sn_si.basic, selecione **Sim/Não** como o tipo de resultado. Se você tiver a função security_admin, poderá criar um tipo de resultado personalizado com vários valores de saída personalizados. Por exemplo, você pode definir uma tarefa com valores dependentes com base na categoria de ameaça. Para obter mais informações, consulte Listas de seleção
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído será selecionado.
Atribuído a	O indivíduo atribuído para executar a tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Uma descrição da tarefa do playbook de incidente de segurança.
Descrição	Insira uma descrição para a tarefa selecionada.

3. Ao concluir suas entradas, clique em **Adicionar tarefa**.
   A tarefa é inserida no playbook após a tarefa atual.

Pesquisas de detecções sobre ataques de phishing e malware relatados pelo usuário

Realize pesquisas de detecções em e-mails ou observáveis para determinar com que frequência determinados tipos de ataques, como ataques de phishing ou comunicações com um IP ou URL mal-intencionado, ocorrem em sua rede. Cada ocorrência é considerada uma detecção. As pesquisas de detecções de observáveis devem ser configuradas para seus armazenamentos de log ou gestão de eventos e informações de segurança (SIEM).

Como usar o recurso de pesquisa de detecções para localizar usuários phishing e rastrear observáveis de phishing e malware no armazenamento de logs em sua rede.

Assista a este vídeo de três minutos para saber como usar o recurso de pesquisa de detecções para localizar usuários phishing e rastrear observáveis de phishing e malware no armazenamento de logs em sua rede.

Os termos a seguir são usados para descrever ataques de phishing relatados pelo usuário:

- Usuário phishing: um usuário que recebeu um e-mail de phishing.
- Usuário vítima: um usuário que interagiu com o URL de phishing, normalmente clicando em um link no e-mail de phishing. Esta ação pode expor as credenciais ao invasor.

Ao começar a analisar um incidente de phishing, você pode realizar uma pesquisa de detecções por e-mail ou realizar uma pesquisa de detecções observável para identificar outros usuários em sua organização que foram afetados pelo mesmo ataque de phishing. Pesquise seus armazenamentos de log para identificar usuários vitimados e phishing. Depois de identificar a lista de usuários afetados, crie incidentes de segurança secundários para executar procedimentos abrangentes de resposta a incidentes usando as ferramentas disponíveis em Security Incident Response.

Nota: Você também pode usar a seguinte abordagem para executar uma pesquisa de detecções:

- Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes** e clique em um incidente de segurança.
- Clique em **Mostrar IoC** em Links relacionados. Uma lista de observáveis é exibida.
- Selecione um observável na lista e, na lista **Ações**, selecione uma das seguintes opções:
  - Executar pesquisa de detecções de tráfego na web
  - Executar pesquisa de detecções de tráfego de e-mails
- Especifique o intervalo de tempo e clique em **Pesquisar** para realizar uma pesquisa de detecções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de pesquisa de detecções salvas

Configure pesquisas de detecções e crie configurações salvas para SIEMs ou outros armazenamentos de log para instâncias de observáveis para determinar a presença de observáveis mal-intencionados em seu ambiente.

Nota: Pesquisas salvas e consultas no local são compatíveis somente com a integração do Splunk.

Informações relacionadas

Criar registros de configuração de pesquisa de detecções

Executar uma pesquisa de detecções de e-mail para ataques de phishing relatados pelo usuário

Pesquise usuários que receberam e-mails de phishing com base em observáveis, como assunto do e-mail, nome do remetente ou ID da mensagem. Você pode conter e erradicar esses e-mails de phishing da sua organização.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Pesquise os logs de tráfego de e-mail do Splunk para coletar a lista de destinatários de um e-mail suspeito. A pesquisa pode ser realizada usando o remetente do e-mail, o ID da mensagem de e-mail ou o assunto do e-mail associado a um incidente de segurança como critérios.

Nota:

- Esta implementação de pesquisa de detecções para observáveis baseados em e-mail foi testada somente com o armazenamento de log do Splunk Enterprise.
- Os eventos de log do Splunk devem ser compatíveis com o modelo de informações comuns (CIM) para que a consulta de pesquisa de detecções retorne resultados precisos.

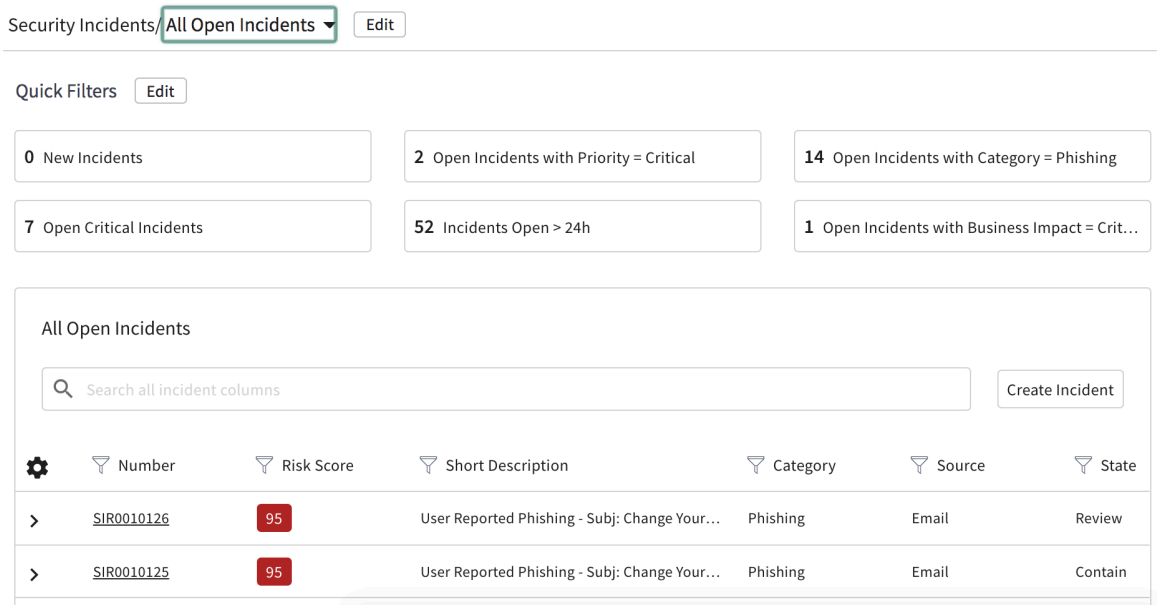
Procedimento

1. Para ver os incidentes de segurança atribuídos à sua equipe, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.
2. Na lista **Incidentes de segurança**, selecione um dos filtros, como todos **os incidentes abertos**, **todos os incidentes atribuídos a você**ou **todos os incidentes**.

   Para exibir incidentes de segurança de um tipo específico, como incidentes críticos ou e-mails de phishing, clique em um dos **Filtros rápidos**.

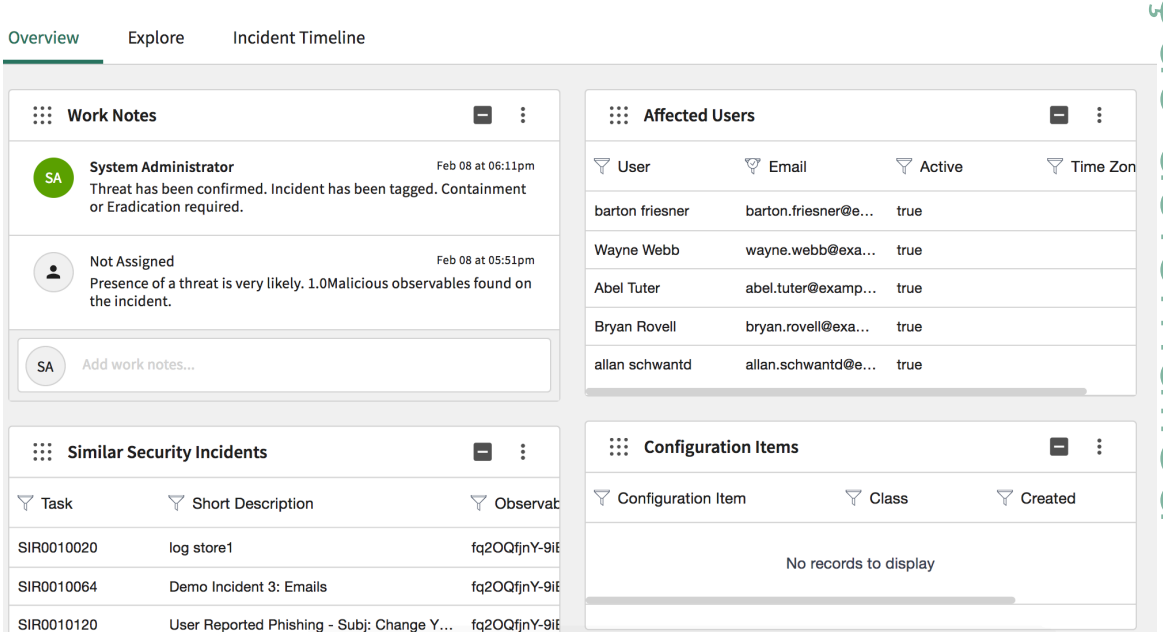
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique no incidente de segurança que você deseja analisar.

A guia Visão geral fornece uma visão geral do incidente de segurança, incluindo uma lista de observáveis, usuários afetados e incidentes de segurança semelhantes.

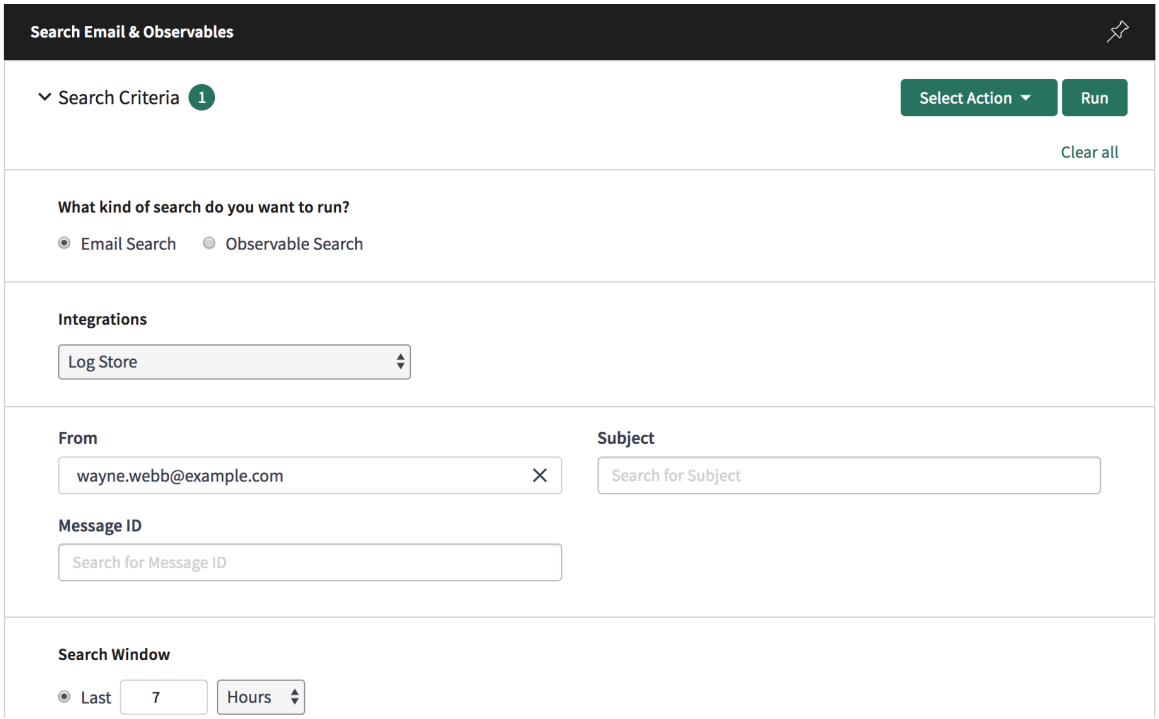


4. Clique na guia **Explorar**.

5. Em **Dados do incidente**, navegue até **Investigação** > **Pesquisar e-mail e observáveis**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Expanda a seção Critérios de pesquisa.
7. Selecione **Pesquisa de e-mail** como o tipo de pesquisa que você deseja executar e especifique o restante dos critérios de pesquisa.

Formulário de critérios de pesquisa

Campo	Descrição
Integrações	Tipo de integrações. Selecione **Armazenamento de logs** na lista. **Nota:** Este recurso é compatível somente com o armazenamento de log do Splunk.
De	Endereço de e-mail completo do remetente (por exemplo, jane.doe@example.com).
ID da Mensagem	ID da mensagem de e-mail do armazenamento de logs.
Assunto	Assunto do e-mail de phishing.
Janela de Pesquisa	Janela de tempo para a pesquisa (por exemplo, as últimas 24 horas).

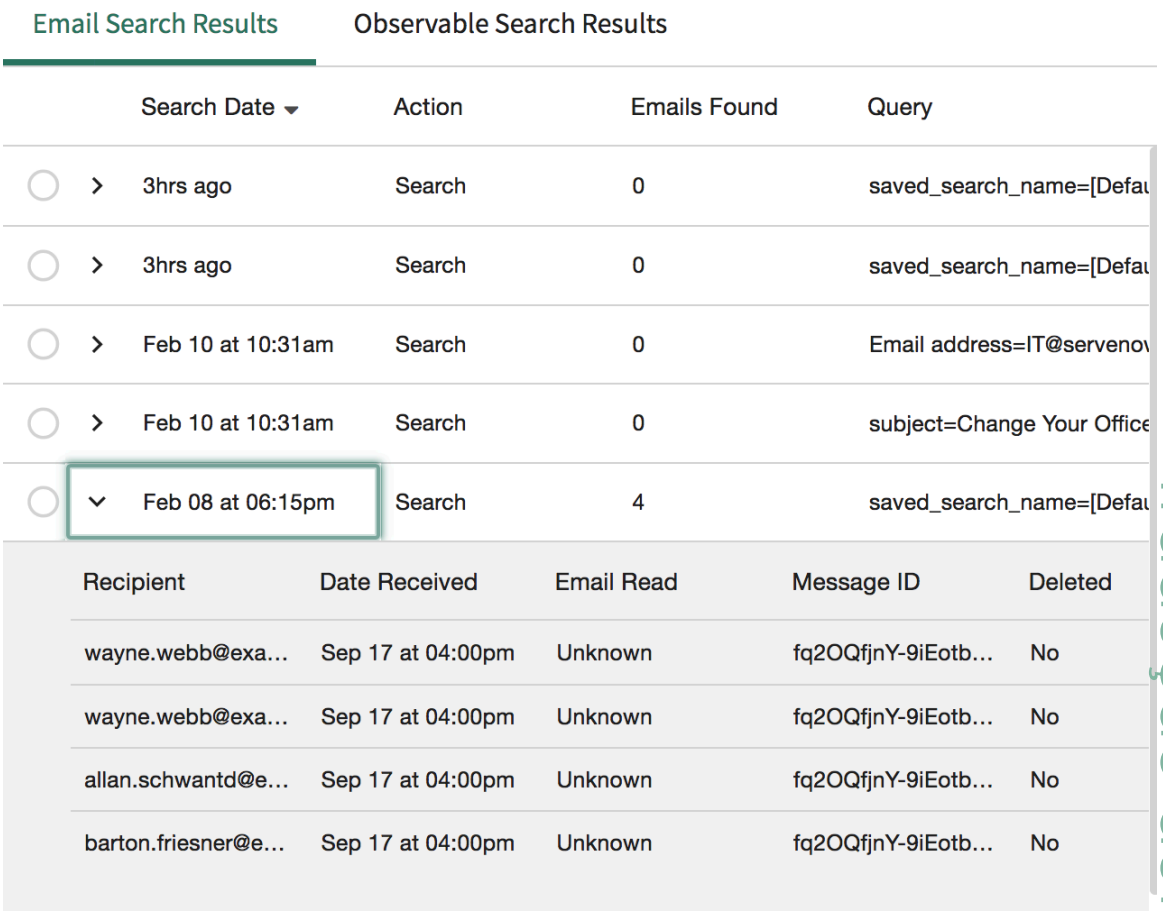
8. Na lista **Selecionar ação**, selecione **Pesquisar** e clique em **Executar**.

   O armazenamento de log do Splunk é pesquisado usando os critérios que você insere e os usuários-alvo do ataque de phishing são mostrados na guia **Resultados da pesquisa de e-mail**. O número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o destinatário e o ID da mensagem, são exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Para exibir a lista de usuários que receberam o e-mail de phishing, clique no símbolo **>** na coluna Data de pesquisa.



10. Para exibir uma lista de usuários que receberam o e-mail, navegue até **Usuários** > **Usuários afetados**.

    A coluna Usuário phishing identifica os destinatários do e-mail.

    Nota: A página Usuários afetados mostra somente os registros de usuário que estão presentes na instância da ServiceNow.

11. Para investigar melhor os usuários que são alvos do ataque de phishing, siga estas etapas:

    a. Marque as caixas de seleção ao lado dos nomes de usuário.

    b. Na lista, selecione **Criar incidente de segurança secundário**e clique em **Executar**. Uma mensagem é exibida para mostrar que um incidente de segurança secundário foi criado. Para exibir os incidentes de segurança secundários associados a um incidente primário, clique na guia **Explorar** e navegue até **Incidentes** > **Incidentes de segurança secundário**.

Resultados
A lista de usuários com phishing é exibida.

Executar uma pesquisa de detecções de observável para ataques de phishing e malware relatados pelo usuário

Execute pesquisas de detecções em observáveis para descobrir quantos usuários visitaram um site mal-intencionado ou suspeito em um período específico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Você pode executar uma pesquisa de tráfego de rede em observáveis, como a URL, o host de destino ou o endereço IP de destino associado a um incidente de segurança.

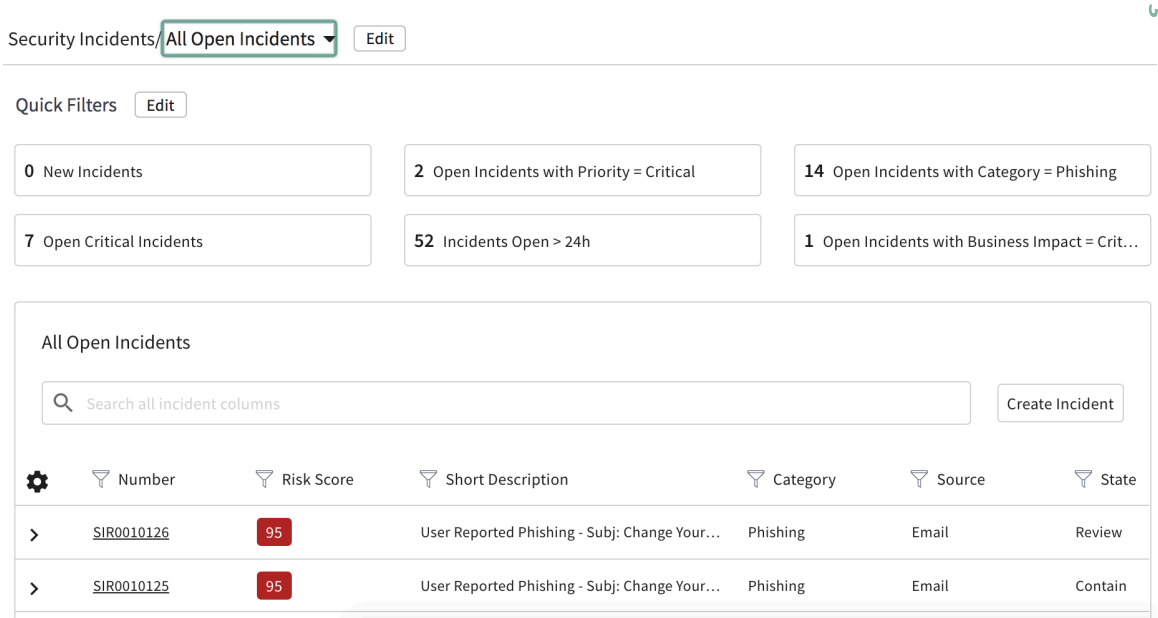
Nota:

- Esta implementação de pesquisa de detecções para observáveis foi testada somente com o armazenamento de log do Splunk Enterprise.
- Os eventos de log do Splunk devem ser compatíveis com o modelo de informações comuns (CIM) para que a consulta de pesquisa de detecções retorne resultados precisos.

Procedimento

1. Para ver os incidentes de segurança atribuídos à sua equipe, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.
2. Na lista **Incidentes de segurança**, selecione um filtro diferente, como todos os **incidentes atribuídos a mim**, **todos os incidentes abertos**ou **todos os incidentes**.

   Para exibir incidentes de segurança de um tipo específico, como incidentes críticos ou e-mails de phishing, clique em um dos **Filtros rápidos**.

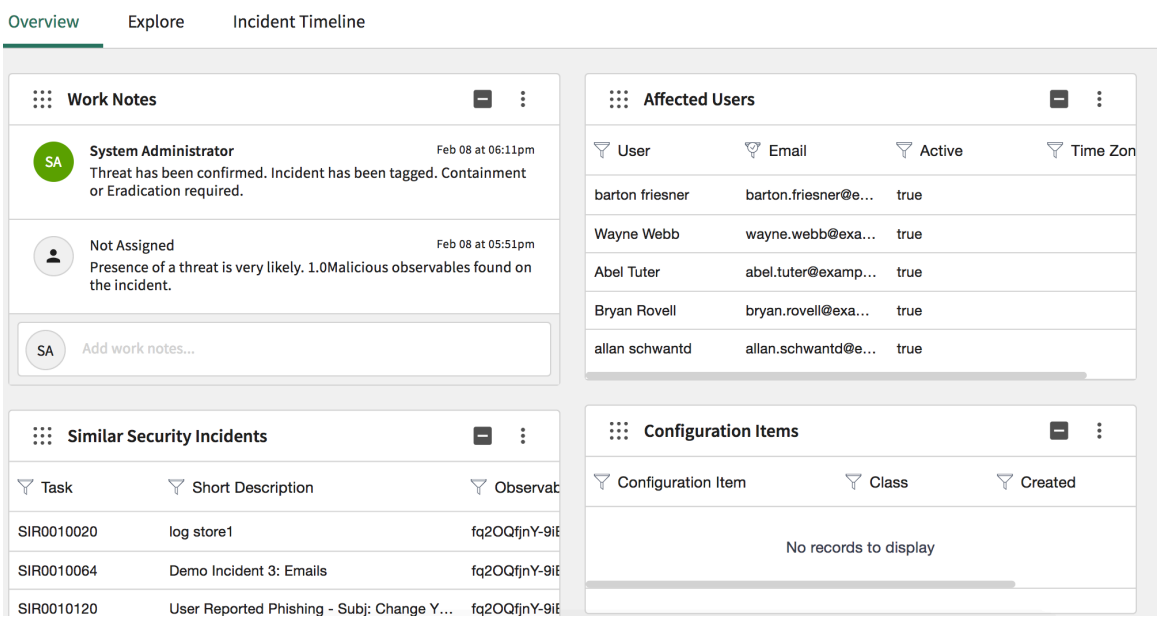


3. Clique no incidente de segurança que você deseja analisar.

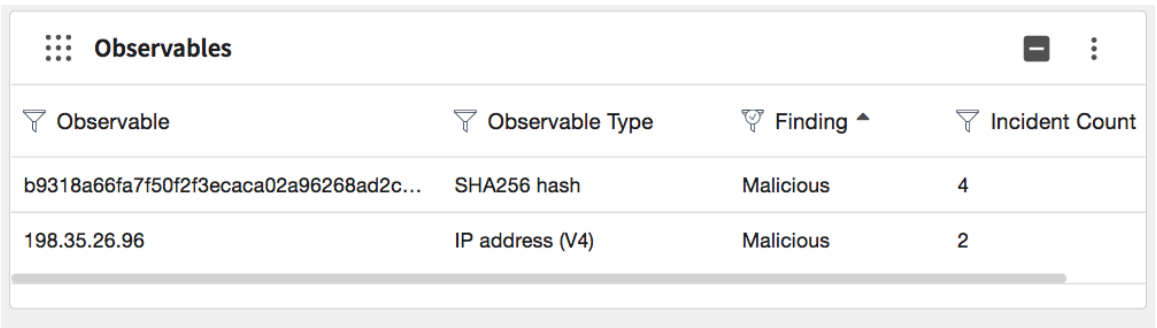
   Você pode ter uma visão geral do incidente de segurança, incluindo uma lista de observáveis, usuários afetados e incidentes de segurança semelhantes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



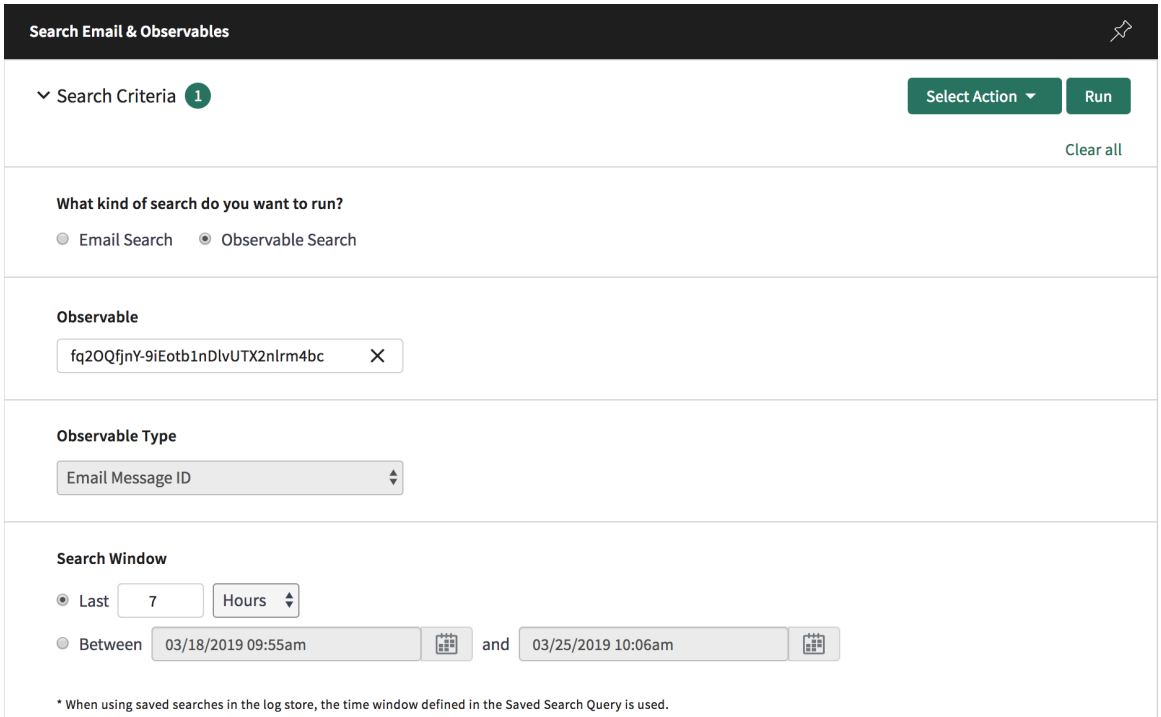
Na seção Observáveis, observe que a coluna Observável mostra o endereço de e-mail, o assunto e a URL. Observe também que a coluna Descoberta mostra que a URL foi verificada automaticamente quando o e-mail de phishing foi enviado e determinado como uma URL mal-intencionada conhecida. A coluna Contagem de incidentes mostra os outros incidentes que compartilham o mesmo observável. Esses artefatos indicam que você provavelmente está pronto para prosseguir para os procedimentos de contenção deste ataque de phishing, incluindo a determinação de quantos usuários na organização foram afetados.



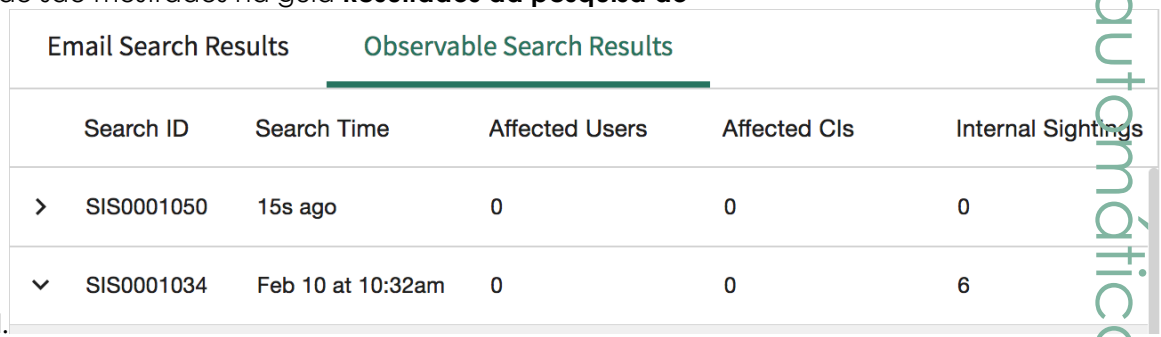
4. Navegar até **Explorar** > **Investigação** > **Pesquisar e-mail e observáveis**.
5. Expanda a seção Critérios de pesquisa e clique em **Pesquisa de observável**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Insira o observável que você está procurando e uma janela de tempo para a pesquisa (por exemplo, Últimas 24 horas).
7. Na lista **Selecionar ação**, selecione **Pesquisar**.
   O armazenamento de log do Splunk é pesquisado usando os critérios que você inseriu e os principais usuários-alvo do ataque mal-intencionado são mostrados na guia **Resultados da pesquisa do observável**.



8. Para exibir os usuários que receberam o e-mail, navegue até **Usuários** > **Usuários afetados**.

   A coluna Usuário phishing identifica os destinatários do e-mail de phishing e a coluna Interação do usuário identifica usuários que clicaram em um URL de phishing ou interagiram com um endereço de e-mail suspeito. A coluna Interação do usuário é definida como verdadeira ou falsa, dependendo se o usuário clicou no link ou no IP mal-intencionado.

   Nota: A página Usuários afetados mostra somente os registros de usuário que estão presentes na instância da ServiceNow.

9. Para investigar melhor os usuários que clicaram no e-mail de phishing e possivelmente comprometeram suas credenciais:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Nas colunas Usuário phishing e Interação do usuário, marque as caixas de seleção ao lado dos nomes de usuário que mostram **verdadeiro**.

b. Clique em **Criar incidente de segurança secundário** e, em seguida, clique em **Executar**. Uma mensagem é exibida para mostrar que um incidente de segurança secundário foi criado. Para exibir os incidentes de segurança secundários associados a um incidente primário, clique na guia **Explorar** e navegue até **Incidentes** > **Incidentes de segurança secundário**.

Resultados
A lista de usuários com phishing é exibida.

Criar registros de configuração de pesquisa de detecções

Crie vários registros de configuração de pesquisa de detecções e use-os ao consultar vários armazenamentos de log ou variar os parâmetros de pesquisa.

Antes de Iniciar
Função necessária: sn_si.admin

- O complemento CIM deve ser instalado na instância do Splunk.
- Pesquisas salvas e consultas no local são compatíveis somente com a integração do Splunk.

Por Que e Quando Desempenhar Esta Tarefa
Você também pode criar registros de configuração de pesquisa de detecções para invocar pesquisas salvas no armazenamento de log do Splunk Enterprise.

Nota: As consultas de configuração de pesquisa dependem dos dados de log do Splunk para serem compatíveis com o Splunk Common Information Model (CIM).

Com as configurações de pesquisa salvas, você pode:

- Crie pesquisas personalizadas que combinem vários registros de eventos.
- Pesquisas eficazes e com design eficiente.
- Use entradas com parâmetros na pesquisa salva do Splunk.

O sistema de base inclui as configurações de exemplo, conforme mostrado nesta imagem:

Configurações de pesquisa salvas

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

A pesquisa salva e as consultas de configuração no local são consultas de exemplo e podem ser substituídas por parâmetros apropriados para o seu ambiente. Crie configurações adicionais de pesquisa salva conforme necessário. Quando você define uma configuração de pesquisa salva, o nome e os parâmetros na consulta de pesquisa devem corresponder à configuração salva definida em sua instância do Splunk. Se o nome e os

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

parâmetros não forem os mesmos, talvez você não veja resultados precisos ao executar uma pesquisa de detecções.

Nota: Em sua instância do Splunk, navegue até a página Pesquisas, relatórios e alertas e localize sua consulta de pesquisa salva. Clique no link **Permissões** para navegar até a página Permissões. Selecione o botão de opção **Todos os aplicativos** e habilite a opção **Permissão de leitura** para **Todos**. Isso mudará o valor da coluna Compartilhamento de Privado para App para sua consulta de pesquisa salva. Se não estiver definido, a consulta de pesquisa salva poderá não retornar resultados.

Para verificar se a configuração de pesquisa salva corresponde à configuração definida na sua instância do Splunk:

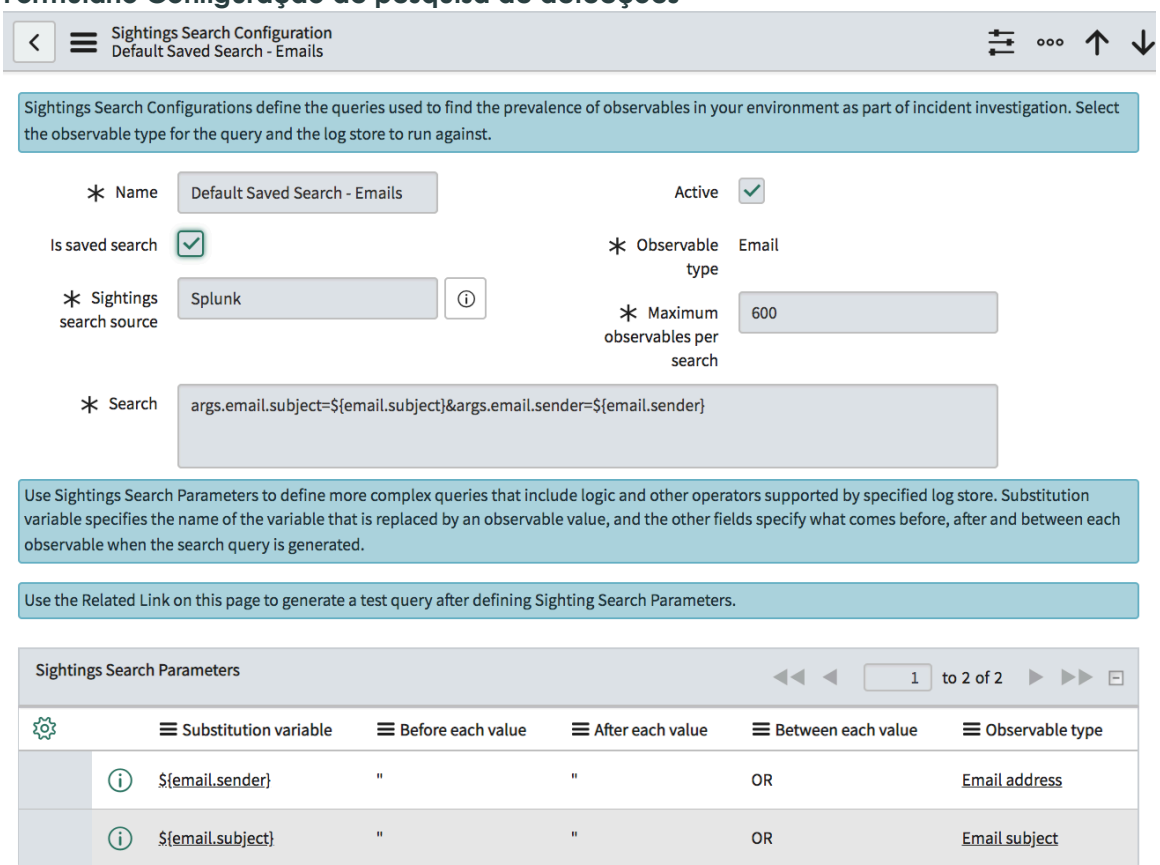
1. Navegar até **Configurações** > **Pesquisas, relatórios e alertas**.
2. Mude o **contexto da aplicação** para **Todos**.

   Uma lista de relatórios de pesquisa é exibida.

3. Confirme se a consulta de pesquisa salva está presente na lista.

Por exemplo, o formulário Configuração de pesquisa de detecções contém o endereço de e-mail e o remetente do e-mail como parâmetros de pesquisa:

Formulário Configuração de pesquisa de detecções



Na instância do Splunk, defina a pesquisa salva com o mesmo nome, Pesquisa salva padrão - e-mails e os mesmos parâmetros de pesquisa para o endereço de e-mail e o assunto do e-mail. Se o nome e os parâmetros de pesquisa não forem os mesmos, a pesquisa de detecções não gerará resultados precisos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Operações de segurança** > **Integrações** > **Configuração da Pesquisa de detecções** e crie um novo registro (consulte a tabela para obter as descrições dos campos).

Formulário Configuração de pesquisa de detecções

Campo	Descrição
Nome	Nome da configuração.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem da pesquisa de detecções	A origem da pesquisa de detecções. Selecione o armazenamento de log do Splunk como a origem.
Ativo	Opção para o status de pesquisa salva. Somente configurações de pesquisa ativa podem ser usadas para executar uma pesquisa de detecções.
Tipo de observável	O tipo de observável pode ser qualquer tipo de observável, como IP, valor de hash, URL, nome de domínio e assim por diante.
Máximo de observáveis por pesquisa	Número máximo de observáveis a serem retornados da pesquisa.
Pesquisar	A cadeia de caracteres de pesquisa padrão é `$(observable)`, mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com o armazenamento de log do Splunk.

2. Clique em **Enviar**.

Resultados
Você criou um registro de configuração de pesquisa de detecções.

O que Fazer Depois
Depois de definir a consulta de pesquisa, clique em **Gerar consulta de teste de pesquisa de detecções**e especifique uma lista de valores observáveis para gerar uma consulta de teste com base nesta configuração de pesquisa salva.

Recursos do playbook

O Security Incident Response fornece um conjunto avançado de recursos de playbook que inclui uma biblioteca abrangente de playbooks, subfluxos e ações. Você pode criar ou configurar playbooks de forma rápida e fácil sem escrever códigos complicados. Você pode usar esses playbooks para resolver ameaças à segurança passo a passo.

Os recursos do playbook incluem o seguinte:

Security Incident Response playbooks	Ações do playbook do Security Incident Response
Os playbooks fornecidos com o sistema de base foram projetados para acelerar	Ações complexas que são críticas para a criação de playbooks estão disponíveis

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Incident Response playbooks	Ações do playbook do Security Incident Response
o processo de investigação de incidentes de segurança, automatizando tarefas complexas e mundanas. Os playbooks são altamente configuráveis e criados usando a tecnologia Flow Designer da ServiceNow. Para configurar, copie o playbook fornecido com o sistema de base e modifique-o usando a interface gráfica simples de arrastar e soltar. Consulte Security Incident Response playbooks.	como **Bibliotecas de Ação**. Essas bibliotecas de ação permitem que os administradores de segurança criem playbooks sem escrever nenhum código complicado. Consulte Ações do playbook do Security Incident Response.

Ativar um fluxo Security Incident Response

Os administradores de segurança e os designers de fluxo podem usar os fluxos Security Incident Response para automatizar o processo de resolução de incidentes de segurança na organização.

Antes de Iniciar

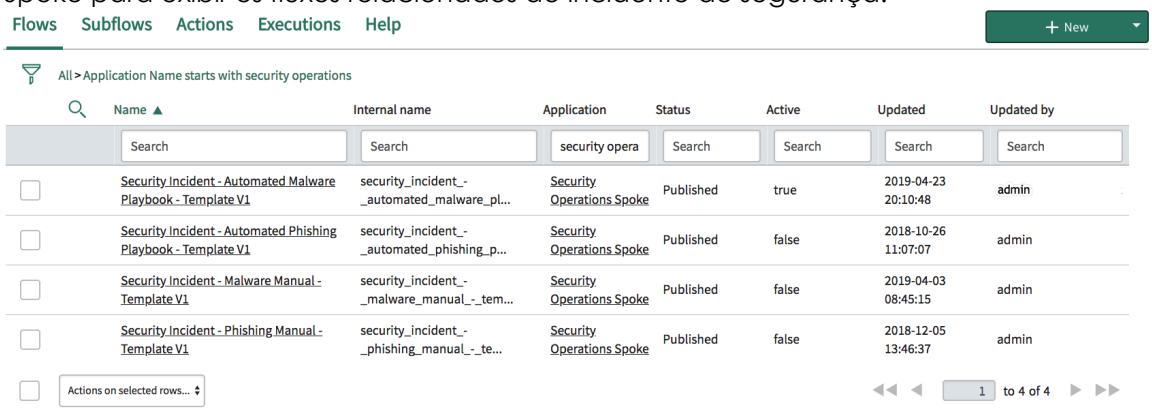
Função necessária: sn_si.admin, action_designer e flow_designer

Por Que e Quando Desempenhar Esta Tarefa

Os fluxos fornecidos com o sistema de base estão em um estado inativo. Ative esses fluxos antes de usá-los.

Procedimento

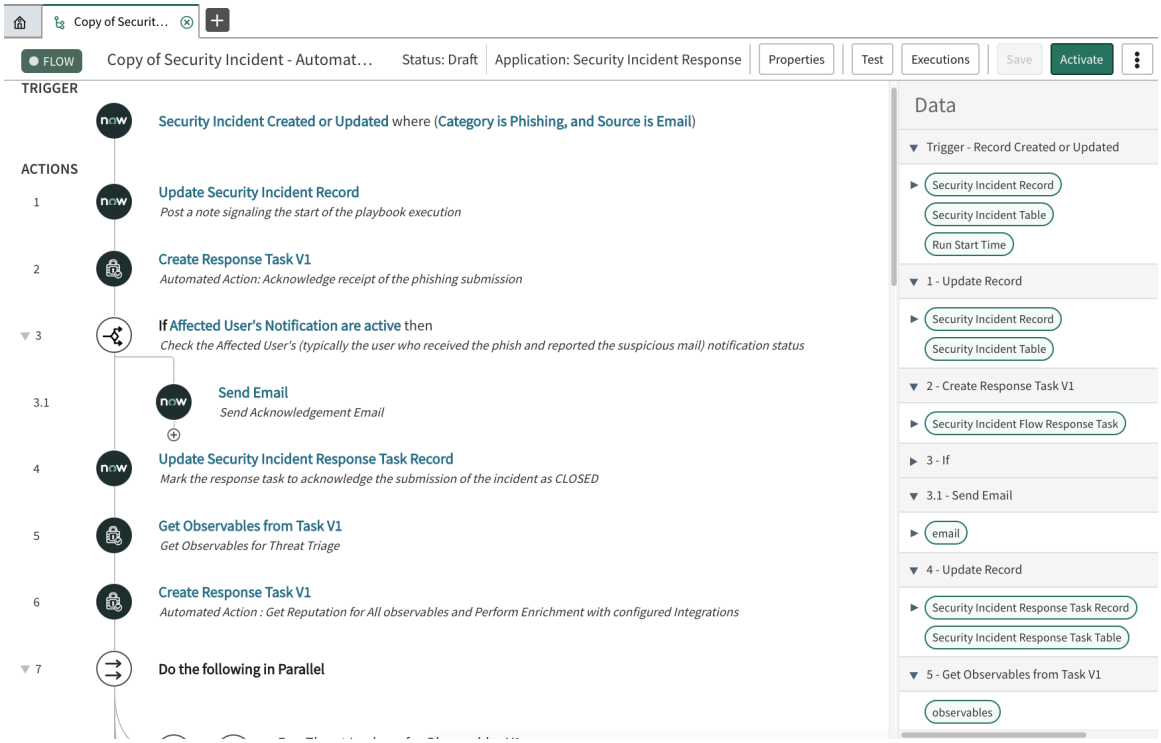
1. Baixe e instale a aplicação Operações de segurança Spoke.
   Esta aplicação Spoke fornece ações de operações de segurança que você pode usar ao definir Security Incident Response fluxos.
2. Navegar até **Flow Designer** > **Designer** e pesquise a aplicação Operações de segurança Spoke para exibir os fluxos relacionados ao incidente de segurança.



   Observe que os fluxos têm um status publicado e estão inativos.
3. Por exemplo, se você quiser ativar o fluxo do Automated Malware Playbook, clique no link **Incidente de segurança - Automated Phishing Playbook - Template V1** para exibir o fluxo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você não pode editar os fluxos fornecidos com o sistema de base, pois são fluxos somente leitura. Você pode usar esses fluxos como estão ou fazer uma cópia e modificá-los conforme necessário.

4. Clique em **Ativar** para ativar o fluxo.

Resultados

O fluxo do Automated Phishing Playbook está ativo e pronto para uso.

Security Incident Response playbooks

Você pode invocar o fluxo do playbook de incidente de segurança automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook funciona somente para os processos criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados do Flow Designer existentes, ele continuará a funcionar e as atividades continuarão a ser renderizadas como tarefas de resposta.

Security Incident Response O é compatível com dois tipos de Playbooks:

- Playbooks baseados em processo
- Playbooks baseados em fluxo

Além dos playbooks listados, também há subfluxos no Spoke das Operações de segurança que podem ser chamados a partir do playbook de fluxos. O ransomware é um desses subfluxos.

Ative esses fluxos antes de usá-los. Para obter mais informações, consulte Como ativar um fluxo do Security Incident Response.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbooks baseados em processo

O componente do playbook funciona somente para playbooks criados em Workflow Studio e não para fluxos. No entanto, os playbooks baseados em fluxo existentes continuarão a funcionar e as atividades continuarão a ser renderizadas como tarefas de resposta.

Security Incident Response fornece os seguintes playbooks com o sistema de base.

Playbook para phishing manual

O Playbook de phishing manual fornece orientação passo a passo para seus analistas sobre como eles podem resolver manualmente tipos específicos de ameaças à segurança em suas atividades de phishing.

Visão geral

O modelo de Playbook de phishing manual foi projetado para executar as tarefas de resposta de phishing manualmente e inclui uma sequência de ações que inclui condições de gatilho. Você pode usar os modelos de PAD para executar as etapas no playbook de resposta a phishing e resolver esses incidentes com eficiência.

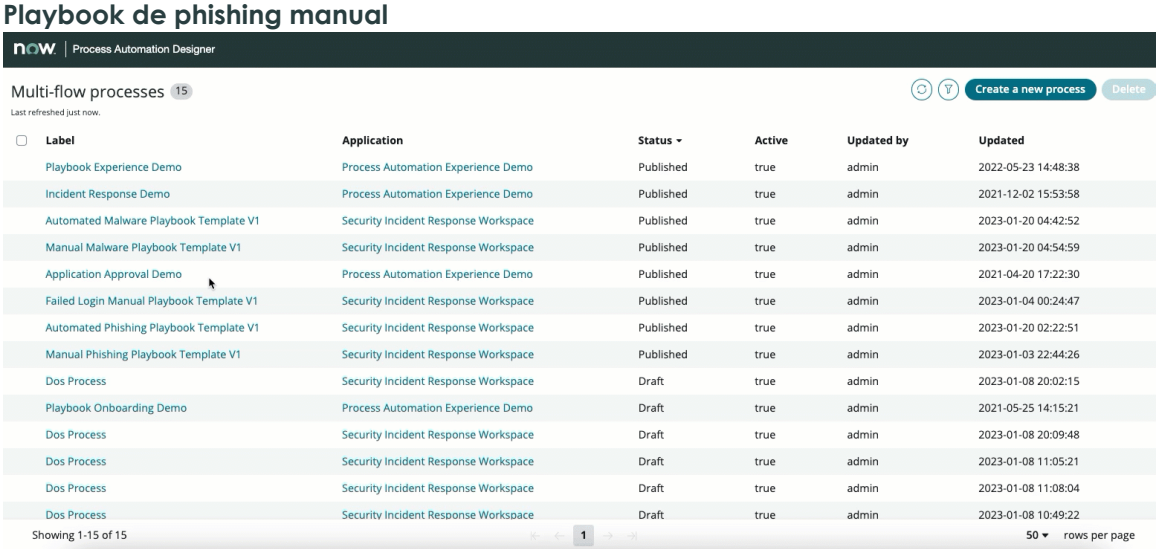
Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o Playbook de phishing manual no Designer de automação de processos (PAD) e executar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Playbook de phishing manual



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

conclui tarefas e fases. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar playbooks para phishing manual no Workflow Studio

Use estas etapas para criar playbooks para phishing manual em Workflow Studio.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

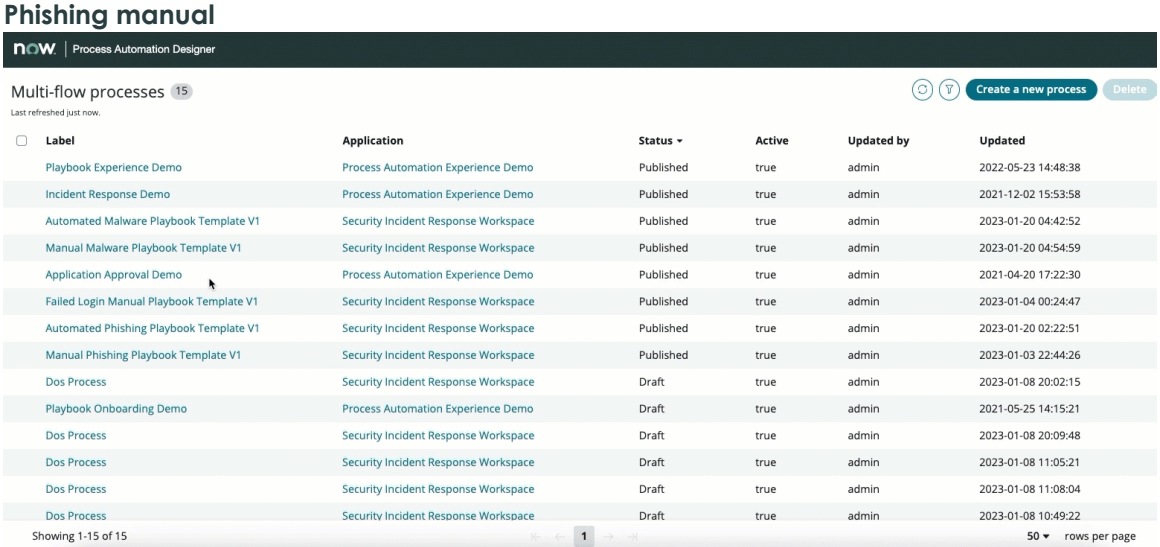
Procedimento

1. Clicar **Todos** > **Designer de automação de processos** > > **Novo** e selecione **Playbook**.

   Por exemplo, Modelo de playbook de phishing manual V1.

2. Insira um nome para o playbook, a descrição e a aplicação para a qual o playbook está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o playbook deve ser executado.
5. Clique **em Definir suas condições de gatilho**.
6. Escolha as condições para definir quando o playbook deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Phishing manual



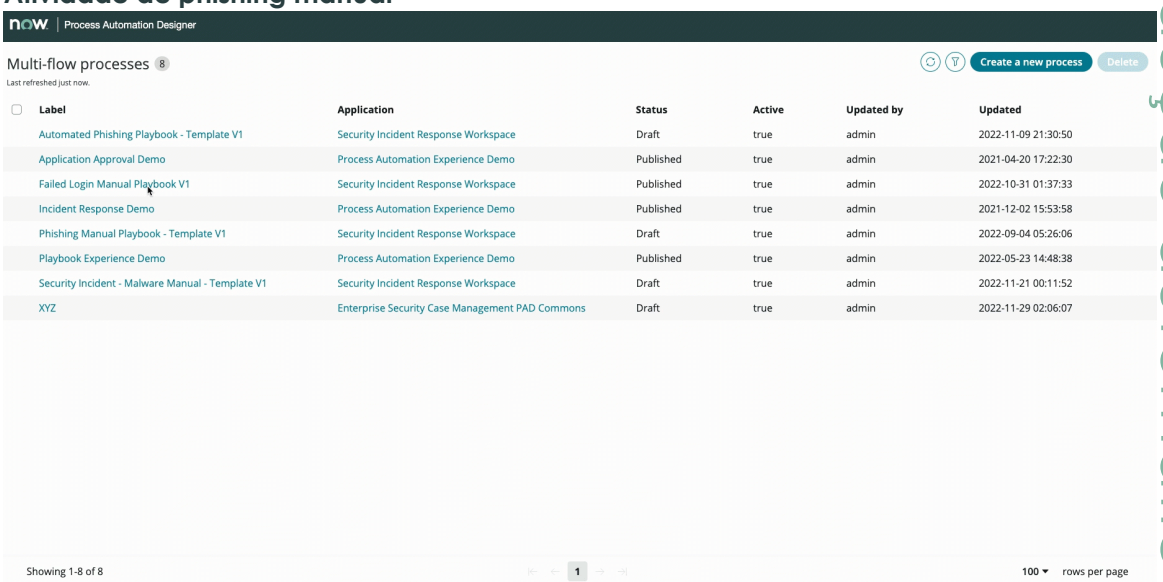
7. Clique **em Ir para Designer**.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova fase**.
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a fase seria executada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Clique **em Salvar e fechar**.
11. Para adicionar outra fase, clique em **Adicionar outra fase**.
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Eliminar e Revisar, respectivamente. No exemplo a seguir, a fase **Análise** começa imediatamente e não tem condição de execução. A fase de**contenção** começa após a conclusão da fase anterior e tem uma condição de execução que se baseia no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique em **Adicionar outra atividade** em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de maneira semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Atividade de phishing manual



14. No painel de propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Adicionar atividades paralelas

Se o campo **Quando iniciar** estiver definido como **Com o anterior**, as atividades paralelas poderão ser iniciadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para passar de uma fase para a próxima

Se nenhuma condição de execução for definida, as fases e atividades serão executadas sequencialmente.

Você pode usar a condição de execução para ignorar atividades ou fases. Neste exemplo, **a fase Conter começa quando o resultado de "O e-mail tem indicadores de ameaça?" é Sim**.

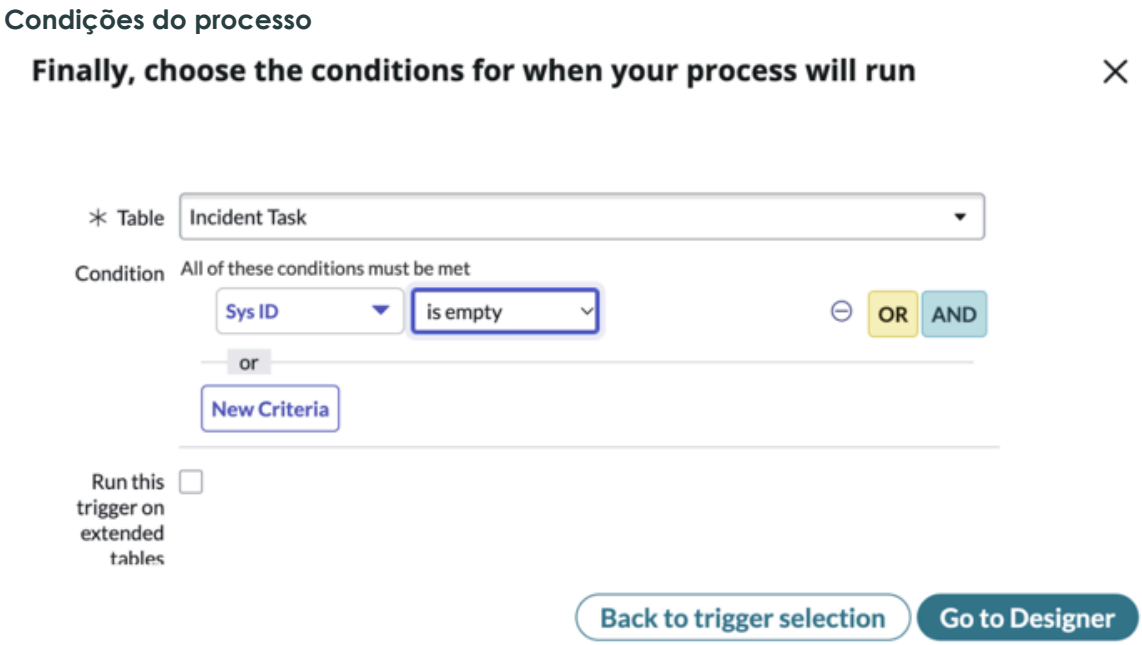
Para passar de uma fase para outra, você pode usar a **definição de atividade fornecida pela plataforma - Atualizar registro**. Isso atualizará o campo de estado do incidente de segurança e retomará a execução do playbook para a próxima fase.

No entanto, o desafio com esta definição de atividade é que, se dizer que o playbook está na fase de análise e se o usuário tiver atualizado manualmente o estado para dizer revisão, a atividade Atualizar registro mudará novamente o estado para Conter para continuar o playbook execução. Isso substituirá a mudança manual feita.

Para superar isso, no sistema de base, é fornecida uma definição de atividade chamada **Atualizar estado da tarefa**. Esta atividade não substituirá o estado do incidente de segurança se o estado atual do estado da segurança estiver à frente da fase no playbook.

Criar uma definição de processo com condição de gatilho fictícia

Uma definição de processo sempre requer uma condição de gatilho. Mas, se você não tiver certeza de quando o processo deve ser acionado, ainda poderá criar uma definição de processo com uma condição de gatilho fictícia. Defina a condição do gatilho como **sys_id está vazio**. Esta condição nunca será atendida.



Tradução automática

Como usar o playbook de phishing manual

Use estas etapas para saber como você pode usar o playbook de phishing manual no espaço do analista SIR e suas capacidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

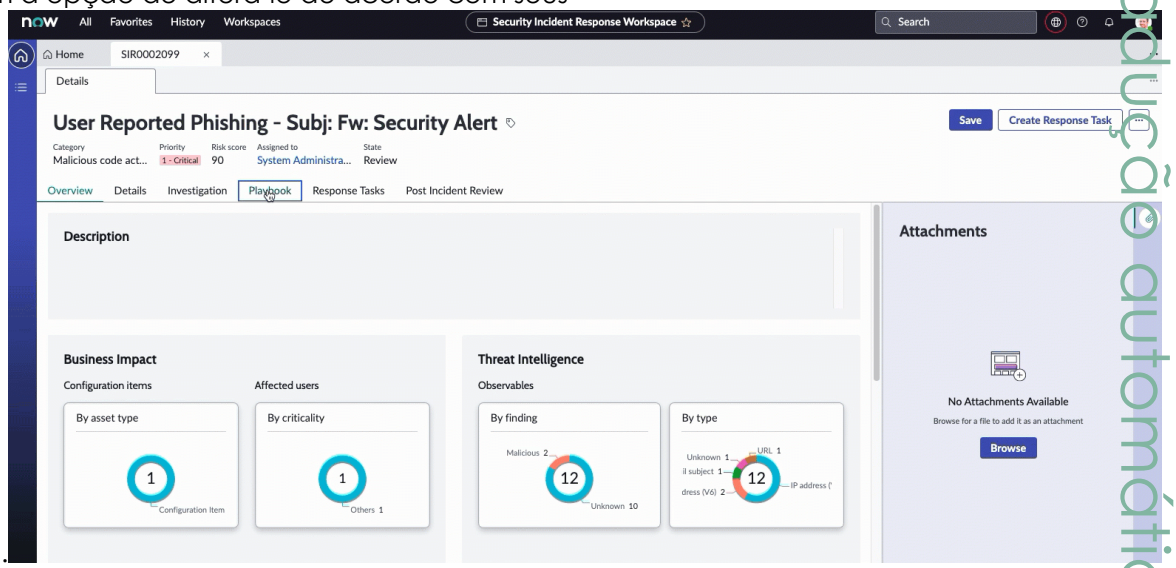
Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

   Nota: Se você não vir nenhum playbook listado, precisará acessar o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook de phishing manual**.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise. Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Eliminar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Resumo do playbook do espaço

A seguir está descrito o resumo do processo.

- Entenda o playbook baseado em fluxo legado.
- Liste as possíveis atividades e fases depois de analisar o fluxo. Procure as etapas em que a Orquestração verdadeira pode ser criada.
- Faça cada atividade e verifique se a definição de atividade fornecida pelo sistema de base pode atender ao caso de uso ou não.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Listar casos de uso de atividade que precisam de novas definições de atividade para serem implementados. Classifique-os como interativos, não interativos ou automatizados. Para criar uma definição de atividade:
  - Crie um subfluxo ou uma ação para o caso de uso.
  - Decida se os dados associados devem ser capturados na tabela de dados de fluxo ou em uma tabela personalizada.
  - Se estiver usando a tabela de dados de fluxo, crie a definição de dados de fluxo em **sys_flow_data_definition**. Ao criar um registro de dados de fluxo no subfluxo, selecione a definição de dados de fluxo criada.
  - Crie uma **definição de atividade**.
  - Mapeie o plano de automação.
  - Preencha as propriedades de **experiência de atividade**.
  - Crie uma ação em Ações do Playbook. Deve haver uma ação de atividade existente para atribuí-la à definição de atividade.
  - Para substituir a experiência do cartão padrão com base no tipo de experiência selecionado, adicione a substituição do playbook usando o conceito de IU de atividade.
- Algumas atividades podem ser feitas para lidar com automáticas e interativas usando o sinalizador aguardar entrada do usuário no subfluxo. Esta entrada pode ser passada ao configurar a atividade na definição do processo.
- Depois de ter todas as definições de atividade necessárias para o processo, comece a criar a definição de processo usando Workflow Studio.

Playbook for Automated Phishing

O playbook de phishing automatizado fornece orientação passo a passo para seus analistas sobre como eles podem resolver tipos específicos de ameaças à segurança em suas atividades de phishing automatizado.

Visão geral

O modelo de playbook de phishing automatizado foi projetado para automatizar as tarefas de resposta de phishing e contém uma sequência de ações que inclui condições de gatilho. Você pode usar os modelos de playbook em Workflow Studio para automatizar as etapas no playbook de resposta de phishing e resolver esses incidentes com eficiência. Este modelo de playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que você pode anotar.

Neste playbook, não haverá interação do usuário quando a categoria de um incidente de segurança estiver definida como phishing. Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o Automated Phishing Playbook em Workflow Studio, e este playbook executa automaticamente todas as tarefas, como análise, contenção, erradicação e revisão.

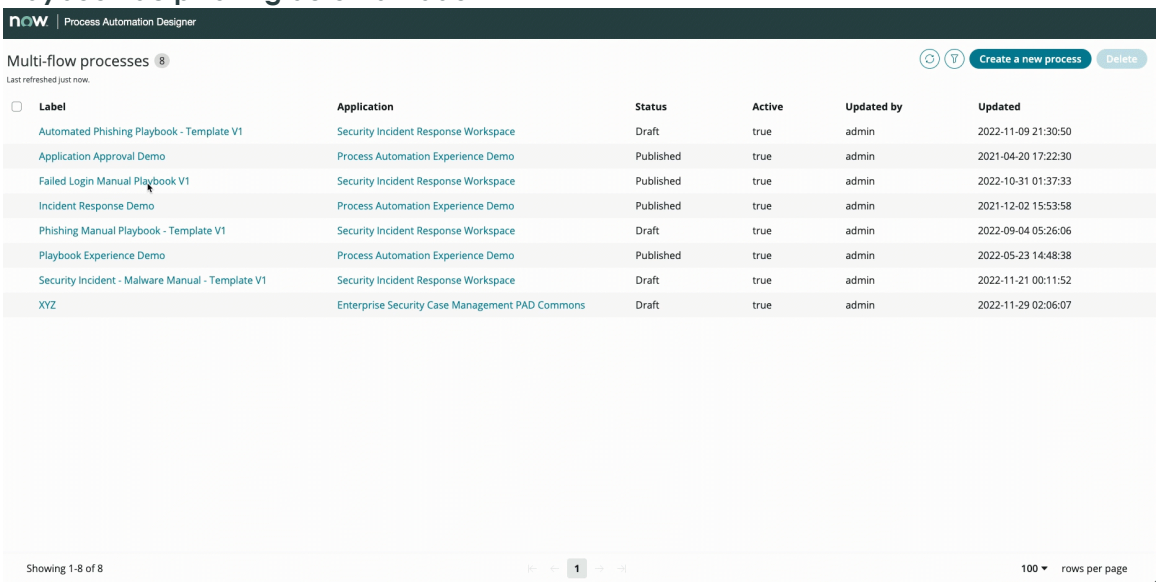
A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

- Análise
- Contém
- Erradicar
- Revisão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada fase tem atividades dentro dela.

Playbook de phishing automatizado



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você conclui tarefas e fases. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para phishing automatizado no PAD

Use estas etapas para criar processos de phishing automatizado no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

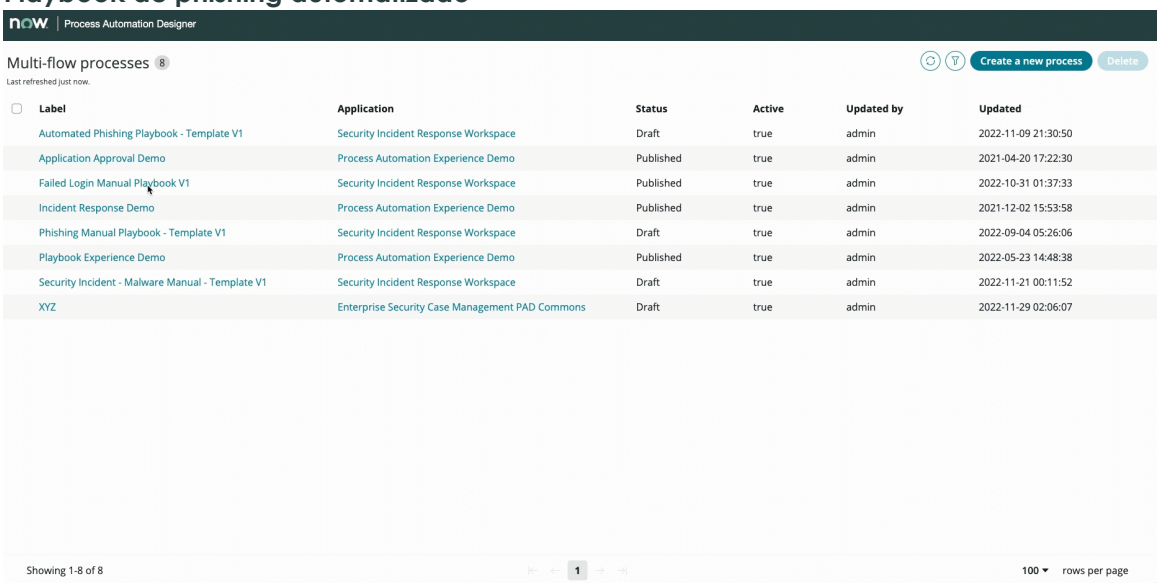
   Por exemplo, Automated Phishing Playbook Template V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir suas condições de gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

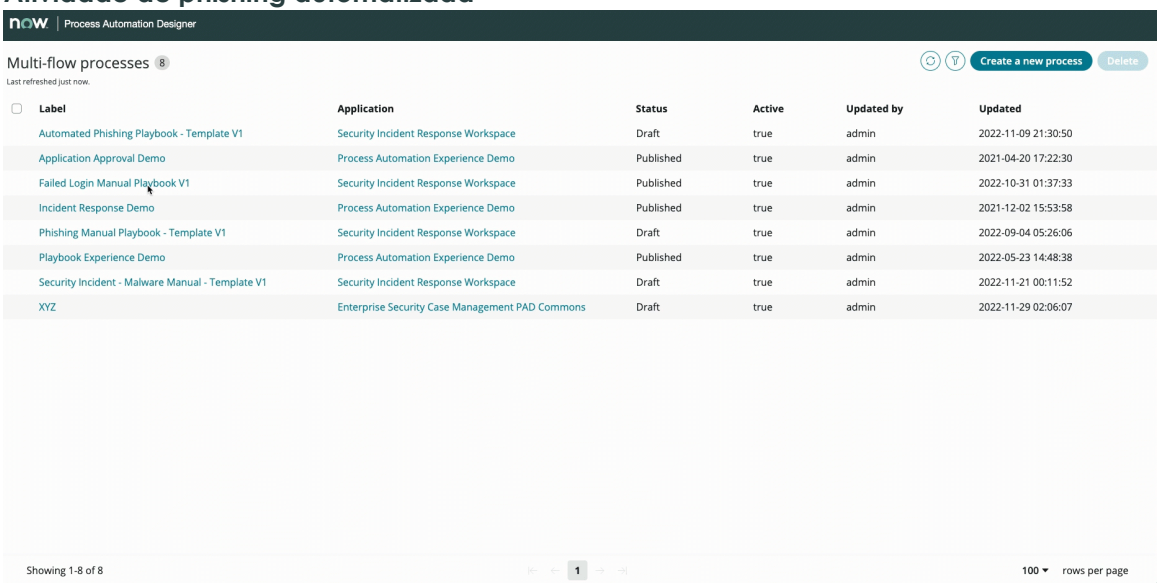
Playbook de phishing automatizado



7. Clique **em Ir para Designer**.
   A página do Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova fase**.
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a fase seria executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra fase, clique em **Adicionar outra fase**.
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Eliminar e Revisar, respectivamente. No exemplo a seguir, a fase **Análise** começa imediatamente e não tem condição de execução. A fase de**contenção** começa após a conclusão da fase anterior e tem uma condição de execução que se baseia no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique na **atividade Adicionar outro processo** em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de maneira semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de phishing automatizada



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook de phishing automatizado

Use estas etapas para saber como você pode usar o playbook de phishing automatizado no Espaço do analista de SIR e suas capacidades.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

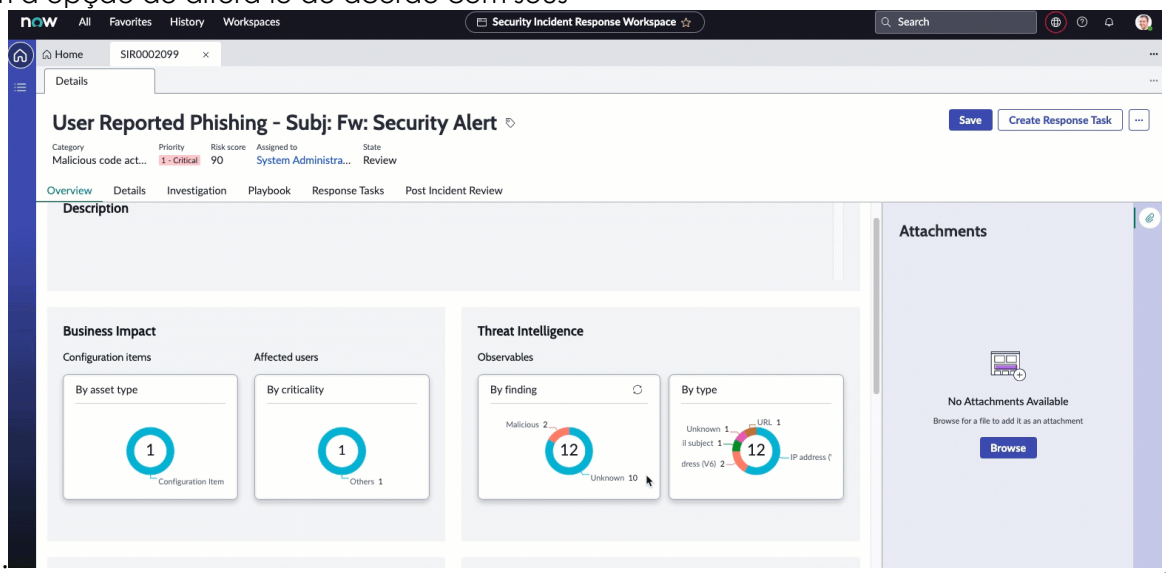
   Nota: Se você não vir nenhum playbook listado, precisará acessar o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook de phishing automatizado**.
   Para phishing automatizado, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Eliminar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para malware manual

O manual de malware manual fornece orientação passo a passo sobre como os analistas podem resolver manualmente alertas de malware com mais eficiência.

O modelo de playbook manual de malware foi projetado para executar manualmente as etapas envolvidas no processamento de alertas de malware do endpoint ou da rede. Você pode usar os modelos de playbook em Workflow Studio para executar as etapas no playbook de malware manual e resolver esses alertas com eficiência. Este playbook inclui condições de gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de malware. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se o malware for criado ou atualizado. Você precisa ativar o Playbook manual de malware em Workflow Studio e criar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as fases da definição do processo e correspondem ao estado de alerta de malware:

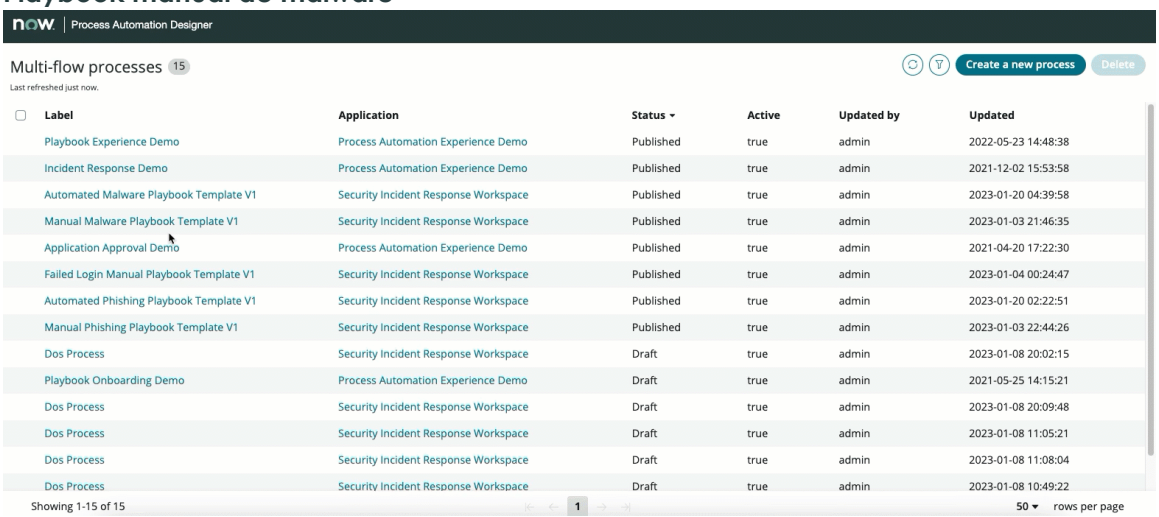
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual de malware



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você conclui tarefas e fases. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para malware manual no PAD

Use estas etapas para criar processos para malware manual no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

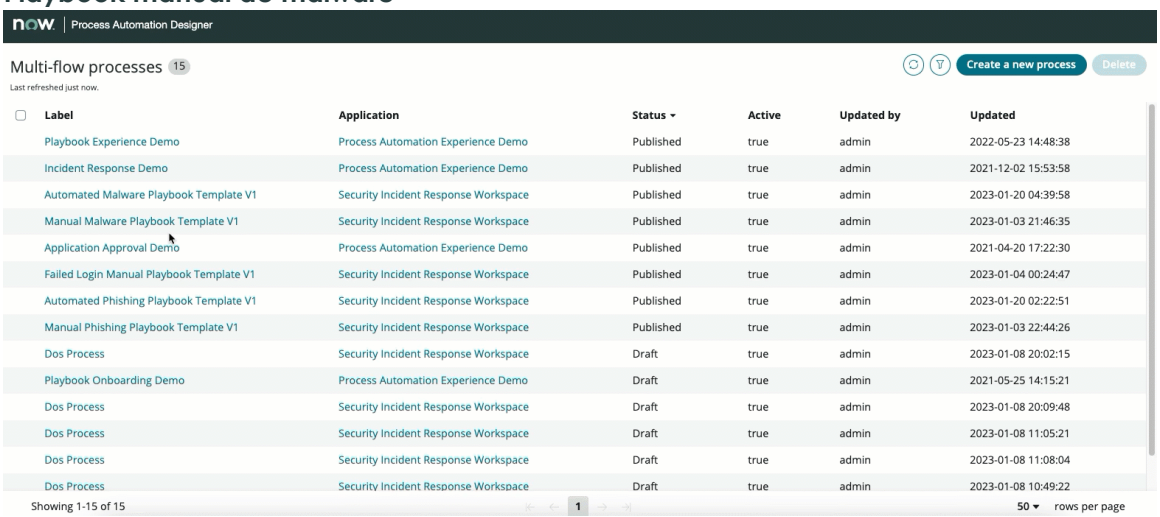
   Por exemplo, Modelo de playbook manual de malware V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir suas condições de gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual de malware

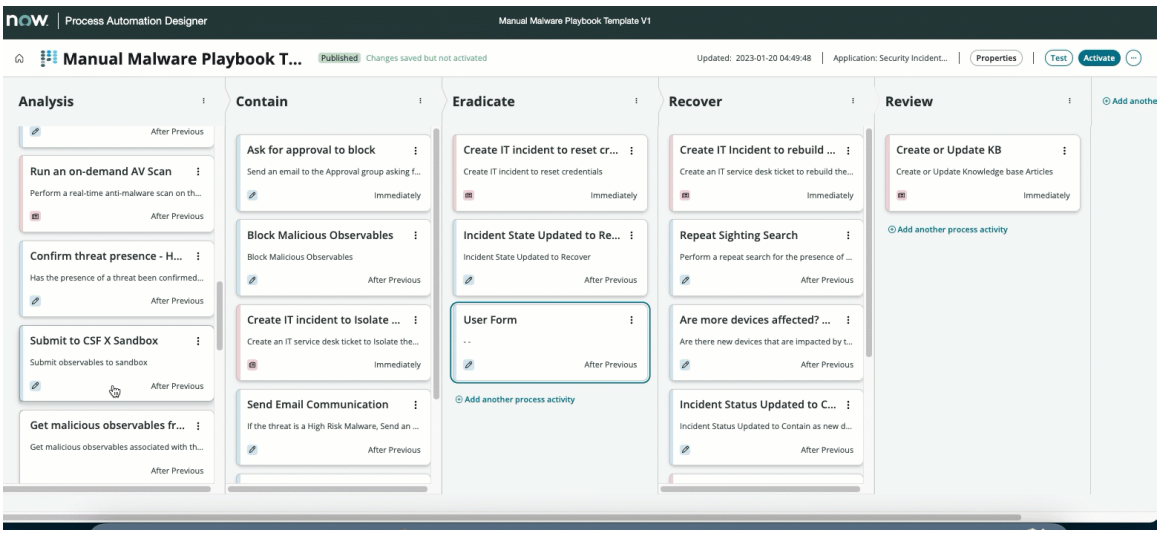


7. Clique **em Ir para Designer**.
   A página do Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova fase**.
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a fase seria executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra fase, clique em **Adicionar outra fase**.
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Eliminar e Revisar, respectivamente. No exemplo a seguir, a fase **Análise** começa imediatamente e não tem condição de execução. A fase de**contenção** começa após a conclusão da fase anterior e tem uma condição de execução que se baseia no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique na **atividade Adicionar outro processo** em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de maneira semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade manual de malware



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook manual de malware

Use estas etapas para saber como você pode usar o playbook de malware manual no espaço do analista SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

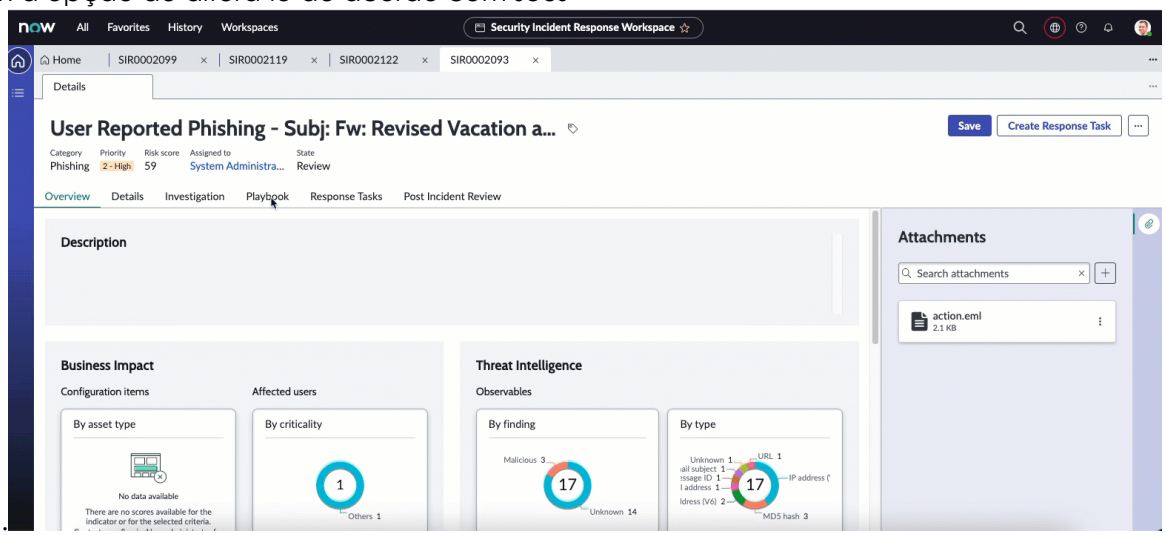
   Nota: Se você não vir nenhum playbook listado, precisará acessar o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook de malware manual**.
   Para malware manual, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Eliminar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para malware automatizado

O playbook de malware automatizado fornece uma sequência de etapas automatizadas que ajudam os analistas a resolver alertas de malware com mais eficiência.

O modelo de playbook de malware automatizado foi projetado para automatizar as etapas envolvidas no processamento de alertas de malware do endpoint ou da rede. Você pode usar os modelos de playbook em Workflow Studio para automatizar as etapas no playbook de malware automatizado e resolver esses alertas com eficiência. Este playbook inclui condições de gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de malware. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o playbook Automated Malware em Workflow Studio, e esse playbook executa automaticamente todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

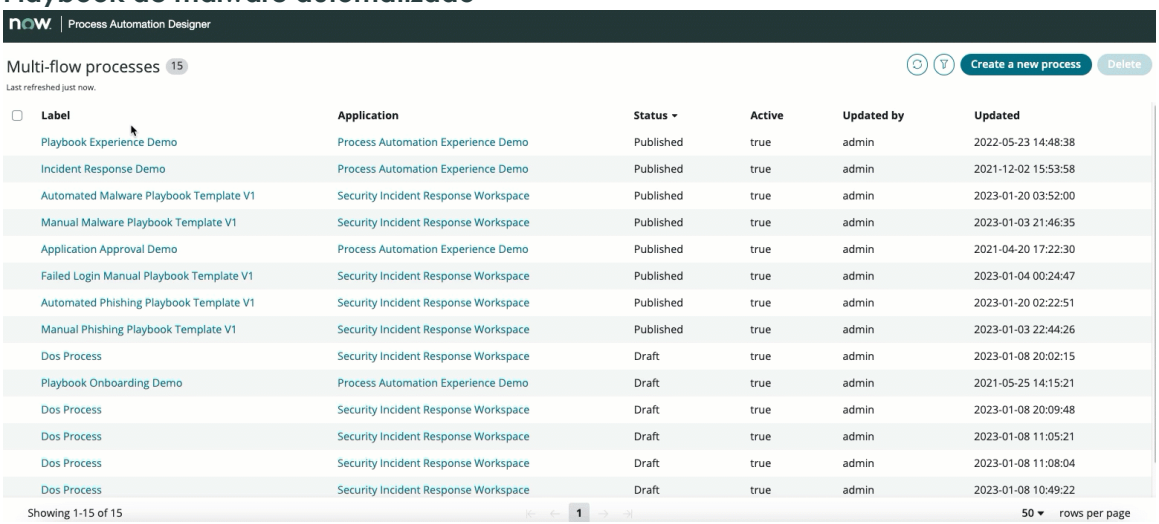
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de malware automatizado



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você conclui tarefas e fases. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos de malware automatizado no PAD

Use estas etapas para criar processos para malware automatizado no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

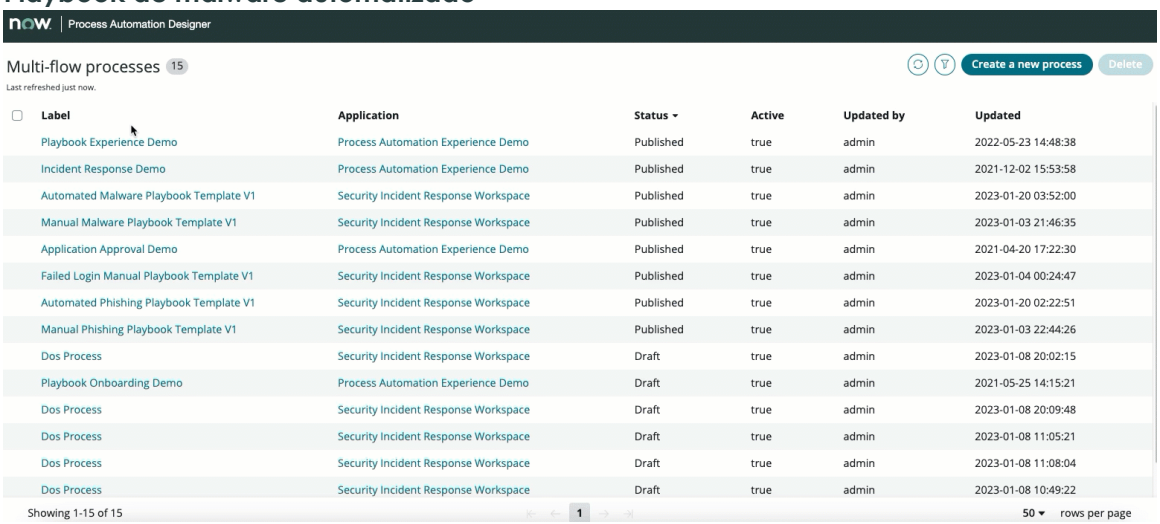
   Por exemplo, Automated Malware Playbook Template V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir suas condições de gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de malware automatizado

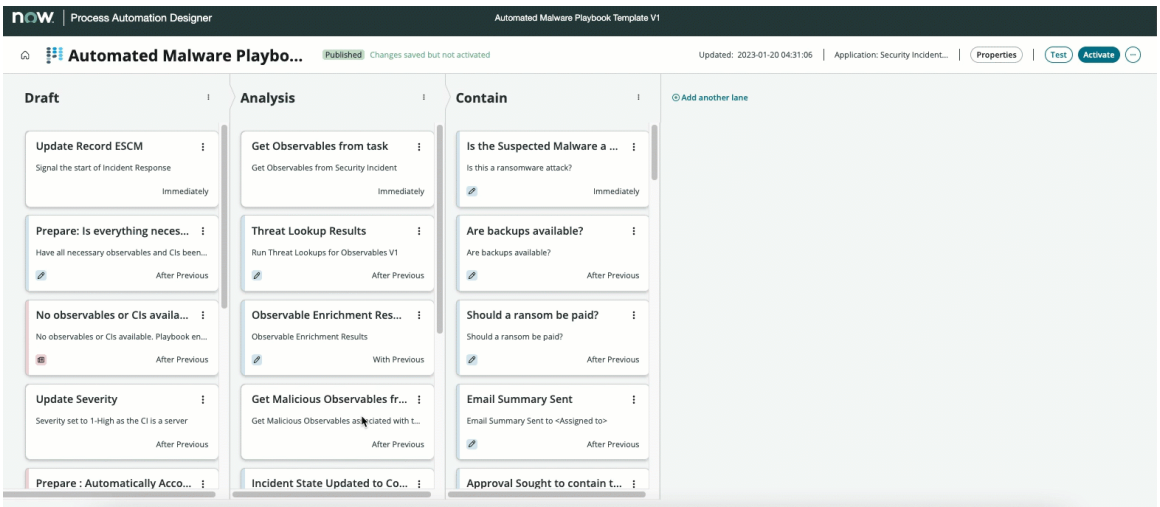


7. Clique **em Ir para Designer**.
   A página do Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova fase**.
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a fase seria executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra fase, clique em **Adicionar outra fase**.
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Eliminar e Revisar, respectivamente. No exemplo a seguir, a fase **Análise** começa imediatamente e não tem condição de execução. A fase de**contenção** começa após a conclusão da fase anterior e tem uma condição de execução que se baseia no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique na **atividade Adicionar outro processo** em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de maneira semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade automatizada de malware



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook de malware automatizado

Use estas etapas para saber como você pode usar o playbook de Malware automatizado no Espaço do analista SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

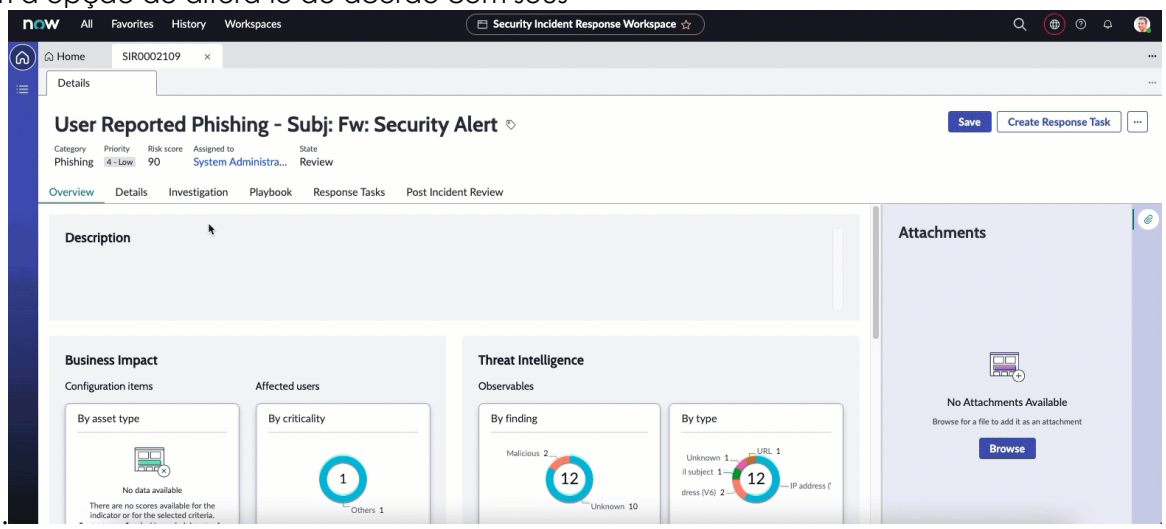
   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

   Nota: Se você não vir nenhum playbook listado, precisará acessar o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Automated Malware Playbook**.
   Para malware automatizado, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Eliminar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de modificá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para login manual com falha

O playbook de login manual com falha fornece orientação e ajuda a otimizar a investigação de incidentes de segurança de login com falha.

Quando um usuário faz determinadas tentativas de login malsucedidas (de acordo com a configuração do SIM), um incidente de segurança é criado. Essas tentativas de login malsucedidas podem ser falso-positivos ou tentativas feitas por invasores de obter acesso às contas de e-mail do usuário.

Você pode usar os modelos de playbook em Workflow Studio para executar as etapas no playbook de login com falha e resolver incidentes de segurança de login com falha com eficiência. Este playbook inclui condições de gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a incidentes de segurança de login com falha. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se um incidente de segurança de login com falha for criado ou atualizado. Você precisa ativar o Playbook manual de login com falha em Workflow Studio e criar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as fases da definição do processo e correspondem ao estado do incidente de segurança:

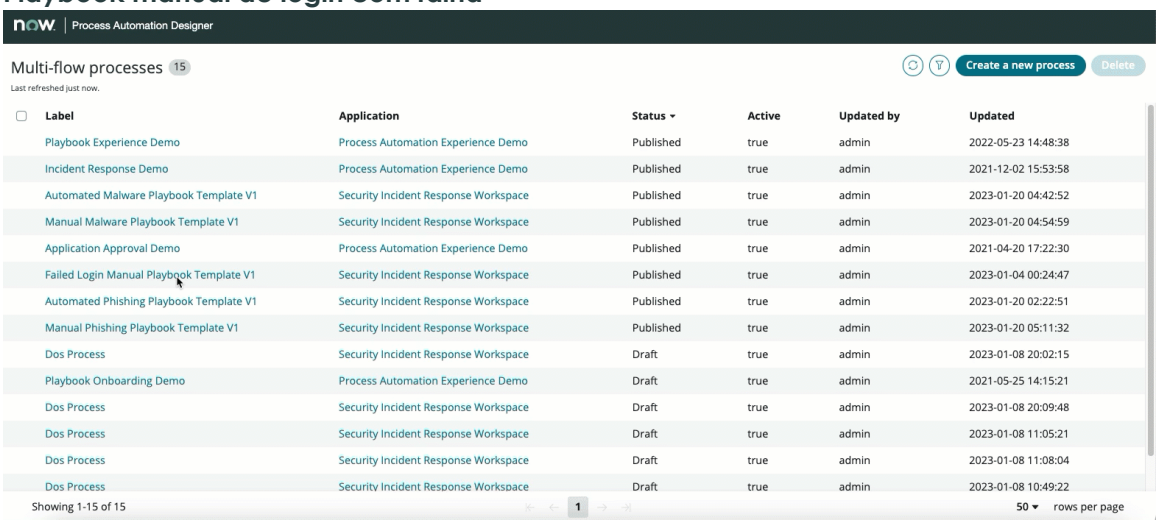
- Análise
- Contém
- Erradicar
- Revisão

Cada fase tem atividades dentro dela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual de login com falha



Depois de marcar uma tarefa como concluída em uma fase, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma fase, você pode passar para a próxima fase. O status é refletido no painel esquerdo conforme você conclui tarefas e fases. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as fases. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para login manual com falha no PAD

Use estas etapas para criar processos para Falha no login manual no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

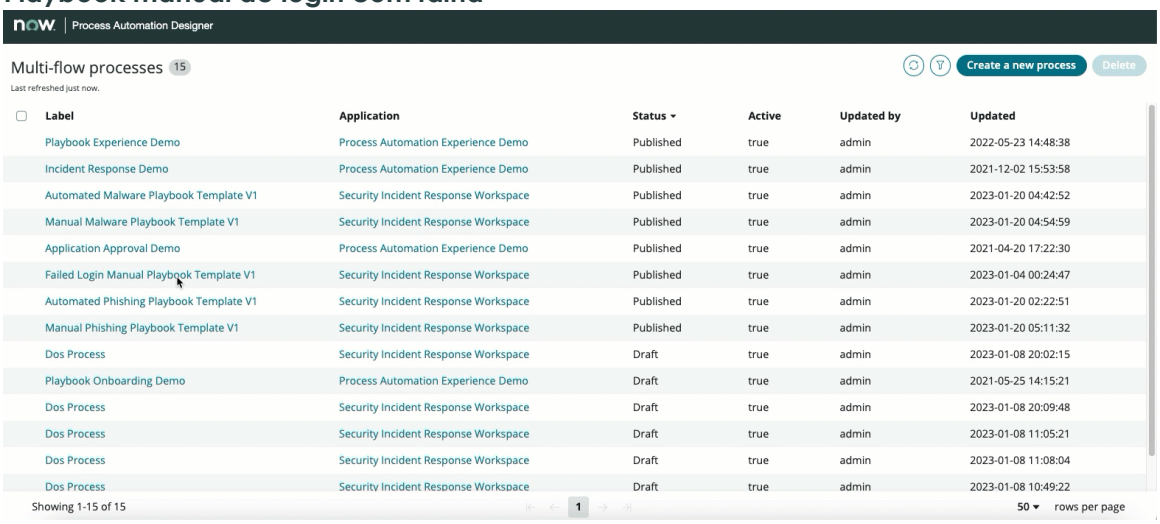
   Por exemplo, Failed Login Manual Playbook Template V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir suas condições de gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual de login com falha

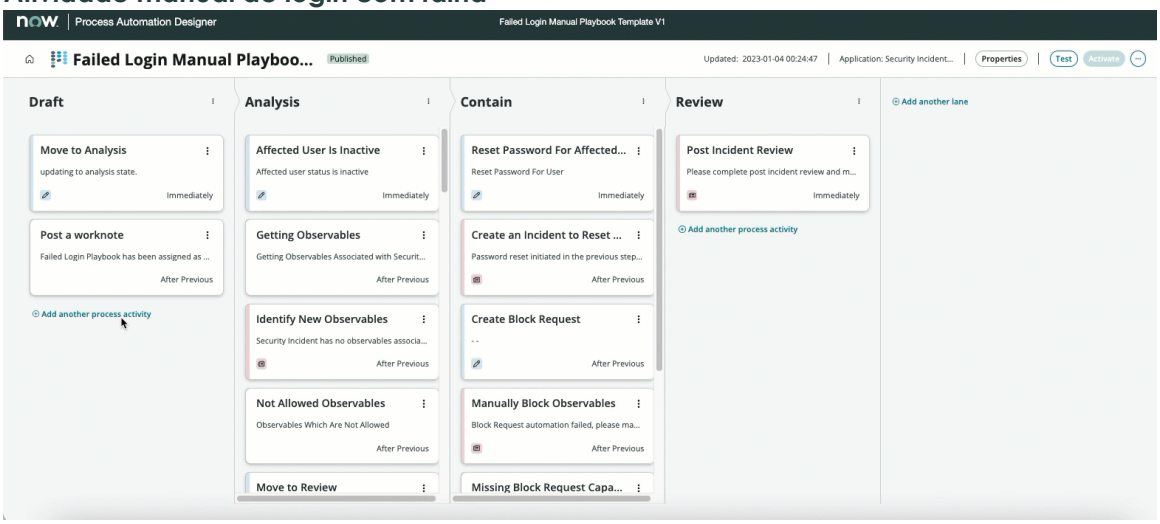


7. Clique **em Ir para Designer**.
   A página do Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova fase**.
   O painel de propriedades da fase é aberto no lado direito da IU.
9. No painel de propriedades da fase, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a fase seria executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra fase, clique em **Adicionar outra fase**.
    Da mesma forma, você pode criar quantas fases quiser. Neste exemplo, você pode criar uma fase para Análise, Conter, Eliminar e Revisar, respectivamente. No exemplo a seguir, a fase **Análise** começa imediatamente e não tem condição de execução. A fase de**contenção** começa após a conclusão da fase anterior e tem uma condição de execução que se baseia no resultado de uma atividade na fase anterior.
    Depois de adicionar as fases, você precisa adicionar atividades de processo para cada fase.
12. Clique na **atividade Adicionar outro processo** em uma fase específica (por exemplo, fase de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de maneira semelhante às fases. Da mesma forma, você pode criar outras atividades de processo em cada fase.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade manual de login com falha



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook manual de login com falha

Use estas etapas para saber como você pode usar o playbook Manual de login com falha no Espaço do analista SIR e suas capacidades.

Antes de Iniciar
Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

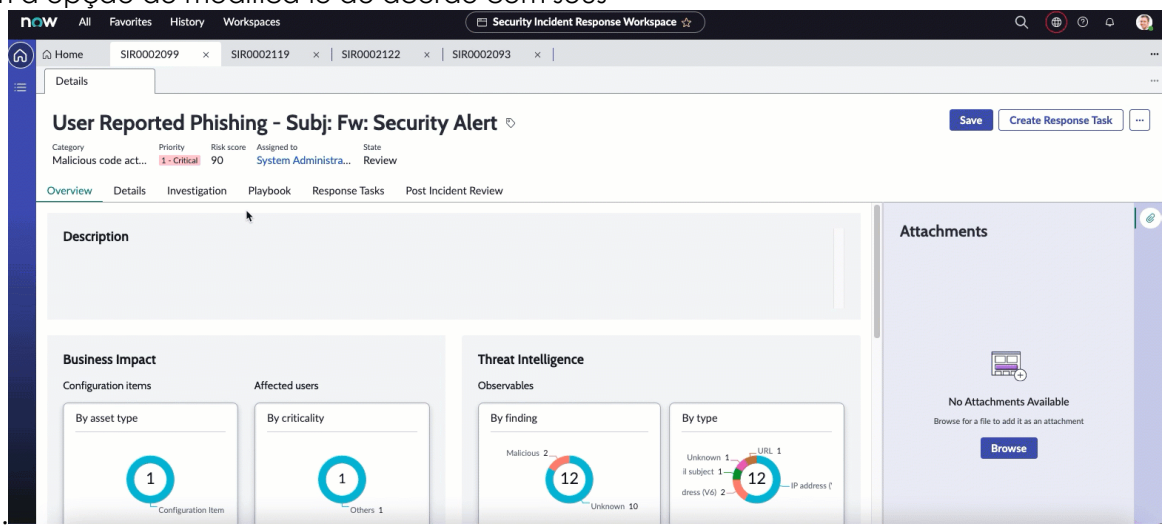
   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

   Nota: Se você não vir nenhum playbook listado, precisará acessar o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook Manual de login com falha**.
   Para Falha no login manual, as tarefas são executadas automaticamente para o incidente de segurança.
4. Clique em cada fase para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de modificá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Eliminar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbooks baseados em fluxo

Usando o Flow Designer, os administradores de segurança e os autores de design de fluxo podem fazer a transição mais facilmente de playbooks manuais ou não documentados para playbooks automatizados e repetíveis. O recurso de arrastar e soltar oferece flexibilidade na movimentação de objetos, verificações de condição, ramificação paralela, tabelas de decisão e muito mais.

Security Incident Response fornece os seguintes playbooks com o sistema de base.

Além dos playbooks listados, também há subfluxos no Spoke das Operações de segurança que podem ser chamados a partir do playbook de fluxos. O ransomware é um desses subfluxos.

Ative esses fluxos antes de usá-los. Para obter mais informações, consulte Como ativar um fluxo do Security Incident Response.

Playbook for Automated Phishing

O playbook de phishing automatizado ajuda a resolver determinados tipos de ameaças à segurança passo a passo. Com os modelos do Flow Designer, você pode automatizar as etapas do playbook de resposta a phishing e resolver incidentes de forma rápida e eficiente.

Você pode usar modelos criados com o Flow Designer para automatizar as tarefas no Playbook de resposta a phishing para analisar e resolver ataques de phishing em sua organização.

O playbook de resposta de phishing inclui os seguintes fluxos e subfluxos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Incidente de segurança - Modelo de resposta de phishing automatizado: este modelo foi projetado para automatizar as tarefas de resposta de phishing e contém uma sequência de ações, incluindo um gatilho.
- Incidente de segurança - Modelo manual de phishing: este modelo é o fluxo de trabalho de resposta de phishing manual existente. Defina a categoria como Phishing para ativar o fluxo.

Esses modelos contêm uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que você pode anotar para facilitar a leitura. Para acessar esses fluxos, você deve instalar ospoke das Operações de segurança .

Nota: Ative esses modelos antes de usá-los. Consulte Ativação de um fluxo do Security Incident Response para obter detalhes.

- Executar pesquisas de ameaças para observáveis: executa pesquisas de ameaças de observáveis selecionados.
- Aprimorar observáveis: permite aprimorar observáveis com informações adicionais de várias fontes.
- Avaliar o impacto do e-mail de phishing: permite que você avalie o impacto do e-mail de phishing. Quando você recebe um e-mail no endereço de e-mail de phishing, este subfluxo analisa o anexo .EML e compara as informações com as regras de correspondência de e-mail.
- Eliminar e-mails de phishing: permite excluir ou erradicar e-mails de phishing para ajudar a reduzir a exposição a um ataque específico.
- Executar pesquisa de detecções em observáveis: determina a prevalência de uma ameaça ao longo do tempo ou testa os esforços de correção ou erradicação.
- Criar solicitações de bloqueio: bloqueia a comunicação com observáveis associados ao incidente.

Esses subfluxos representam um conjunto de operações reutilizáveis que você pode usar em vários playbooks. Você pode usar esses subfluxos para definir modelos personalizados (fluxos) de acordo com seus requisitos.

Para criar modelos personalizados (fluxos), siga as instruções em Fluxos .

Executar o fluxo do playbook de resposta automatizada de phishing

Usando o Flow Designer, você pode definir e automatizar tarefas no playbook para analisar e resolver ataques de phishing contra sua organização.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer e action_designer
- Instale e configure as seguintes integrações com as credenciais corretas:
  - Bloquear solicitação (Operações de segurança Integração de NGFW da Palo Alto Networks)
  - Aprimoramento de Observável
  - Pesquisa de detecção
  - Pesquisa de ameaças
  - Microsoft Office Exchange

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

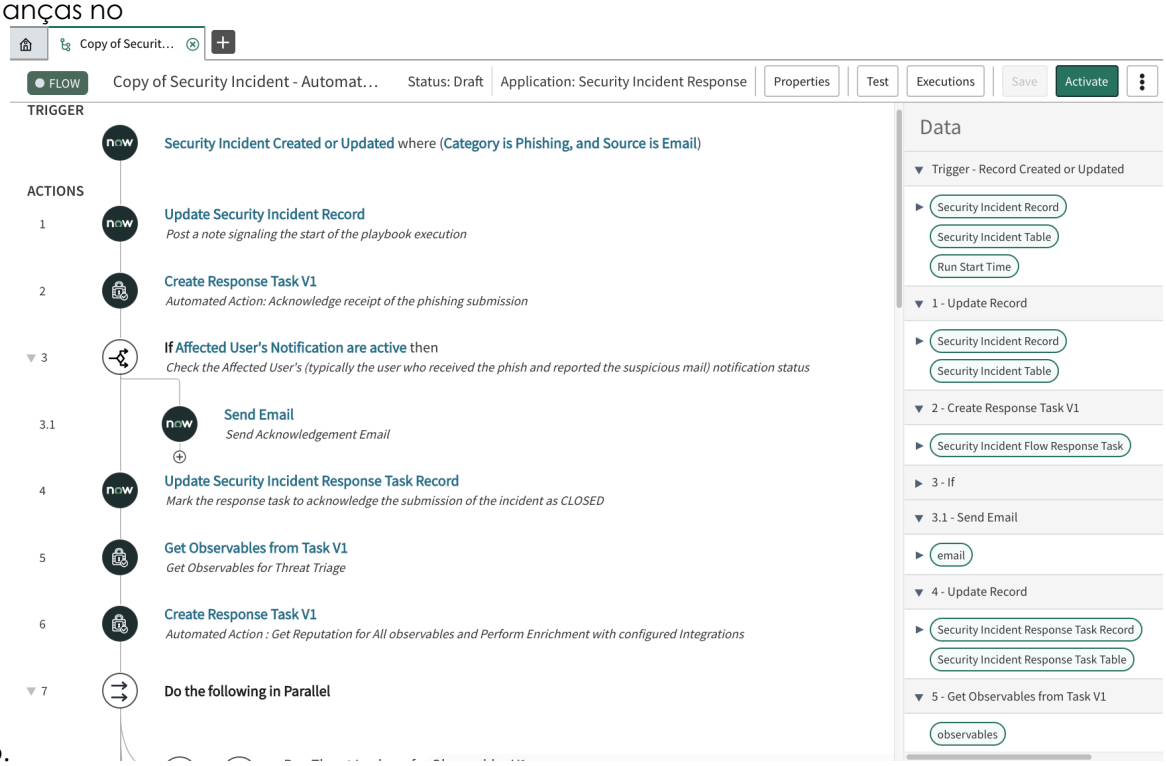
Quando os funcionários recebem um e-mail suspeito que contém os sinais comuns de um ataque de phishing (conforme definido por suas políticas de segurança), eles podem enviá-lo como um anexo .EML para o endereço de e-mail de phishing definido por sua organização. Usando as tarefas definidas no fluxo do playbook de phishing automatizado, você pode fazer a triagem, analisar, conter e erradicar uma ameaça de phishing. Essas tarefas podem ser invocadas como parte de diferentes estados de incidente (por exemplo, Análise, Conter e assim por diante). Quando um incidente de segurança de phishing é criado, o fluxo de phishing automatizado pode ser acionado automaticamente. Usando o Flow Designer, você pode exibir os detalhes das várias ações de resposta do incidente conforme elas são invocadas.

Nota: O fluxo do playbook Incidente de segurança - Modelo de resposta de phishing automatizado V1 é Somente leitura. Você pode fazer uma cópia do fluxo e fazer mudanças conforme necessário.

As etapas a seguir descrevem como fazer uma cópia do modelo de playbook de phishing e orientam você em algumas das tarefas no fluxo.

Procedimento

1. Navegar até **Todos** > **Flow Designer** > **Designer** para exibir os fluxos disponíveis com o Operações de segurança Spoke.
2. Clique no link **Incidente de segurança - VI do Modelo de resposta de phishing automatizado**.
3. Na página Fluxo, clique no ícone mais ícone , faça uma cópia do fluxo e abra-o para uso.
   Você pode modificar as condições do gatilho, adicionar ou remover ações e fazer outras mudanças no fluxo.



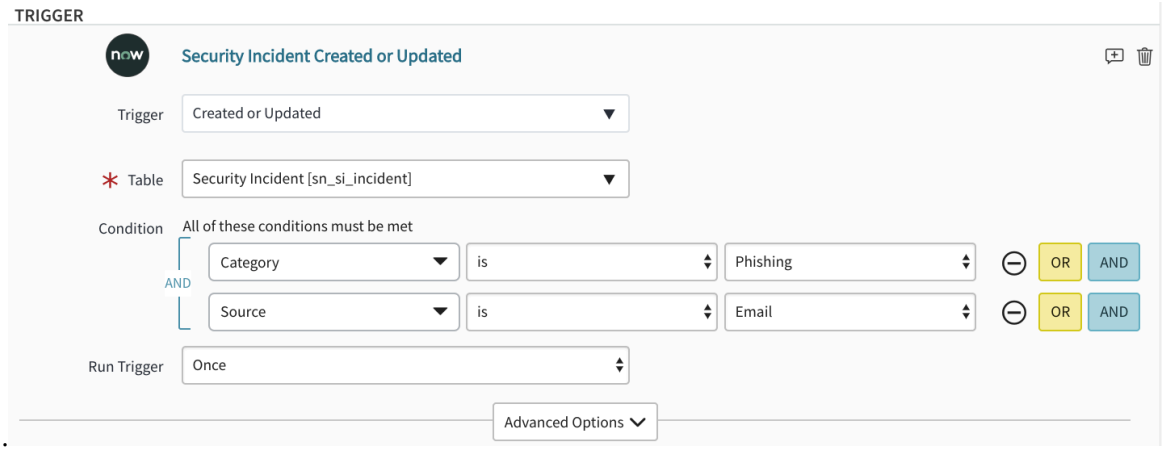
   Esta imagem mostra as condições do gatilho e as etapas que o fluxo executa. O painel direito mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

4. Clique no ícone do **gatilho**.

Tradução automática

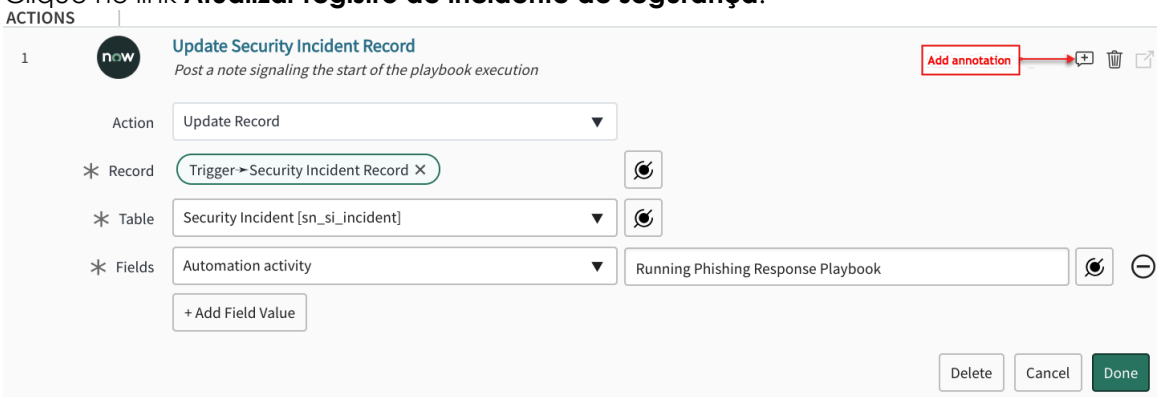
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na primeira etapa, você define ou define o gatilho do fluxo. Especifique as condições do gatilho e com que frequência você deseja que o fluxo execute o gatilho.



Quando as condições definidas no fluxo (Categoria é Phishing e Origem é E-mail) são atendidas no registro do incidente, as tarefas no fluxo de phishing automatizado começam a ser executadas sequencialmente. Você pode modificar o gatilho, adicionar anotações, adicionar ou excluir condições e assim por diante.

5. Clique no link **Atualizar registro de incidente de segurança**.

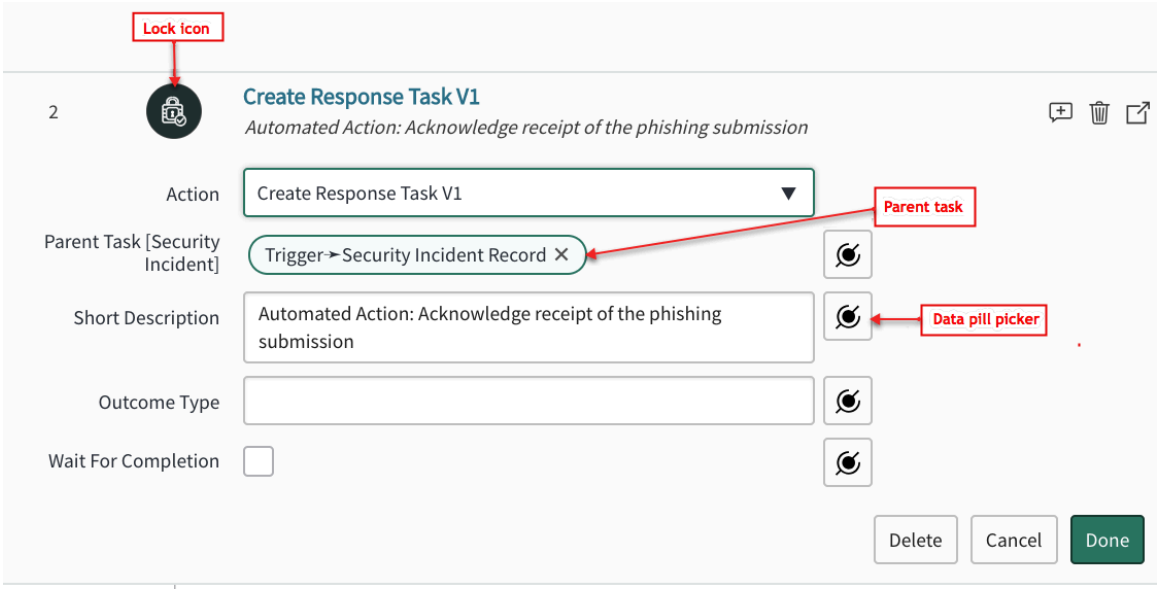


Atualizar registro de incidente de segurança é a primeira etapa do fluxo. Clique no ícone de anotação ícone de para adicionar uma anotação ao analista de segurança indicando que ocorreu um incidente de phishing e que o fluxo do playbook de phishing automatizado começou a ser executado.

6. Prossiga com a etapa 2 no fluxo e clique no link **Criar tarefa de resposta**.

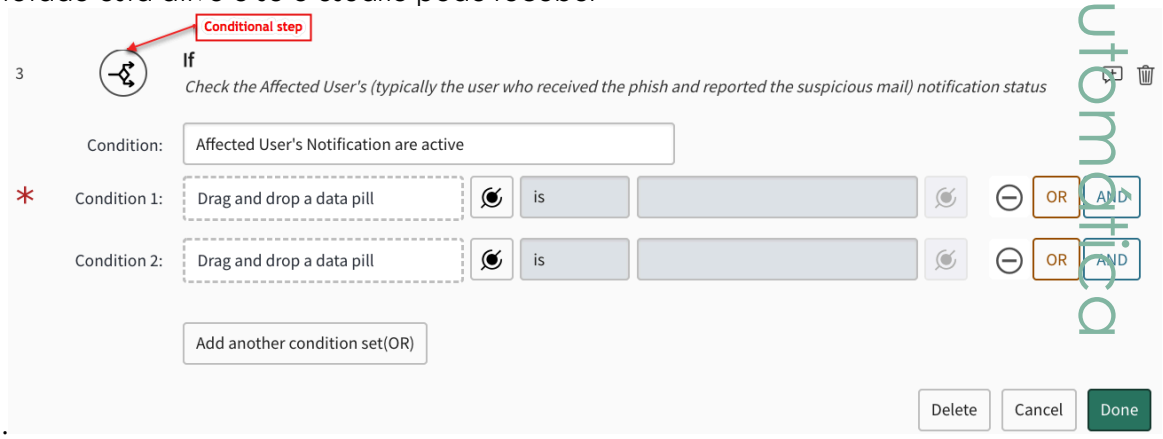
Nesta etapa, o fluxo cria uma tarefa de resposta automatizada para confirmar o recebimento ao remetente do incidente ou ao usuário afetado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Observe que o campo **Tarefa primária [Incidente de segurança]**faz referência ao registro primário associado a esta etapa. Você pode escolher qualquer registro de referência usando o ícone do seletor de cápsula de ou arrastar o item de referência relevante do painel direito. Observe o ícone de cadeado Ícone de . O ícone de cadeado indica que essa etapa não requer nenhuma intervenção do usuário.

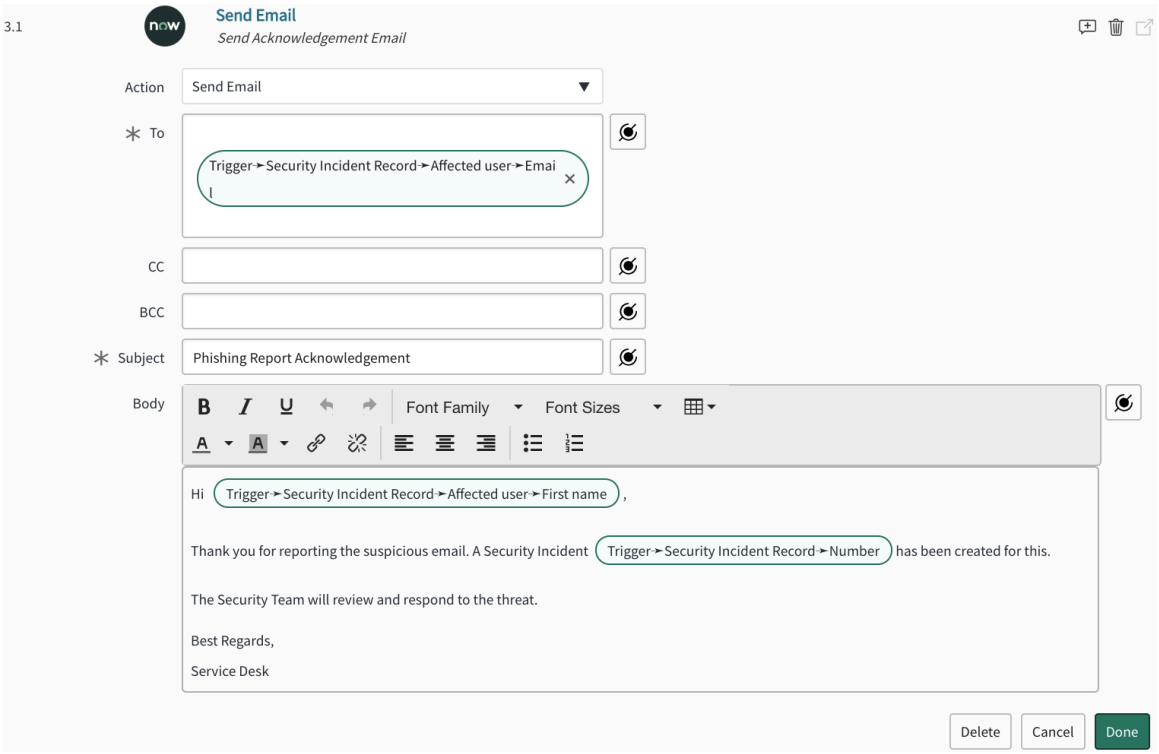
7. Na etapa 3, o fluxo coleta detalhes adicionais do usuário afetado (normalmente o usuário que enviou o incidente) para garantir que ele possa enviar uma notificação com sucesso. Você pode especificar condições para verificar se o status do usuário afetado está ativo e se o usuário pode receber notificações.



Observe o ícone de etapa na etapa 3. O fluxo executará a próxima etapa (3.1) somente se as condições especificadas forem atendidas.

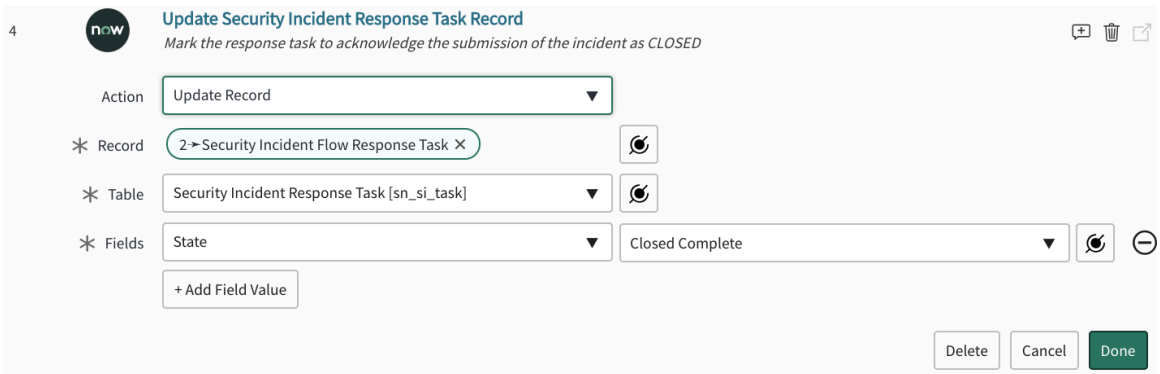
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando as condições definidas na etapa 3 forem atendidas com sucesso, o e-mail será enviado.

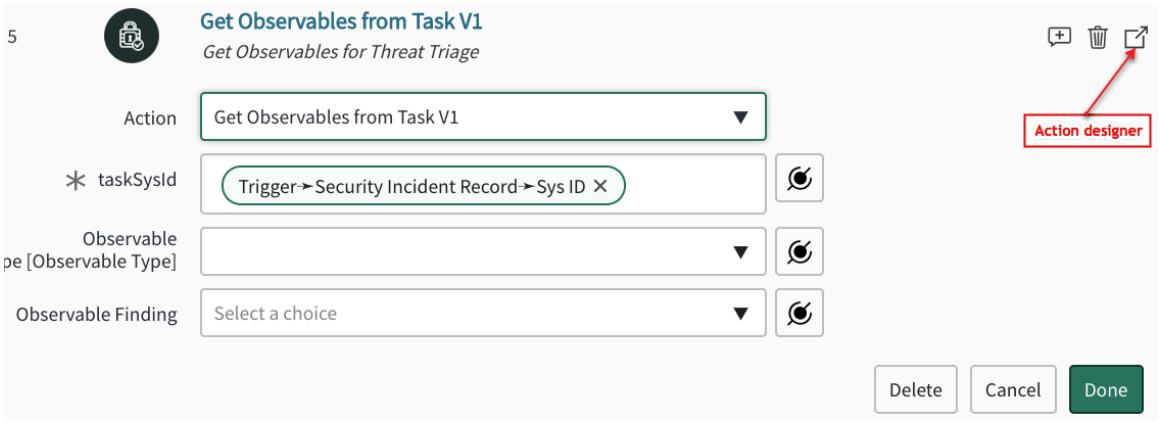
8. Na etapa 4, depois que o e-mail é enviado, a tarefa de resposta é marcada como encerrada.



9. Na etapa 5, todos os observáveis envolvidos no incidente (como assunto do e-mail, endereço de e-mail do qual o e-mail de phishing foi enviado, URL de phishing) ou observáveis pertencentes a uma categoria selecionada (hash, arquivo ou domínio) são coletados para executar automatizações adicionais ações nas etapas subsequentes do playbook.

Tradução automática

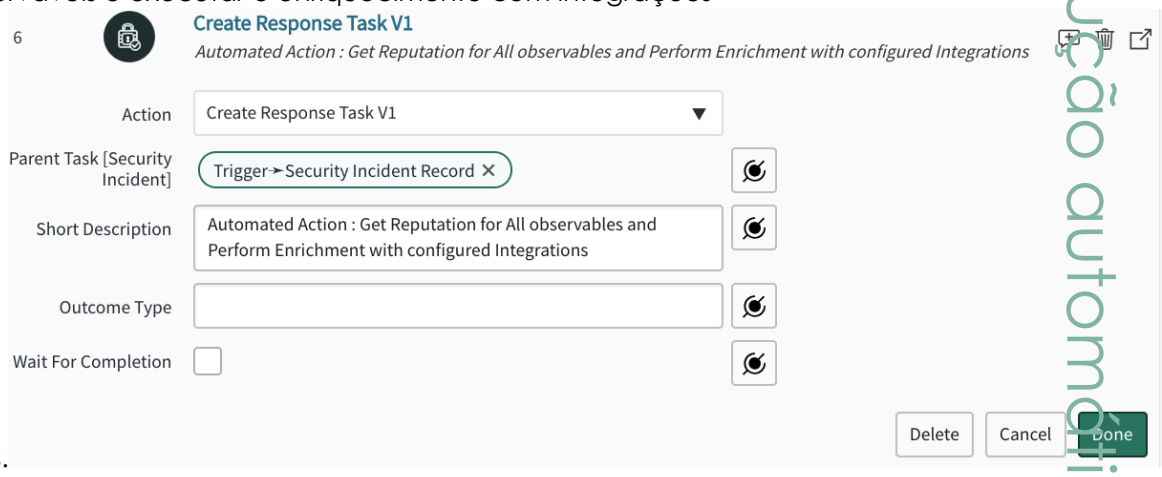
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique no ícone do designer de ações ícone do Designer de para ter uma exibição detalhada da ação.

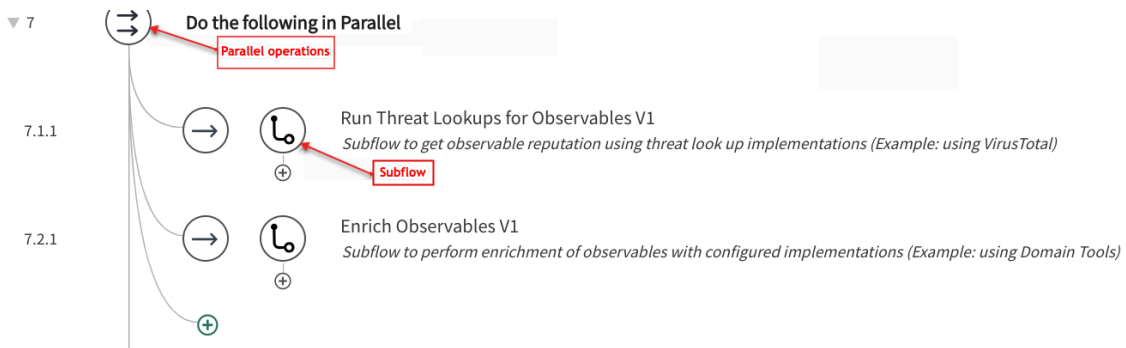
Para exibir a página do Designer de ações, expanda uma etapa no fluxo e clique no ícone do Designer de ações.

10. Na etapa 6, uma tarefa de resposta automatizada é criada.
Esta tarefa captura o início do processo para obter a reputação de todos os observáveis e executar o enriquecimento com integrações configuradas.



11. Na etapa 7, dois subfluxos são chamados:

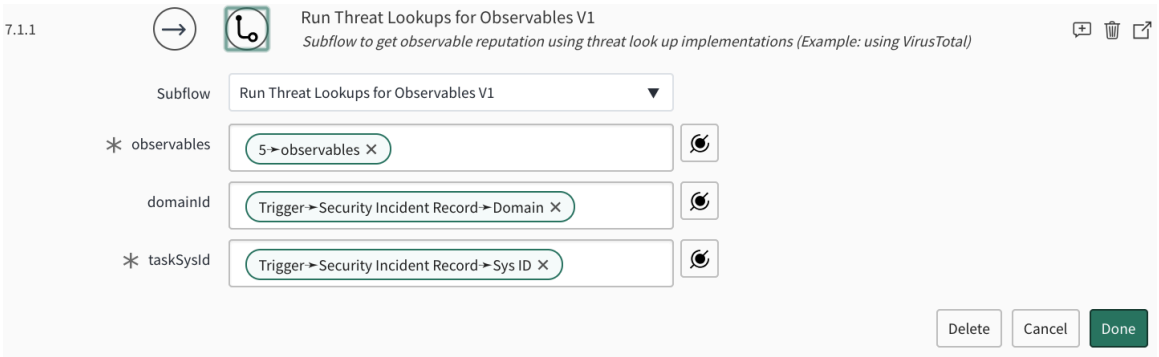
- Executar pesquisas de ameaças para observáveis: este subfluxo é usado para obter a reputação de todos os observáveis usando implementações de pesquisa de ameaças.
- Aprimorar observáveis: este subfluxo é usado para realizar o enriquecimento de observáveis com implementações configuradas.



Tradução automática

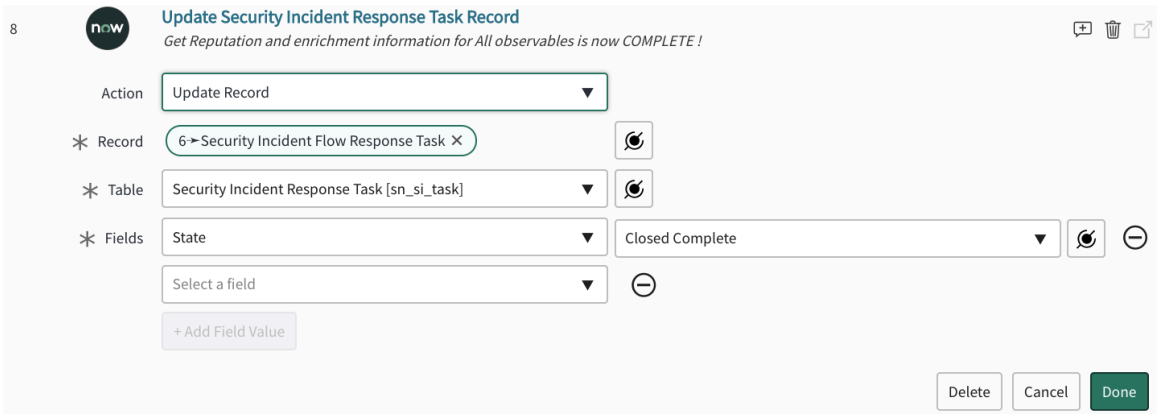
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observe os ícones para esta tarefa. O ícone de operações paralelas O ícone de indica que ambas as tarefas serão executadas em paralelo e o ícone de subfluxo de subfluxo indica que a tarefa que está sendo executada é um subfluxo, conforme mostrado abaixo:

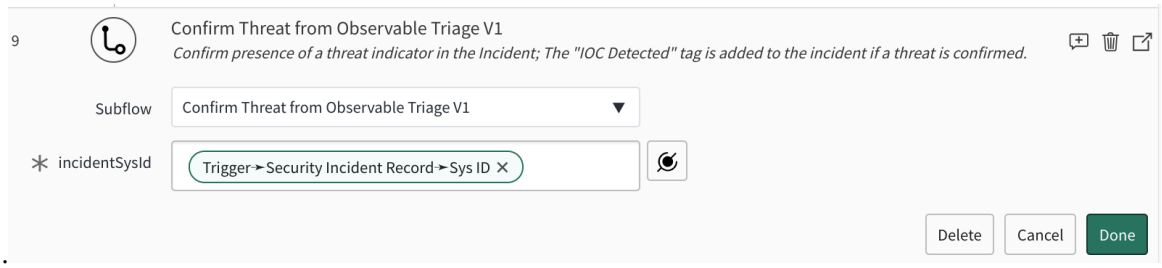


Observe o número 5 no campo de observáveis. Isso indica que a pesquisa de ameaças será executada em observáveis recuperados na etapa 5. Este subfluxo, por sua vez, chama fluxos de trabalho e ações existentes, conforme mostrado no Designer de subfluxo.

12. Na etapa 8, depois que os subfluxos forem concluídos, a tarefa de resposta será marcada como Encerrada.



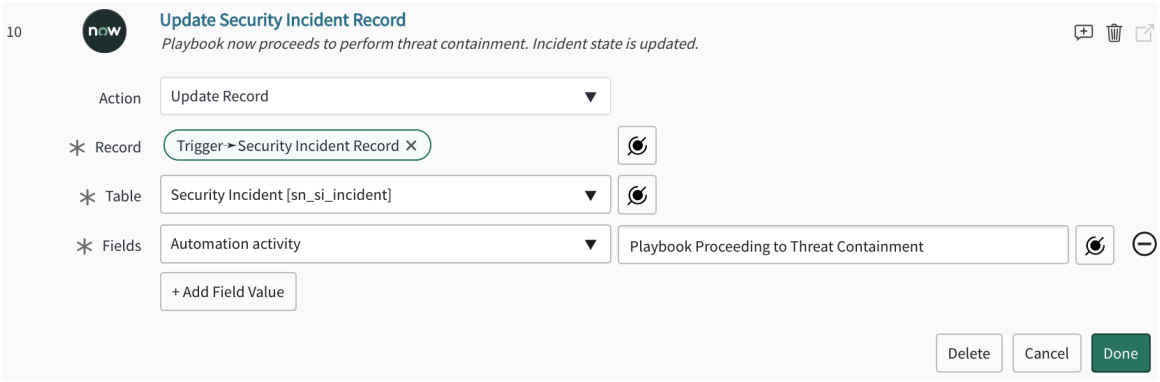
13. Na etapa 9, o subfluxo Confirmar ameaça da triagem de observável é chamado. Este subfluxo é usado para confirmar a presença de um indicador de ameaça no incidente. Se a ameaça for confirmada, um sinalizador "IOC detectado" será adicionado ao incidente.



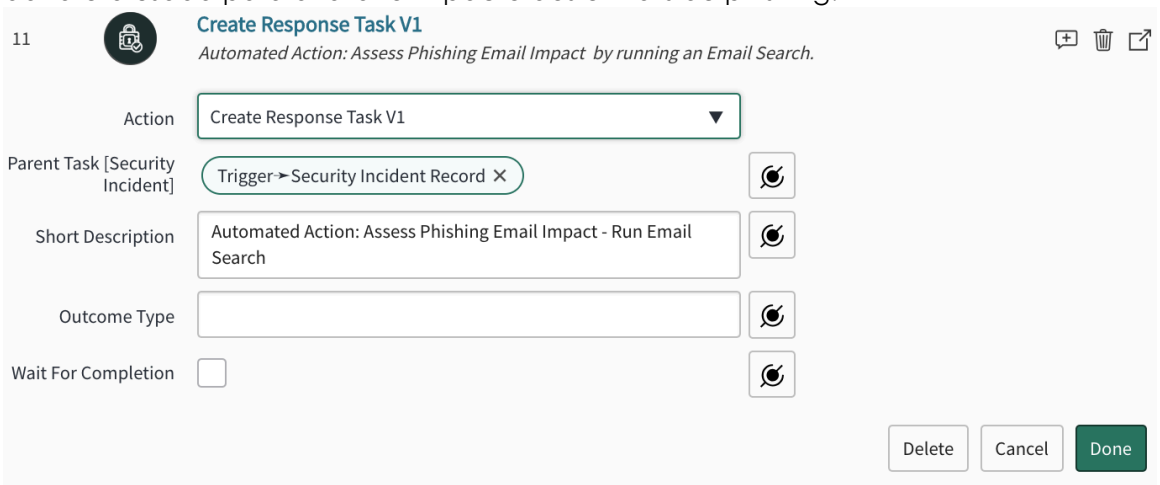
14. Quando a ameaça for confirmada, na etapa 10, você atualiza o incidente de segurança e adiciona uma anotação indicando que as tarefas de contenção de ameaças serão iniciadas.

Tradução automática

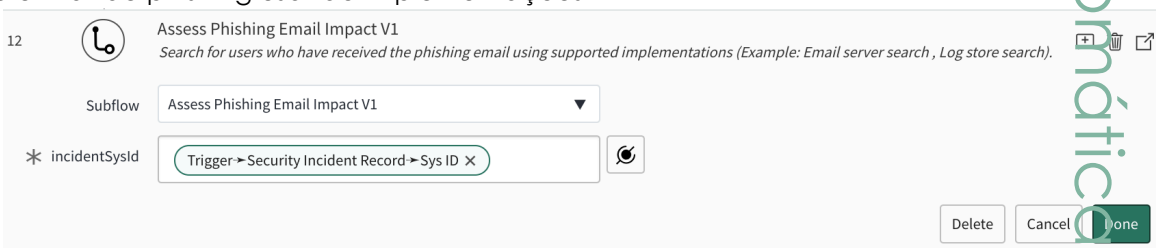
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



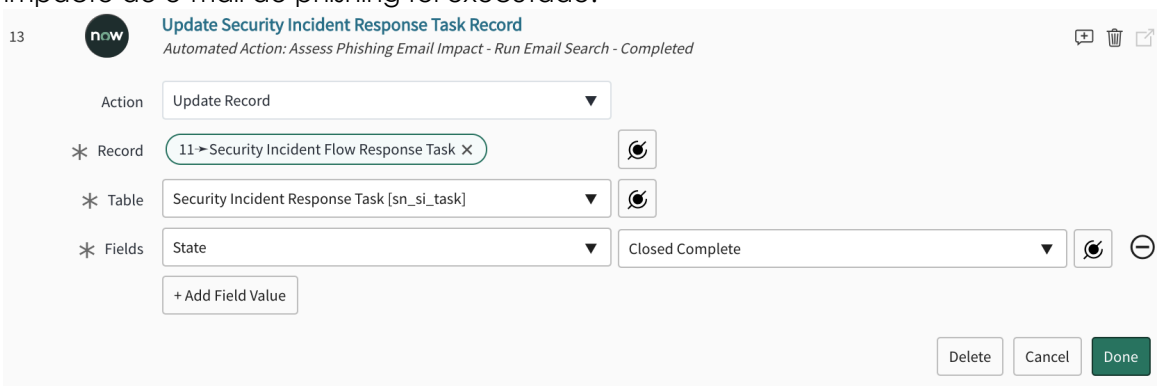
15. A etapa 11 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa usada para avaliar o impacto dos e-mails de phishing.



16. Na etapa 12, o subfluxo Avaliar impacto de e-mail de phishing é chamado. Este subfluxo é usado para pesquisar usuários que receberam o e-mail de phishing usando implementações compatíveis.



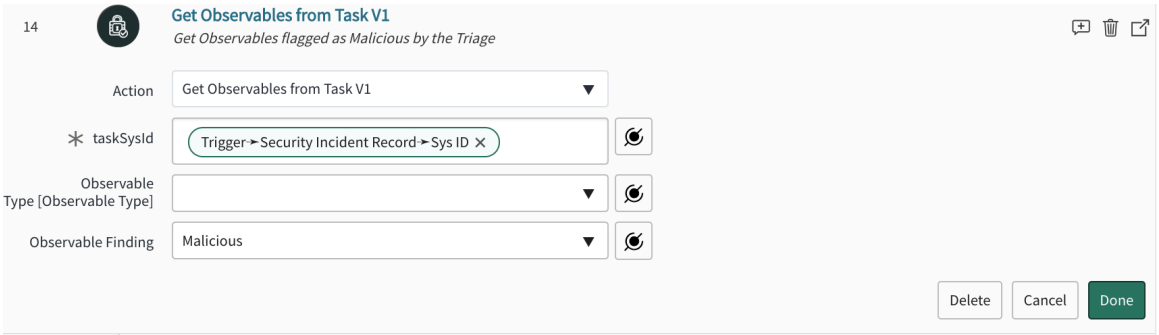
17. Na etapa 13, a tarefa é marcada como encerrada para indicar que o subfluxo Avaliar impacto de e-mail de phishing foi executado.



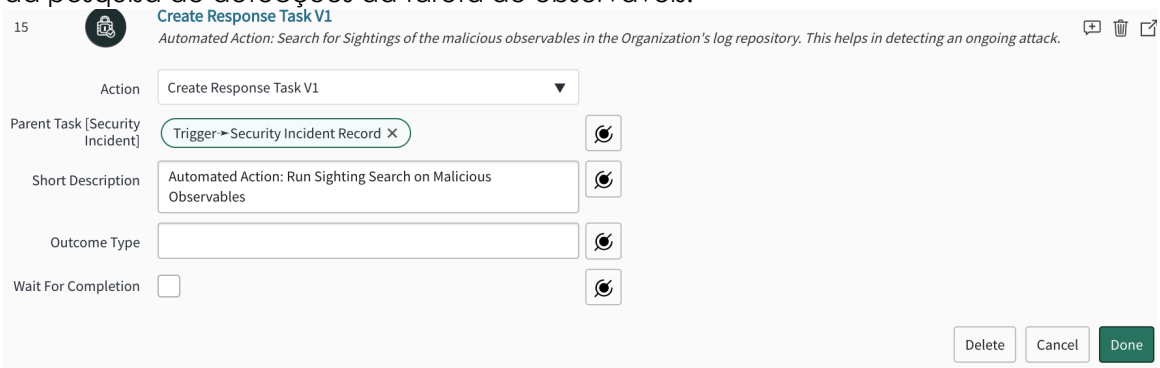
18. A etapa 14 é usada para recuperar todos os observáveis que foram marcados como mal-intencionados.

Tradução automática

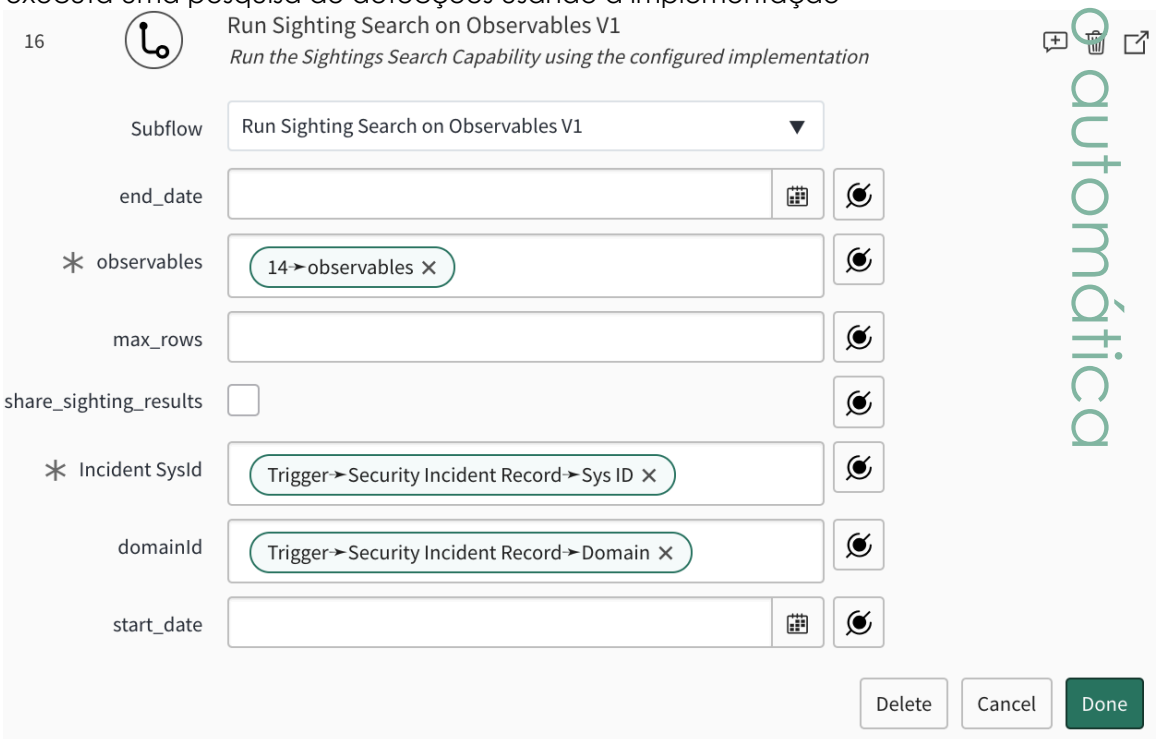
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



19. A etapa 15 é uma tarefa de resposta automatizada que captura o início e a conclusão da pesquisa de detecções da tarefa de observáveis.



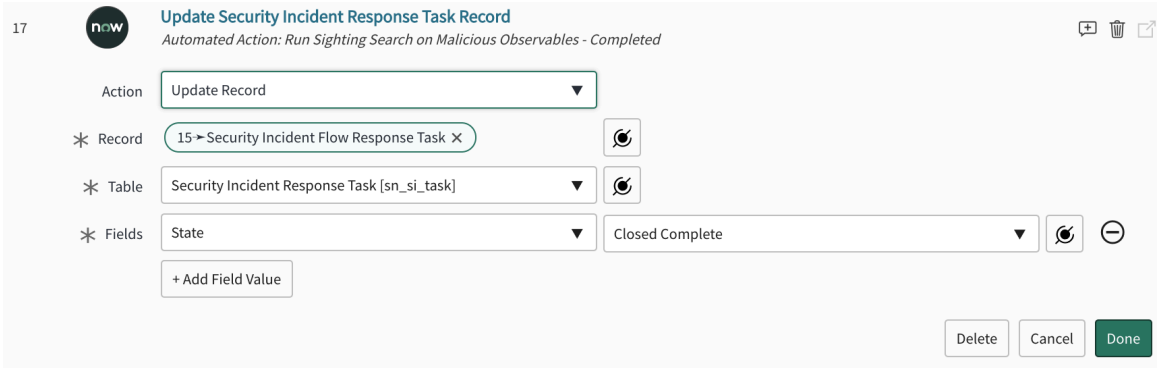
20. Na etapa 16, o subfluxo Executar pesquisa de detecções em observáveis é chamado. Este subfluxo executa uma pesquisa de detecções usando a implementação configurada.



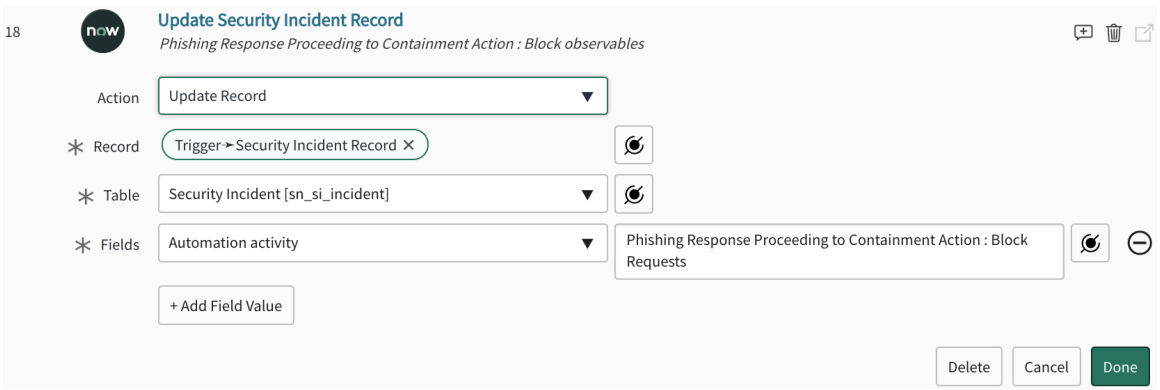
21. Na etapa 17, a tarefa é marcada como encerrada para indicar que o subfluxo Executar pesquisa de detecções em observáveis foi concluído.

Tradução automática

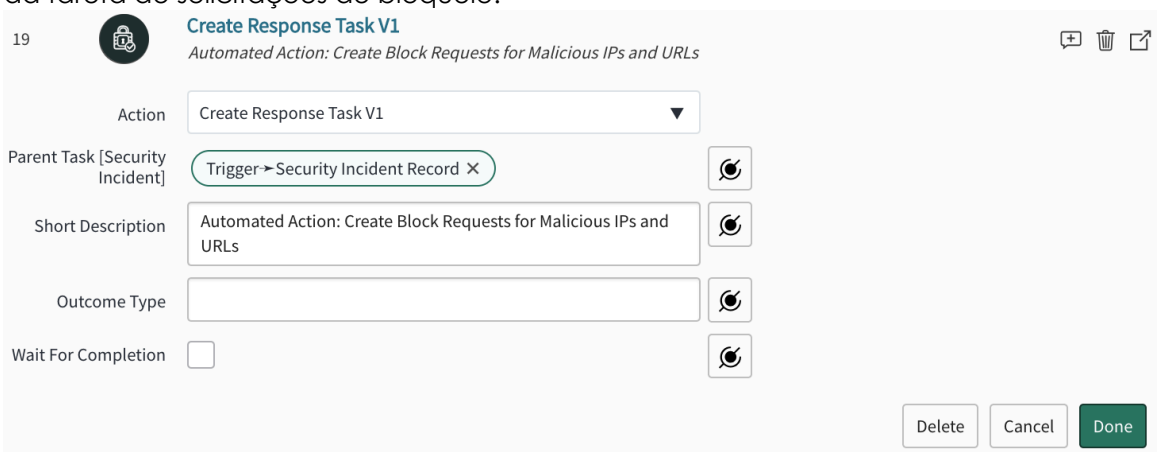
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



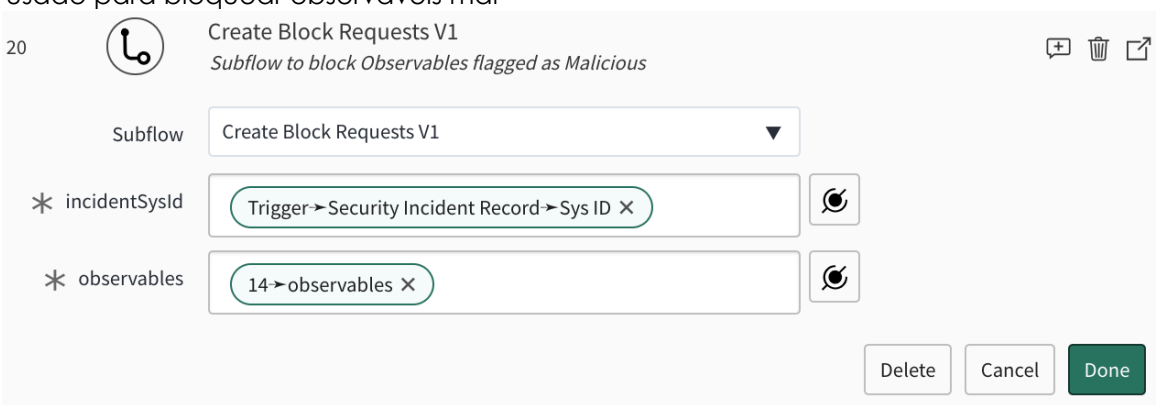
22. Depois de identificar os observáveis mal-intencionados, na etapa 18, você atualiza o registro do incidente de segurança para indicar que as ações de contenção serão iniciadas.



23. A etapa 19 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa de solicitações de bloqueio.



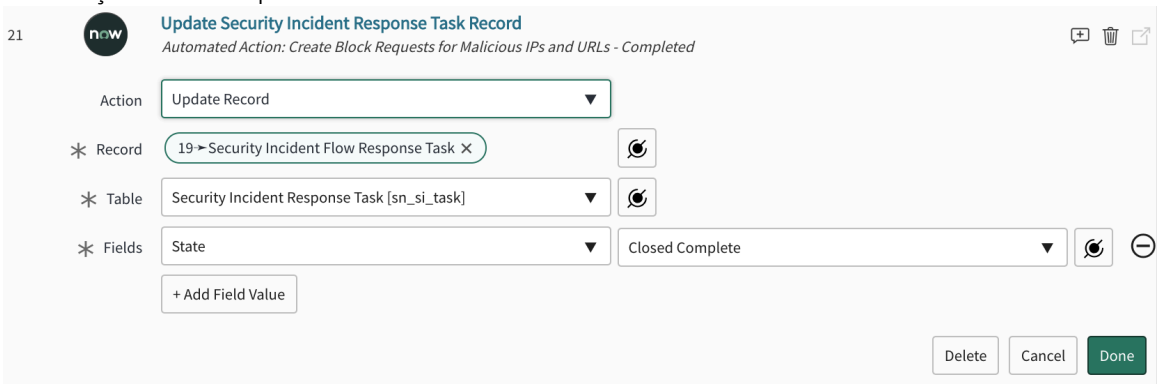
24. Na etapa 20, o subfluxo Criar solicitações de bloqueio é chamado. Este subfluxo é usado para bloquear observáveis mal-intencionados.



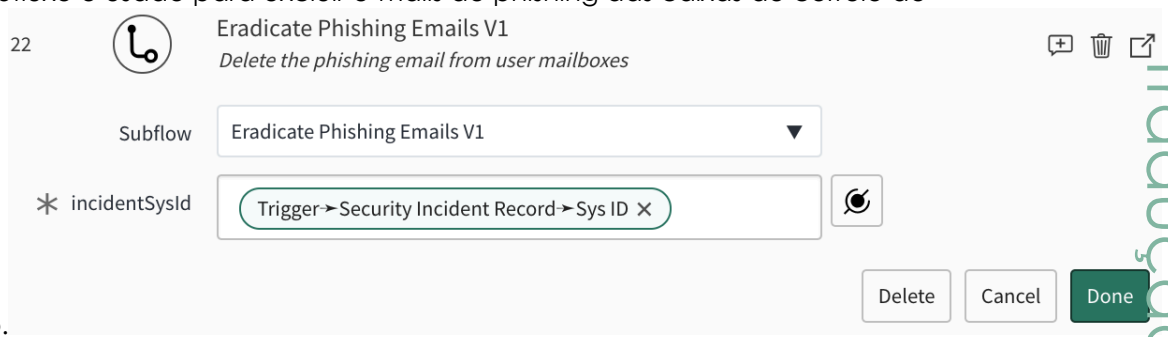
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

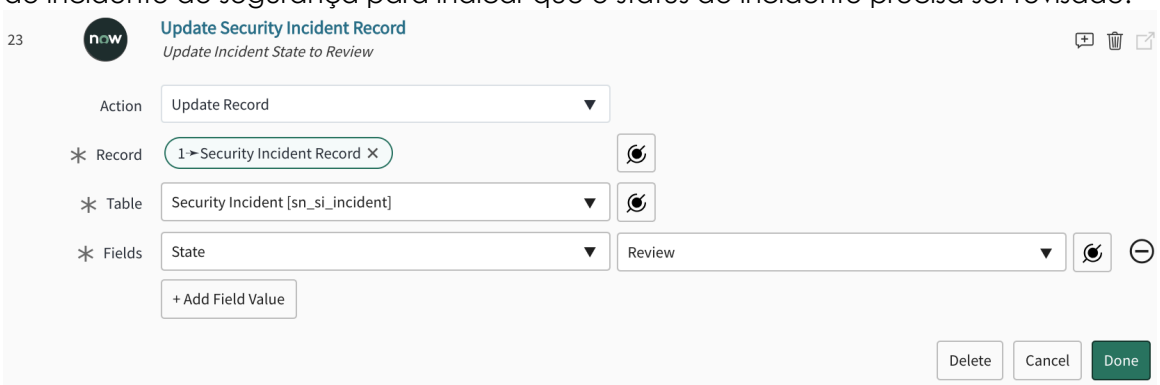
25. Na etapa 21, a tarefa é marcada como encerrada para indicar que o subfluxo Criar solicitações de bloqueio foi concluído.



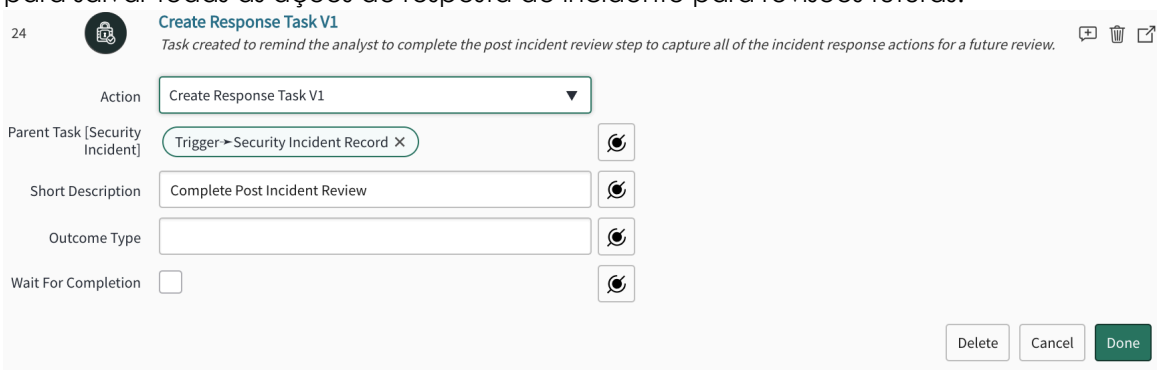
26. Na etapa 22, o subfluxo Erradicar e-mails de phishing é chamado. Este subfluxo é usado para excluir e-mails de phishing das caixas de correio do usuário.



27. Depois que os e-mails de phishing forem excluídos, na etapa 23, você atualizará o registro do incidente de segurança para indicar que o status do incidente precisa ser revisado.



28. Na última etapa, o fluxo cria uma tarefa de resposta automatizada. Esta tarefa é usada para enviar um lembrete ao analista de segurança para salvar todas as ações de resposta do incidente para revisões futuras.



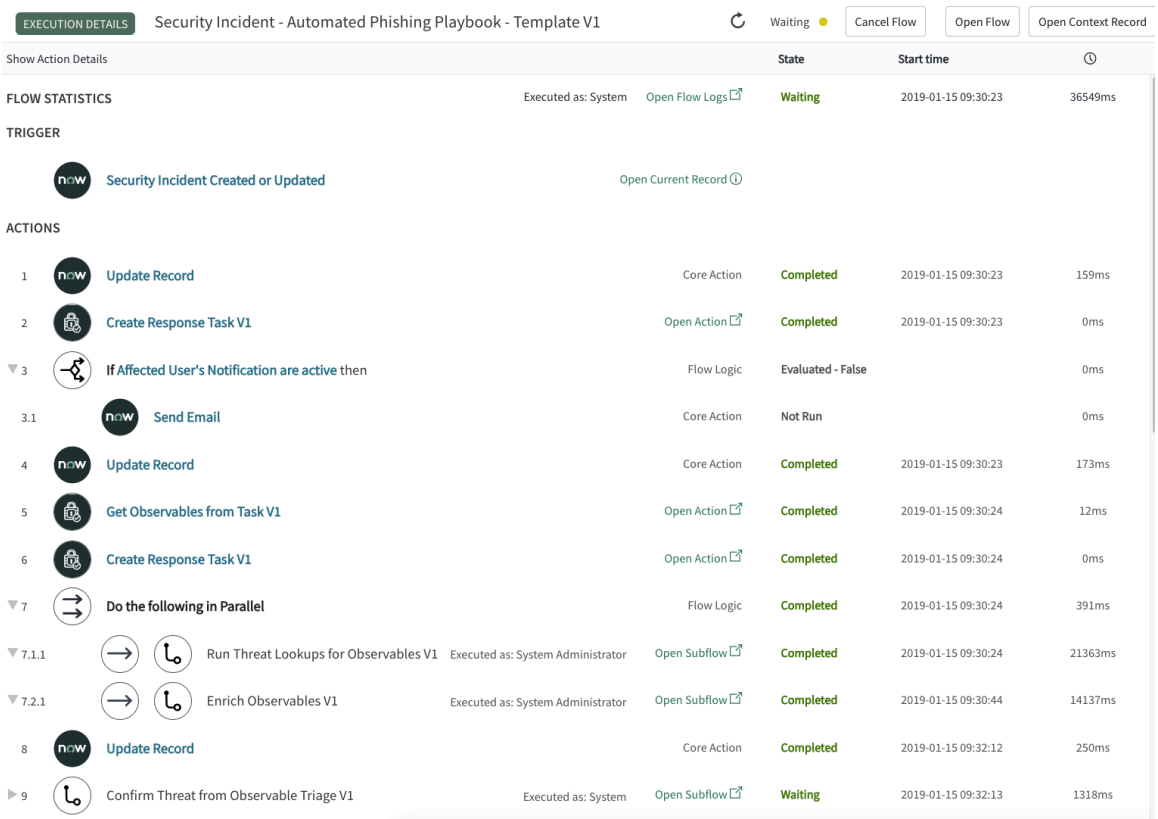
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Você pode clicar em **Testar** para simular as ações no fluxo antes de publicá-lo. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo e executá-lo.

Clique em **Execuções** para exibir os detalhes de execução do fluxo.



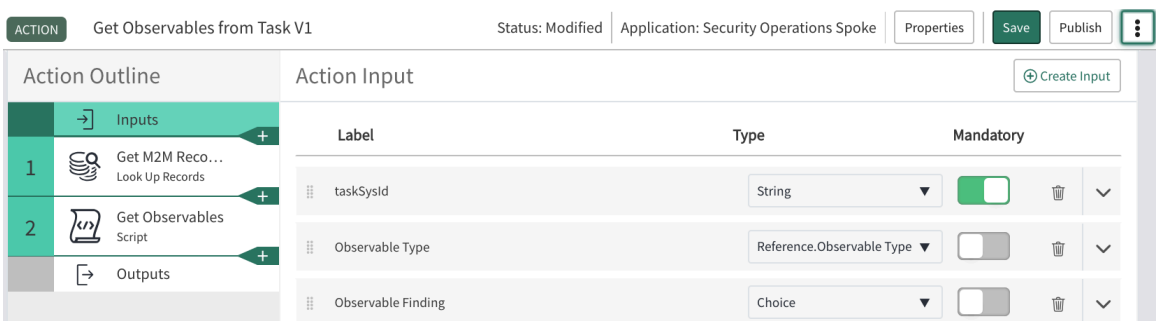
Exibir o designer de ação de fluxo do playbook de resposta automatizada de phishing

Você pode fazer o detalhamento ativo do Designer de ações para exibir informações detalhadas sobre as ações que estão sendo executadas para uma etapa específica no fluxo do playbook de resposta automatizada de phishing.

Esta página descreve a página do Designer de ações para a etapa Obter observáveis da tarefa. Clique em uma tarefa no painel Descrição da ação para exibir os detalhes.

Ação de entrada

Esta seção mostra detalhes sobre como a ação foi criada, incluindo o ID do incidente, o tipo de observável (hash ou IP) e a descoberta de observável (somente e-mails maliciosos).

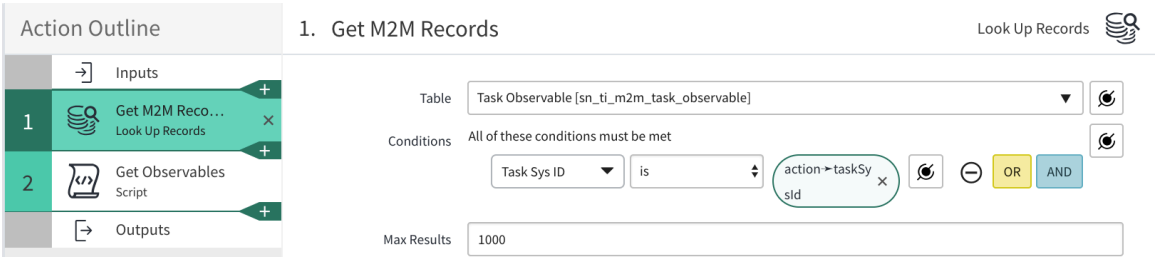


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

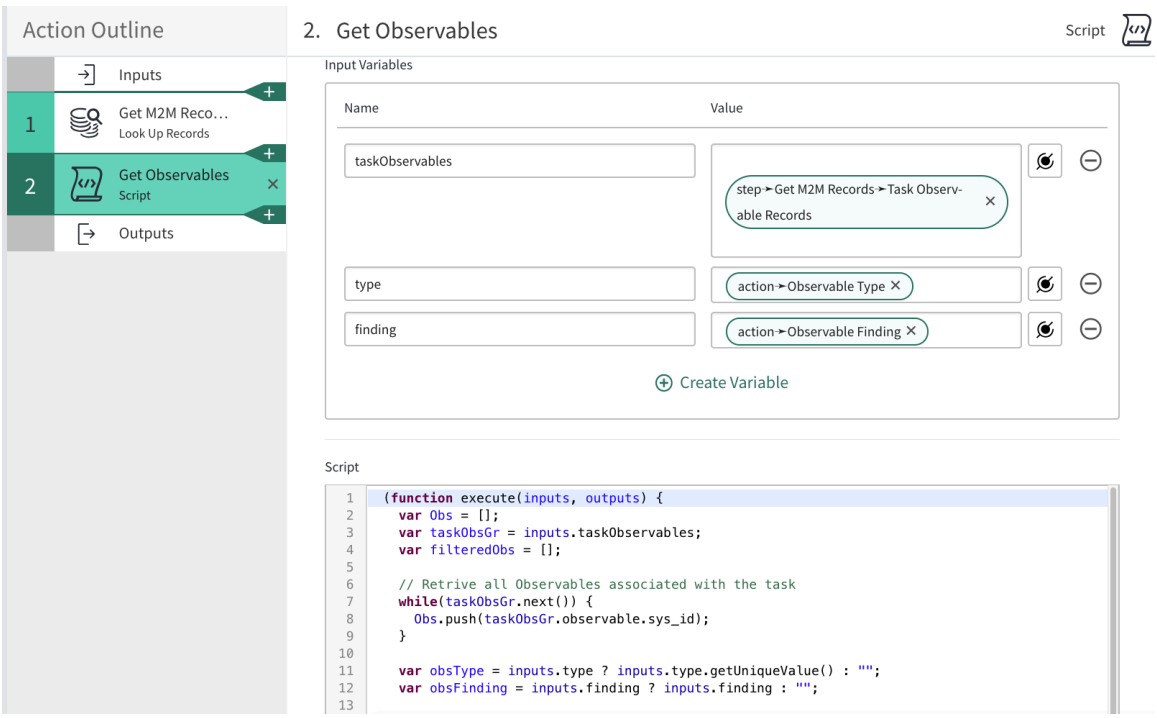
Obter registros M2M

Esta seção mostra as condições que foram definidas para pesquisar observáveis em uma tabela especificada.



Obter observáveis

Esta seção mostra o script usado para recuperar observáveis com base nas condições de filtro especificadas. Por fim, os observáveis que atendem a esses critérios e a contagem são exibidos.



Nota: Todas as ações definidas neste fluxo são reutilizáveis e podem ser modificadas de acordo com seus requisitos.

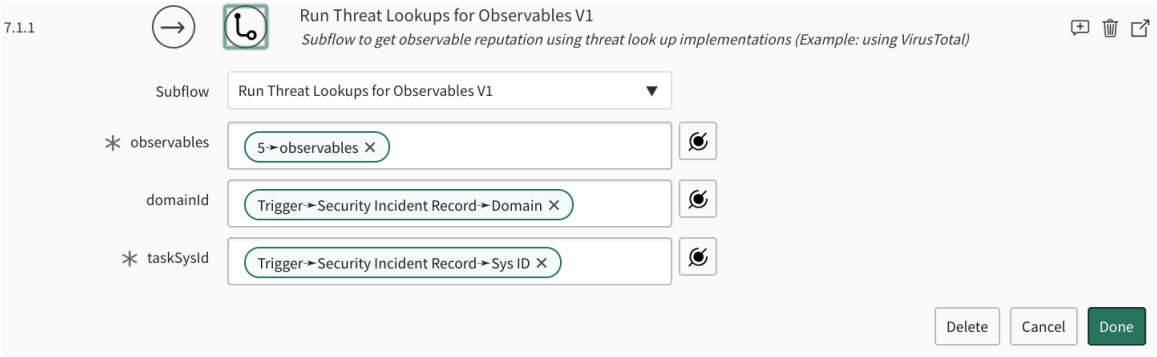
Exibir o designer de subfluxo do playbook de resposta automatizada de phishing

Você pode fazer o detalhamento ativo do Designer de subfluxo para exibir informações detalhadas sobre o subfluxo que está sendo executado como parte do fluxo do playbook de resposta automatizada de phishing.

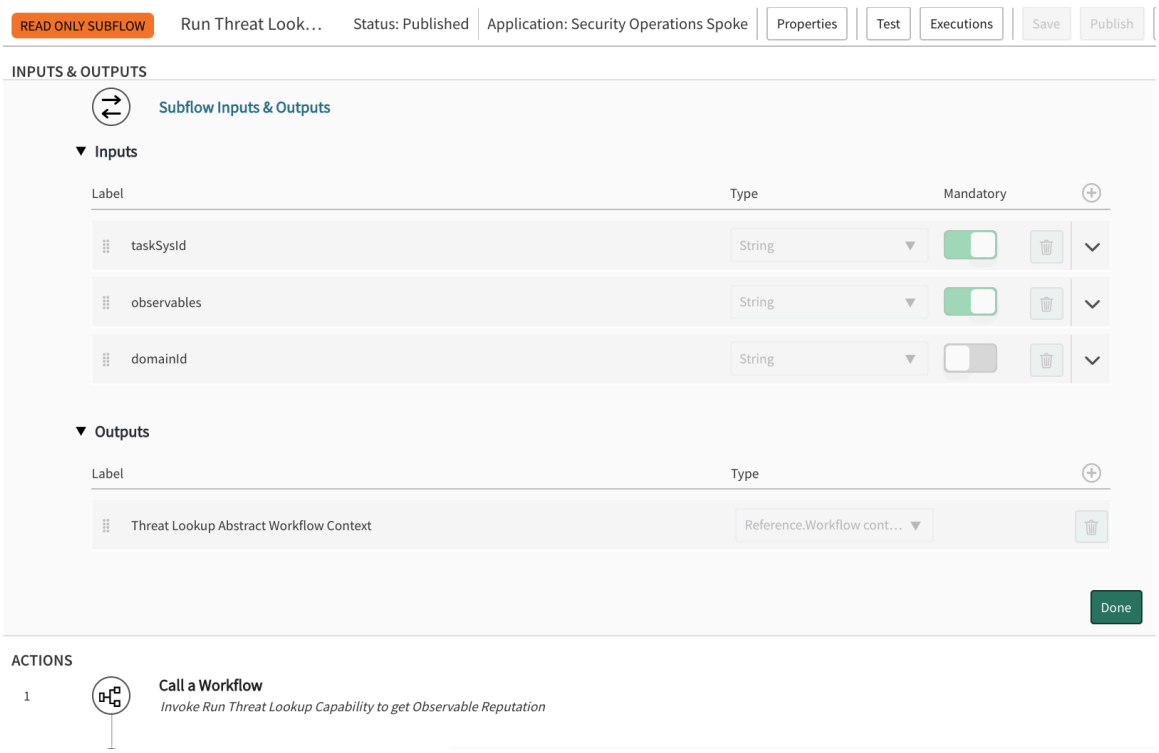
Você pode iniciar o Designer de Subfluxo para exibir detalhes adicionais de um subfluxo. A página do Designer de subfluxo para o subfluxo Executar pesquisas de ameaças para observáveis é mostrada aqui. Clique no ícone do na imagem abaixo para exibir o Designer de subfluxo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Na página do Designer de subfluxo, você pode ver as entradas e saídas deste subfluxo e as ações de fluxo de trabalho subjacentes que estão sendo executadas.



Nota: Este subfluxo é somente leitura e não pode ser editado. Você pode adicionar ou excluir subfluxos da etapa, mas não pode modificar o subfluxo.

Playbook para malware automatizado

O playbook de malware automatizado fornece uma sequência de etapas automatizadas que ajudam a resolver alertas de malware de forma rápida e eficiente.

Use o fluxo do playbook de malware para automatizar as etapas envolvidas no processamento de alertas de malware do endpoint ou da rede. O modelo de fluxo inclui condições de gatilho, uma sequência de ações e subfluxos anotados para facilitar a leitura.

Esses modelos contêm uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que são anotados para facilitar a leitura. Para acessar esses fluxos, você deve instalar ospoke das Operações de segurança e o app Palo Alto Networks - WildFire das Operações de segurança a partir do ServiceNow Store.

Nota: Você deve ativar esses modelos antes de usá-los.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os seguintes fluxos e subfluxos estão incluídos:

- Incidente de segurança - Modelo de playbook de malware automatizado: este modelo foi projetado para automatizar as respostas a alertas de malware e contém uma sequência de ações, incluindo um gatilho.
- Incidente de segurança - Modelo manual de malware: este modelo é o fluxo de trabalho de resposta manual a malware existente que é ativado quando a categoria é definida como Atividade de código malicioso.

Subfluxos

- Confirmar ameaça do observável: verifica se os observáveis são mal-intencionados e precisam ser resolvidos.
- Definir gravidade do incidente: define um status de gravidade para o incidente.
- Playbook de ransomware: determina se é um ataque de ransomware.

Esses subfluxos representam um conjunto de operações reutilizáveis que podem ser usadas em vários playbooks. Você pode usar esses subfluxos para definir modelos personalizados (fluxos) de acordo com seus requisitos.

Para criar modelos personalizados (fluxos), siga as instruções em Fluxos .

Executar o fluxo automatizado do playbook de malware

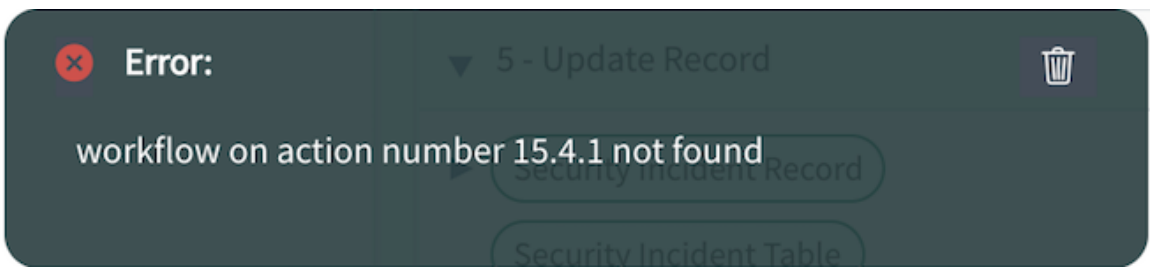
Use este fluxo para automatizar tarefas no playbook para analisar e resolver ataques de malware contra sua organização.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer e action_designer
- Instale e configure as seguintes integrações com as credenciais corretas:
  - Palo Alto Networks WildFire for Security Operations
  - Pesquisa de detecções (Splunk)
  - Bloquear solicitações
  - Pesquisa de ameaças
  - Aprimorar observáveis

  Verifique se essas integrações estão funcionando corretamente antes de ativar o modelo de playbook de incidente de segurança - Automated Malware.

- Aplicativo Security Operations Palo Alto Networks WildFire: para acessar o fluxo do playbook automatizado de malware, você deve instalar o Spoke do Security Operations e o aplicativo Security Operations Palo Alto Networks - WildFire a partir do ServiceNow Store. Se o aplicativo Security Operations Palo Alto Networks WildFire não estiver instalado, você verá um erro "Fluxo de trabalho na ação número 15.4.1 não encontrado", conforme mostrado abaixo:



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você não quiser instalar este aplicativo, exclua as etapas **15.2, 15.3 e 15.4** do fluxo do playbook de malware automatizado.

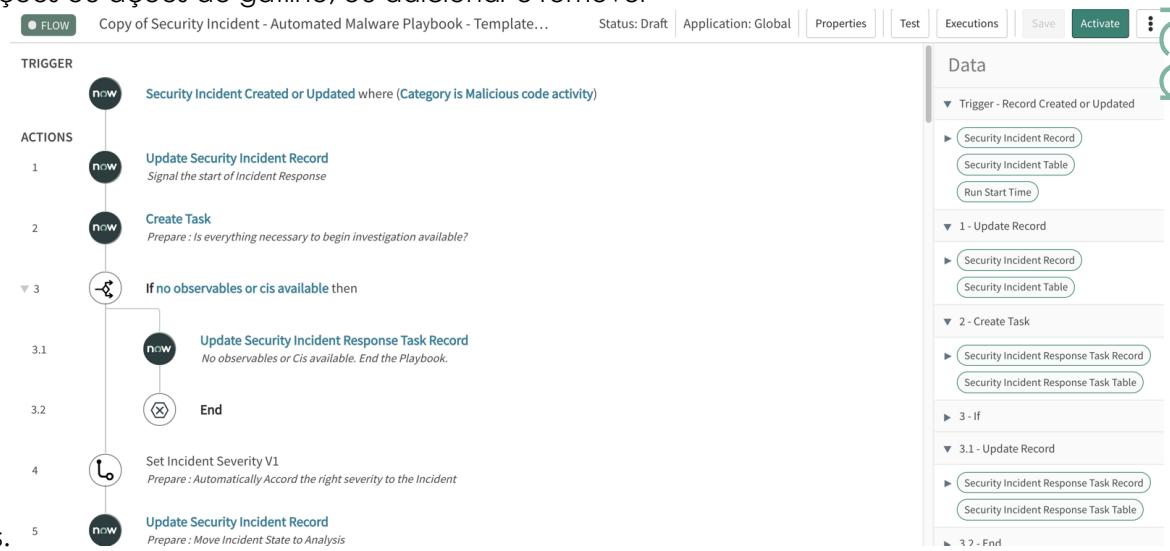
- Certifique-se de que as seguintes condições tenham sido atendidas:
  - O incidente de segurança foi atribuído a um analista de segurança que pertence ao grupo de aprovação apropriado.
  - O analista de segurança que lida com o incidente deve ter um endereço de e-mail válido.
  - Os itens de configuração e observáveis necessários foram adicionados ao incidente de segurança.
- Para **a etapa 21 (Pedir aprovação)**, altere o Grupo de **Atribuição de incidente de segurança** para o seu grupo preferencial.
- A etapa 21 do fluxo é uma etapa de aprovação de tarefa obrigatória em que uma solicitação de aprovação é enviada ao administrador. Para aprovar a solicitação, o administrador deve navegar até a página Aprovações de tarefa e definir o campo Estado como **Aprovado**. Se a tarefa não for aprovada, o Flow Designer não poderá prosseguir e o processo será encerrado.

Por Que e Quando Desempenhar Esta Tarefa

Quando uma atividade de código mal-intencionado é detectada na rede, um incidente de segurança é criado e o fluxo automatizado do playbook de malware é iniciado. Você pode usar as tarefas definidas no fluxo do playbook automatizado de malware para fazer a triagem, analisar, conter e erradicar a ameaça.

Procedimento

1. Navegar até **Todos** > **Flow Designer** > **Designer** para exibir os fluxos disponíveis com o spoke das Operações de segurança.
2. Clique no link **Incidente de segurança - Automated Malware Playbook Template VI**.
3. Na página Fluxo, clique no ícone mais ícone , faça uma cópia do fluxo e abra-o para uso.
   Agora você pode fazer mudanças no fluxo, como modificar condições ou ações do gatilho, ou adicionar e remover ações.

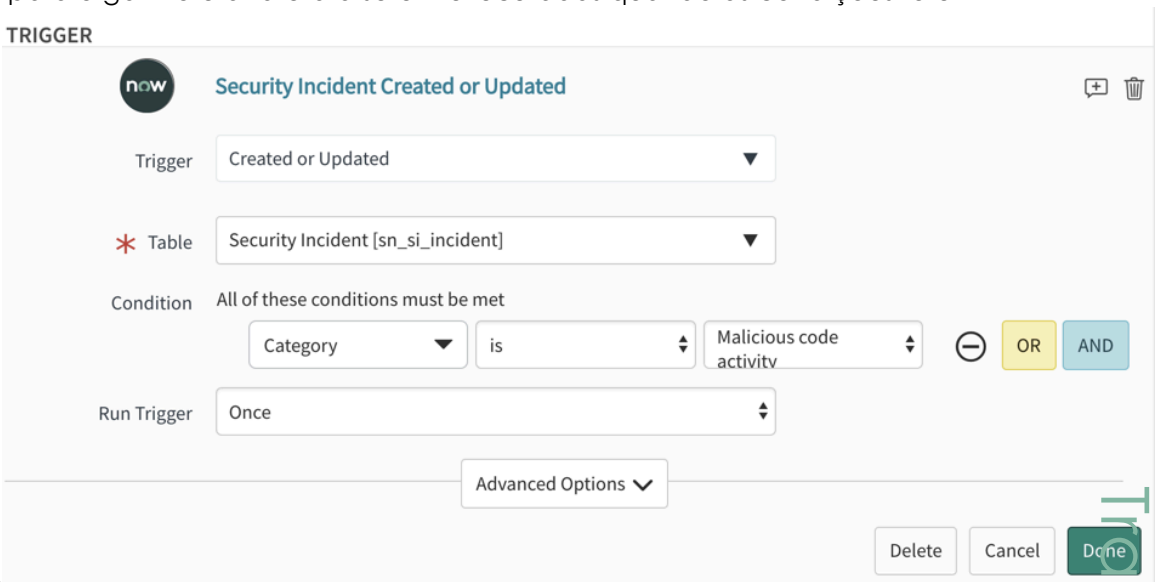


Mostra o gatilho e as etapas que serão executadas com o fluxo. O painel direito mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

Tradução automática

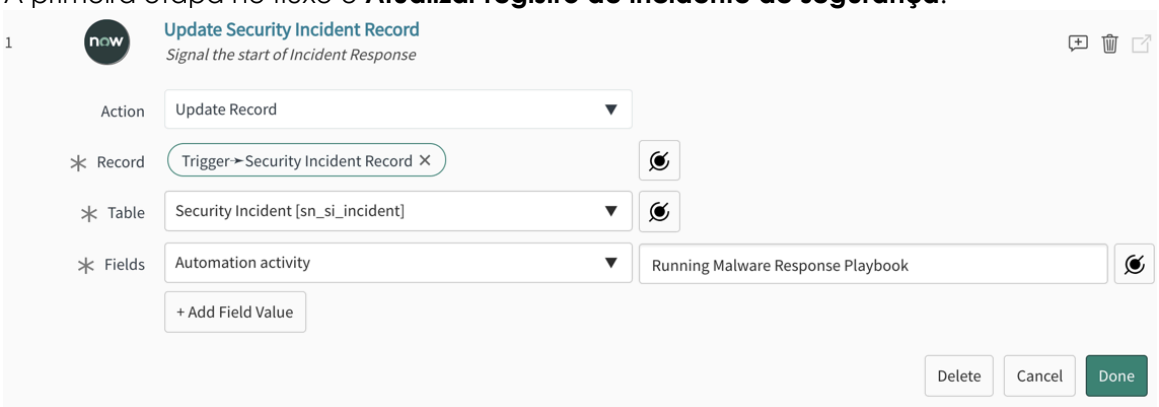
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no ícone do **gatilho**.
   Na primeira etapa, você define ou define o gatilho do fluxo. Especifique as condições para o gatilho e a tarefa a serem executadas quando as condições forem atendidas.



   Quando a condição definida no fluxo (Categoria é a atividade Código malicioso) é atendida no registro do incidente, as tarefas no fluxo de phishing automatizado começam a ser executadas sequencialmente. Você pode modificar o gatilho, adicionar anotações, adicionar ou excluir condições e assim por diante.

5. A primeira etapa no fluxo é **Atualizar registro de incidente de segurança**.

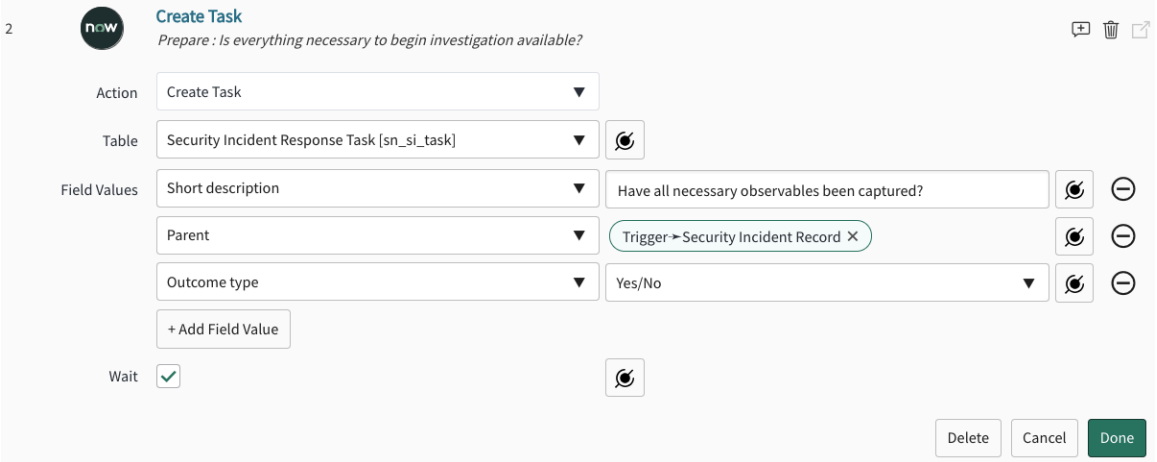


   Clique no link e clique no ícone de anotação Ícone de para adicionar uma anotação ao analista de segurança indicando que houve alguma atividade de código mal-intencionado e que o fluxo do playbook de resposta automatizada a malware começou a ser executado.

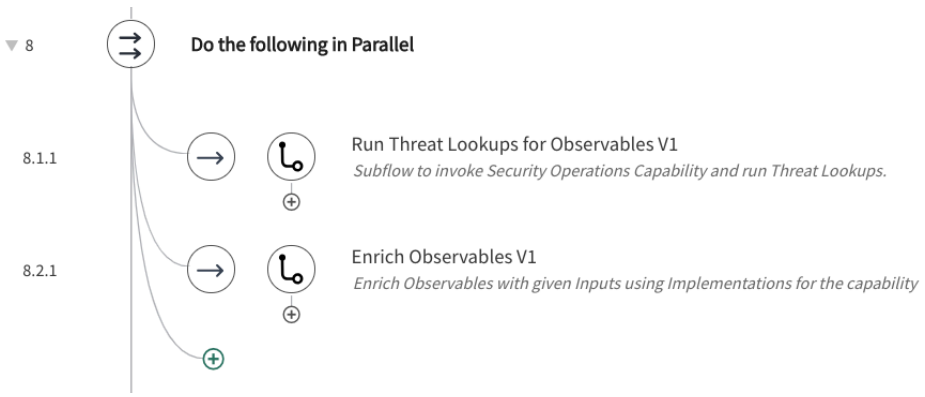
6. Prossiga com a etapa 2 no fluxo e clique no link **Criar tarefa**.

   Nesta etapa, uma tarefa de resposta automatizada é criada para verificar se todos os observáveis necessários foram capturados e se a investigação pode começar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

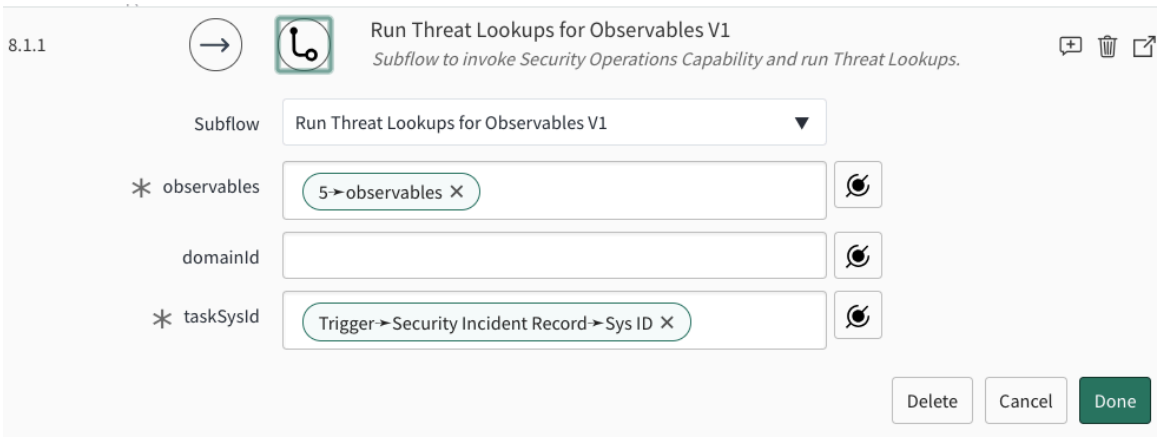


7. Se o Tipo de resultado for **Não**, isso indica que não há observáveis e ICs disponíveis para iniciar a investigação.
   Atualize o registro do incidente de segurança para indicar que o playbook não pode prosseguir.
8. Se o Tipo de resultado for **Sim**, o subfluxo Definir gravidade do incidente atribuirá automaticamente a gravidade correta ao incidente de segurança.
9. Na próxima etapa, o registro do incidente de segurança é atualizado.
10. Na próxima etapa, todos os observáveis envolvidos no incidente ou em uma categoria selecionada são coletados para executar ações automatizadas adicionais nas etapas subsequentes do playbook.
11. Na próxima etapa, uma tarefa de resposta automatizada será criada.
    Esta tarefa captura o início do processo para obter a reputação de todos os observáveis e executar o enriquecimento com integrações configuradas.
12. Na etapa 8, dois subfluxos são chamados:
    - Executar pesquisas de ameaças para observáveis: este subfluxo é usado para obter a reputação de todos os observáveis usando implementações de pesquisa de ameaças.
    - Aprimorar observáveis: este subfluxo é usado para realizar o enriquecimento de observáveis com implementações configuradas.



Observe os ícones para esta tarefa. O ícone de operações paralelas O ícone de indica que ambas as tarefas serão executadas em paralelo e o ícone de subfluxo de subfluxo indica que a tarefa que está sendo executada é um subfluxo, conforme mostrado abaixo:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Observe o número 5 no campo de observáveis. Isso indica que a pesquisa de ameaças será executada em observáveis recuperados na etapa 5. Este subfluxo, por sua vez, chama fluxos de trabalho e ações existentes.

13. Na próxima etapa, a ação Executar a pesquisa de registros é executada.
Esta ação é usada para pesquisar registros de contexto de fluxo de trabalho em que os fluxos de trabalho primários podem ser um dos seguintes.
    - Contexto de fluxo de trabalho abstrato de Pesquisa de ameaças
    - Contexto de Fluxo de Trabalho Abstrato de Aprimoramento de Observável
14. Na próxima etapa, os resultados de reputação e enriquecimento são revisados para cada 8 registros.
15. Continue revisando as próximas etapas:
    a. Atualizar registro de incidente de segurança: atualiza o registro de incidente de segurança para indicar que as atividades de enriquecimento e pesquisa de reputação foram concluídas.
    b. Obter observáveis da tarefa: recupera todos os observáveis maliciosos associados ao incidente de segurança.
    c. Criar tarefa: verifica e confirma se as execuções de triagem automatizadas foram bem-sucedidas.
16. Se houver observáveis que foram sinalizados como mal-intencionados:
    a. Atualizar registro de incidente de segurança: publique uma anotação de trabalho indicando que uma ameaça foi detectada.
    b. Criar consulta de entrada a partir de observáveis: se mais de dez observáveis tiverem sido sinalizados como mal-intencionados, a Pesquisa de detecções no subfluxo de observáveis (em Splunk ou Carbon Black) será executada.
17. Se os observáveis não forem sinalizados como mal-intencionados, o fluxo continuará com as seguintes etapas:
    a. Atualizar registro de incidente de segurança: publique uma anotação de trabalho indicando que nenhuma ameaça foi detectada
    b. Obter observáveis da tarefa: identifica todos os IDs de hash SHA256 do incidente.
    c. Pesquisar registros observáveis: pesquisa registros que atendem a esses critérios.
18. Continue revisando as próximas etapas:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para cada observável mal-intencionado, o fluxo de trabalho **Operações de segurança Palo Alto Networks - Obter aprimoramento de dados do Wildfire** é executado.

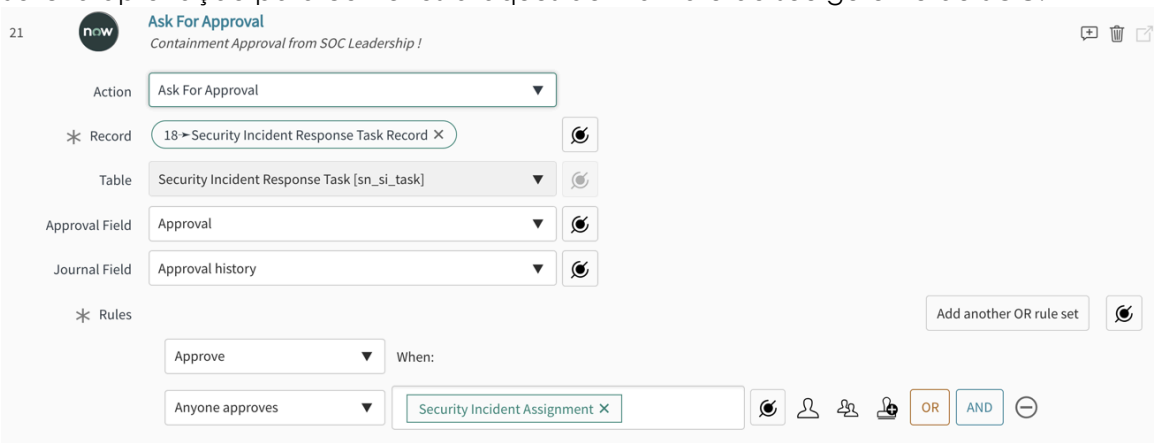
b. Revisa os resultados da investigação para ver se eles são satisfatórios.
Uma tarefa de resposta é criada para verificar se o malware suspeito é um ataque de ransomware. Em caso afirmativo, o subfluxo do Playbook de Ransomware será executado.

c. Na próxima etapa, um e-mail é enviado com um resumo da análise e a solicitação de aprovação para iniciar os procedimentos de contenção.

d. Uma tarefa é criada para capturar detalhes da aprovação solicitada.

e. A próxima etapa é atualizar o registro do incidente de segurança.
Publique uma anotação de trabalho informando ao analista de segurança que a solicitação de aprovação foi feita.

f. Solicita aprovação para conter os ataques de malware do seu gerente de SOC.



Nota: Quando uma solicitação de aprovação for gerada pelo fluxo, a Anotação de trabalho será atualizada com a seguinte mensagem:

`Uma solicitação de aprovação foi feita para<task id> continuando com a contenção.` Para aprovar esta tarefa, como gerente do SOC, siga estas etapas manualmente:

- Navegue até a página Aprovações de tarefa.
- Você verá a lista de aprovações. Clique em<task id> que será aprovado.
- Mude o estado para **Aprovar** e Salvar o atualizado<task id> .

g. Na próxima etapa, o registro do incidente de segurança é atualizado para rastrear o status de aprovação.

h. Em seguida, uma tarefa é criada para iniciar procedimentos de contenção.

i. O subfluxo Executar o Criar solicitações de bloqueio para observáveis maliciosos é executado e um registro de incidente é criado com uma solicitação para recriar o dispositivo infectado e seus ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

j. Em seguida, uma tarefa é criada para executar a pesquisa de detecções para confirmar se o ambiente é seguro.
A pesquisa de detecções é repetida até que nenhuma detecção seja encontrada.

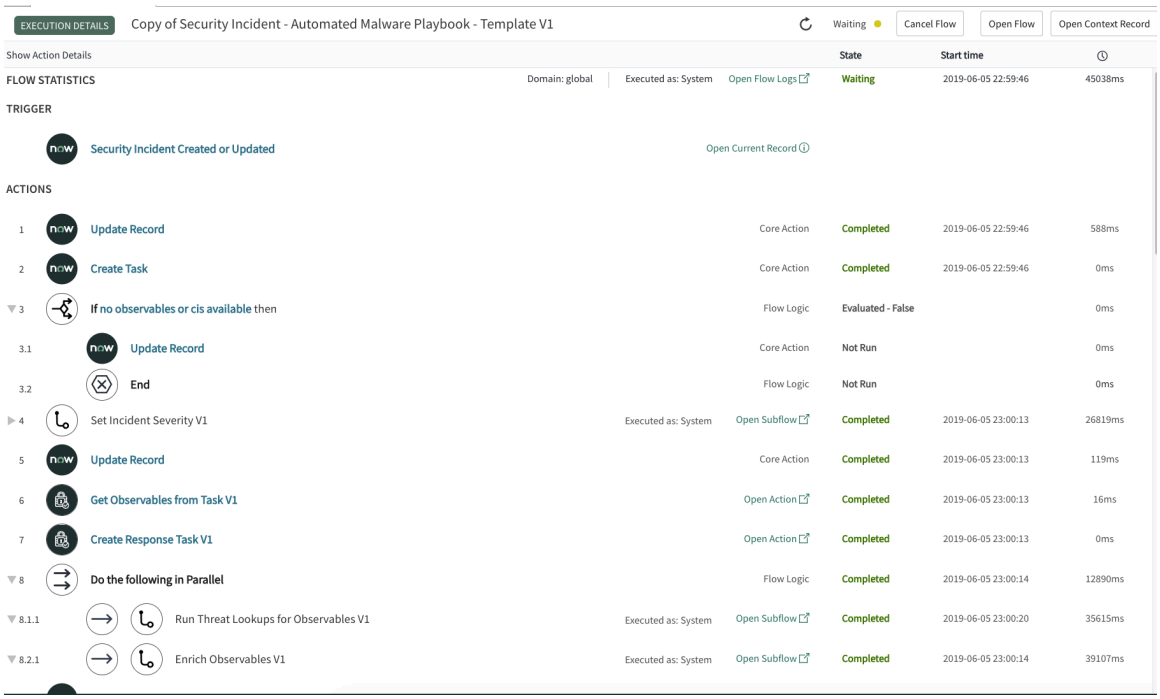
k. Em seguida, uma tarefa é criada para indicar que o registro do incidente de segurança está pronto para revisão.

l. Por fim, o registro é atualizado e movido para a fase Revisão.

O que Fazer Depois

Você pode clicar em **Testar** para simular as ações no fluxo antes que ele seja publicado. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo para que ele possa ser executado.

Clique em **Execuções** para exibir os detalhes de execução do fluxo.



Playbook para login manual com falha

Quando um usuário faz determinadas tentativas de login malsucedidas (de acordo com a configuração do SIM), um incidente de segurança é criado.

Essas tentativas de login malsucedidas podem ser falso-positivos ou tentativas feitas por invasores de obter acesso às contas de e-mail do usuário. Nesses cenários, o playbook de login manual com falha pode fornecer orientação e ajudar a otimizar a investigação de incidentes de segurança de login com falha.

Pré-requisitos

Função necessária:

- sn_si.admin
- flow_designer

Spoke: Instalar Spoke das Operações de segurança (sn_sec_spoke)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidades-chave

O playbook de login com falha cobre os seguintes recursos para investigar incidentes de segurança:

1. Verifica se o usuário afetado é um usuário ativo/inativo
2. Filtra observáveis da lista de permitidos
3. Aprimora os observáveis
4. Executa a pesquisa automatizada de ameaças.
5. Envia e-mail automatizado ao usuário para confirmar a falha na tentativa de login.
6. Atribui tarefas ao analista para investigar o acesso do usuário
7. Identifica observáveis maliciosos e bloqueia IPs e URLs.
8. Redefine a senha do usuário.
9. Atualiza o status do incidente de segurança
10. Atribui tarefas a um analista de segurança para lidar com a revisão pós-incidente.

Capacidades necessárias

- Pesquisa de ameaças (total de vírus, análise híbrida)
- Aprimoramento de observável (Whois, ReverseWhois)
- Pesquisa de detecções (Splunk, QRadar)
- Bloqueio de observável (CheckPoint, Palo Alto)

Para obter mais informações, consulte a ServiceNow Store .

Experiência do analista de segurança

Para entender como resolver ameaças à segurança passo a passo, consulte Resolver ameaças à segurança com o playbook.

Como usar o playbook de login com falha com capacidades do Flow Designer

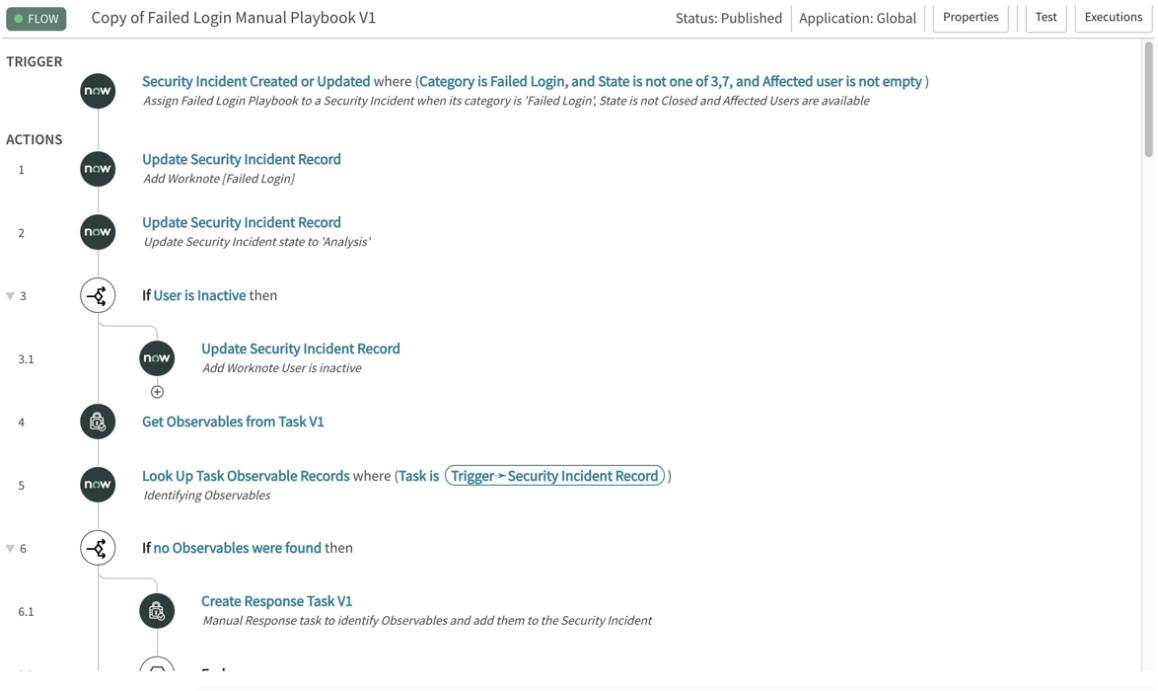
Introdução

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Flow Designer** > **Designer** e clique no playbook de **login com falha**.
3. Faça uma cópia dos fluxos a seguir para copiar o Playbook de login com falha e fazer as modificações necessárias. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
   - Playbook manual de login com falha V1
   - Falha de login - Analisar resposta do usuário e atualizar tarefa de resposta V1
4. Faça as modificações necessárias de acordo com seus requisitos. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
5. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível com o sistema de base.
   - Ative os fluxos copiados depois de fazer modificações de acordo com seus requisitos.

Tradução automática

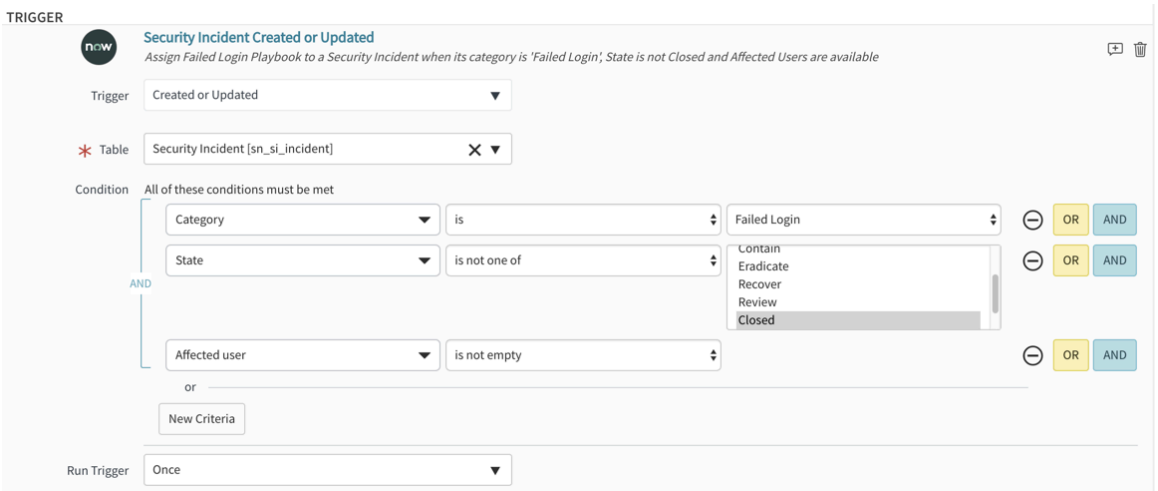
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A imagem a seguir mostra uma cópia do playbook de login manual com falha. Revise as etapas abaixo para entender as várias ações no playbook.



Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- Categoria é login com falha
- Tem um ou mais usuários afetados
- O incidente de segurança não foi encerrado ou cancelado

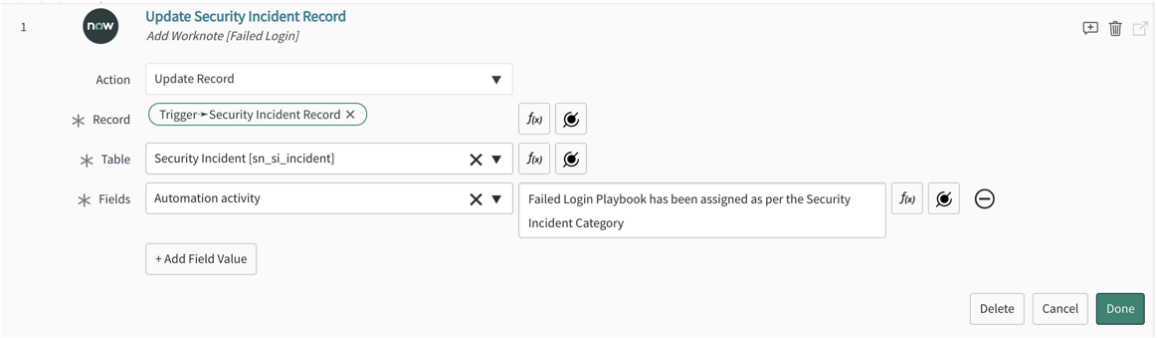


As etapas a seguir orientam você nas ações, tarefas e subfluxos que estão disponíveis no playbook de login manual com falha.

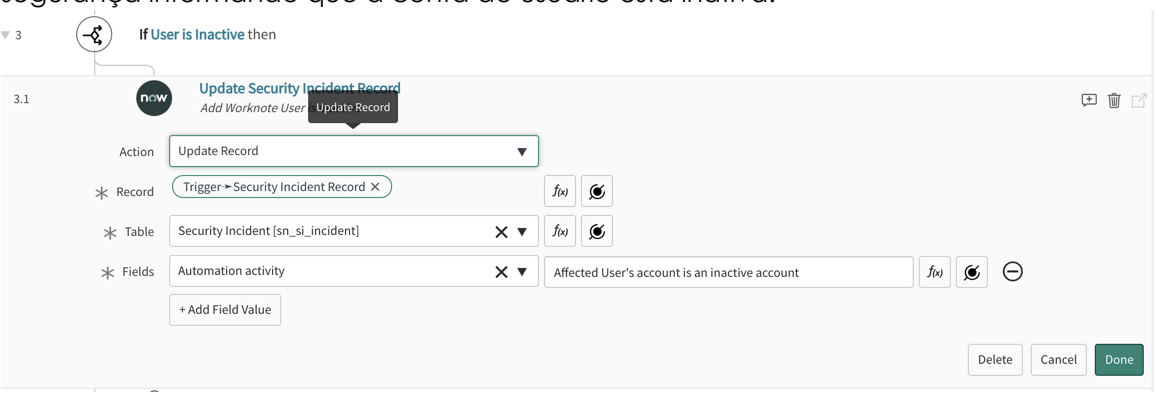
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Quando o playbook começa a ser executado, na Etapa 1, ele é atualizado automaticamente com uma anotação de trabalho mostrando que o incidente de segurança com a categoria de login com falha foi atribuído.



2. Na Etapa 2, o playbook é atualizado e movido para o estado Análise.
3. Na Etapa 3, o playbook verifica se o usuário afetado é um usuário ativo ou inativo. Se o usuário estiver inativo, uma anotação de trabalho será adicionada ao incidente de segurança informando que a conta do usuário está inativa.



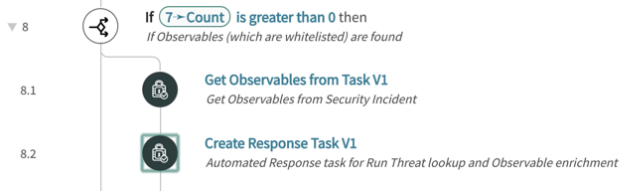
Nota: Na etapa 3 do fluxo, o fluxo verifica os usuários inativos na tabela *sn_si_incident* disponível em ServiceNow. Esta etapa é fornecida como uma diretriz e deve ser modificada para seu ambiente específico. Se você quiser usar essa funcionalidade, recomendamos que tenha uma integração do Active Directory configurada em seu ambiente. Você pode verificar com a integração do Active Directory para encontrar o status do usuário e, dependendo da resposta, você pode projetar as próximas etapas para o seu playbook.

Se você não tiver uma integração do Active Directory, substitua esta etapa por uma tarefa manual para o analista de segurança trabalhar com a equipe de TI para bloquear o usuário e seguir em frente com o restante das etapas do playbook.

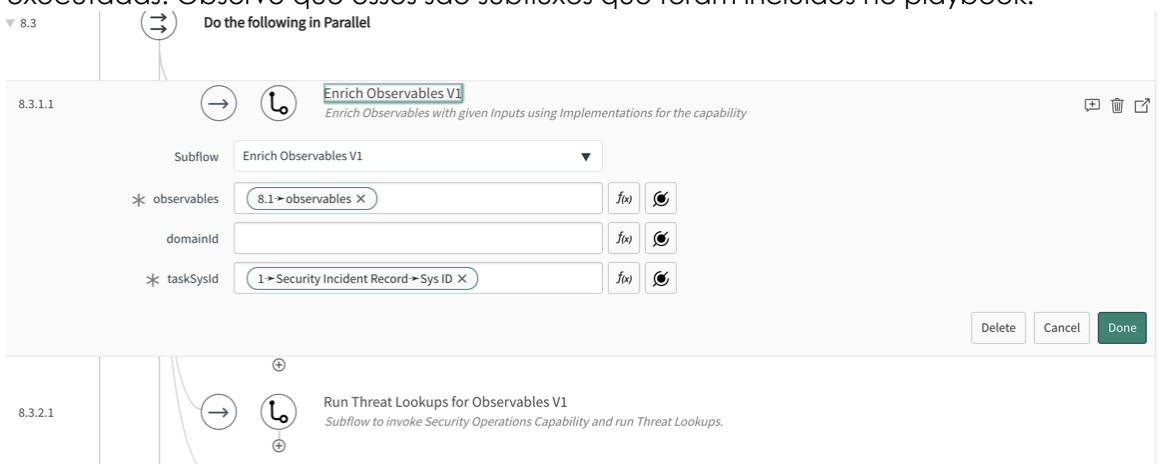
4. Na Etapa 4, os observáveis do incidente de segurança são recuperados.
5. Na Etapa 5, os observáveis são identificados.
6. Se nenhum observável for encontrado, uma tarefa de resposta manual será criada na Etapa 6 e o fluxo será encerrado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Se observáveis forem encontrados na Etapa 7, os observáveis que não são permitidos na lista serão identificados.
8. Se pelo menos um dos observáveis estiver na lista de não permitidos, as seguintes etapas serão executadas:
   a. As etapas 8.1 e 8.2 são executadas. Os observáveis são recuperados e uma tarefa de resposta automatizada é iniciada.

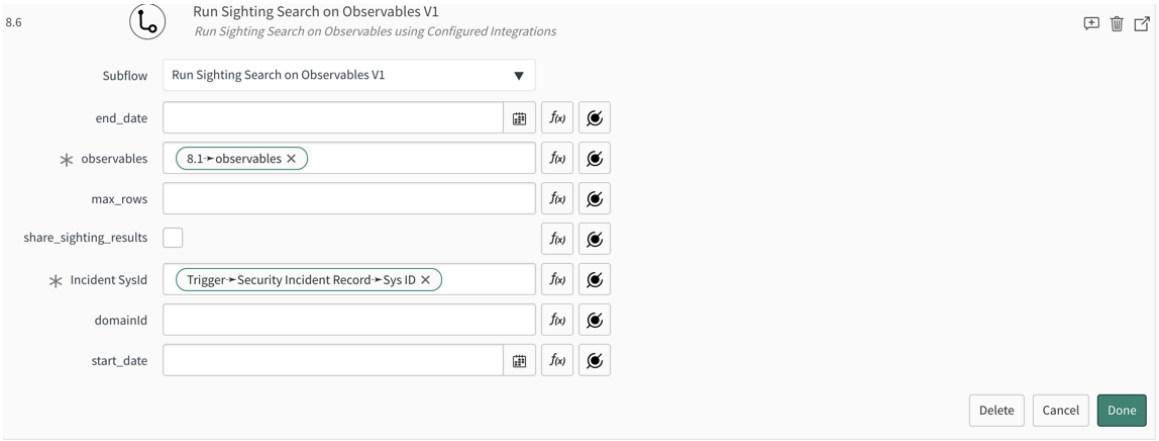


   b. Depois que a tarefa automatizada for criada, a Etapa 8.3 (8.3.1.1 e 8.3.2.1) será executada e as integrações Aprimorar observáveis e Pesquisa de ameaças serão executadas. Observe que esses são subfluxos que foram incluídos no playbook.



   c. Na Etapa 8.4, após a conclusão das integrações, o registro de incidente de segurança é atualizado.
   d. Na Etapa 8.5, uma nova tarefa de resposta é criada para indicar a próxima tarefa automatizada que ocorrerá.
   e. Na Etapa 8.6, a integração da Pesquisa de detecções será executada nos observáveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Depois que o subfluxo Pesquisa de detecções for concluído, na Etapa 8.7, o incidente de segurança será atualizado.

g. Na Etapa 8.8, os observáveis são verificados para ver se são mal-intencionados.

h. Se os observáveis não forem mal-intencionados e se a conta do usuário estiver ativa, um e-mail automatizado será enviado ao usuário para confirmar novamente as tentativas de login malsucedidas. Uma tarefa de resposta manual é criada para identificar os observáveis e adicioná-los ao incidente de segurança. O playbook termina nesta fase.

i. Se os observáveis forem mal-intencionados, três tarefas de resposta serão criadas:

  i. Um e-mail automatizado é enviado ao usuário para confirmar **(sim ou não)** as tentativas de login malsucedidas. Se o usuário responder Sim:

    1. O status do incidente de segurança é atualizado para **Conter**.

    2. Um e-mail automatizado é enviado ao usuário para redefinir a senha.

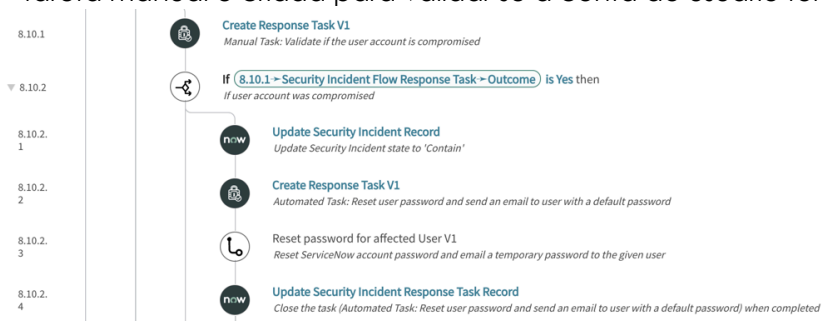
    3. O subfluxo de redefinição de senha é iniciado e um e-mail é enviado ao usuário quando a tarefa é concluída.

> **Nota:** A etapa Redefinir senha é fornecida como uma diretriz. As etapas no fluxo redefinem a senha da conta do usuário no sistema ServiceNow. Mas o processo para redefinir a senha pode ser diferente dependendo do seu ambiente. Você pode verificar com a integração do Active Directory para redefinir a senha dos usuários automaticamente. Se você não tiver uma integração do Active Directory, substitua esta etapa por uma tarefa manual para o analista de segurança trabalhar com a respectiva equipe de TI para redefinir a senha dos usuários e prosseguir com o restante das etapas do playbook após concluir as respectivas tarefa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ii. Se o usuário responder Não, um e-mail automatizado será enviado ao usuário para confirmar novamente a resposta. O analista de segurança precisa executar manualmente as ações apropriadas.

iii. Se o usuário não responder ao e-mail automatizado, o analista de segurança deverá atualizar o incidente de segurança manualmente e fornecer uma resposta. Uma tarefa manual é criada para validar se a conta do usuário foi comprometida.



9. Na Etapa 8.10.3, o estado do incidente de segurança é atualizado.
10. Na Etapa 8.10.4, uma tarefa automatizada é criada para verificar se a implementação da capacidade Criar solicitações de bloqueio para IPs e URLs maliciosos está disponível. Se a implementação da capacidade estiver disponível, o subfluxo Criar solicitações de bloqueio será executado. Se não estiver disponível, o incidente de segurança será atualizado e uma anotação de trabalho será publicada para indicar que a implementação da capacidade não está disponível.
11. Na Etapa 9, o incidente de segurança é atualizado e o estado é definido como **Revisar**.
12. Na Etapa 10, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para automação de incidentes de segurança secundários

Incidentes de segurança duplicados são categorizados como incidentes de segurança secundários e são acumulados nos incidentes de segurança primários.

O playbook de automação de incidentes de segurança secundários ajuda a reduzir o tempo necessário para investigar e fechar incidentes de segurança duplicados. Este playbook acumula automaticamente artefatos exclusivos específicos do incidente de segurança secundário (observáveis, usuários afetados, ICs) para o incidente de segurança primário.

Pré-requisitos

Função necessária:

- sn_si.admin
- flow_designer

Spoke: Instalar Spoke das Operações de segurança (sn_sec_spoke)

Capacidades-chave

O playbook de automação secundária cobre os seguintes recursos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Move o incidente de segurança para a fase de **Análise**.
2. Elimina duplicatas e adiciona (acumula) os usuários e ICs afetados ao incidente de segurança primário.
3. Adiciona observáveis do incidente secundário ao incidente de segurança primário.
4. Encerra ou cancela o incidente de segurança secundário quando o incidente de segurança primário é encerrado.

Capacidades necessárias

Para obter mais informações, consulte a ServiceNow Store .

Experiência do analista de segurança

Para entender como resolver ameaças à segurança passo a passo, consulte Resolver ameaças à segurança com o playbook.

Compreensão mais profunda do playbook de automação de incidentes de segurança secundários com capacidades do Flow Designer

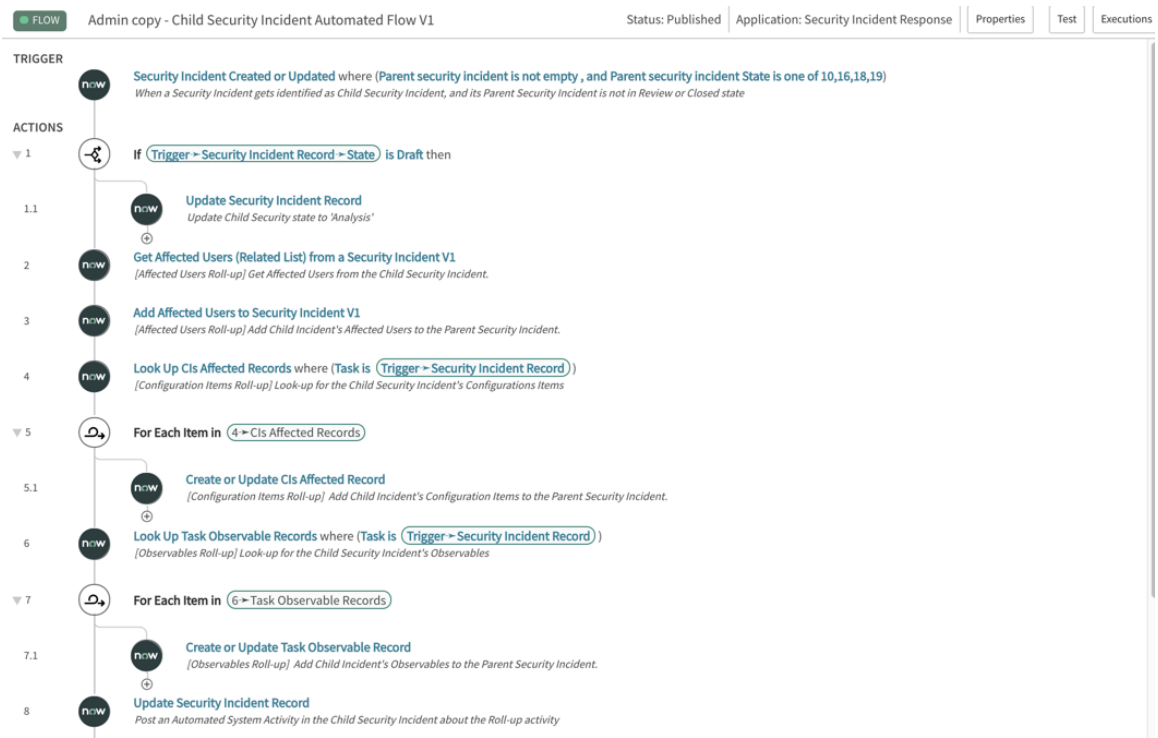
Introdução

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Flow Designer** > **Designer** e clique no playbook de login com falha.
3. Faça uma cópia do playbook de automação de incidentes de segurança secundários e faça as modificações necessárias. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
4. Faça as modificações necessárias de acordo com seus requisitos. (Esta é uma etapa opcional. Siga esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo).
5. Ative o playbook.
   - Ative o fluxo principal para usar o playbook disponível com o sistema de base.
   - Ative o fluxo copiado depois de fazer modificações de acordo com seus requisitos.

A imagem a seguir mostra uma cópia do playbook de automação de incidentes de segurança secundários. Revise as etapas abaixo para entender as várias ações no playbook.

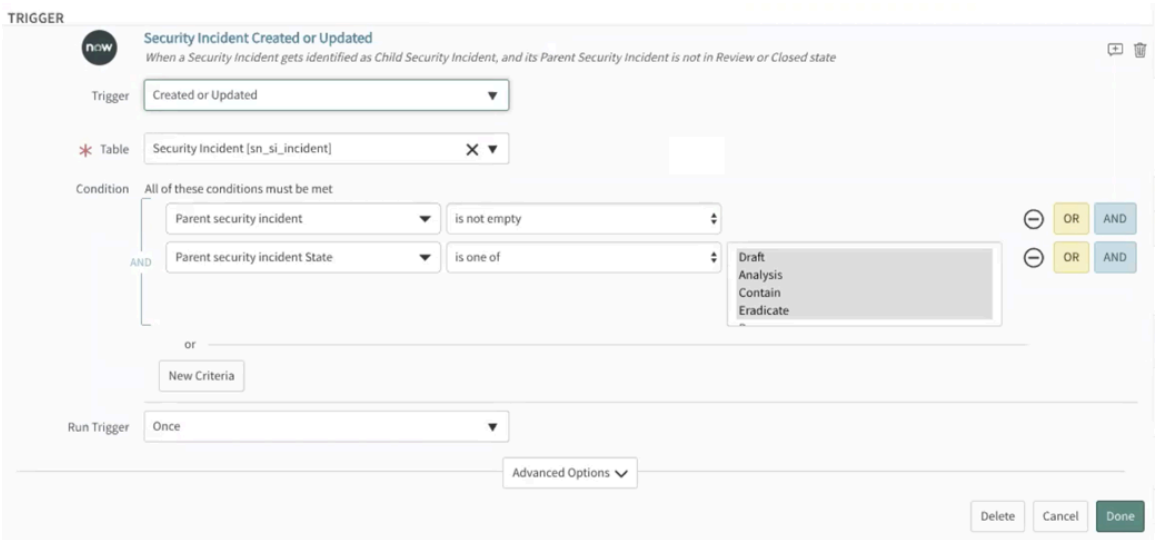
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este playbook é acionado quando:

- O campo de incidente de segurança primário não está vazio.
- O incidente de segurança primário está no estado Rascunho, Análise, Conter ou Eliminar.

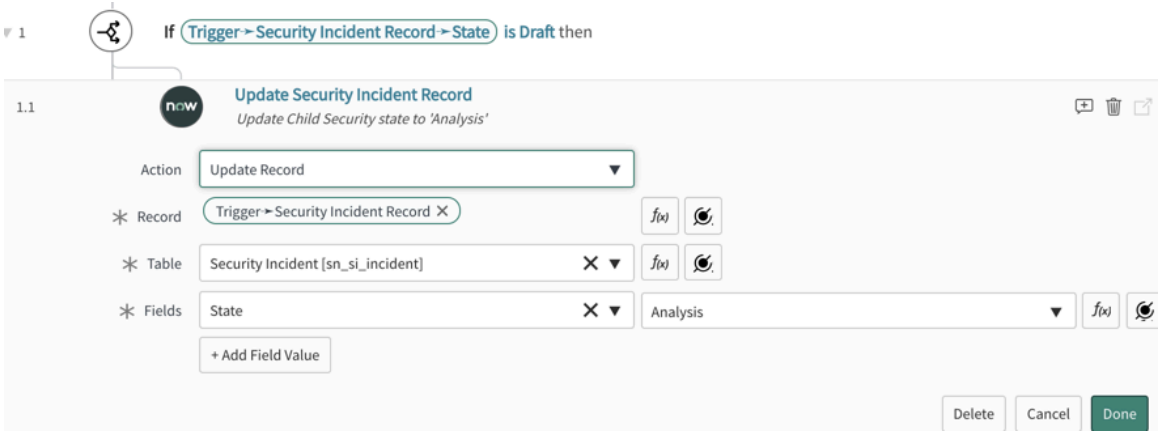


As etapas a seguir orientam você nas ações e tarefas que estão disponíveis no playbook de automação de incidentes de segurança secundários.

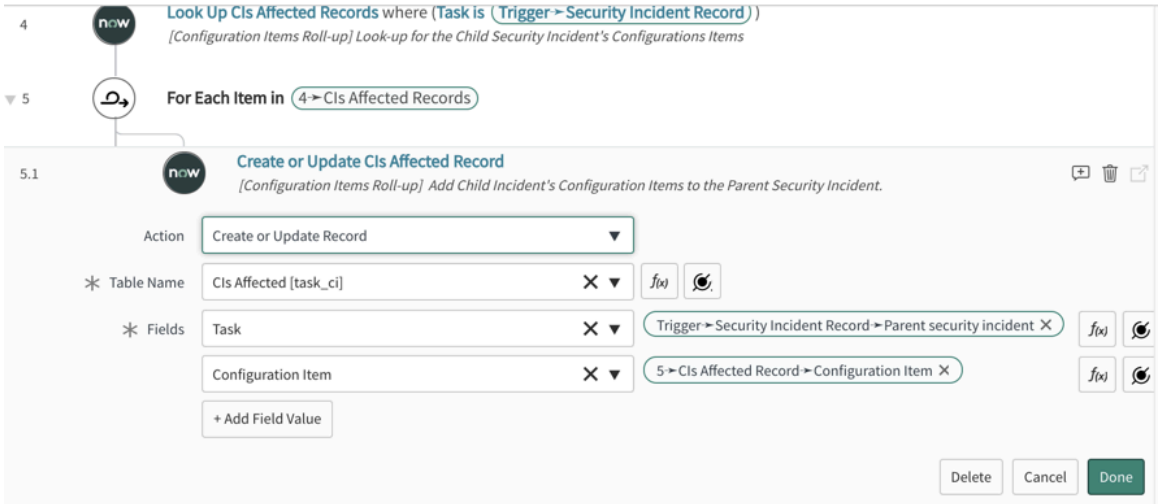
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Quando o playbook começar a ser executado, na Etapa 1, se o incidente de segurança estiver no estado Rascunho, ele será atualizado e definido para o estado Análise.

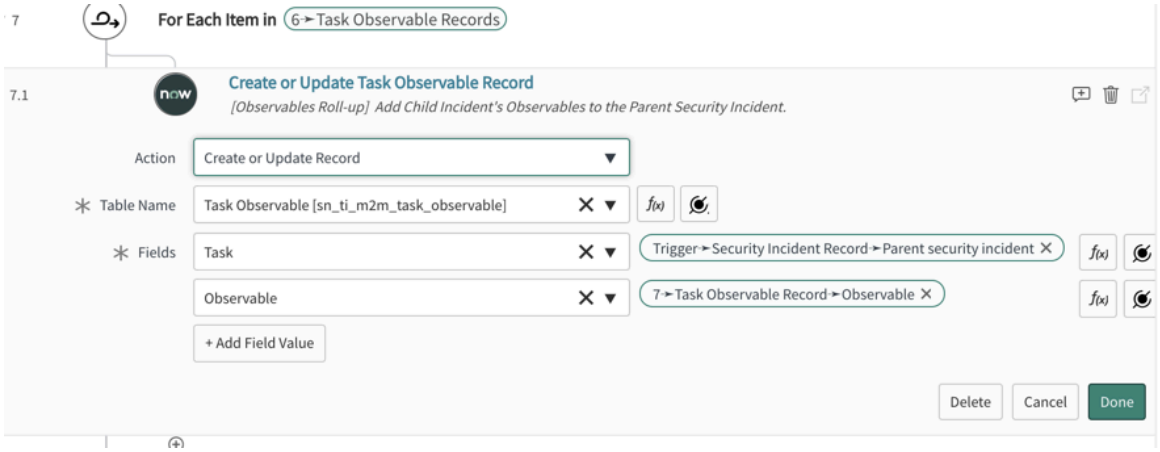


2. Nas etapas 2 e 3, os usuários afetados pelo incidente de segurança são recuperados e acumulados para o incidente de segurança primário. Todos os usuários duplicados são eliminados.
3. Nas etapas 4 e 5, os itens de configuração associados ao incidente de segurança secundário são recuperados e os ICs exclusivos são acumulados para o incidente de segurança primário.



4. Nas etapas 6 e 7, os observáveis associados ao incidente de segurança secundário são recuperados e os observáveis exclusivos são acumulados para o incidente de segurança primário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Nas etapas 8 e 9, anotações de trabalho automatizadas são publicadas nos incidentes de segurança primários e secundários, indicando que os usuários, itens de configuração e observáveis afetados foram acumulados do incidente de segurança primário.

Playbook for Office 365 - Arquivo malicioso detectado

Este playbook fornece etapas de correção sistemática para investigar arquivos mal-intencionados detectados no Office 365.

Quando arquivos mal-intencionados são detectados no Office 365, você pode usar o playbook 365 - Arquivo mal-intencionado detectado no Flow Designer para obter orientação e ajudar a otimizar a investigação desses arquivos mal-intencionados.

Configurar o playbook de arquivo malicioso detectado do Office

Use as etapas a seguir para configurar o playbook Arquivo malicioso detectado do Office.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

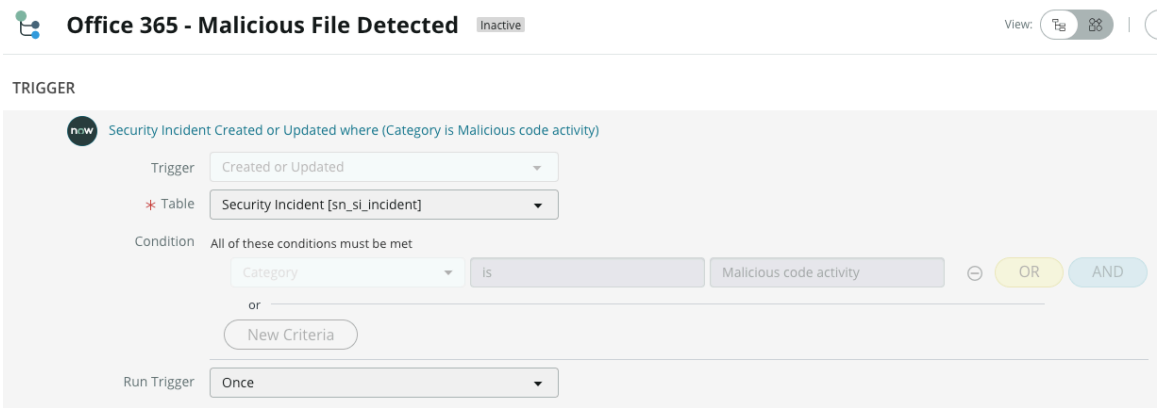
1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **Office 365 - Arquivo malicioso detectado**.
3. Opcional: Você pode criar uma cópia do fluxo do playbook do Office 365 - Arquivo malicioso detectado e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando a **categoria** é uma **atividade de código malicioso**.



Use o playbook de arquivo malicioso detectado do Office 365

Use este playbook para investigar arquivos mal-intencionados detectados no Office 365. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Arquivos maliciosos detectados do Office 365.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

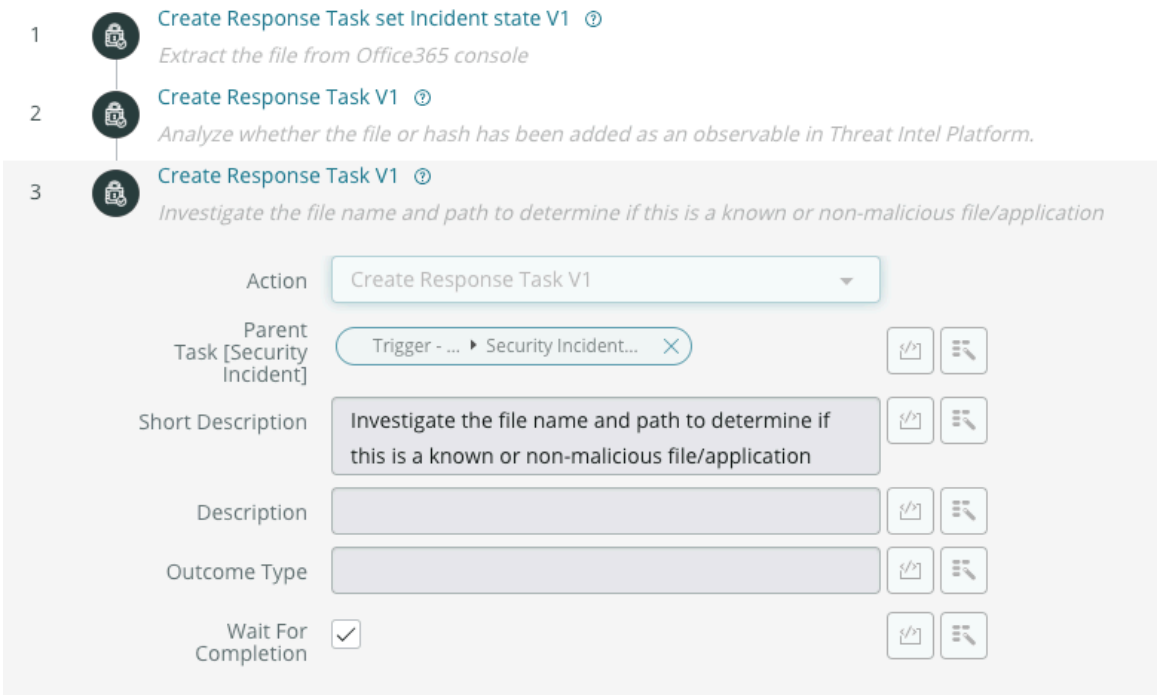
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa extrair o arquivo mal-intencionado do console do Office 365.
2. Na Ação 2, você precisa analisar se o arquivo ou hash foi adicionado como um observável na plataforma de inteligência contra ameaças.
3. Na Ação 3, você precisa investigar o nome e o caminho do arquivo para determinar se é uma aplicação/arquivo conhecido ou não malicioso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de arquivo malicioso detectado do Office 365

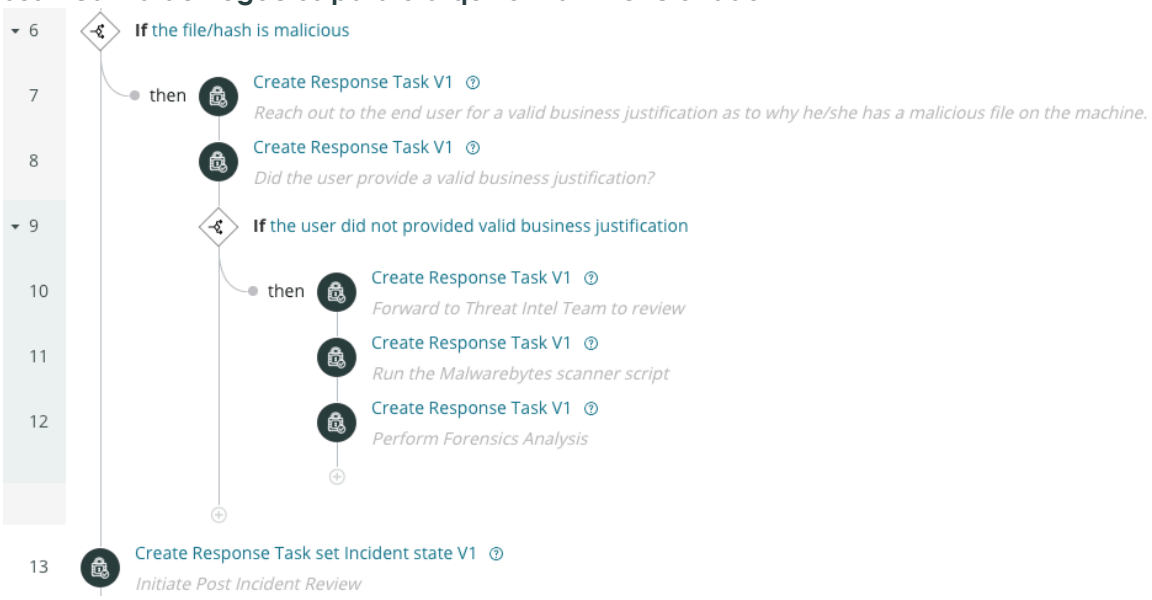


4. Na Ação 4, você precisa enviar o arquivo para a Sandbox para analisar os resultados.
5. Na Ação 5, com base na investigação feita até o momento, você precisa verificar se o arquivo ou hash é mal-intencionado ou não.
   Se o arquivo ou hash não for mal-intencionado, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.
6. Na Ação 6, se o arquivo ou hash for mal-intencionado, as Ações 7 e 8 serão executadas.
7. Na Ação 7, você precisa entrar em contato com o usuário final para obter uma justificativa comercial válida do motivo pelo qual ele tem um arquivo mal-intencionado no dispositivo.
   Se o arquivo ou hash for mal-intencionado, você poderá usar o modelo de e-mail pré-existente no playbook para enviar um e-mail ao usuário final solicitando esclarecimentos.
8. Na Ação 8, você precisa verificar se o usuário final forneceu uma justificativa de negócios válida ou não.
   Se o usuário final forneceu uma justificativa de negócios válida, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.
9. Na Ação 9, se o usuário não forneceu uma justificativa de negócio válida, as Ações 10, 11 e 12 serão executadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Justificativa de negócios para o arquivo mal-intencionado



10. Na Ação 10, como não havia justificativa de negócio válida, você pode encaminhar o arquivo ou hash mal-intencionado para a equipe de informações sobre ameaças para revisão.
11. Na Ação 11, você precisa executar o script do scanner de bytes de malware para verificar se o arquivo ou hash é mal-intencionado.
12. Na Ação 12, você precisa executar uma análise forense para verificar se o arquivo ou hash é mal-intencionado.
13. Na Ação 13, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de repetição

Este playbook ajuda a determinar se a resposta do incidente foi fornecida em um relatório de phishing exato ou semelhante no passado e funciona automaticamente no novo relatório de forma semelhante.

O playbook de detecção de repetição verifica se o incidente de phishing relatado recentemente se parece com um incidente anterior. Quando a detecção de repetição é identificada, o incidente de segurança correspondente e os detalhes da resolução são fornecidos ao analista, que pode usá-los no incidente recém-relatado, resultando em uma correção rápida do incidente de segurança.

Configurar o playbook de detecção de repetição

Use as etapas a seguir para configurar o playbook de detecção de repetição.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*). Você tem a opção de modificar as seguintes propriedades do sistema:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- *sn_sec_spoke.similarphish.earlyterminationspontuação*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparisonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook de **detecção de repetição**.
3. Opcional: Você pode criar uma cópia do fluxo do playbook de detecção de repetição e fazer as modificações necessárias.

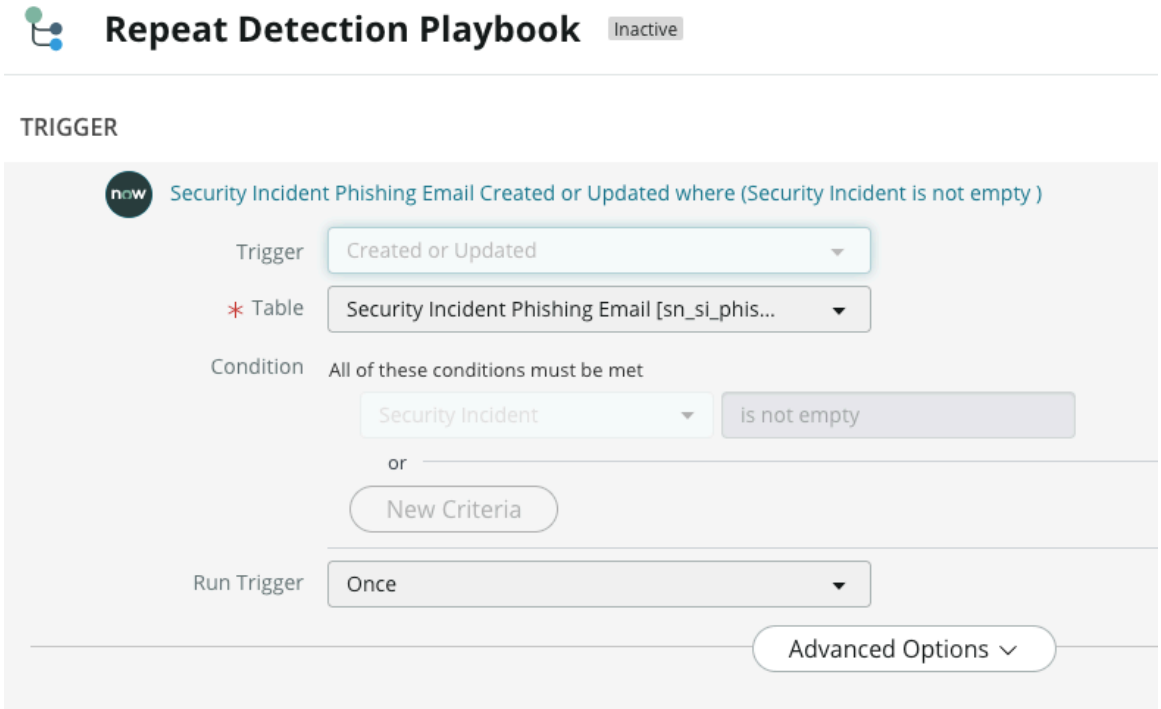
   Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado quando o **incidente de segurança não está vazio**.



Usar o playbook de detecção de repetição

Use este playbook para investigar se a resposta do incidente foi fornecida em um relatório de phishing exato ou semelhante no passado e funciona automaticamente no novo relatório de forma semelhante. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de repetição.

Antes de Iniciar

Função necessária:

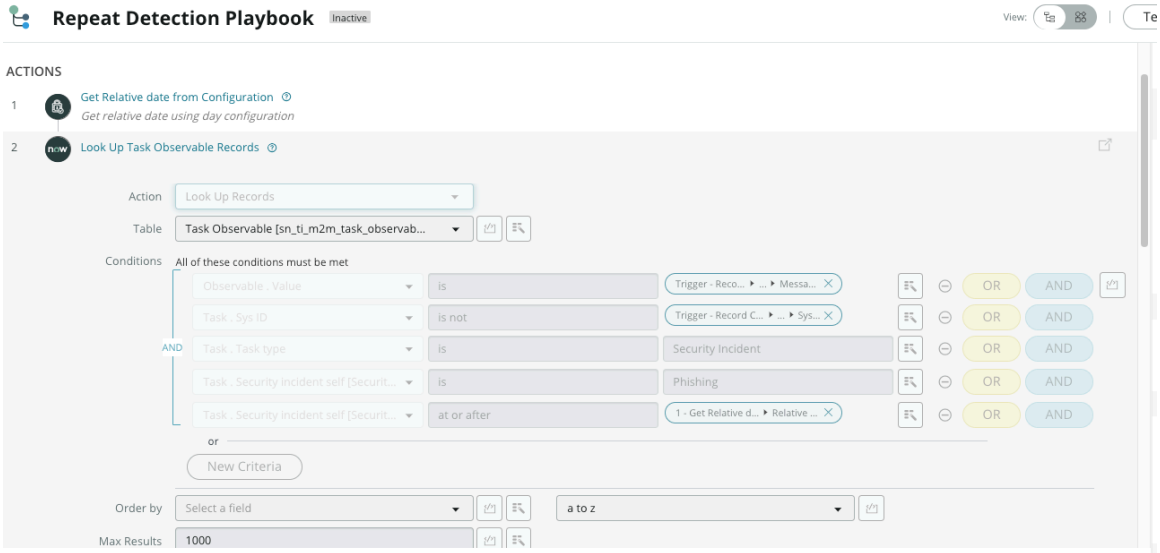
- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, o playbook recupera a data relativa do incidente de segurança usando a configuração de dia.
2. Na Ação 2, o playbook pesquisa os registros do observável de tarefa na tabela *sn_ti_m2m_task_observable* que correspondem ao incidente com base no ID da mensagem.

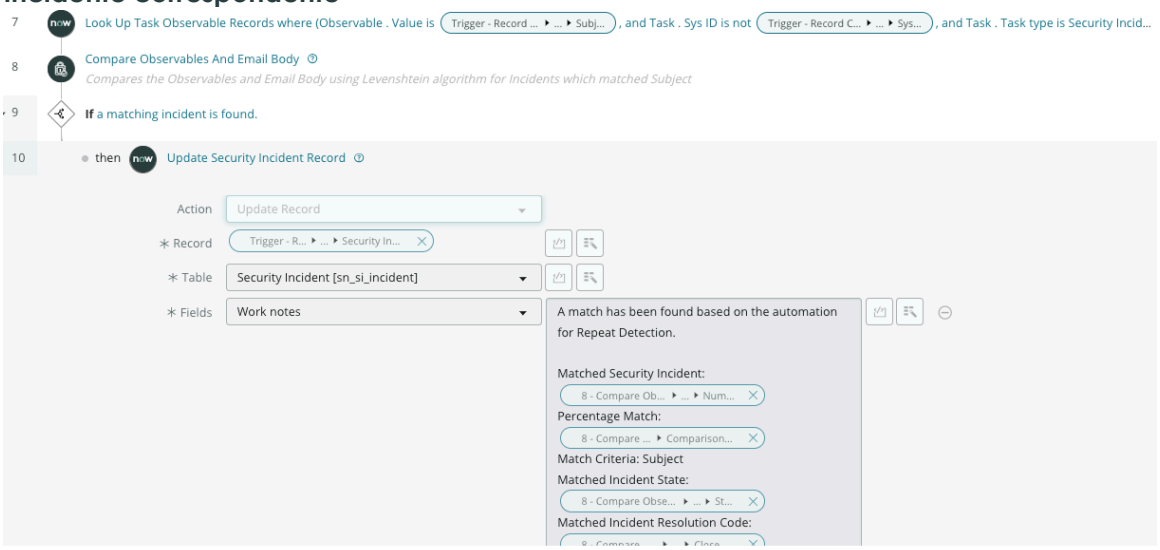
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de detecção de repetição



3. Na Ação 3, o playbook compara os observáveis da tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao ID da mensagem.
4. Na Ação 4, com base na investigação feita até o momento, o playbook verifica se o incidente correspondente foi encontrado com base na ID da mensagem ou não. Na Ação 5, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho de que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Ação 6, o fluxo termina.
5. Se o incidente correspondente não for encontrado, na Ação 7, o playbook pesquisará os registros do observável de tarefa na tabela *sn_ti_m2m_task_observable* que correspondem ao incidente com base no assunto.
6. Na Ação 8, o playbook compara os observáveis da tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao assunto.
7. Na Ação 9, o playbook verifica se o incidente correspondente foi encontrado ou não. Na Ação 10, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho de que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Ação 11, o fluxo termina.

Incidente correspondente



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Na Ação 12, o playbook pesquisa os registros do observável de tarefa na tabela *sn_ti_m2m_task_observable* que correspondem ao incidente com base no endereço.
9. Na Ação 13, o playbook compara os observáveis de tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao endereço.
10. Na Ação 14, o playbook verifica se o incidente correspondente foi encontrado com base no Endereço ou não.
    Na Ação 15, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho de que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Ação 16, o fluxo termina.

Playbook para e-mails falsificados (usando o mesmo nome de exibição)

Este playbook fornece etapas de correção sistemática para investigar e-mails falsificados, que são acionados quando nomes falsificados de e-mails são enviados para os funcionários da organização.

Configurar o playbook de e-mails falsificados

Use as etapas a seguir para configurar o playbook de e-mails falsificados.

Antes de Iniciar

Função necessária:

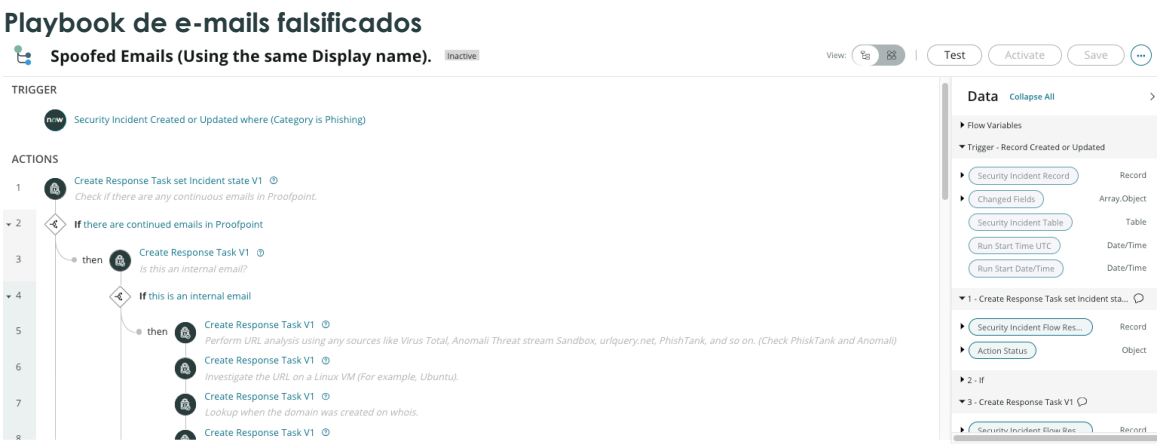
- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **E-mails falsificados (usando o mesmo nome de exibição)**.
3. Opcional: Você pode criar uma cópia do fluxo do playbook de detecção de repetição e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



4. Ative os playbooks.

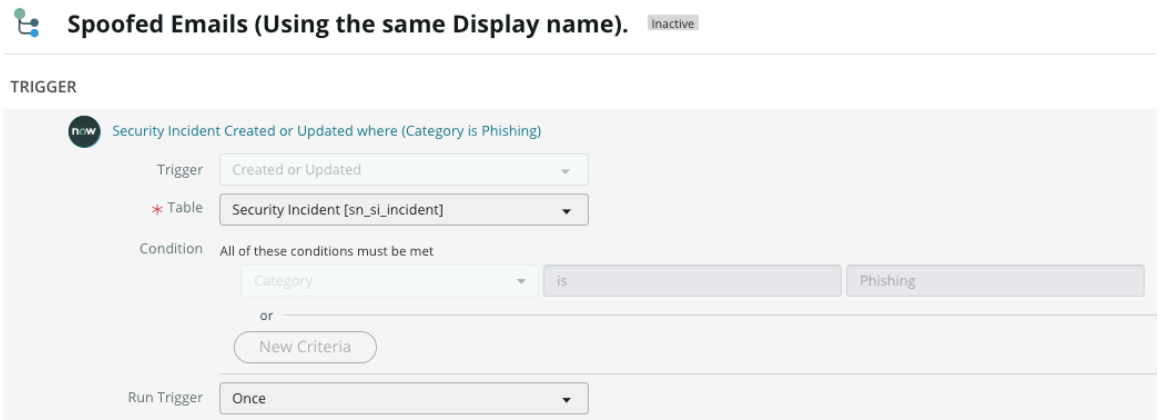
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ative o fluxo principal para usar o playbook disponível no sistema de base.
- Ative os fluxos copiados depois de fazer as mudanças necessárias.

5. Defina uma **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando a **categoria** é **Phishing**.



Usar o playbook de e-mails falsificados (usando o mesmo nome de exibição)

Use este playbook para investigar e-mails falsificados, que são acionados quando nomes falsificados de e-mails são enviados para os funcionários da organização. As etapas a seguir fornecem instruções das ações, tarefas e subfluxos que estão disponíveis no playbook de e-mails falsificados (usando o mesmo nome de exibição).

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se há e-mails falsificados contínuos no Proofpoint.
2. Na Ação 2, se houver e-mails contínuos no Proofpoint, verifique se este é um e-mail interno falsificado ou não.
3. Na Ação 3, se este for um e-mail falsificado interno, execute as seguintes ações:

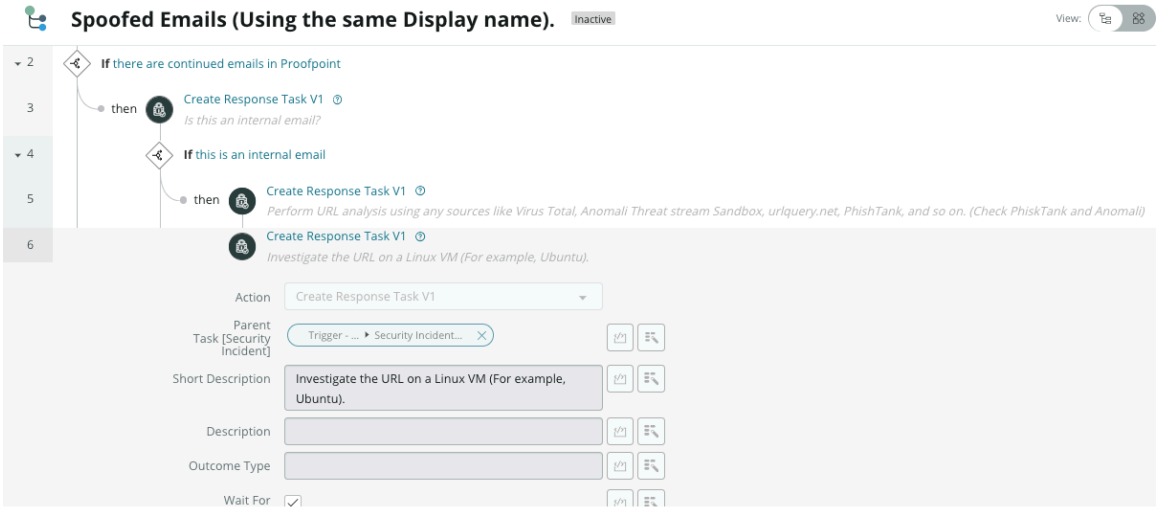
   a. Na Ação 5, você precisa executar a análise de URL usando todas as origens, como Total de vírus, Sandbox de fluxo de ameaças anômalas, urlquery.net, PhishTank (por exemplo, verifique PhiskTank e Anomali).

   b. Na Ação 6, você precisa investigar o URL em uma VM Linux (por exemplo, Ubuntu).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

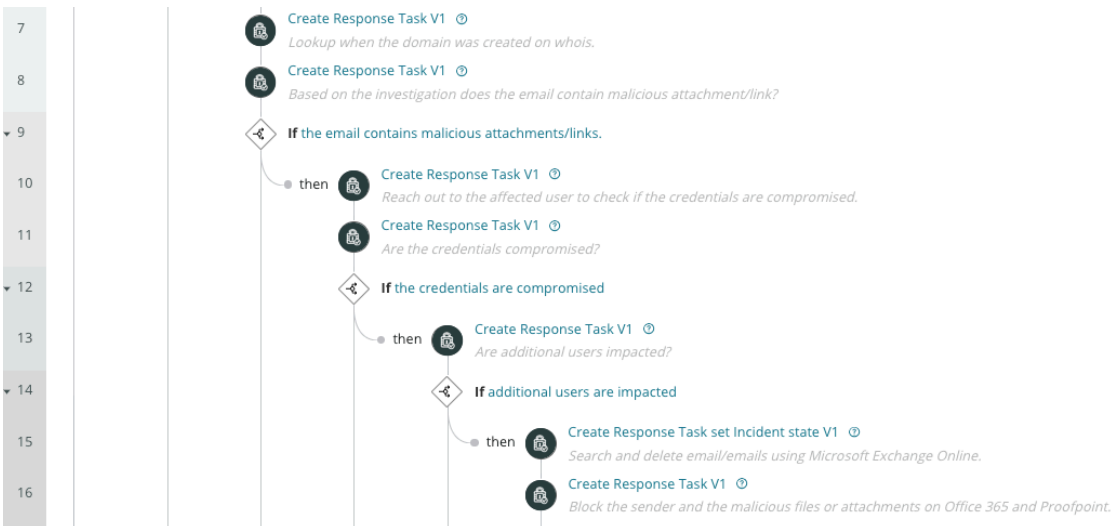
Playbook de e-mails falsificados (usando o mesmo nome de exibição)



c. Na Ação 7, você precisa pesquisar quando o domínio foi criado no WHOIS.
Procure domínios registrados recentemente (na última semana) que sejam suspeitos e tenham uma alta probabilidade de ataques de phishing.

d. Na Ação 8, com base na investigação feita até o momento, você precisa verificar se este e-mail contém um link ou anexo malicioso.
Se este e-mail não contiver um anexo ou link mal-intencionado, o fluxo será encerrado.

O e-mail falsificado contém anexos ou links maliciosos



e. Na Ação 9, se o e-mail contiver anexos ou links mal-intencionados, execute as ações a seguir.

i. Na Ação 10, você precisa entrar em contato com o usuário afetado para verificar se as credenciais estão comprometidas. Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário afetado.

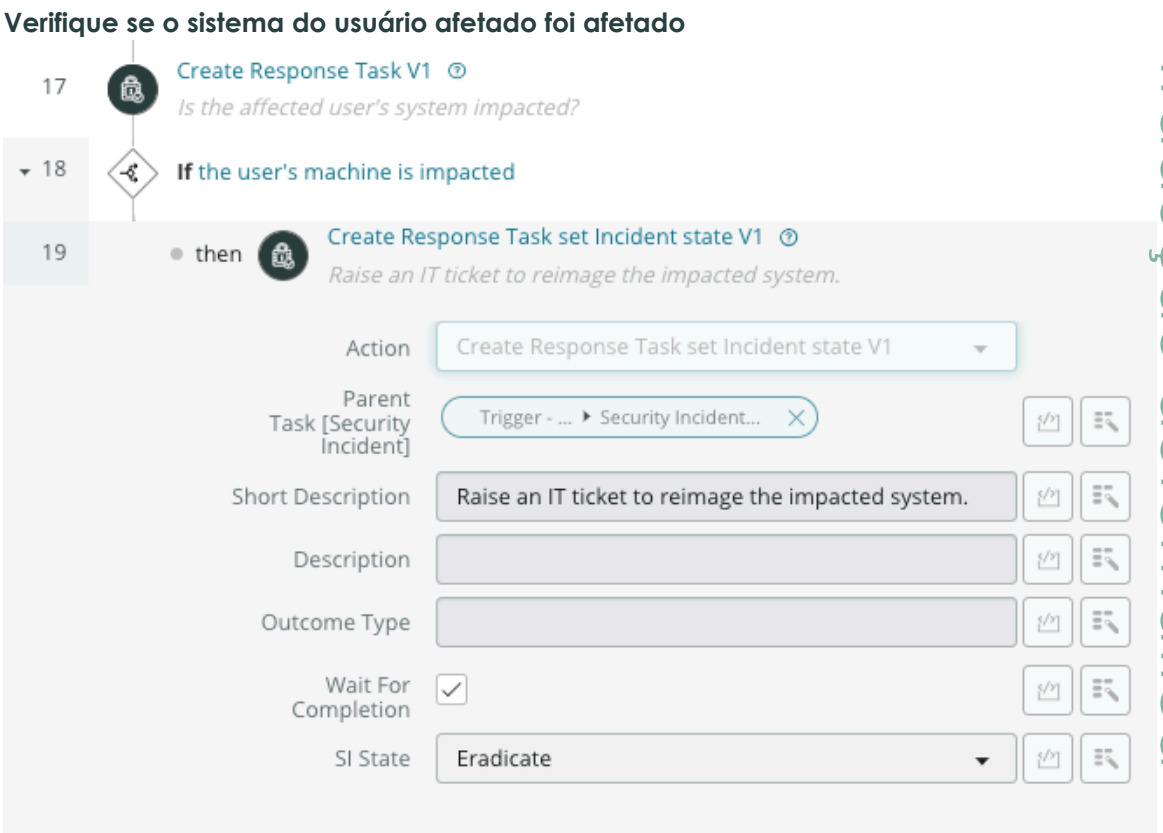
ii. Na Ação 11, você precisa verificar se as credenciais estão comprometidas com base na resposta do e-mail. Se as credenciais não foram comprometidas, o fluxo será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Na Ação 12, se as credenciais estiverem comprometidas, na Ação 13, você precisará verificar se usuários adicionais foram afetados. Se nenhum usuário adicional for afetado, o fluxo será encerrado.
2. Na Ação 14, se usuários adicionais forem afetados, execute as seguintes ações:
   a. Na Ação 15, você precisa pesquisar e excluir e-mails usando o Microsoft Exchange Online.
   b. Na Ação 16, você precisa bloquear o remetente e os arquivos ou anexos mal-intencionados no Office 365 e no Proofpoint.

4. Na Ação 17, se este não for um e-mail interno falsificado, você precisará verificar se o sistema do usuário afetado foi afetado.
5. Na Ação 18, se o sistema do usuário for afetado, na Ação 19, gere um tíquete de TI para recriar a imagem do sistema afetado.



6. Na Ação 20, uma tarefa de resposta é criada para você concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de endpoint

Este playbook fornece etapas de correção sistemática para investigar alertas de malware acionados em um host ou endpoint (por exemplo, uma detecção de arquivo mal-intencionado).

Quando os alertas do CrowdStrike são acionados em um host ou endpoint, você pode usar o playbook de detecção de endpoint no Flow Designer para obter orientação e ajudar a otimizar a investigação desses arquivos mal-intencionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o playbook de detecção de endpoint

Use as etapas a seguir para configurar o playbook de detecção de endpoint.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

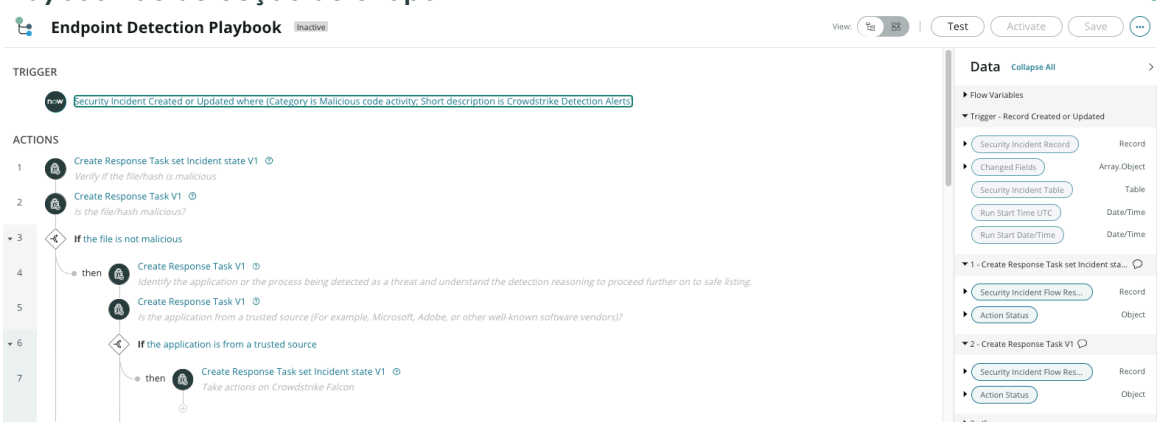
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook de **detecção de endpoint**.
3. Opcional: Você pode criar uma cópia do fluxo do playbook de detecção de endpoint e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   Playbook de detecção de endpoint

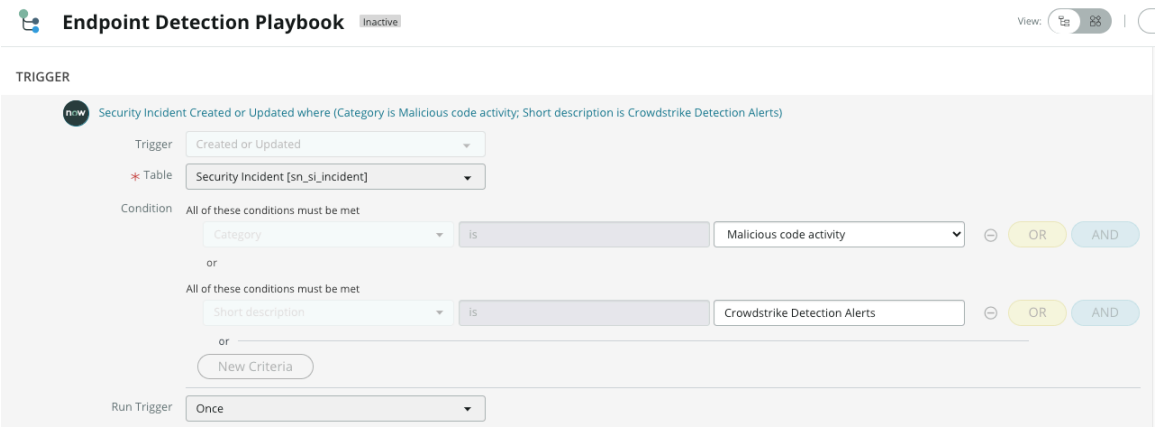
   

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A **categoria** é **atividade de código malicioso**.
- **A descrição resumida** é **Alertas de detecção do CrowdStrike**.



Usar o playbook de detecção de endpoint

Use este playbook para investigar alertas de malware acionados em um host ou endpoint. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de endpoint.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

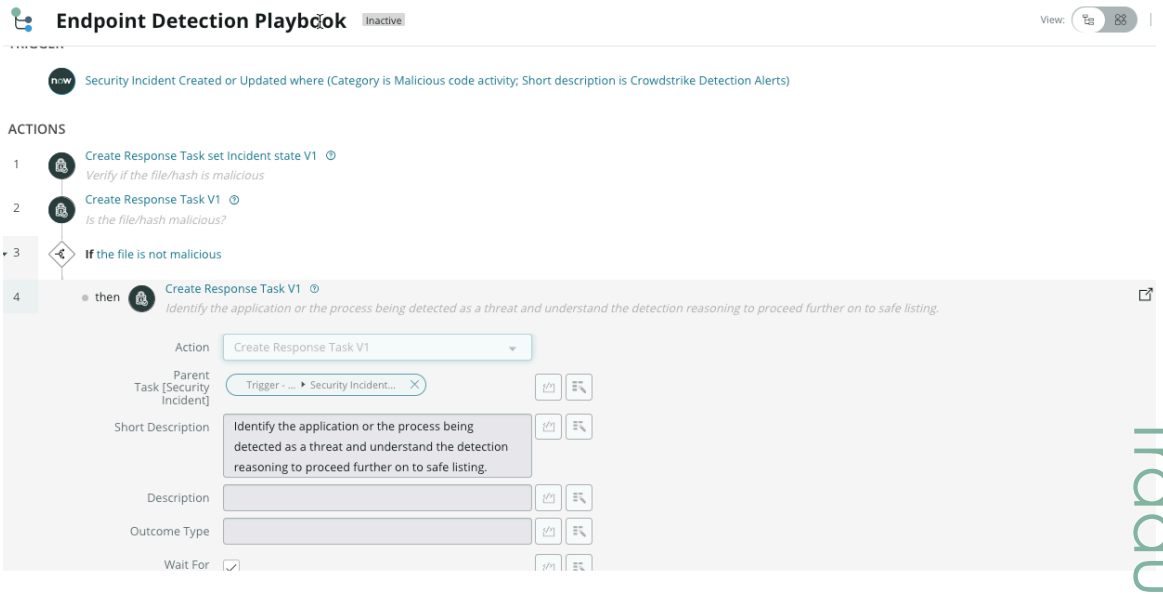
1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se o arquivo ou hash é mal-intencionado analisando os resultados da pesquisa de ameaças no SIR e coletando informações de VirusTotal, WildFire, ThreatCrowd etc.
2. Na Ação 2, você precisa verificar se o arquivo ou hash é mal-intencionado ou não.
3. Na Ação 3, se o arquivo ou hash for mal-intencionado, execute as seguintes ações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 4, você precisa identificar a aplicação ou o processo que está sendo detectado como uma ameaça e coletar informações sobre o raciocínio da detecção para prosseguir para a listagem segura.

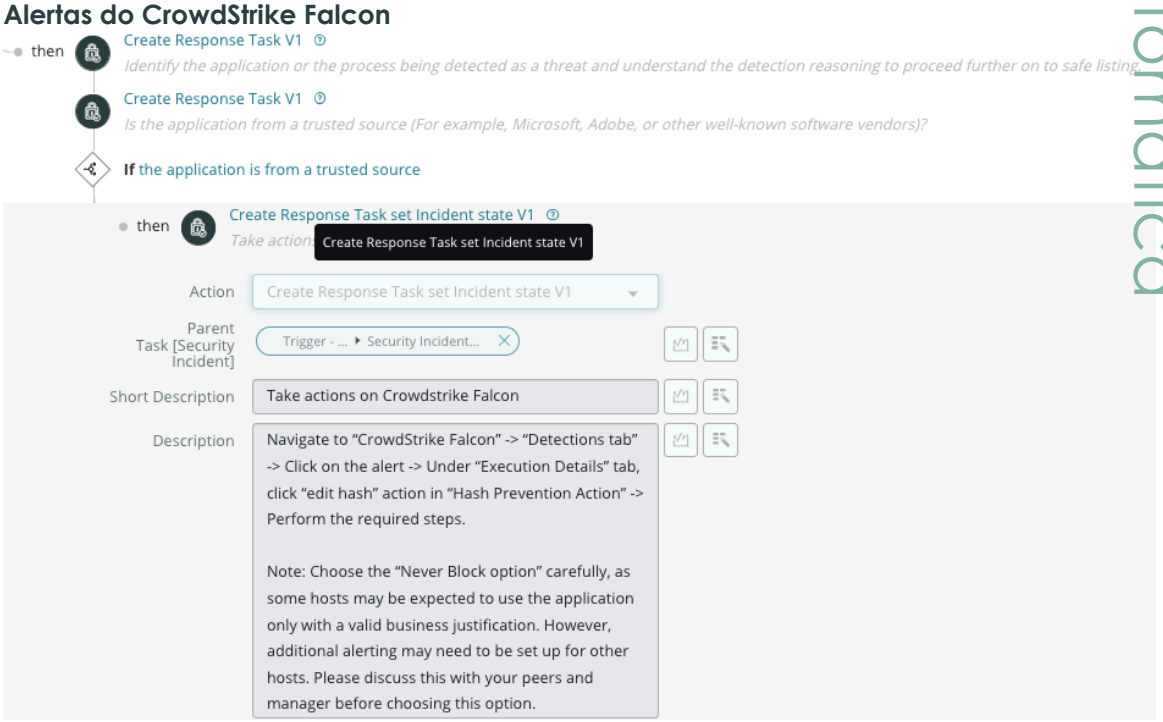
Playbook de detecção de endpoint



b. Na Ação 5, você precisa verificar se a aplicação é de uma fonte confiável (por exemplo, Microsoft, Adobe ou outros fornecedores de software conhecidos).

c. Na Ação 6, se a aplicação for de uma fonte confiável, você precisará executar uma ação nos alertas do CrowdStrike Falcon.

Alertas do CrowdStrike Falcon



d. Na Ação 7, execute as seguintes ações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Navegar até **CrowdStrike Falcon** > **Detecções** guia.

ii. Clique no alerta do CrowdStrike Falcon.

iii. Na guia Detalhes da execução, clique em **Editar** ação de hash em Ação de prevenção de hash.

iv. Execute as etapas necessárias.

> **Nota:** Escolha a opção **Nunca bloquear** com cuidado, pois somente determinados hosts podem ter permissão para usar a aplicação com uma justificativa de negócios válida. No entanto, alertas adicionais podem precisar ser configurados para outros hosts.

e. Na Ação 8, se a aplicação não for de uma fonte confiável, você precisará escolher se deseja dispensar o arquivo ou a aplicação do dispositivo localmente.
Na Ação 10, se você quiser dispensar o arquivo ou a aplicação do dispositivo localmente, execute as seguintes ações:

i. Na Ação 11, navegue até a guia **Arquivos em quarentena** e filtre o endpoint pesquisando o nome do dispositivo.

ii. Selecione o arquivo que precisa ser dispensado localmente e clique em **Liberar**.

> **Nota:**
>
> - O arquivo ainda é executado neste endpoint específico. No entanto, a detecção e a quarentena continuam acontecendo em todos os outros hosts.
> - Para liberar em massa o arquivo de quarentena em vários hosts, selecione o nome e o status do arquivo apropriados. Clique em **Selecionar**e selecione **Versão**.

Na Ação 12, se você não quiser dispensar o arquivo ou a aplicação do dispositivo localmente, poderá redirecionar o usuário para o Suporte de TI para solicitar a instalação das aplicações aprovadas.

4. Na Ação 14, se o arquivo ou hash não for mal-intencionado, execute as seguintes ações:

a. Na Ação 15, você precisa determinar se o arquivo/hash é de alto risco ou baixo risco com base na função do usuário (departamento ou posição que lida com informações confidenciais), o tipo de aplicação (ransomware, root kit etc.) e o impacto da aplicação (quantos usuários foram afetados).

b. Na Ação 16, se o arquivo for de alto risco, execute as seguintes ações:

i. Na Ação 17, revise os resultados com a equipe de informações sobre ameaças.

ii. Na Ação 18, execute a verificação de byte de malware no arquivo.

iii. Na Ação 19, inicie a Análise forense.

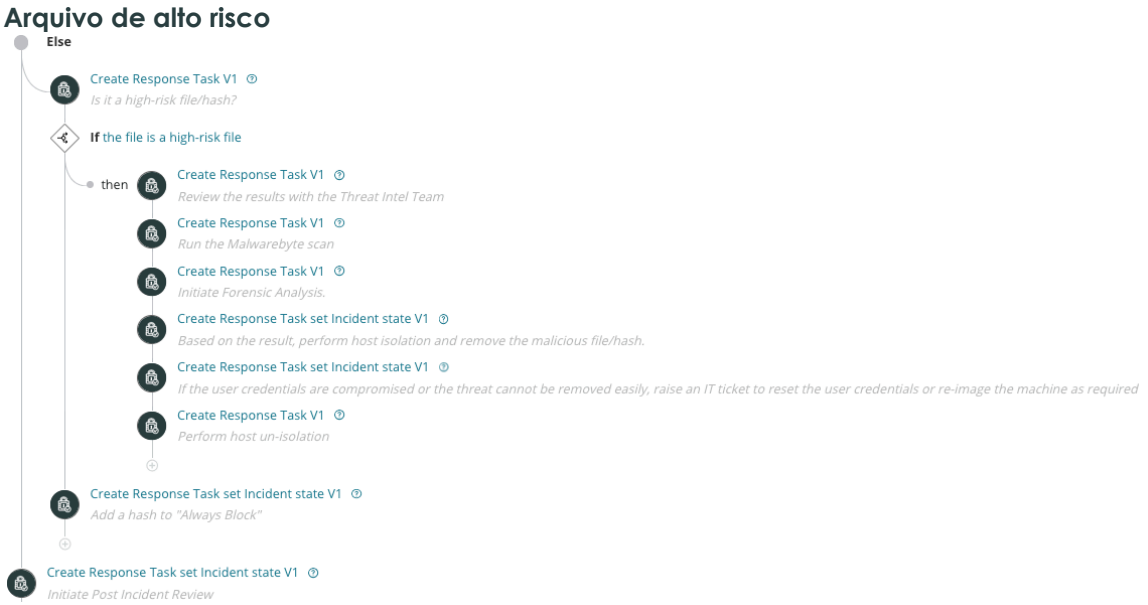
iv. Na Ação 20, com base no resultado da análise forense, execute o isolamento do host e remova o arquivo/hash mal-intencionado.

v. Na Ação 21, se as credenciais do usuário estiverem comprometidas ou a ameaça não puder ser removida facilmente, gere um tíquete de TI para redefinir as credenciais do usuário ou recriar a imagem da máquina conforme necessário.

vi. Na Ação 22, execute o cancelamento do isolamento de host.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Na Ação 23, se o arquivo não for um arquivo de alto risco, execute as seguintes ações:

i. Navegar até **CrowdStrike Falcon** > **Configurações** guia.

ii. Na guia Configurações, navegue até **Hashes de prevenção** > > **Carregar hash** > **Adicionar o hash**.

iii. Escolha o SO necessário e selecione **Sempre bloquear**.

5. Na Ação 24, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para possível spam de senha

Este playbook fornece etapas de correção sistemática para investigar alertas de spam de senha acionados por vários logins com falha (muitas falhas de autenticação de mais de um endereço IP para o mesmo usuário).

Configurar o playbook de spray de senha possível

Use as etapas a seguir para configurar o playbook de Possível senha de spam.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.

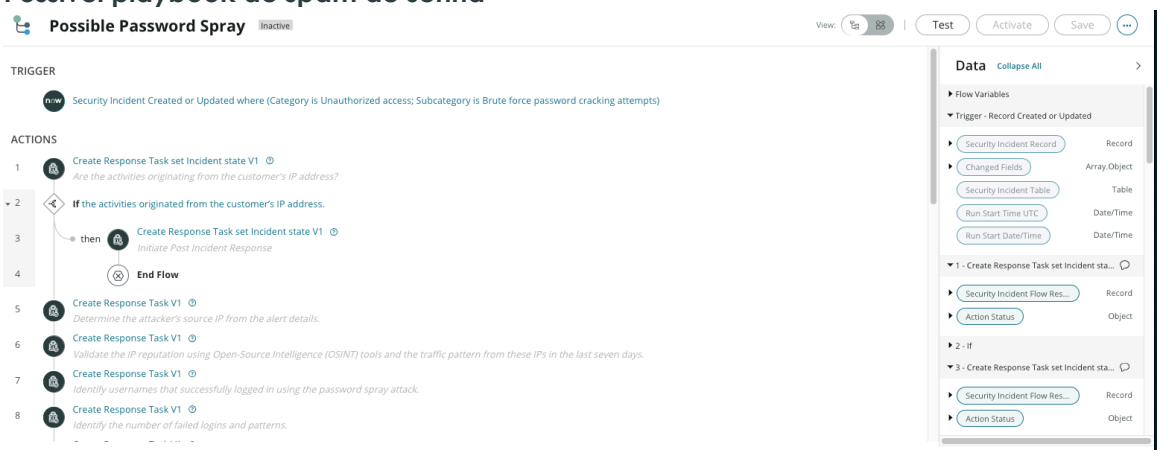
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook de Aplicação de **senha possível**.

3. Opcional: Você pode criar uma cópia do fluxo do playbook de Aplicação de senha possível e fazer as modificações necessárias.

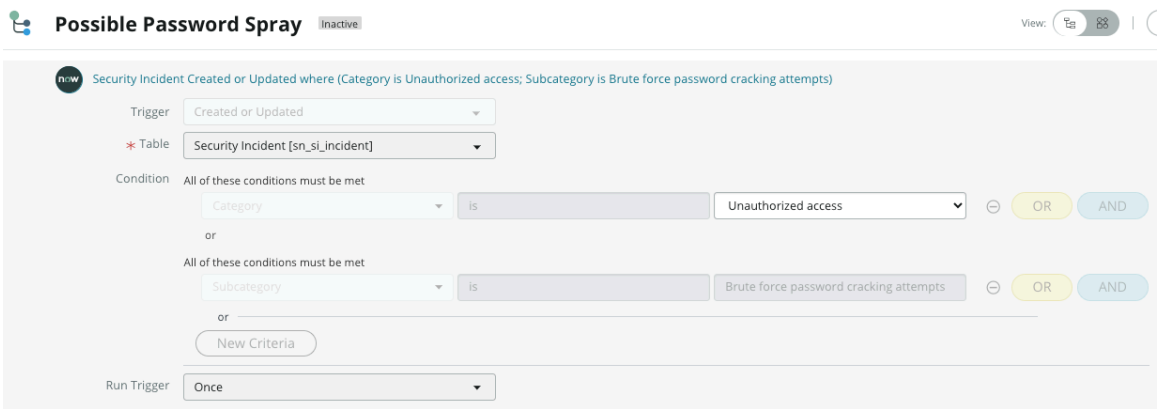
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Possível playbook de spam de senha



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:
   - A**categoria** é **Acesso não autorizado**.
   - **A subcategoria** é **Tentativas de força bruta de quebra de senha**.



Usar o playbook de spray de senha possível

Use este playbook para investigar alertas de spam de senha acionados por vários logins com falha (muitas falhas de autenticação de mais de um endereço IP para o mesmo usuário). As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de Possível senha de spam.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Tradução automática

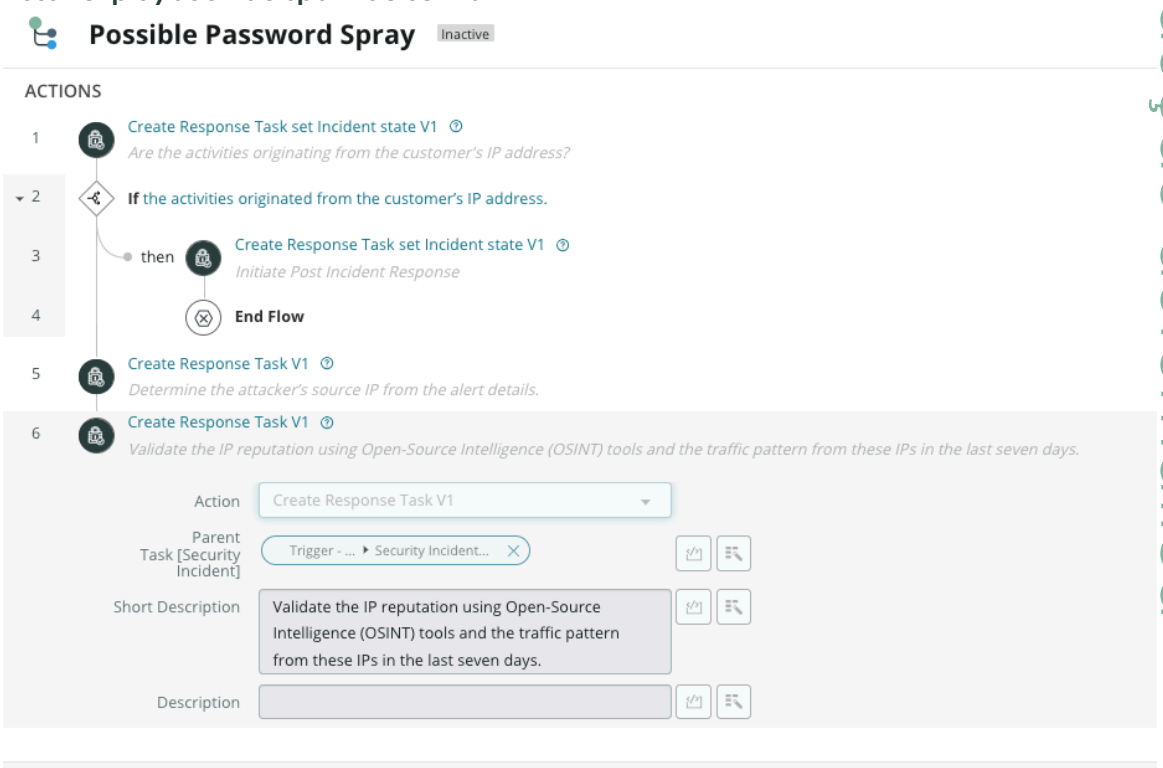
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se as atividades são originadas do endereço IP do cliente.
   Identifique os endereços IP que executam o ataque de spam de senha. Por exemplo, use os TXIDs (IDs de transação) do alerta e pesquise-os em relação aos logs F5.
2. Na Ação 2, se as atividades foram originadas do endereço IP do cliente, execute as seguintes ações:
   a. Na Ação 3, você precisa iniciar uma revisão pós-incidente do possível ataque de spam de senha.
   b. Na Ação 4, o fluxo termina.
3. Na Ação 5, se as atividades não tiverem origem no endereço IP do cliente, determine o IP de origem do invasor a partir dos detalhes do alerta.
4. Na Ação 6, você precisa validar a reputação do IP usando as ferramentas da Inteligência de código aberto (OSINT) e o padrão de tráfego desses IPs nos últimos sete dias.

Possível playbook de spam de senha



5. Na Ação 7, você precisa identificar os nomes de usuário que fizeram login com sucesso usando o ataque de spam de senha.
6. Na Ação 8, você precisa identificar o número de logins e padrões com falha.
7. Na Ação 9, você precisa identificar os indicadores de verdadeiro positivo.
   - Verifique o tráfego dos IPs de origem nos últimos 60 dias. Nenhum tráfego histórico pode ser uma indicação de um verdadeiro positivo.
   - Verifique os padrões de nome de usuário com falhas de autenticação e a contagem. Quanto maior a contagem, maior a probabilidade de ser um verdadeiro positivo.

Tradução automática

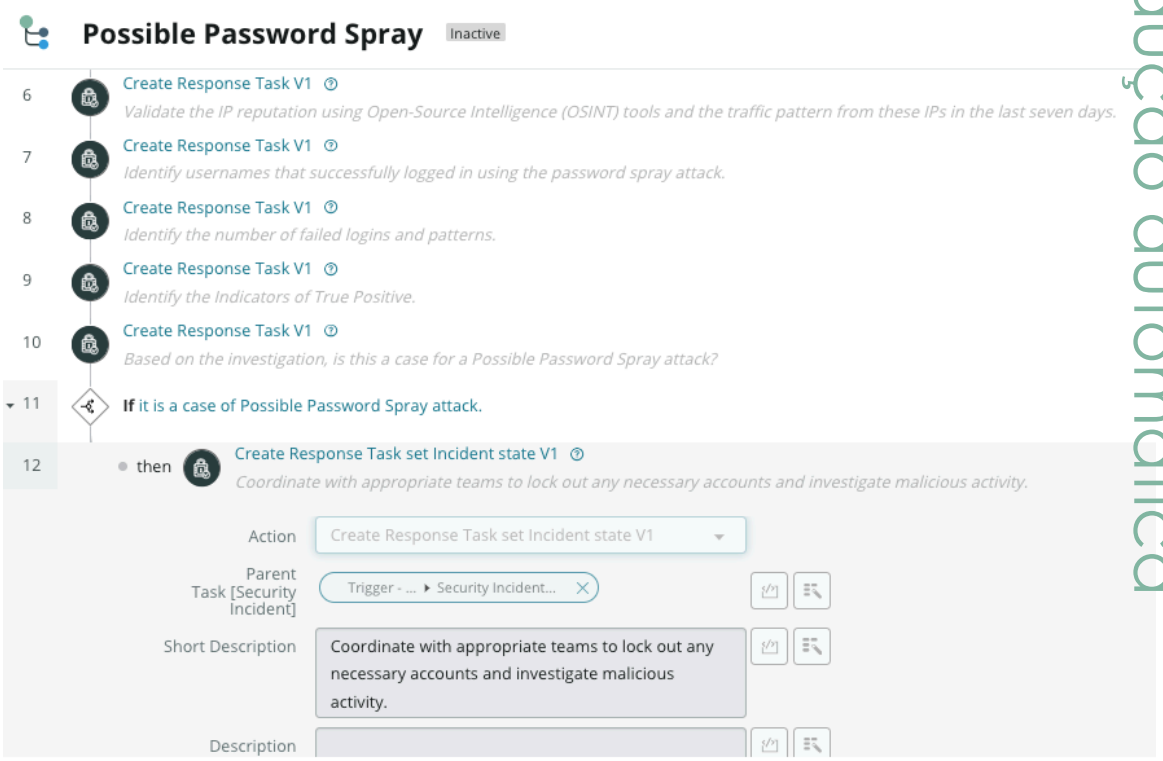
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O nome de usuário se parece com uma base de dicionário (começando de A a Z) e pode ter nomes de administrador comuns, como admin, sysadmin, root e assim por diante
- O mesmo nome de usuário pode ter padrões diferentes no ataque de spam, como o mesmo alerta pode ter falhas para john.doe, johnd, jdoe, john_doe, jdoe7 etc., indicando que os invasores adivinham o padrão de nome de usuário com base em casos de uso comuns.
- Observe o agente do usuário e os URIs dos logs F5 na etapa acima e veja se os IOCs estão relacionados aos alertas do Red Condor. Se eles corresponderem, será um evento positivo verdadeiro.

8. Na Ação 10, com base na investigação feita até o momento, você precisa verificar se este é um caso de possível ataque de spam de senha ou não.
9. Na Ação 11, se este for o caso de um possível ataque de spam de senha, execute as seguintes ações:

   a. Na Ação 12, você precisa coordenar com as equipes apropriadas para bloquear todas as contas necessárias e investigar atividades mal-intencionadas.

Possível playbook de spam de senha



   b. Na Ação 13, você precisa iniciar uma revisão pós-incidente do possível ataque de spam de senha.

   c. Na Ação 14, o fluxo termina.

10. Na Ação 15, você precisa verificar se este não é um caso de possível ataque de spam de senha.
11. Na Ação 16, se este não for um caso de possível ataque de spam de senha, execute as seguintes ações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 17, você precisa documentar as descobertas até o momento.

b. Na Ação 18, você precisa iniciar uma revisão pós-incidente do possível ataque de spam de senha.

c. Na Ação 19, o fluxo termina.

12. Na Ação 20, você precisa consultar os colegas e o gerente do GIR para obter orientação.

13. Na Ação 21, uma tarefa de resposta é criada para concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1003 - Detectar ferramentas de despejo de credenciais

Este playbook fornece etapas de correção sistemática para investigar um incidente que envolve atividades de despejo de credenciais.

Configurar o playbook T1003 - Detectar ferramentas de despejo de credenciais

Use as etapas a seguir para configurar o playbook T1003 - Detectar ferramentas de despejo de credenciais.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1003 - Detectar ferramentas de despejo de credenciais**.

3. Opcional: Você pode criar uma cópia do fluxo do playbook T1003 - Detectar despejo de credenciais e fazer as modificações necessárias.

Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

T1003 - Detectar playbook de ferramentas de despejo de credenciais

4. Ative os playbooks.

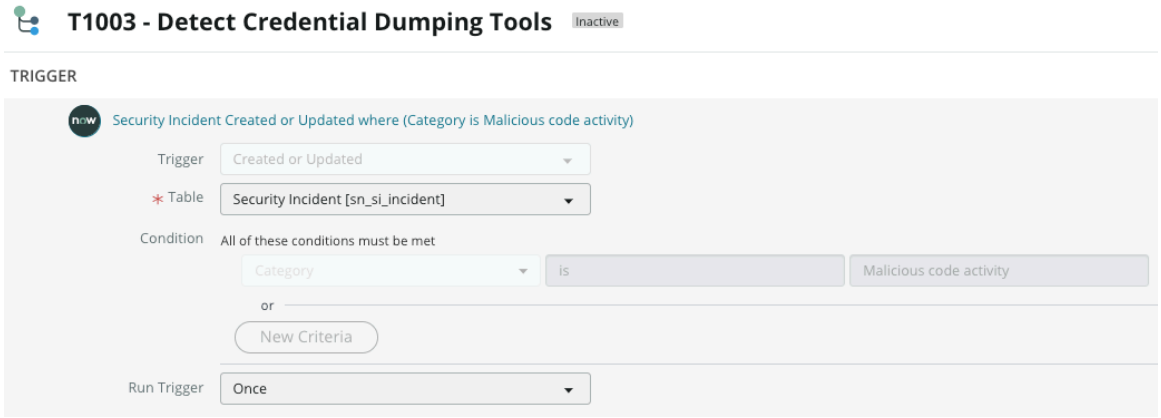
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ative o fluxo principal para usar o playbook disponível no sistema de base.
- Ative os fluxos copiados depois de fazer as mudanças necessárias.

5. Defina uma **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando a **categoria** é uma **atividade de código malicioso**.



Use o playbook T1003 - Detectar ferramentas de despejo de credenciais

Use este playbook para investigar um incidente que envolve atividades de despejo de credenciais. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Detectar despejo de credenciais.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

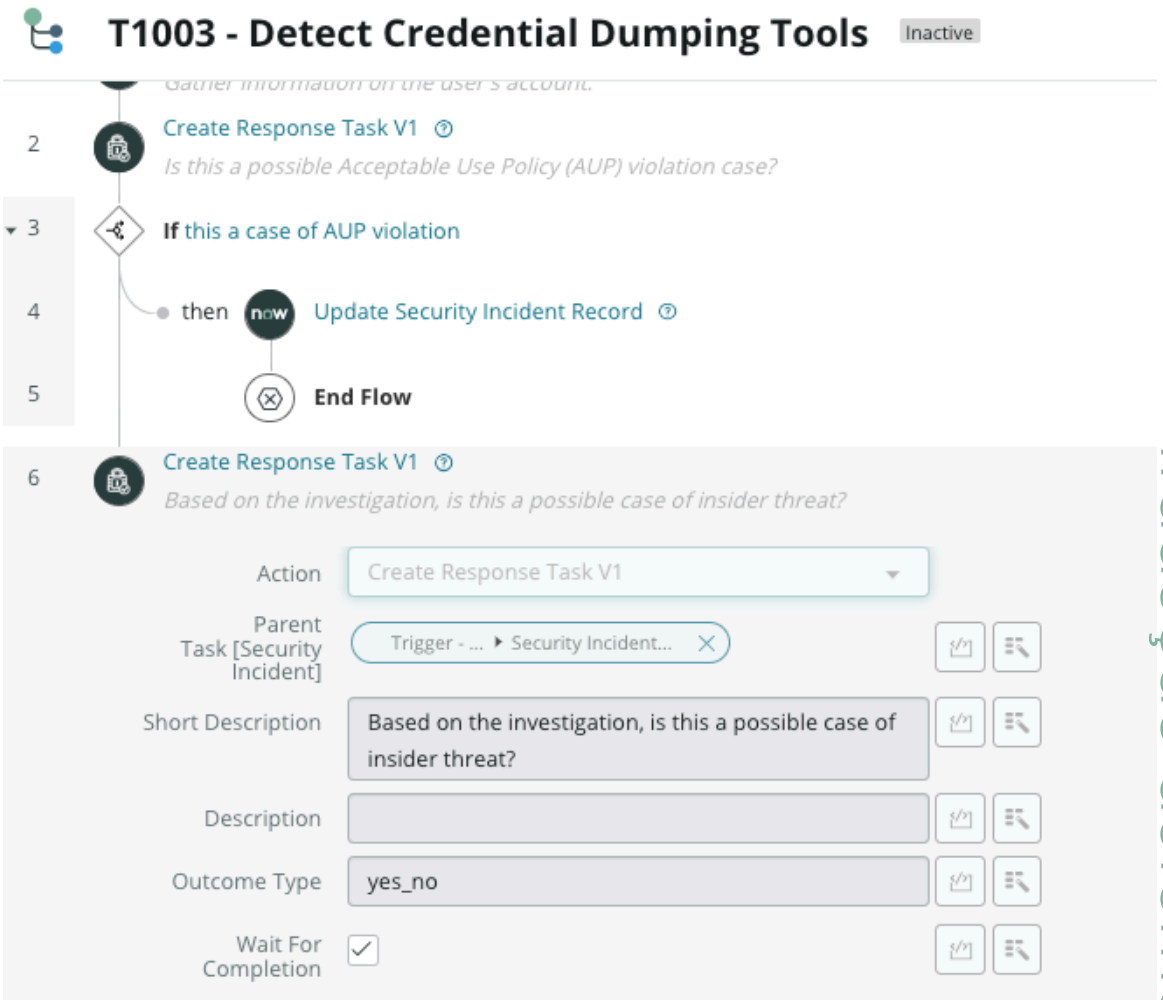
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa coletar informações sobre a conta do usuário.
   - Você precisa verificar a atividade do host para procurar atividades suspeitas.
   - Você precisa identificar o proprietário do servidor/endpoint/VM e capturar os dados correlacionados à ferramenta.
   - Você precisa coletar informações sobre as outras contas do usuário.
2. Na Ação 2, você precisa verificar se este é um possível caso de violação da Política de uso aceitável (AUP).
   Você pode fazer uma revisão por pares com as evidências coletadas e consultar o gerente de incidentes regional para entrar em contato com o usuário.
3. Na Ação 3, se este for um caso de violação da Política de Uso Aceitável (AUP), execute as seguintes ações:
   a. Na Ação 4, você precisa atualizar o incidente de segurança de que este é um caso de violação de AUP
   b. Na Ação 5, o fluxo termina.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na Ação 6, com base na investigação feita até o momento, você precisa verificar se este é um possível caso de ameaça interna ou não.

T1003 - Detectar playbook de ferramentas de despejo de credenciais



5. Na Ação 7, se este for um caso de ameaça interna, execute as seguintes ações:

a. Na Ação 8, você precisa entrar em contato com o suporte de TI e solicitar um congelamento de conta.

b. Na Ação 9, você precisa bloquear IPs mal-intencionados.

c. Na Ação 10, você precisa entrar em contato com os funcionários internos por e-mail. Você pode usar o modelo de e-mail fornecido para entrar em contato com seus funcionários internos.

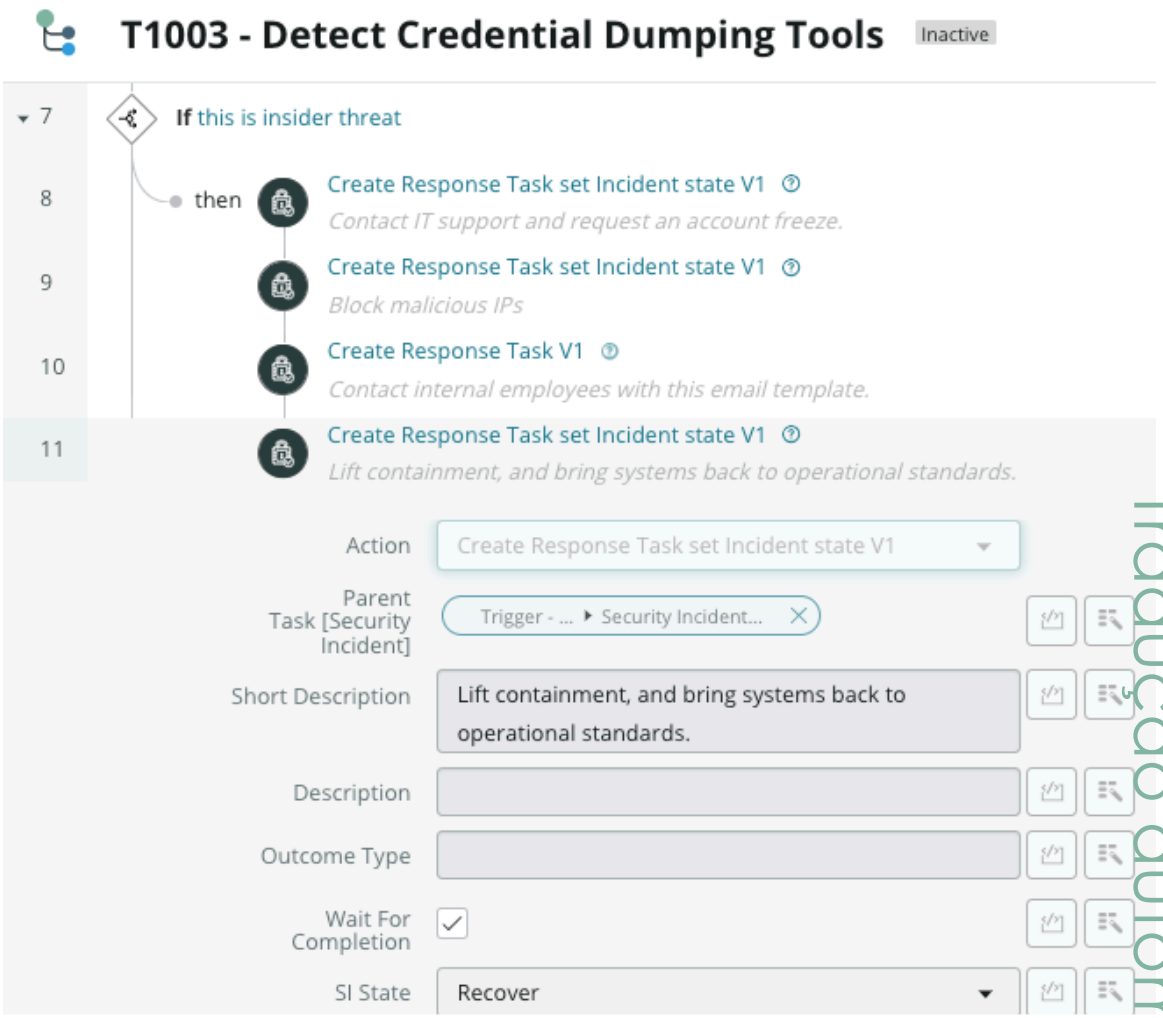
d. Na Ação 11, você precisa suspender a contenção e trazer os sistemas de volta aos padrões operacionais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O fluxo termina.

Tarefas de resposta para suspender a contenção



6. Na Ação 12, se este não for um caso de ameaça interna, na Ação 13, você precisará executar uma revisão por pares para determinar se isso precisa ser adicionado à lista de exclusões.
   O fluxo termina.
7. Na Ação 14, uma tarefa de resposta é criada para concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de falsificação de domínio de e-mail

Este playbook ajuda na triagem de estágio inicial de envios de phishing relatados pelo usuário, alertando o analista sobre a possibilidade de um domínio semelhante no endereço de e-mail do phishing.

O playbook de detecção de falsificação de domínio de e-mail procura encontrar uma correspondência de semelhança entre o domínio de e-mail do remetente do Phisher com um nome de domínio confiável existente no repositório do observável. Quando uma correspondência de domínio de e-mail de remetente falsificada é identificada pelo playbook, os analistas são alertados com um marcador.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para a investigação de incidentes. Cada ponto de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

decisão no playbook foi convertido em uma tarefa orientada por resultados e o fluxo muda de direção com base no resultado dessas tarefas.

Configurar o playbook de detecção de falsificação de e-mail

Use as etapas a seguir para configurar o playbook de detecção de falsificação de e-mail.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

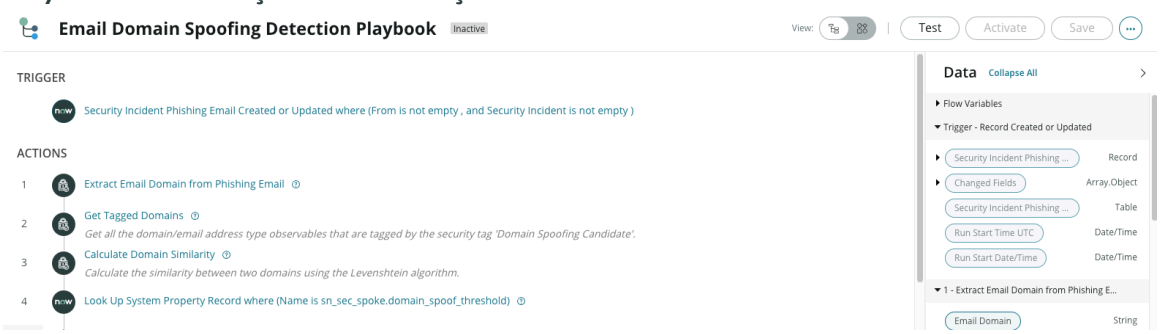
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook de detecção de falsificação de domínio de e-mail**.
3. Opcional: Você pode criar uma cópia do fluxo do playbook de detecção de falsificação de domínio de e-mail e fazer as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   Playbook de detecção de falsificação de domínio de e-mail

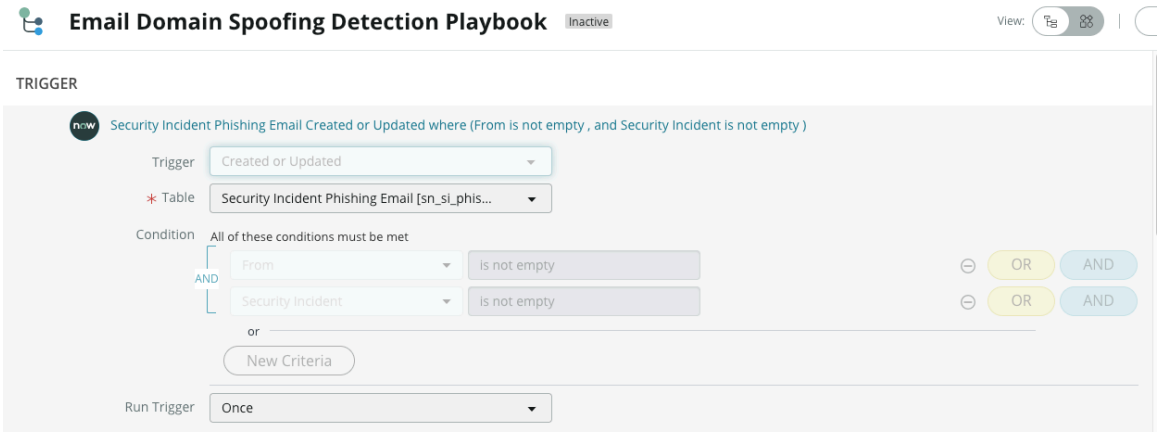
   

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **De** não está **vazio**.
- **O incidente de segurança** não está **vazio**.



Use o playbook de detecção de falsificação de domínio de e-mail

Use este playbook para encontrar uma correspondência de semelhança entre o domínio de e-mail do remetente do Phisher com um nome de domínio confiável no repositório do observável. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de falsificação de domínio de e-mail.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

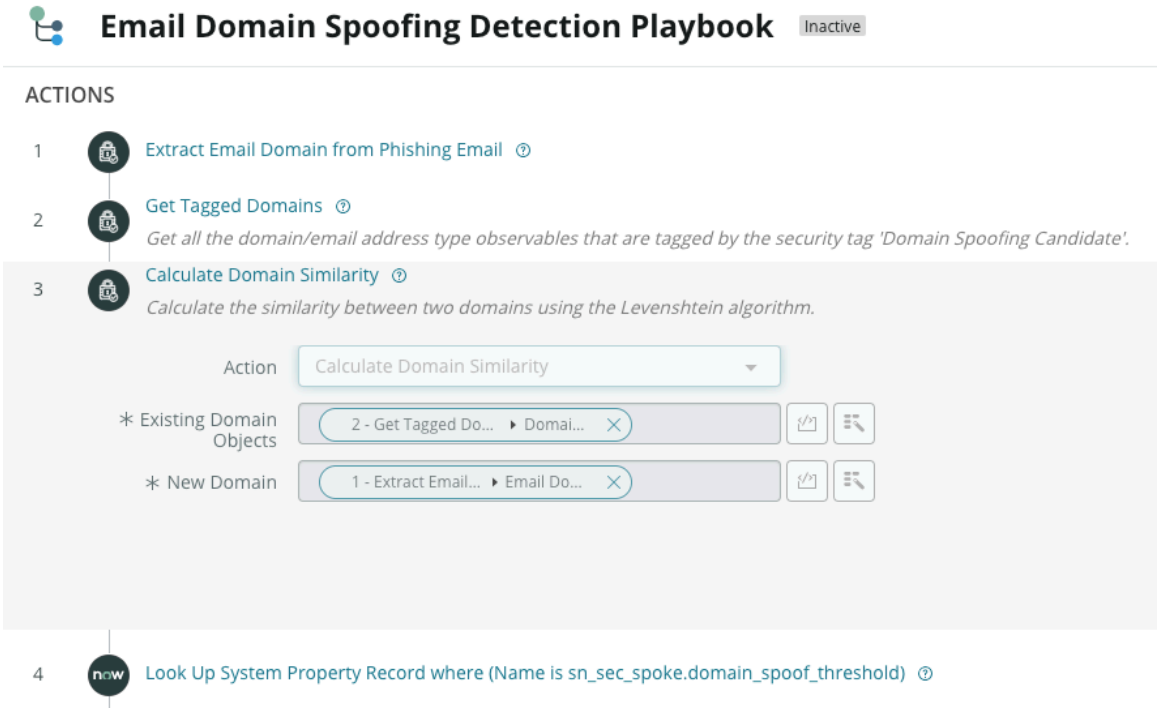
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, o playbook extrai o domínio de e-mail do e-mail de phishing.
2. Na Ação 2, o playbook recupera todos os observáveis de tipo de endereço de e-mail/domínio marcados pelo marcador de segurança "Candidato a falsificação de domínio".
3. Na Ação 3, o playbook calcula a semelhança entre o domínio Obter Marcado e o domínio E-mail usando o algoritmo Levenshtein.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de detecção de falsificação de domínio de e-mail

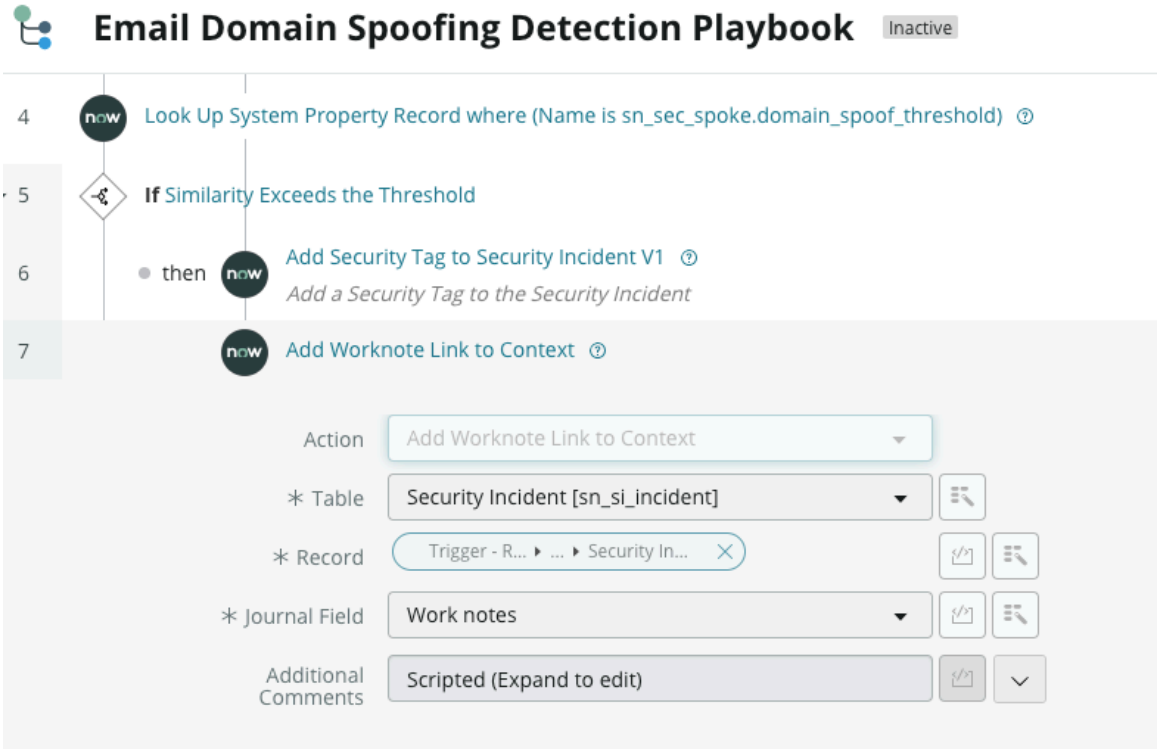


4. Na Ação 4, o playbook pesquisa o registro de propriedade do sistema com base nas seguintes condições:
   - O nome é sn_sec_spoke.domain_spoof_threshold, (OR)
   - O nome vai de A a Z e, se vários registros forem encontrados, retorne somente o primeiro registro.
5. Na Ação 5, com base na investigação feita até o momento, o playbook verifica se a semelhança dos dois domínios excede o limite ou não.
   Se a semelhança dos dois domínios não exceder o limite, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado. Se a semelhança dos dois domínios exceder o limite, as ações 6 e 7 serão executadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A semelhança excede o limite



6. Na Ação 6, o playbook adiciona o marcador de segurança de falsificação de domínio de e-mail ao incidente de segurança.
7. Na Ação 7, o playbook adiciona um link de anotação de trabalho ao contexto usando a opção de script.
8. Na Ação 8, o fluxo termina.

Playbook para domínio com erro de digitação

Este playbook fornece procedimentos sistemáticos para investigar domínios com erros ortográficos e colaborar com o departamento jurídico da organização para remoções. Domínios com erro de digitação são nomes de domínio com erros ortográficos que se parecem muito com nomes legítimos. Os invasores aproveitam os erros ortográficos para conduzi-los a um site mal-intencionado para exploração financeira ou outras atividades mal-intencionadas.

Os domínios de erro de digitação são relatados para a equipe de operações de segurança de diferentes origens, como soluções de proteção de risco digital (Sombras digitais) e plataformas de inteligência contra ameaças (Anomali Threatstream). Depois que um incidente de segurança é criado, esta solução ajuda a identificar se o domínio é realmente um domínio de erro de digitação. Se for um domínio de erro de digitação, o analista poderá relatá-lo à equipe jurídica para que outras ações possam ser tomadas.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para a investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultados e o fluxo muda de direção com base no resultado dessas tarefas.

Configurar o playbook de domínio de erro de digitação

Use as etapas a seguir para configurar o playbook de domínio de erro de digitação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

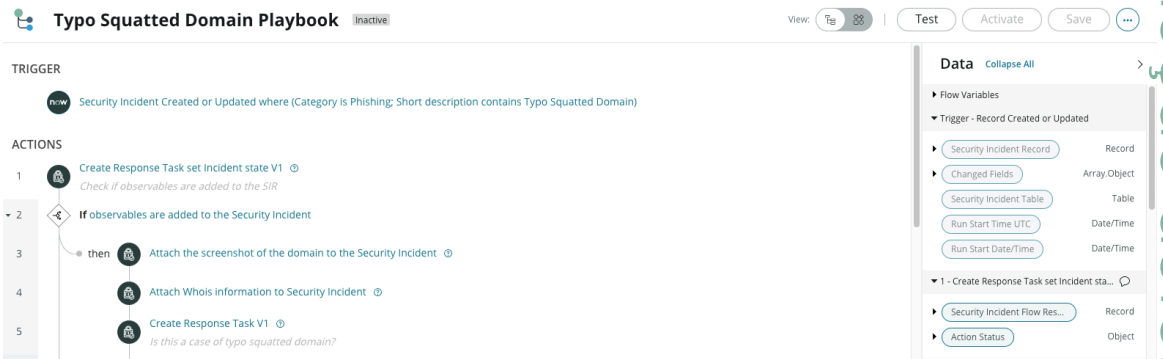
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **Domínio** de erro de digitação.
3. Opcional: Você pode criar uma cópia do fluxo do playbook de domínio de erro de digitação e fazer as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   Playbook de domínio de erro de digitação

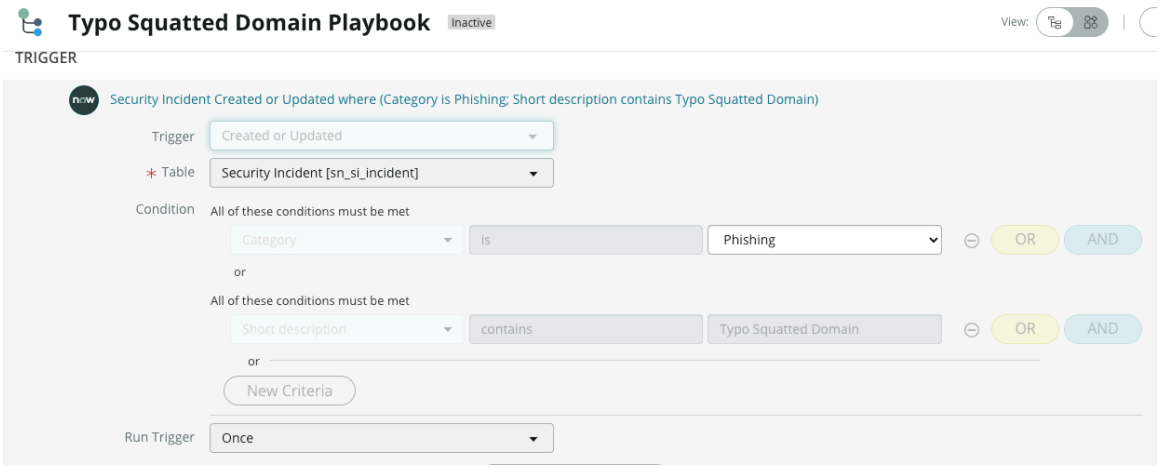
4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A**categoria** é **Phishing**.
- **A descrição resumida** contém **domínio**de erro de digitação.



Usar o playbook de domínio de erro de digitação

Use este playbook para investigar domínios com erros ortográficos e colaborar com o departamento jurídico da organização para remoções. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de domínio alocado por erro de digitação.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

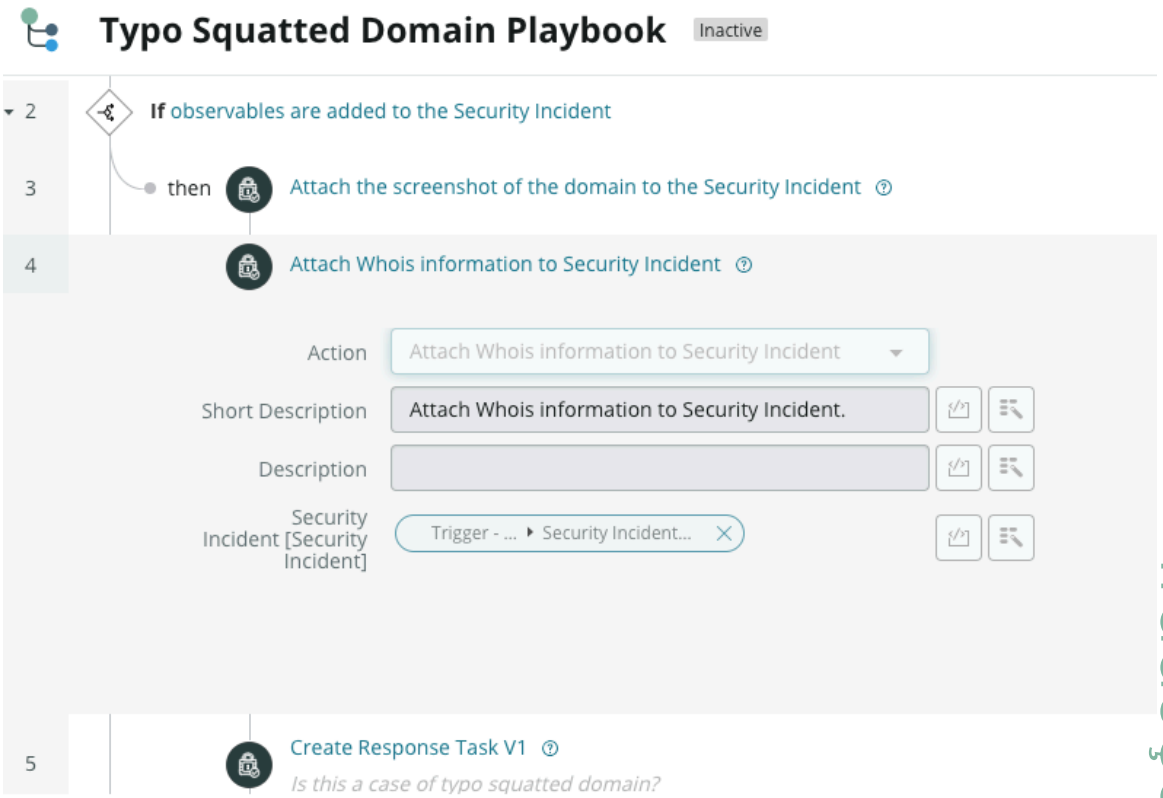
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Ação 1, você precisa verificar se os observáveis foram adicionados ao Security Incident Response (SIR).
   Se os observáveis não forem adicionados ao SIR, adicione-os antes de prosseguir. Se os observáveis não estiverem disponíveis, a Ação 10 será executada e o incidente de segurança será encerrado.
2. Na Ação 2, se os observáveis forem adicionados ao incidente de segurança, as ações a seguir serão executadas.
3. Na Ação 3, você precisa anexar a captura de tela do domínio Erro de digitação ao incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de domínio de erro de digitação



4. Na Ação 4, você precisa anexar as informações de Whois ao incidente de segurança.
5. Na Ação 5, com base na investigação feita até o momento, o playbook verifica se este é um caso de domínio de erro de digitação ou não.
   Se este não for um caso de domínio de erro de digitação, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.
6. Na Ação 6, se este for um caso de domínio de erro de digitação, a ação 7 será executada.
7. Na Ação 7, você precisa enviar um e-mail e informar às equipes jurídicas e outras equipes necessárias que este é um caso de domínio de erro de digitação e tomar as medidas necessárias para erradicá-lo.
   Se este não for um caso de domínio de erro de digitação, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso de domínio de erro de digitação

8. Na Ação 9, uma tarefa de resposta é criada para você concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para sniffing de credenciais

Este playbook fornece etapas de correção do sistema para investigar um incidente que envolve atividades de detecção de credenciais realizadas por meio da tabela *sys_installation_exit* em uma instância da ServiceNow.

O playbook de detecção de credenciais fornece um campo de script para processar os logins do banco de dados (DB), Single Sign-on (SSO) e LDAP (Lightweight Directory Access Protocol) usando os registros na tabela *sys_installation_exit*. Esses campos de script privilegiados permitem ouvir solicitações e parâmetros do usuário para as instâncias durante o login, incluindo credenciais do usuário, como nome de usuário e senha.

Um usuário mal-intencionado pode criar um script para ouvir as solicitações do usuário e registrar essas solicitações na instância. A tabela *sys_installation_exit* em uma instância define as regras de processamento das atividades de login e logout de todos os usuários nessa instância.

Configurar o playbook de sniffing de credenciais

Use as etapas a seguir para configurar o playbook de detecção de credenciais.

Antes de Iniciar
Função necessária:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_si.admin
- flow_designer

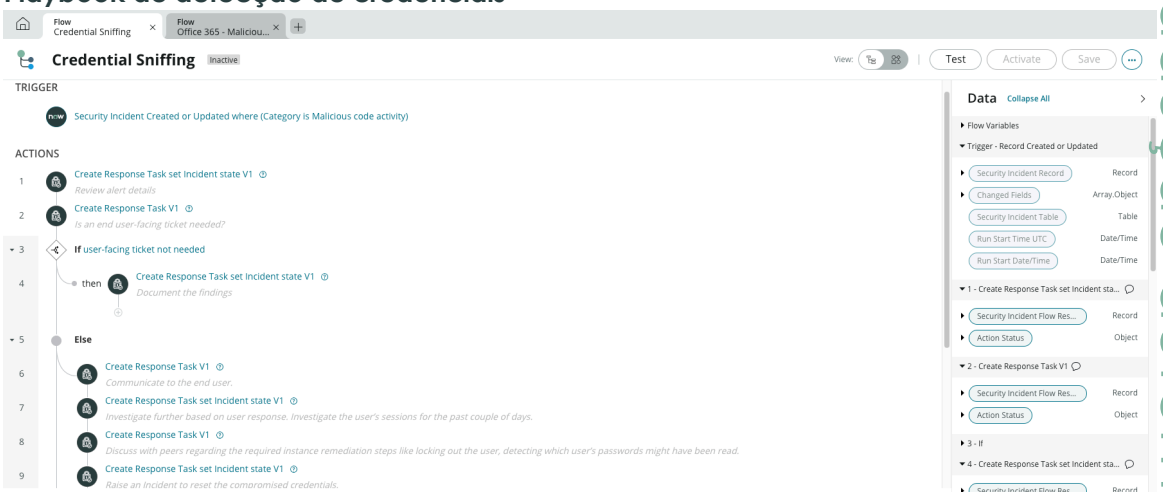
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook de **credencial Sniffing**.
3. Opcional: Crie uma cópia do fluxo do playbook de detecção de credenciais e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Playbook de detecção de credenciais



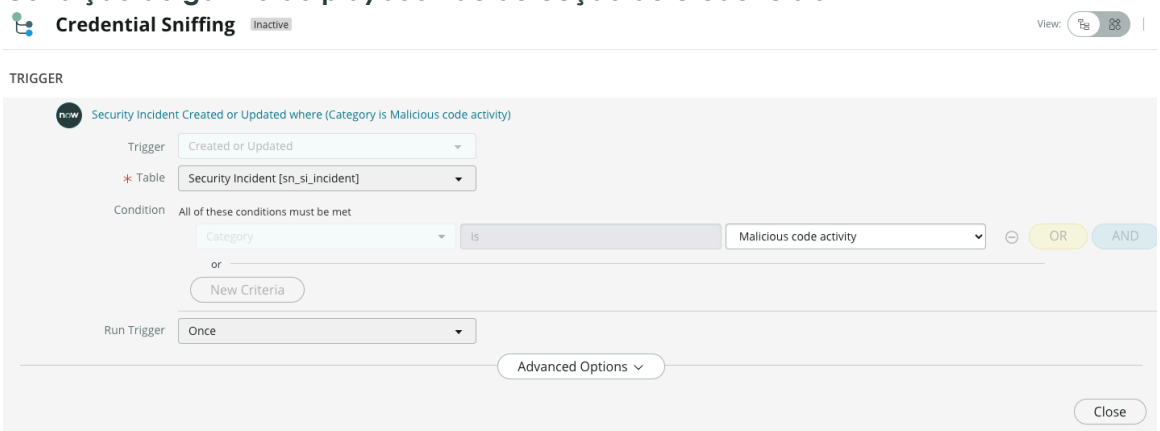
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando a **categoria** é uma **atividade de código malicioso**.

Condição do gatilho do playbook de detecção de credenciais



Usar o playbook de detecção de credenciais

Use este playbook para investigar um incidente que envolve atividades de detecção de credenciais realizadas por meio da tabela *sys_installation_exit* em uma instância da ServiceNow. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de credenciais.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, revise os detalhes do alerta a seguir.
   - Instância
   - ID da sessão
   - ID da transação
   - _raw: fornece o script inteiro.

   Script de exemplo:

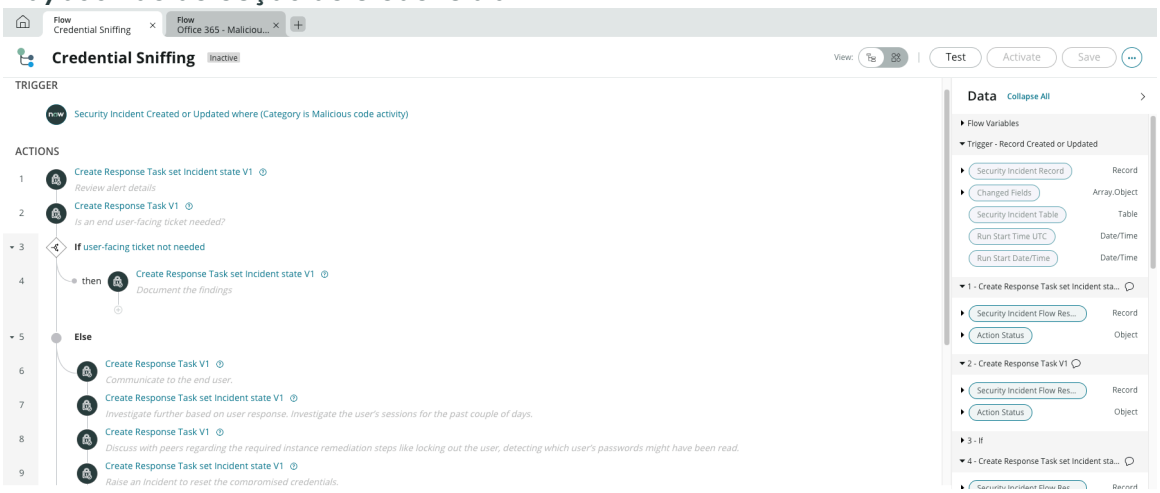
```
Var pass= request.getParameter("user_password");
Gs.log(pass);
```

2. Na Ação 2, com base nos dados coletados até o momento, verifique se um tíquete de usuário final é necessário para este alerta ou não.
3. Na Ação 3, se o alerta não exigir um tíquete de usuário final, na Ação 4, documente as descobertas até o momento.
   O fluxo termina.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de detecção de credenciais



4. Na Ação 5, se o alerta exigir um tíquete de usuário final, execute as seguintes etapas:

   a. Na Ação 6, informe ao usuário final que o alerta requer um tíquete de usuário final.

   b. Na Ação 7, investigue mais com base na resposta do usuário e nas sessões do usuário durante os últimos dias.

   c. Na Ação 8, discuta com colegas sobre as etapas de correção da instância, como bloquear o usuário e detectar quais senhas de usuário podem ter sido lidas.

   d. Na Ação 9, gere um incidente ou tíquete para redefinir as credenciais do usuário comprometido.

   e. Na Ação 10, remova a contenção e restaure os sistemas aos padrões operacionais O fluxo termina.

5. Na Ação 11, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1070 - Logs de eventos do Windows limpos

Este playbook fornece etapas de correção para investigar incidentes que rastreiam tipos de evento em que o usuário remove logs de segurança. Sempre que o log de segurança é limpo, os eventos 517 e 1102 são registrados, independentemente do status da política de eventos do sistema de auditoria.

Este alerta pode rastrear os seguintes tipos de eventos:

- **Evento 517**: os campos Nome de usuário primário e Nome de usuário do cliente identificam o usuário que limpou o log. O nome de usuário primário corresponde ao sistema e o nome de usuário do cliente indica o usuário que limpou o log.
- **Evento 1102**: os campos Nome da conta e Nome do domínio identificam o usuário que limpou o log. O ID de logon permite correlacionar para trás o evento de logon e outros eventos registrados durante a mesma sessão de logon.

Configurar o playbook T1070 - Logs de eventos do Windows limpos

Use as etapas a seguir para configurar o playbook T1070 - Logs de eventos do Windows limpos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

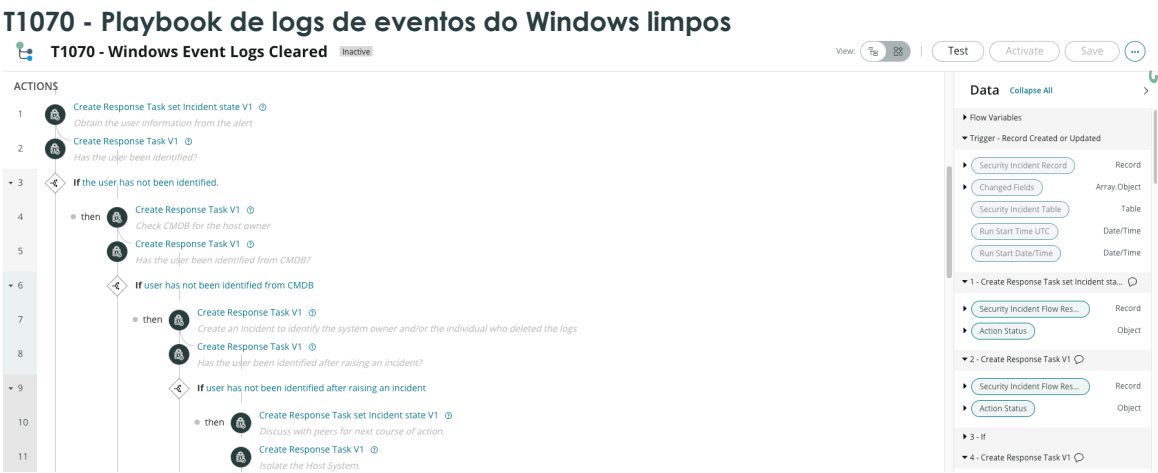
- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1070 - Logs de eventos do Windows limpos**.
3. Opcional: Crie uma cópia do fluxo do playbook T1070 - Logs de eventos do Windows limpos e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.



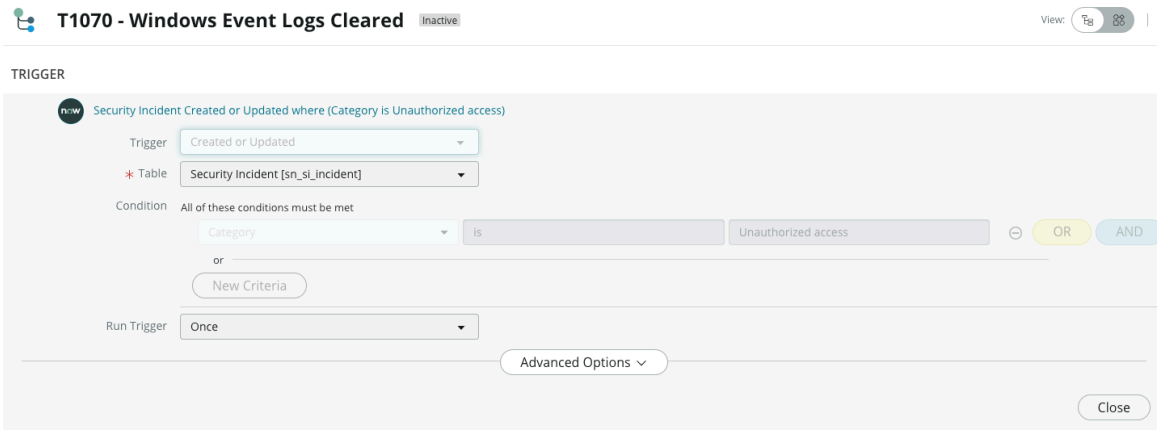
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando a **categoria** é **Acesso não autorizado**.

T1070 – Condição de gatilho do playbook de logs de eventos do Windows limpos



Use o playbook T1070 - Logs de eventos do Windows limpos

Use este playbook para investigar incidentes que rastreiam tipos de evento em que o usuário remove logs de segurança. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1070 - Logs de eventos do Windows limpos.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, obtenha os detalhes do usuário do alerta.
2. Na Ação 2, verifique se o usuário foi identificado ou não.
3. Na Ação 3, se o usuário não tiver sido identificado, execute as seguintes etapas:

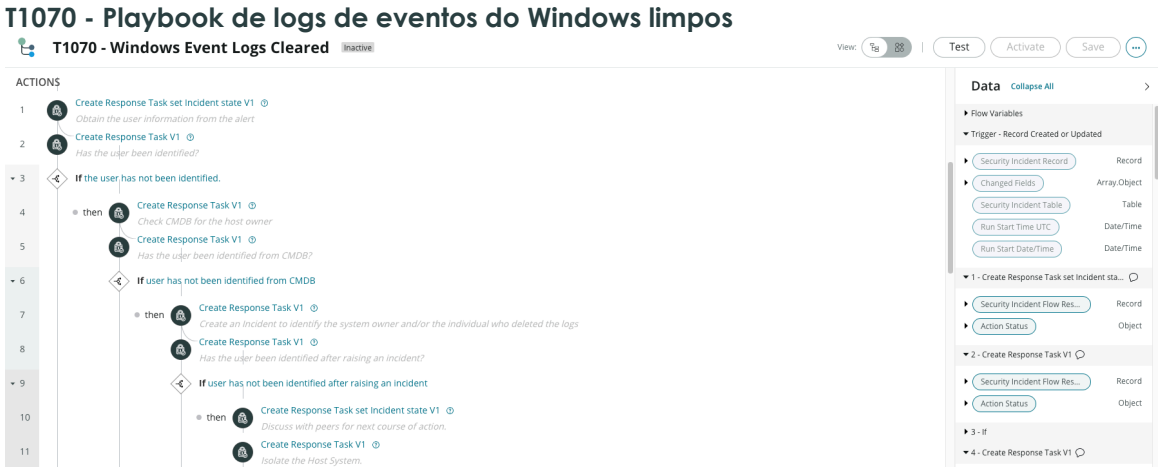
   a. Na Ação 4, verifique o CMDB (banco de dados de gestão de configuração) para obter os detalhes do proprietário do host.

   b. Na Ação 5, verifique se o usuário foi identificado no CMDB ou não.

      Se o usuário tiver sido identificado no CMDB, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Na Ação 6, se o usuário não tiver sido identificado no CMDB, execute as seguintes etapas:

i. Na Ação 7, crie um incidente para identificar o proprietário do sistema e o indivíduo que excluiu os logs.

ii. Na Ação 8, verifique se o usuário foi identificado após gerar um incidente ou não.

Se o usuário tiver sido identificado após gerar um incidente, uma tarefa de resposta manual será criada na Ação 8 e o fluxo será encerrado.

iii. Na Ação 9, se o usuário não tiver sido identificado após gerar um incidente, execute as seguintes etapas:

1. Na Ação 10, discuta o próximo curso de ação com colegas.

2. Na Ação 11, isole o sistema host.

3. Na Ação 12, remova todos os arquivos indesejados que possam ter sido criados e exclua as contas não autorizadas.

4. Na Ação 13, remova a contenção e restaure os sistemas aos padrões operacionais.

5. Na Ação 14, conclua a revisão pós-incidente antes de fechar a tarefa.

Na Ação 15, o fluxo termina.

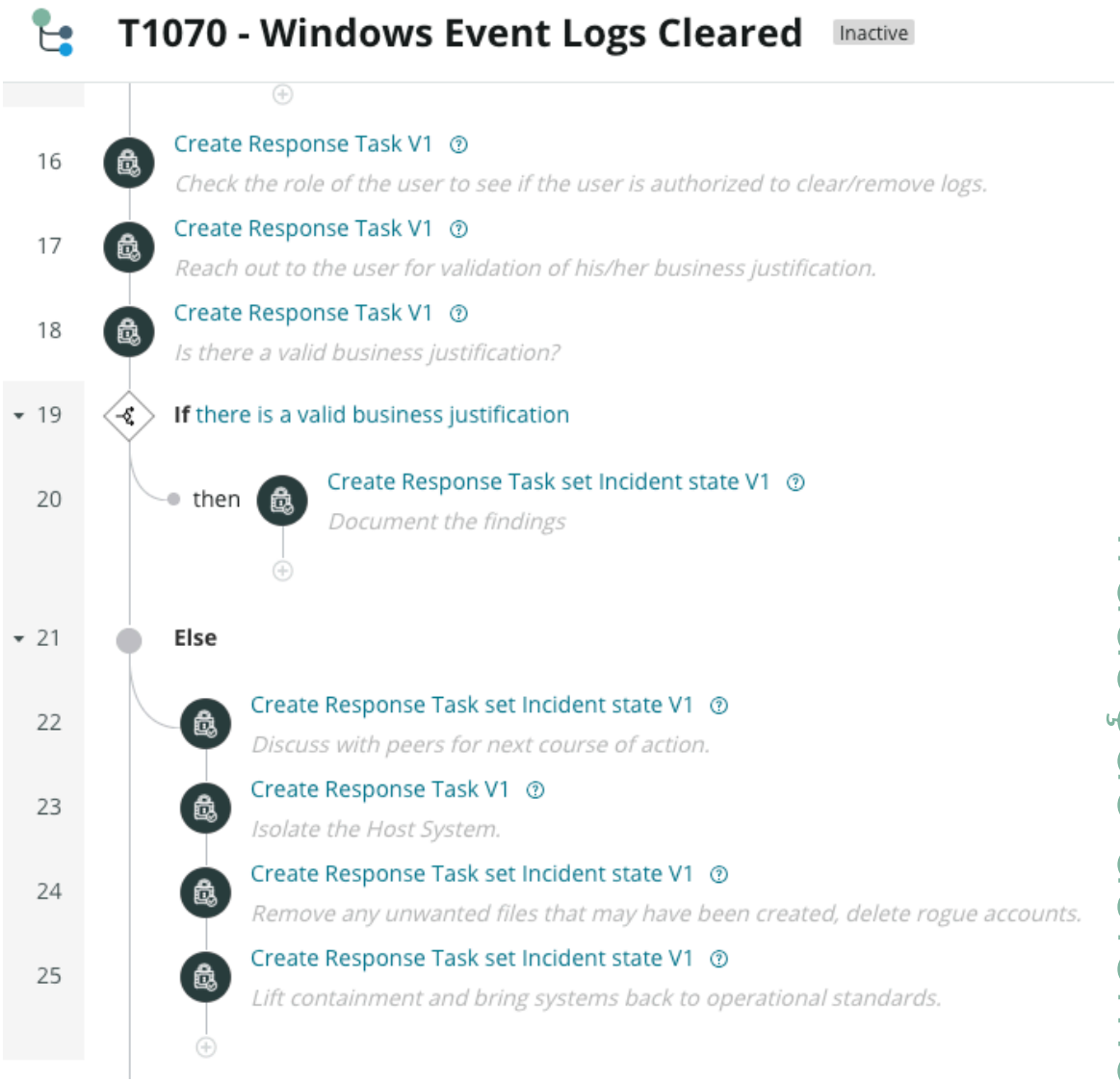
4. Na Ação 16, se o usuário tiver sido identificado, verifique a função do usuário para ver se ele está autorizado a limpar ou remover logs.

5. Na Ação 17, entre em contato com o usuário para validação de sua justificativa de negócios.
Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook T1070 - Logs de eventos do Windows limpos



Tradução automática

6. Na Ação 18, verifique se uma justificativa de negócio válida foi fornecida ou não.
7. Na Ação 19, se houver uma justificativa de negócio válida fornecida, na Ação 20, documente as descobertas até o momento.
   O fluxo termina.
8. Na Ação 21, se não houver uma justificativa de negócio válida fornecida, execute as seguintes etapas:

   a. Na Ação 22, discuta o próximo curso de ação com colegas.

   b. Na Ação 23, isole o sistema host.

   c. Na Ação 24, remova todos os arquivos indesejados que possam ter sido criados e exclua as contas não autorizadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Na Ação 25, remova a contenção e restaure os sistemas aos padrões operacionais. O fluxo termina.

9. Na Ação 26, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para OSquery de endereço externo no arquivo /etc/hosts

Este playbook fornece etapas de correção sistemática para investigar incidentes que indicam que um nome de host ou domínio interno foi atribuído a um endereço IP externo no DNS local (/etc/hosts) de um servidor Linux.

Configurar o OSquery de endereço externo no playbook do arquivo /etc/hosts

Use as etapas a seguir para configurar o OSquery de endereço externo no playbook de arquivo /etc/hosts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

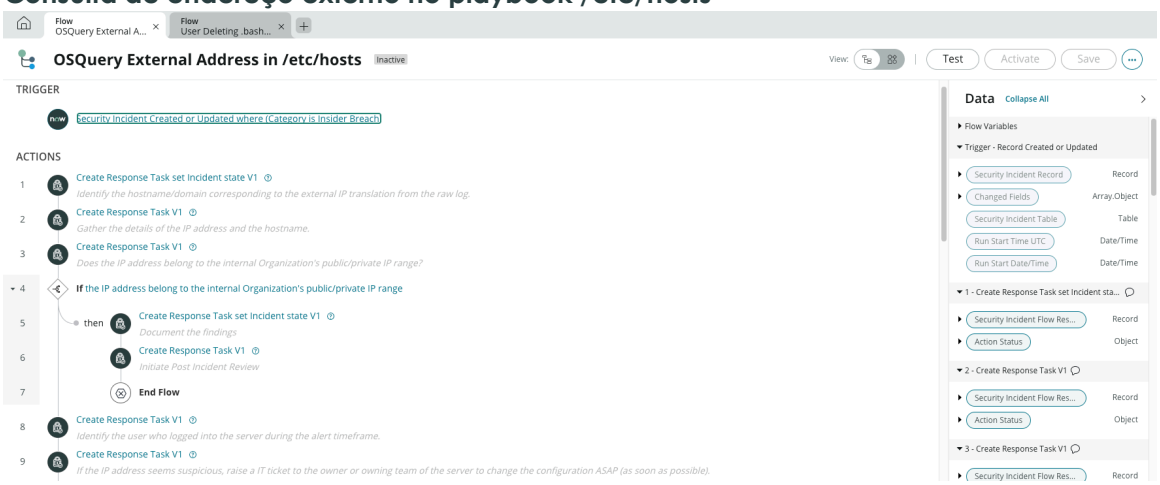
1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Todos** > **Flow Designer** e selecione o **endereço externo OSquery no playbook /etc/hosts**.

3. Opcional: Crie uma cópia do endereço externo do OSquery no fluxo do playbook /etc/hosts e faça as modificações necessárias.

(Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Consulta de endereço externo no playbook /etc/hosts



4. Ative os playbooks.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

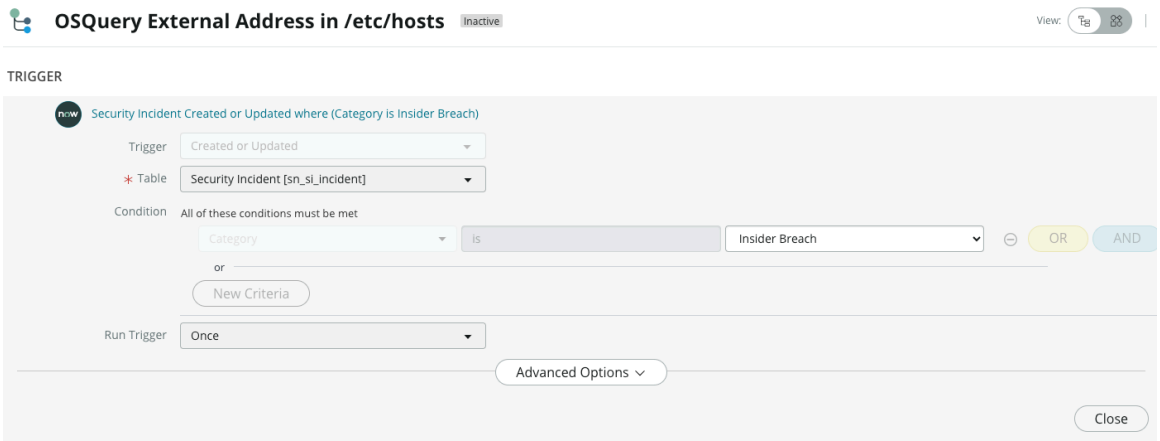
a. Ative o fluxo principal para usar o playbook disponível no sistema de base.

b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

5. Defina uma **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Violação de insider**.

Consulta de endereço externo na condição de gatilho do playbook /etc/hosts



Use a OSquery de endereço externo no playbook do arquivo /etc/hosts

Use este playbook para investigar incidentes que indicam que um nome de host ou domínio interno foi atribuído a um endereço IP externo no DNS local (/etc/hosts) de um servidor Linux. As etapas a seguir fornecem instruções das ações, tarefas e subfluxos que estão disponíveis na consulta do OS de endereço externo no playbook de arquivo /etc/hosts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

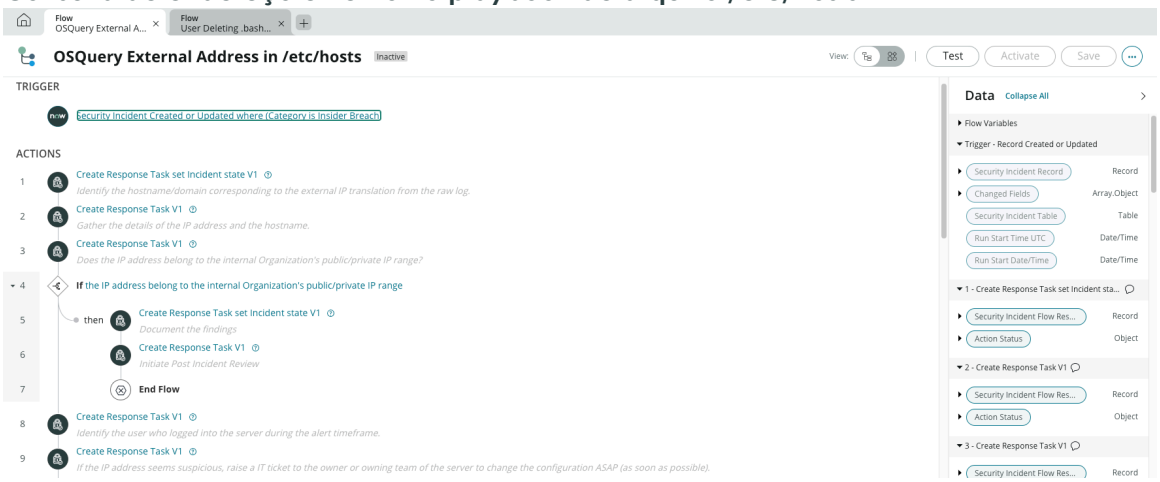
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, identifique o nome do host ou o nome do domínio correspondente à conversão de IP externo do log bruto.
2. Na Ação 2, reúna os detalhes do endereço IP e o nome do host.
3. Na Ação 3, verifique se este endereço IP pertence ou não ao intervalo de IPs públicos/privados da organização interna.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulta de endereço externo no playbook de arquivo /etc/hosts



4. Na Ação 4, se o endereço IP pertencer ao intervalo de IPs públicos/privados da organização interna, execute as seguintes etapas:

   a. Na Ação 5, documente as descobertas até o momento.

   b. Na Ação 6, inicie uma análise pós-incidente.
   Na Ação 7, após a análise pós-incidente, o fluxo termina.

5. Se o endereço IP não pertencer ao intervalo de IPs públicos/privados da organização interna, na Ação 8, identifique o usuário que fez login no servidor durante o intervalo de tempo do alerta.
6. Na Ação 9, se o endereço IP parecer suspeito, gere um tíquete de TI para o proprietário ou a equipe do servidor para mudar a configuração assim que possível.
7. Na Ação 10, verifique se houve alguma atividade mal-intencionada no servidor antes e depois de adicionar a entrada DNS.
8. Na Ação 11, verifique se há conexões com o endereço IP externo do servidor.
9. Na Ação 12, documente as descobertas até o momento.
10. Na Ação 13, verifique se as informações do proprietário ou da equipe estão disponíveis ou não.
11. Na Ação 14, se as informações do proprietário ou da equipe estiverem disponíveis, execute as seguintes etapas:

    a. Na Ação 15, entre em contato com o proprietário ou a equipe do servidor para ver se eles reconhecem a atividade.
    Você pode usar o modelo de e-mail fornecido para entrar em contato com o proprietário ou a equipe do servidor.

    b. Na Ação 16, verifique se o proprietário ou a equipe forneceu uma justificativa de negócio válida ou não.

    c. Na Ação 17, se o proprietário ou a equipe fornecida não fornecer uma justificativa de negócio válida, o fluxo será encerrado.
    Mas, se o proprietário ou a equipe forneceram uma justificativa de negócio válida, execute as seguintes etapas:

Tradução automática

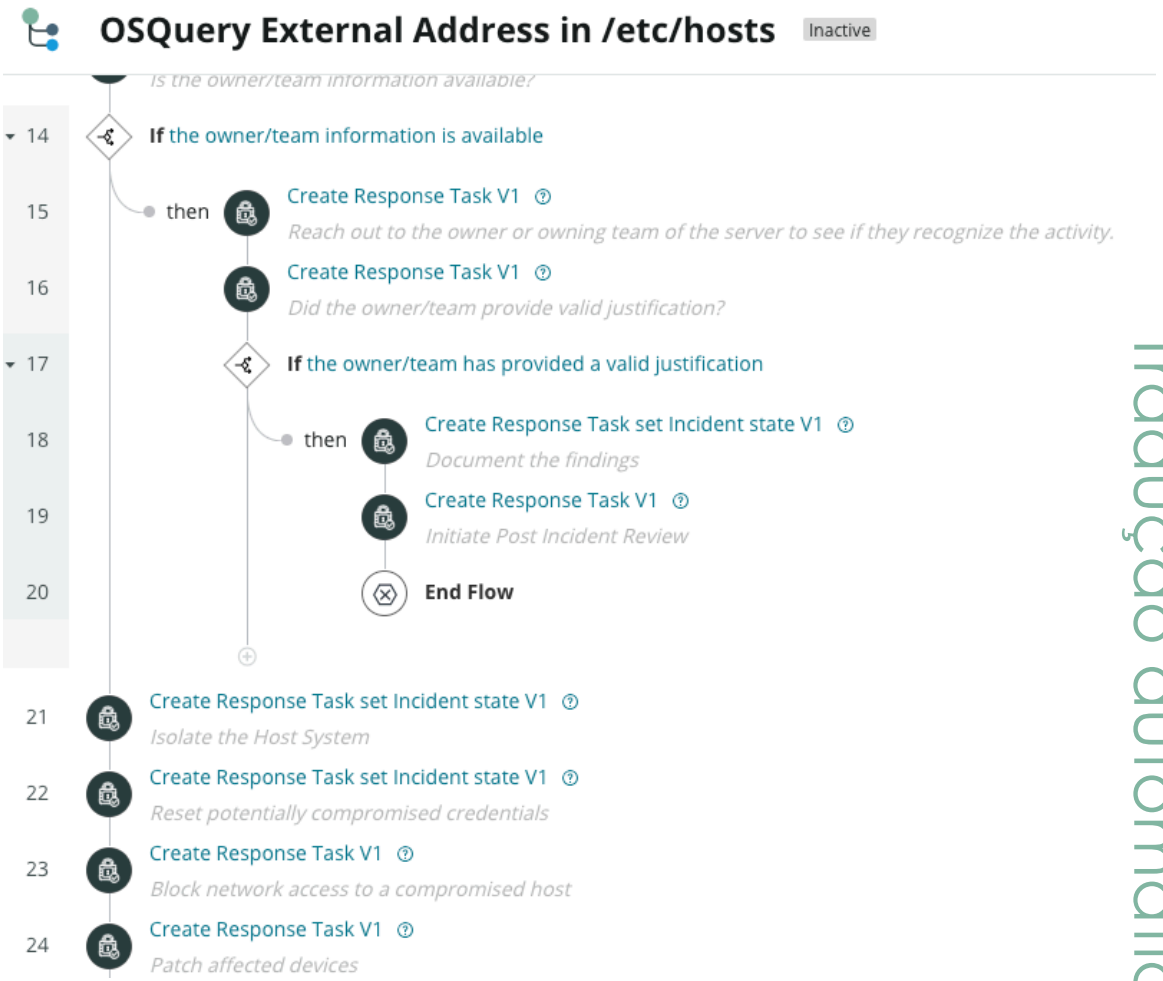
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Na Ação 18, documente as descobertas até o momento.

ii. Na Ação 19, inicie uma análise pós-incidente.

Na Ação 20, após a análise pós-incidente, o fluxo termina.

Como usar o OSquery de endereço externo no playbook do arquivo /etc/hosts



12. Na Ação 21, se as informações do proprietário ou da equipe não estiverem disponíveis, isole o sistema host.
13. Na Ação 22, redefina as credenciais potencialmente comprometidas.
14. Na Ação 23, bloqueie o acesso à rede do host comprometido.
15. Na Ação 24, corrija os dispositivos afetados.
16. Na Ação 25, remova a contenção e traga os sistemas de volta aos padrões operacionais.
17. Na Ação 26, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para usuário que exclui histórico de bash - Nuvem

Este playbook fornece etapas de correção sistemática para investigar incidentes que indicam se alguém tentou remover o arquivo de histórico de bash (`.bash_history`) de um servidor Linux.

Nota: Você precisa atenuar este alerta com cuidado, pois ele raramente é acionado e pode indicar uma ameaça interna.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o playbook de histórico de bash para exclusão de usuário

Use as etapas a seguir para configurar o playbook de histórico de bash para exclusão de usuário.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

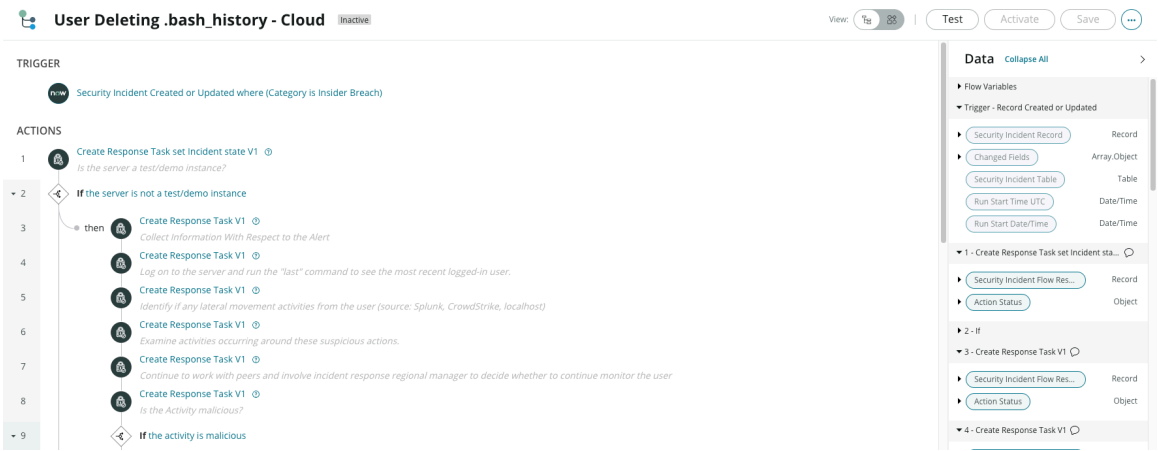
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook Exclusão de usuário .bash_history - Nuvem**.
3. Opcional: Crie uma cópia do fluxo do playbook de exclusão de usuário .bash_history - Nuvem e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Histórico de bash de exclusão de usuário - Playbook de nuvem



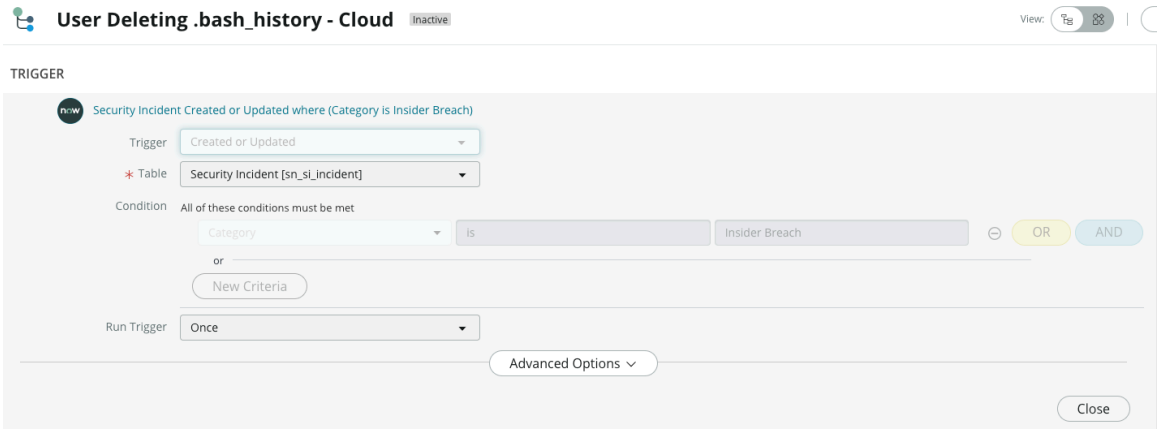
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Violação de insider**.

Histórico de bash de exclusão de usuário - Condição do gatilho do playbook em nuvem



Use o playbook de histórico de bash para exclusão de usuário

Use este playbook para investigar incidentes que indicam se alguém tentou remover o arquivo de histórico bash de um servidor Linux. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Excluir usuário do histórico de bash (`.bash_history`).

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique se o servidor é uma instância de teste ou de demonstração.
2. Na Ação 2, se o servidor não for uma instância de teste ou de demonstração, execute as seguintes etapas:

   a. Na Ação 3, colete as seguintes informações para o alerta:
      - Nome de usuário
      - Endereço IP
      - Comandos maliciosos que tentam excluir o histórico de bash
      - Todos os comandos executados pelo usuário, se disponíveis nos logs do CrowdStrike.

   b. Na Ação 4, faça login no servidor e execute o `último` comando para exibir o usuário conectado mais recentemente.

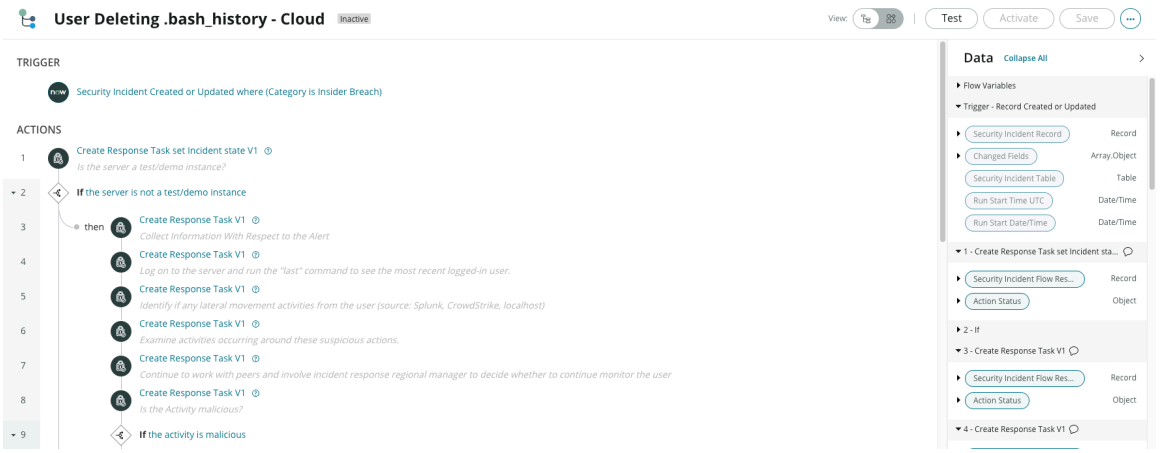
   c. Na Ação 5, identifique se houve atividades de movimento lateral do usuário (Origem: Splunk, CrowdStrike, localhost).

   d. Na Ação 6, examine as atividades que ocorrem em torno dessas ações suspeitas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de histórico de bash para exclusão de usuário



e. Na Ação 7, continue trabalhando com colegas e envolva o gerente regional de resposta a incidentes na decisão de continuar o monitoramento do usuário.

f. Na Ação 8, determine se a atividade é mal-intencionada ou não.

g. Na Ação 9, se a atividade for mal-intencionada, execute as seguintes etapas:

i. Na Ação 10, durante a investigação, entre em contato com o Suporte de TI e solicite o congelamento de conta.

ii. Na Ação 11, certifique-se de que a instância seja restaurada para um estado normal livre de atividades mal-intencionadas.

iii. Na Ação 12, remova a contenção e traga os sistemas de volta aos padrões operacionais.

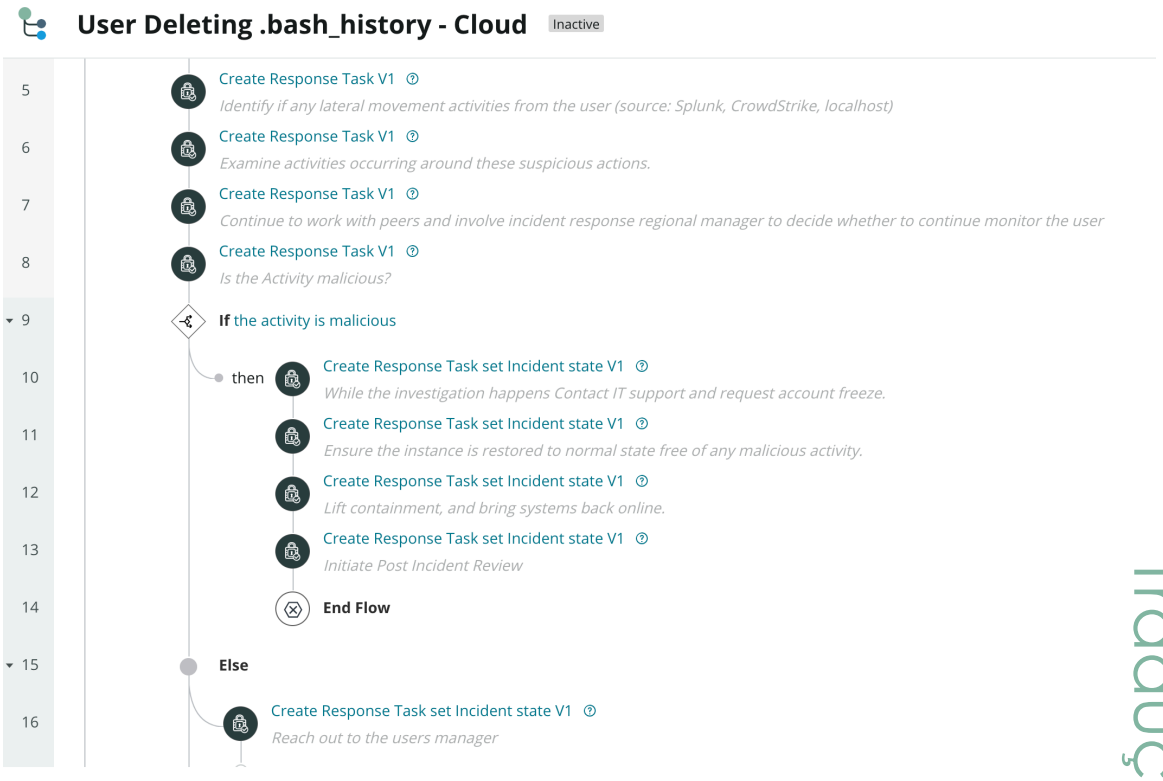
iv. Na Ação 13, inicie uma análise pós-incidente.

Na Ação 14, após a análise pós-incidente, o fluxo termina.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook de histórico de bash para exclusão de usuário



h. Na Ação 15, se a atividade não for mal-intencionada, na Ação 16, entre em contato com o gerente do usuário.
Você pode usar o modelo de e-mail fornecido para entrar em contato com o gerente do usuário e informá-lo sobre a abordagem recomendada.

3. Na Ação 17, documente as descobertas até o momento.

4. Na Ação 18, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para tentativas de VPN bem-sucedidas das contas de serviço - Corp/Cloud

Este playbook fornece etapas de correção sistemática para investigar incidentes que rastreiam tentativas de login bem-sucedidas de contas de serviço por meio de VPN. As contas de serviço não devem ter eventos de login de uma VPN e esses eventos podem ser indicadores de força bruta ou possível exposição das credenciais da conta.

Configurar as tentativas de VPN bem-sucedidas no playbook de contas de serviço

Use as etapas a seguir para configurar as tentativas de VPN bem-sucedidas no playbook de contas de serviço.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Tradução automática

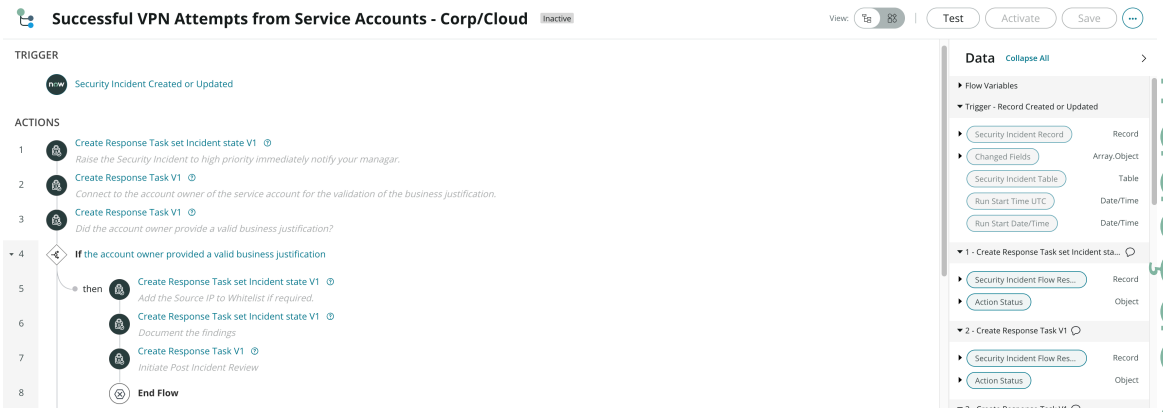
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione **Tentativas de VPN bem-sucedidas no playbook de Contas de serviço**.
3. Opcional: Crie uma cópia das tentativas de VPN bem-sucedidas do fluxo do playbook de contas de serviço e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

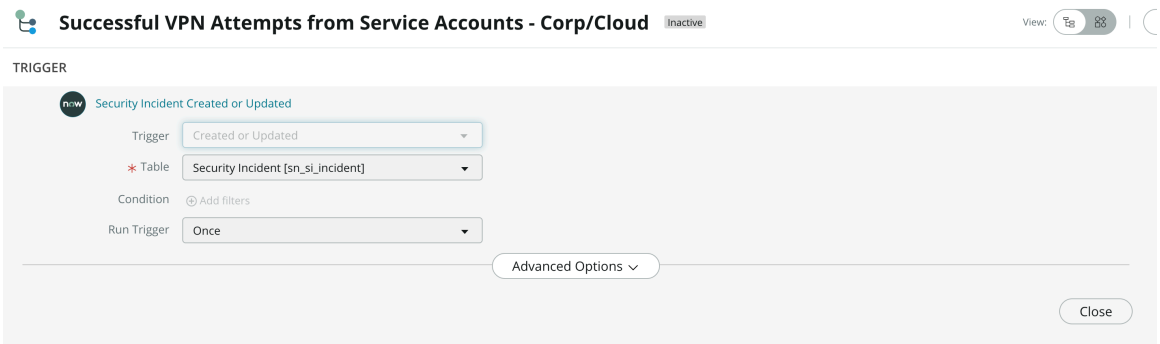
   Tentativas de VPN bem-sucedidas de Contas de serviço - Playbook de Corp/Nuvem

4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

   Este playbook é acionado e associado ao incidente de segurança quando o incidente de segurança é criado ou atualizado com base nas condições necessárias. Por exemplo, quando **Categoria** é **Violação de insider**.

   Tentativas de VPN bem-sucedidas das contas de serviço – Condição de gatilho do playbook Corp/Cloud

Use as tentativas de VPN bem-sucedidas do playbook de contas de serviço

Use este playbook para investigar incidentes que rastreiam tentativas de login bem-sucedidas de contas de serviço por meio de VPN. As etapas a seguir fornecem instruções

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

das ações, tarefas e subfluxos que estão disponíveis nas Tentativas de VPN bem-sucedidas do playbook de Contas de serviço.

Antes de Iniciar

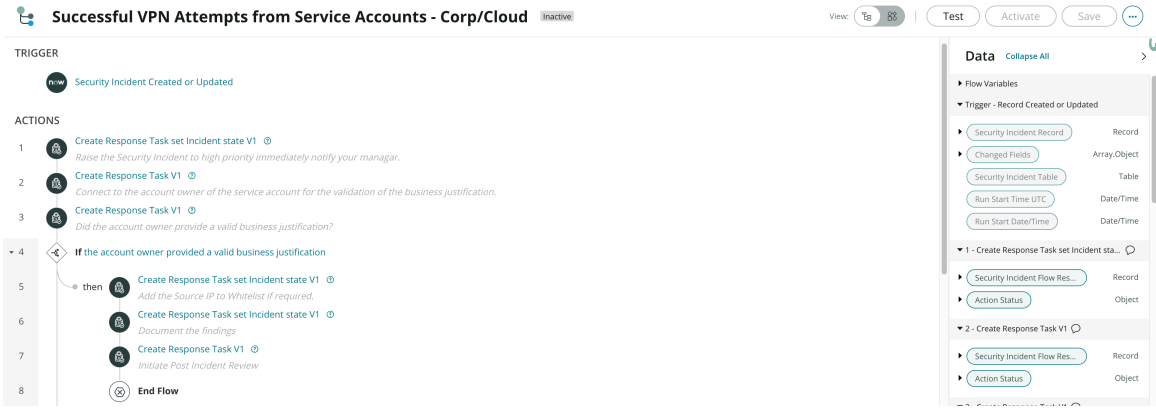
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, eleve o incidente de segurança para alta prioridade e notifique imediatamente o seu gerente.
2. Na Ação 2, entre em contato com o proprietário da conta de serviço para validar a justificativa de negócio.
   Você pode usar o modelo de e-mail fornecido para entrar em contato com o proprietário da conta de serviço para validar a justificativa de negócios.
3. Na Ação 3, verifique se o proprietário da conta de serviço forneceu uma justificativa de negócio válida.

Tentativas de VPN bem-sucedidas de Contas de serviço - Playbook de Corp/Nuvem



4. Na Ação 4, se o proprietário da conta de serviço forneceu uma justificativa de negócio válida, execute as seguintes etapas:

   a. Na Ação 5, adicione o IP de origem à lista de permissões, se necessário.

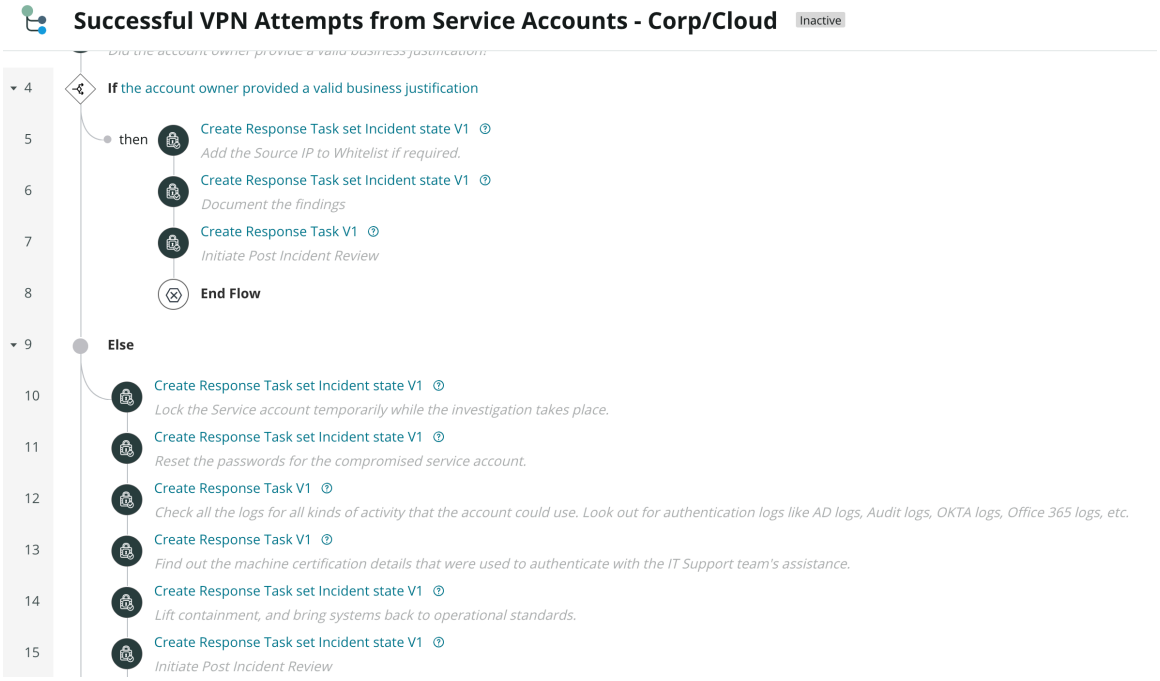
   b. Na Ação 6, documente as descobertas até o momento.

   c. Na Ação 7, inicie uma análise pós-incidente.
   Na Ação 8, após a análise pós-incidente, o fluxo termina.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar as tentativas de VPN bem-sucedidas das contas de serviço - Playbook de Corp/Nuvem



5. Na Ação 9, se o proprietário da conta de serviço não tiver fornecido uma justificativa de negócio válida, execute as seguintes etapas:

a. Na Ação 10, bloqueie temporariamente a conta de serviço enquanto a investigação ocorre.

b. Na Ação 11, redefina as senhas da conta de serviço comprometida.

c. Na Ação 12, verifique os logs de todos os tipos de atividade que a conta pode usar. Procure logs de autenticação, como logs do Active Directory, logs de auditoria, logs do Okta, logs do Office 365 e assim por diante.

d. Na Ação 13, encontre os detalhes de certificação da máquina usados para autenticar com a assistência da equipe de suporte de TI.

e. Na Ação 14, remova a contenção e traga os sistemas de volta aos padrões operacionais.

f. Na Ação 15, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para tentativa de acesso a contas desativadas

Este playbook é acionado quando um funcionário cuja conta está encerrada, desabilitada ou separada tenta fazer login com suas credenciais. O estado de identidade do usuário no ponto de navegação geralmente é atualizado para desabilitado na data de rescisão.

30 dias é o tempo ideal a partir da data de rescisão para que ele seja atualizado para um estado separado. Você pode usar a lógica de negócios no ponto de navegação para excluir as contas RSA e remover as associações de grupo do Active Directory (AD) após 30 dias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o playbook de Conta Desativada de Tentativa de Acesso

Use as etapas a seguir para configurar o playbook de Conta Desativada de Tentativa de Acesso.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **Tentativa de acesso de conta desativada**.
3. Opcional: Crie uma cópia do fluxo do playbook de Conta Desativada de Tentativa de Acesso e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

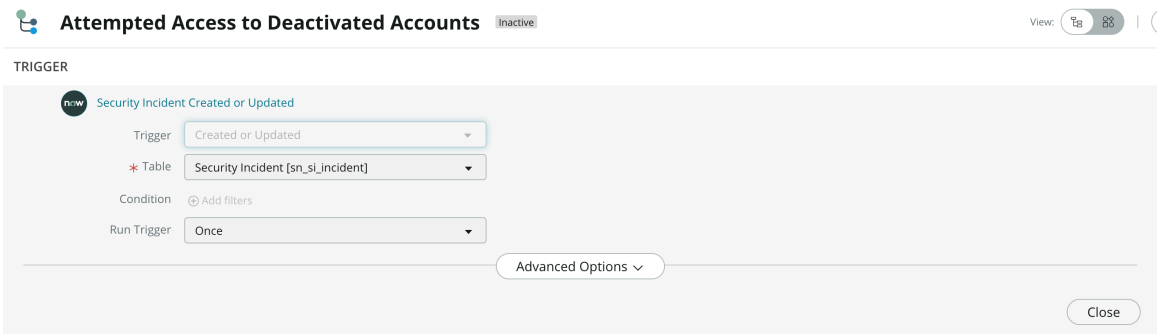
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado quando o incidente de segurança é criado ou atualizado com base nas condições necessárias. Por exemplo, quando a **Categoria** for **Violação de insider**

Condição de gatilho do playbook de tentativa de acesso a contas desativadas



Usar o playbook Tentativa de acesso a contas desativadas

Use este playbook quando um funcionário cuja conta foi encerrada, desabilitada ou separada tentar fazer login com suas credenciais. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Tentativa de acesso a contas desativadas.

Antes de Iniciar

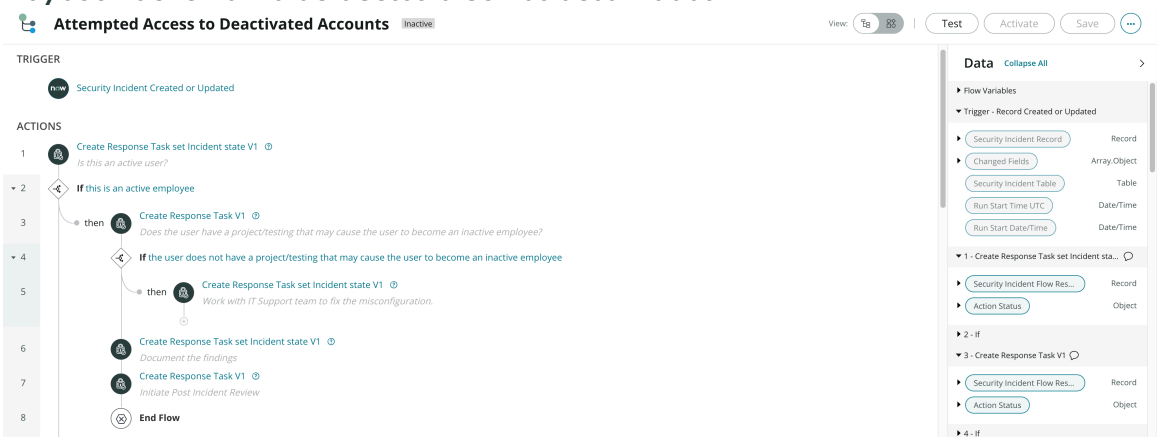
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique se a tentativa de acesso às contas desativadas foi feita por um usuário ativo.
2. Na Ação 2, verifique se a tentativa de acesso às contas desativadas foi feita por um funcionário ativo.

Playbook de tentativa de acesso a contas desativadas



3. Se a tentativa de acesso às contas desativadas tiver sido feita por um funcionário ativo, execute as seguintes etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 3, verifique se o usuário tinha um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo.

b. Na Ação 4, se o usuário não tiver um projeto ou caso de teste que tenha feito com que ele se tornasse um funcionário inativo, trabalhe com a equipe de suporte de TI para corrigir o erro de configuração.
O fluxo termina.

c. Na Ação 5, se o usuário tiver um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo, execute as seguintes etapas:

i. Na Ação 6, documente as descobertas até o momento.

ii. Na Ação 7, inicie uma análise pós-incidente.

Na Ação 8, após a análise pós-incidente, o fluxo termina.

4. Na Ação 9, se a tentativa de acesso à conta desativada não tiver sido feita por um funcionário ativo, execute as seguintes etapas:

a. Na Ação 10, verifique se o usuário teve logins bem-sucedidos.

b. Na Ação 11, verifique quando o funcionário foi desligado.

c. Na Ação 12, investigue os eventos no Splunk para examinar as atividades do usuário durante o período.

d. Na Ação 13, com base na investigação até o momento, determine se o usuário exfiltrou algum dado.

e. Na Ação 14, se o usuário não exfiltrar nenhum dado, execute as seguintes etapas:

i. Na Ação 15, trabalhe com a equipe de suporte de TI para encerrar todas as sessões ativas e desabilitar as contas.

ii. Na Ação 16, documente as descobertas até o momento.

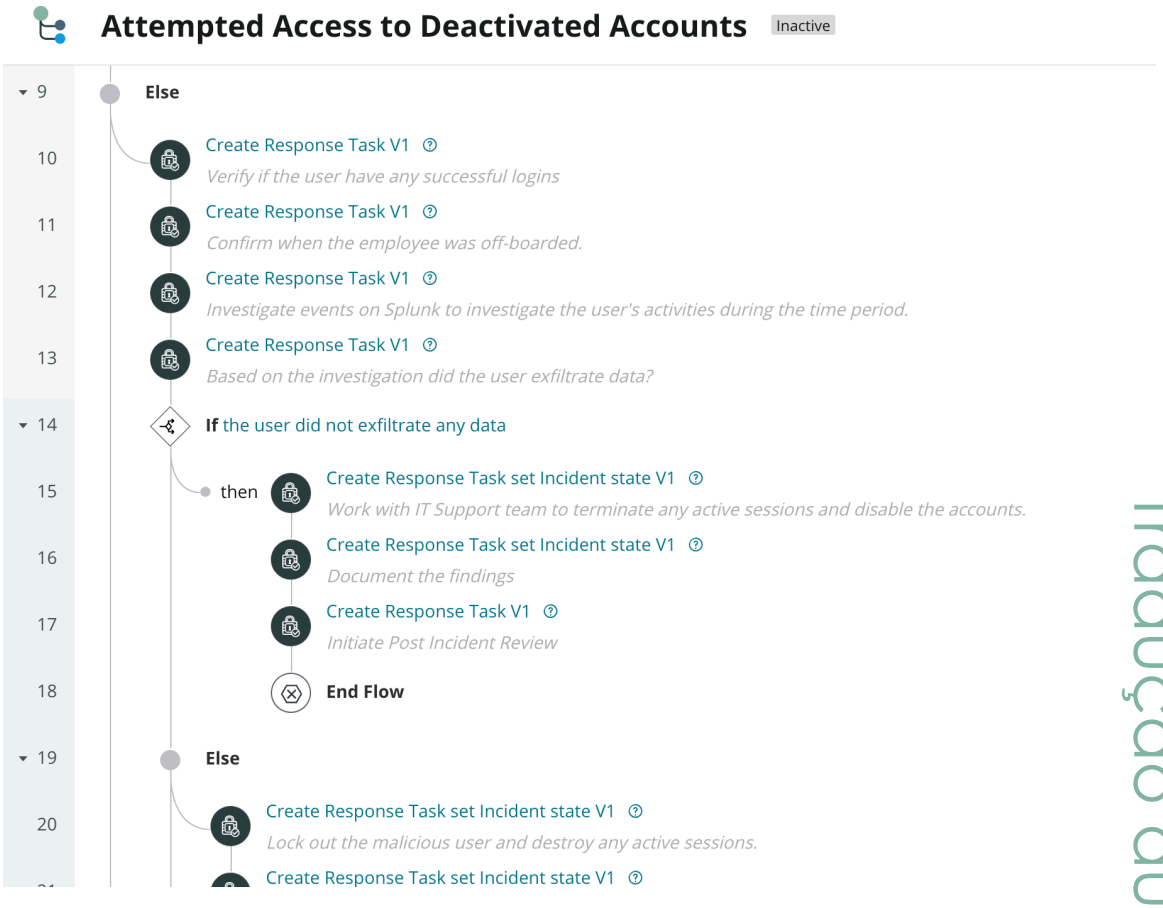
iii. Na Ação 17, inicie uma análise pós-incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na Ação 18, após a análise pós-incidente, o fluxo termina.

Como usar o playbook Tentativa de acesso a contas desativadas



5. Na Ação 19, se o usuário exfiltrar quaisquer dados, execute as seguintes etapas:

a. Na Ação 20, bloqueie o usuário mal-intencionado e destrua todas as sessões ativas.

b. Na Ação 21, trabalhe com a equipe de suporte de TI para desabilitar todas as contas.

c. Na Ação 22, certifique-se de que os recursos sejam restaurados ao estado normal e livres de qualquer atividade mal-intencionada.
Você pode recriar a imagem dos recursos, se necessário.

d. Na Ação 23, remova a contenção e traga os sistemas de volta aos padrões operacionais.

e. Na Ação 24, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook for T1003 - Evasão de defesa - Mimikatz DCShadow

Este playbook fornece etapas de correção sistemática para investigar incidentes suspeitos de serem causados pelo Mimikatz DCShadow. O DCShadow é um recurso do Mimikatz que simula o comportamento de um controlador de domínio (um servidor que controla o Active Directory) para injetar seus próprios dados, ignorando a maioria dos controles de segurança padrão (incluindo SIEMs).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Mimikatz DCShadow ajuda o invasor a estabelecer um controlador de domínio (DC) não autorizado que se torna parte do Active Directory (AD). Depois de registrado, ele pode atuar como um DC legítimo e causar danos.

Configurar o T1003 - Evasão de defesa - Playbook do Mimikatz DCSombra

Use as etapas a seguir para configurar o playbook T1003 - Evasão de defesa - Mimikatz DCSombra.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1003 - Evasão de defesa - Mimikatz DCSombra**.
3. Opcional: Crie uma cópia do fluxo do playbook T1003 - Evasão de defesa - Mimikatz DCSombra e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   T1003 – Evasão de defesa – Playbook do Mimikatz DCShadow

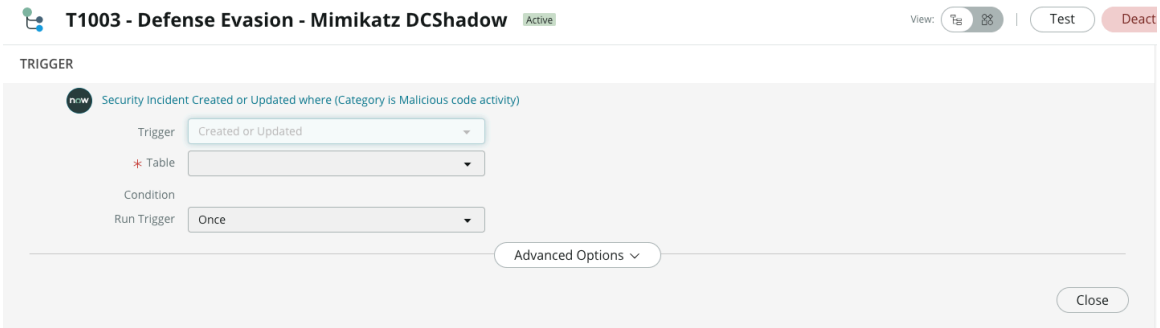
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando a **categoria** é uma **atividade de código malicioso**.

T1003 – Evasão de defesa – Condição de gatilho do playbook do Mimikatz DCShadow



Use o playbook T1003 - Evasão de defesa - Mimikatz DCSombra

Use este playbook para investigar incidentes de segurança suspeitos de serem causados pelo Mimikatz DCShadow. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Evasão de defesa - Mimikatz DCSombra.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, descubra qual conta é responsável pela criação do novo DC (Controlador de domínio).
2. Na Ação 2, entre em contato com o usuário para validar a justificativa de negócio. Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário.
3. Na Ação 3, verifique se o usuário forneceu uma justificativa de negócio válida.
4. Na Ação 4, se o usuário forneceu uma justificativa de negócio válida, execute as seguintes etapas:

T1003 – Evasão de defesa – Playbook do Mimikatz DCShadow

Tradução automática

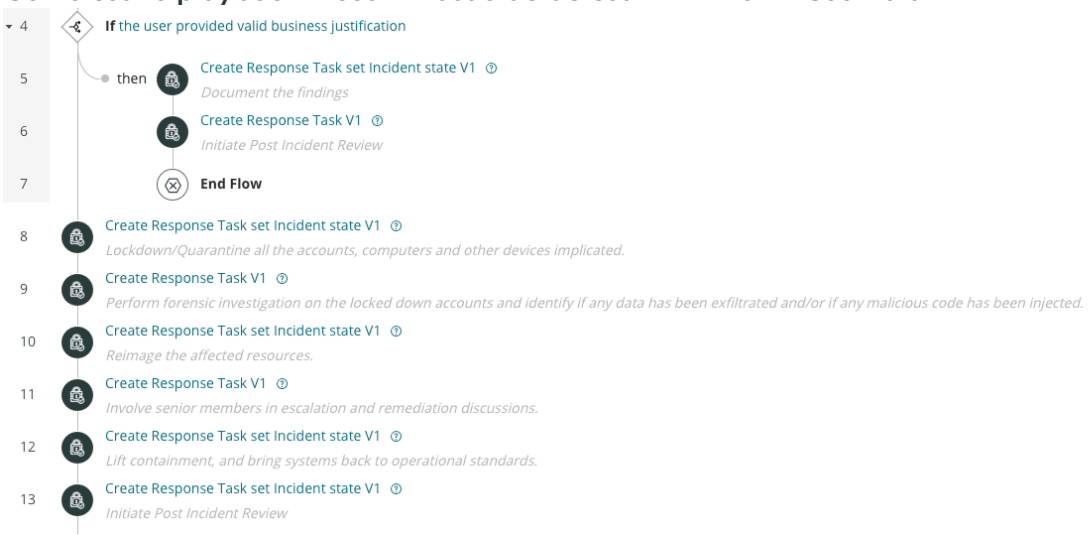
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 5, documente as descobertas até o momento.

b. Na Ação 6, inicie uma análise pós-incidente.
Na Ação 7, após a análise pós-incidente, o fluxo termina.

5. Na Ação 8, se o usuário não forneceu uma justificativa de negócio válida, execute as seguintes etapas:

Como usar o playbook T1003 - Evasão de defesa - Mimikatz DCSombra



a. Na Ação 9, bloqueie ou coloque em quarentena todas as contas, computadores e outros dispositivos envolvidos.

b. Na Ação 10, execute uma investigação forense nas contas bloqueadas e identifique se algum dado foi exfiltrado ou algum código mal-intencionado foi injetado.

c. Na Ação 11, crie novamente a imagem dos recursos afetados.

d. Na Ação 12, remova a contenção e traga os sistemas de volta aos padrões operacionais.

e. Na Ação 13, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para T1003 - Despejo de credenciais - Mimikatz DCSync

Este playbook fornece etapas de correção sistemática para investigar incidentes suspeitos de serem causados pelo Mimikatz DCSync. Este playbook é acionado quando uma das funções do Mimikatz (`lsadump::dcsync`) é usada. A função é normalmente usada em controladores de domínio (DC) atacados.

O Mimikatz é uma ferramenta popular de invasão que permite aos usuários emitir comandos que ajudam a recuperar dados confidenciais do sistema atacado. Os dados confidenciais incluem senhas, seus hashes e outros.

Nota: Este é um alerta de alta fidelidade, que é considerado como raramente acionado. Quando ele for acionado, você deve notificar um membro da equipe sênior ou gerente imediatamente.

Configurar o playbook T1003 - Despejo de credenciais - Mimikatz DCsync

Use as etapas a seguir para configurar o playbook T1003 - Despejo de credenciais - Mimikatz DCsync.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

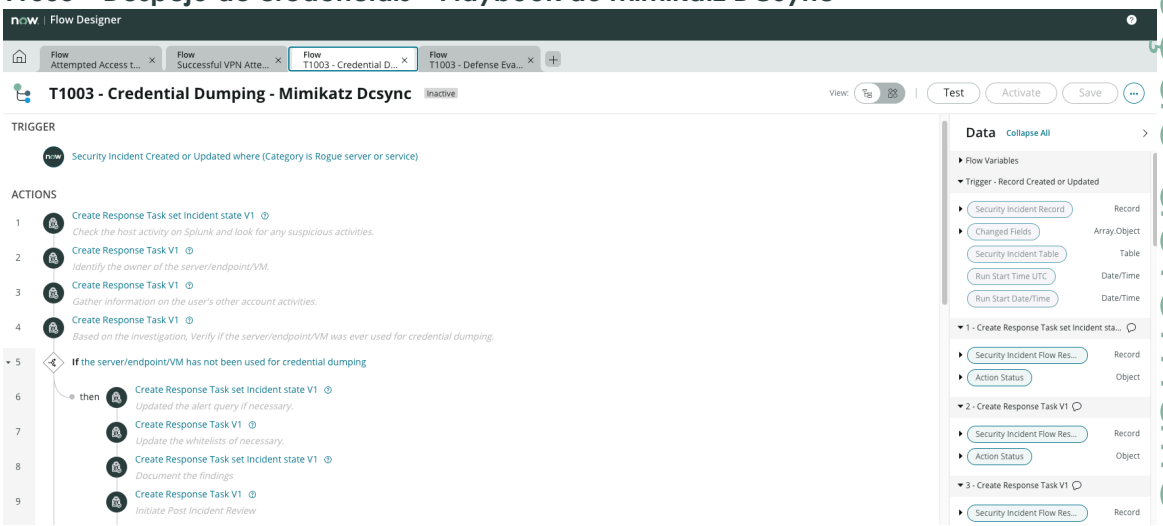
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1003 - Dumping de credenciais - Mimikatz DCsync**.
3. Opcional: Crie uma cópia do fluxo do playbook T1003 - Despejo de credenciais - Mimikatz DCsync e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

   T1003 – Despejo de credenciais – Playbook do Mimikatz DCSync



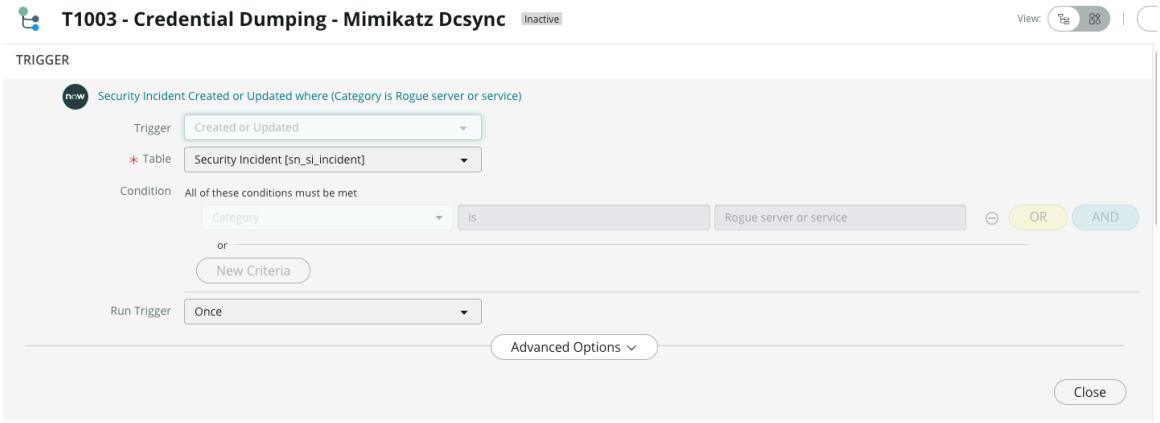
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Servidor ou serviço**não autorizado.

T1003 – Despejo de credenciais – Condição do gatilho do playbook do Mimikatz DCSync



Use o playbook T1003 - Despejo de credenciais - Mimikatz DCsync

Use este playbook para investigar incidentes suspeitos de serem causados pelo Mimikatz DCSync. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Despejo de credenciais - Mimikatz DCsync.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

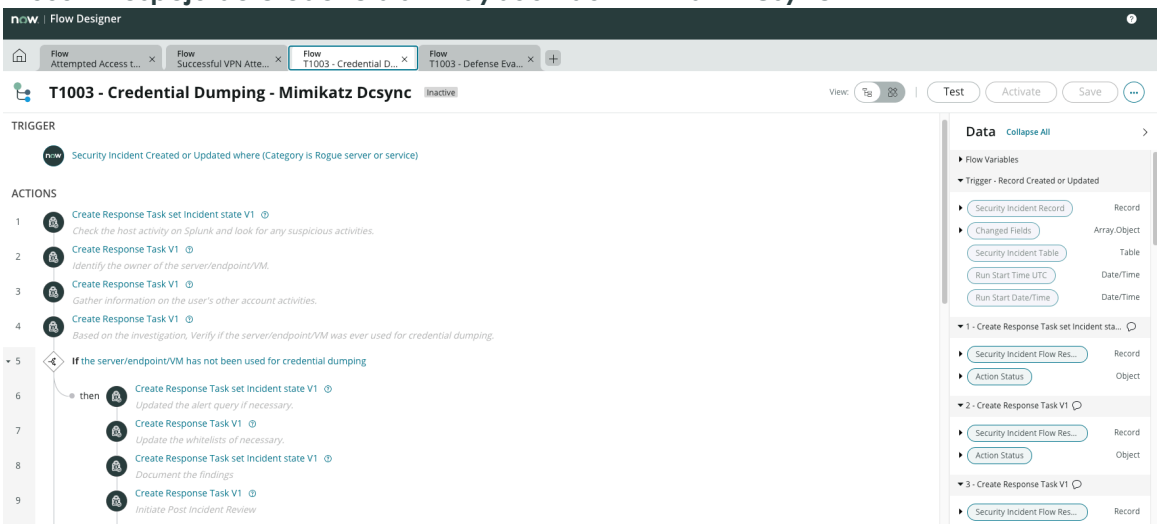
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique a atividade do host no Splunk e procure atividades suspeitas.
2. Na Ação 2, identifique o proprietário do servidor/endpoint/VM.
   Se o usuário estiver on-line, execute o CrowdStrike EDR para obter um escopo melhor das atividades do sistema.
3. Na Ação 3, colete informações sobre outras atividades de conta do usuário.
4. Na Ação 4, com base na investigação, verifique se o servidor/endpoint/VM já foi usado para despejo de credenciais.
5. Na Ação 5, se o servidor/endpoint/VM não tiver sido usado para despejo de credenciais, execute as seguintes ações:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

T1003 – Despejo de credenciais – Playbook do Mimikatz DCsync



a. Na Ação 6, atualize a consulta de alerta, se necessário.

b. Na Ação 7, atualize a lista de permissões, se necessário.

c. Na Ação 8, documente as descobertas até o momento.

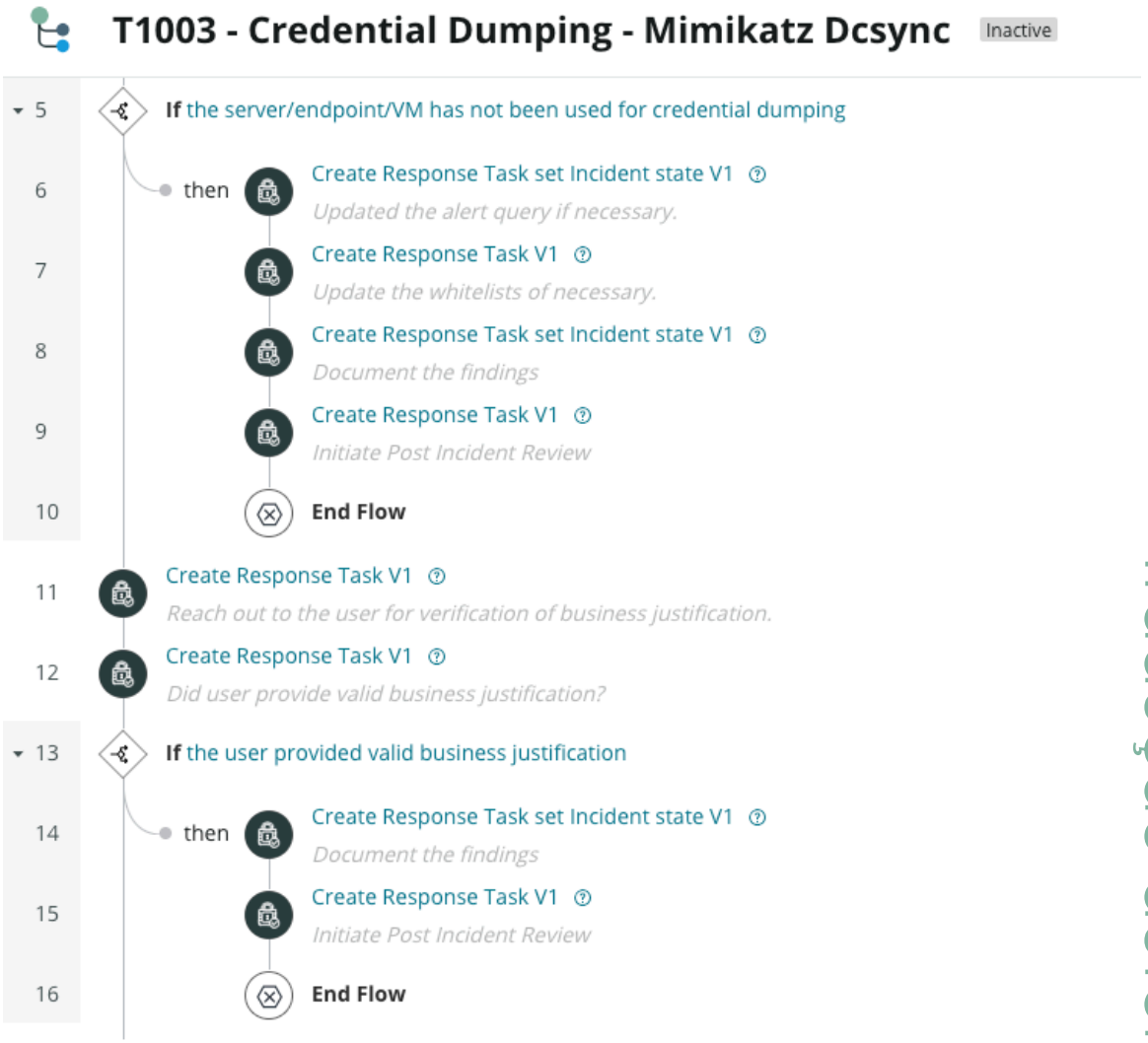
d. Na Ação 9, inicie uma análise pós-incidente.
Na Ação 10, o fluxo termina.

6. Se o servidor/endpoint/VM tiver sido usado para despejo de credenciais, na Ação 11, entre em contato com o usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook T1003 - Despejo de credenciais - Mimikatz DCsync



7. Na Ação 12, entre em contato com o usuário para validar a justificativa de negócio.
8. Na Ação 13, se o usuário forneceu uma justificativa de negócio válida, execute as seguintes Ações:

   a. Na Ação 14, documente as descobertas até o momento.

   b. Na Ação 15, inicie uma análise pós-incidente.
   Na Ação 16, o fluxo termina.

9. Se o usuário não forneceu uma justificativa de negócio válida, na Ação 17, coloque o sistema em quarentena.
10. Na Ação 18, remova todos os arquivos indesejados que possam ter sido criados ou excluídos pelas contas não autorizadas.
11. Na Ação 19, remova a contenção e traga os sistemas de volta aos padrões operacionais.
12. Na Ação 20, conclua a revisão pós-incidente antes de fechar a tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook para falhas de login de usuário do Okta de vários IPs

Este playbook fornece etapas de correção sistemática para investigar incidentes de falhas de login de usuário no Okta.

O playbook Falhas de login de usuário do Okta de vários IPs fornece instruções sobre como analisar o alerta quando falhas de conta da ServiceNow são observadas no Okta de vários IPs que não são da ServiceNow. O alerta relacionado a este playbook verifica os logs do Okta. Ele aciona um alerta quando ocorre uma falha de login para IDs de usuário da ServiceNow de mais de três intervalos de IP não ServiceNow em uma duração de 1 hora.

Configurar o playbook Falhas de login de usuário do Okta a partir de vários IPs

Use as etapas a seguir para configurar o playbook Falhas de login de usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

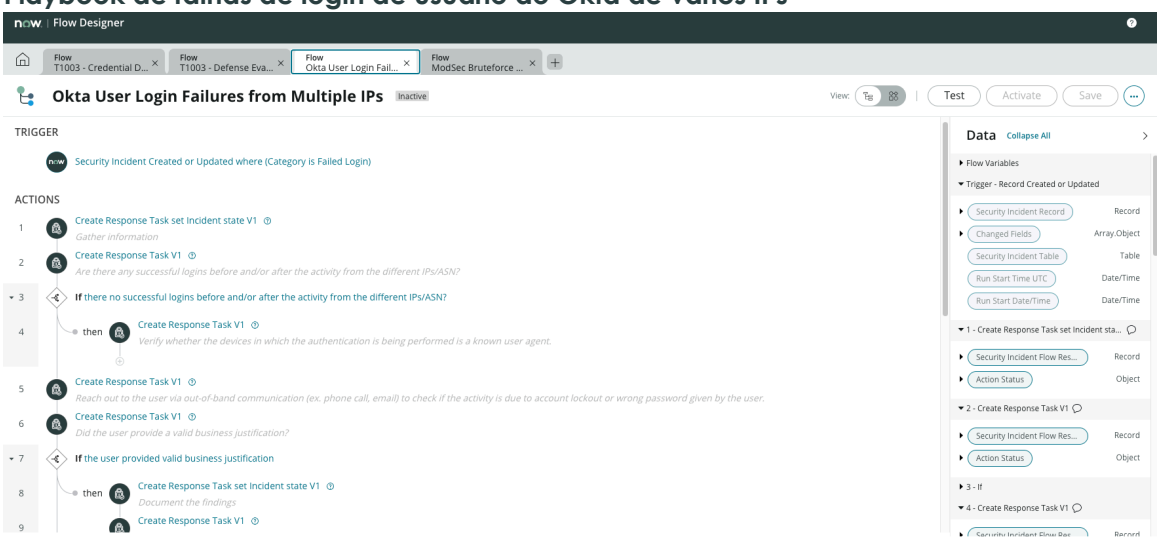
Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **Falhas de login de usuário do Okta de vários IPs**.
3. Opcional: Crie uma cópia do fluxo do playbook Falhas de login de usuário do Okta a partir de vários IPs e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Playbook de falhas de login de usuário do Okta de vários IPs



4. Ative os playbooks.

Tradução automática

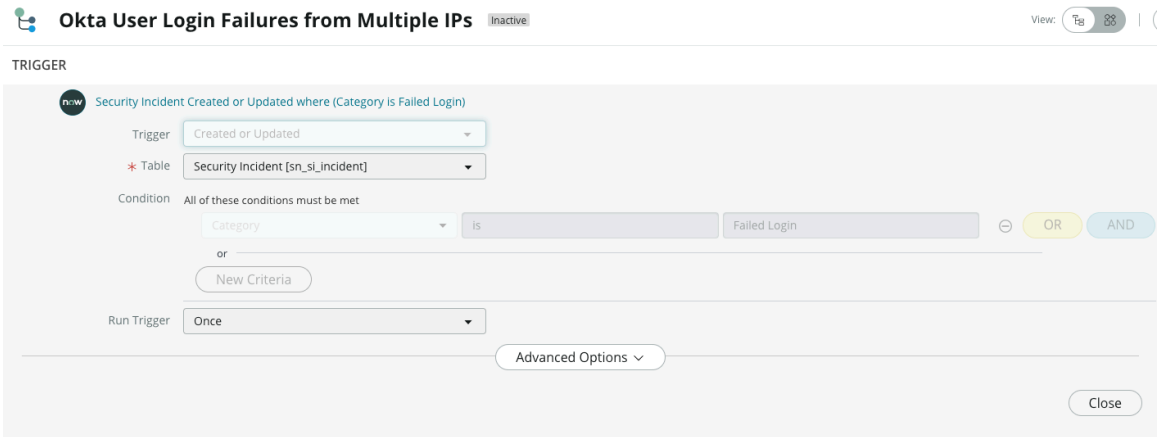
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Ative o fluxo principal para usar o playbook disponível no sistema de base.

b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

5. Defina uma **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Falha de login**.

Falhas de login de usuário do Okta de vários IPs Condição de gatilho do playbook



Usar o playbook Falhas de login de usuário do Okta de vários IPs

Use este playbook para investigar incidentes de segurança relacionados a falhas de login de usuário no Okta. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook Falhas de login de usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

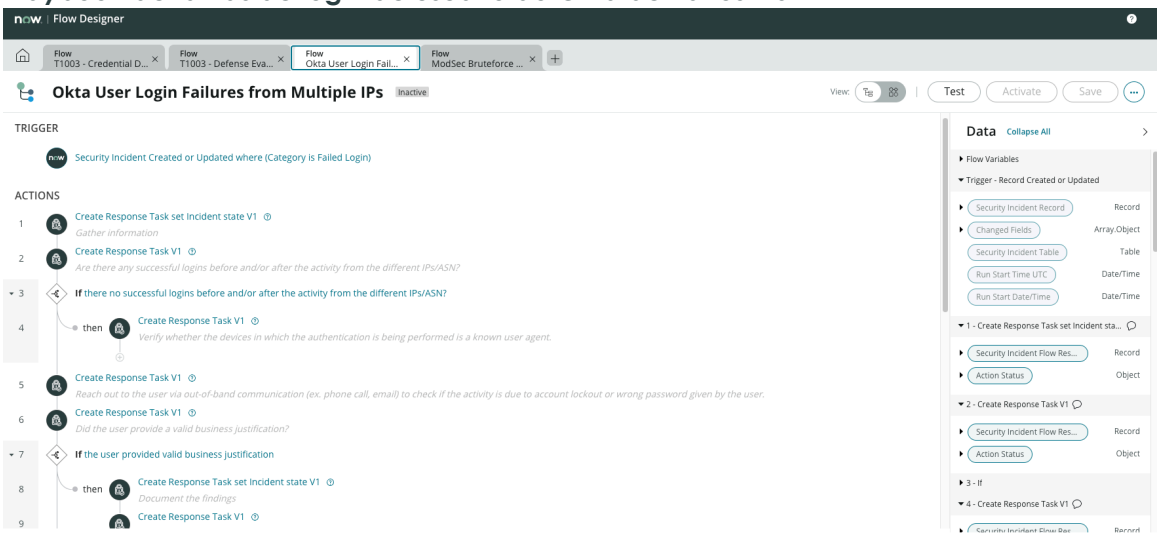
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, execute as seguintes tarefas:
   - Identifique a conta de usuário que está sendo direcionada.
   - Verifique a sub-rede IP e verifique se todas pertencem ao mesmo proprietário de Número de sistema autônomo (ASN).
2. Na Ação 2, verifique se houve logins bem-sucedidos antes ou depois da atividade de diferentes IPs/ASNs.
3. Na Ação 3, se não houve logins bem-sucedidos antes ou depois da atividade de diferentes IPs/ASNs, na Ação 4, verifique se os dispositivos nos quais a autenticação está sendo realizada são agentes de usuário conhecidos.
   Se os dispositivos forem autenticados por agentes de usuário conhecidos, o fluxo será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de falhas de login de usuário do Okta de vários IPs



4. Na Ação 5, com base na investigação, entre em contato com o usuário por meio de comunicação fora de banda (por exemplo, chamada telefônica ou e-mail) para verificar se a atividade se deve ao bloqueio de conta ou a uma senha incorreta fornecida pelo usuário.
5. Na Ação 6, verifique se o usuário forneceu uma justificativa de negócio válida.
6. Na Ação 7, se o usuário forneceu uma justificativa de negócio válida, execute as tarefas a seguir.

   a. Na Ação 8, crie uma tarefa de resposta para documentar as descobertas até o momento.

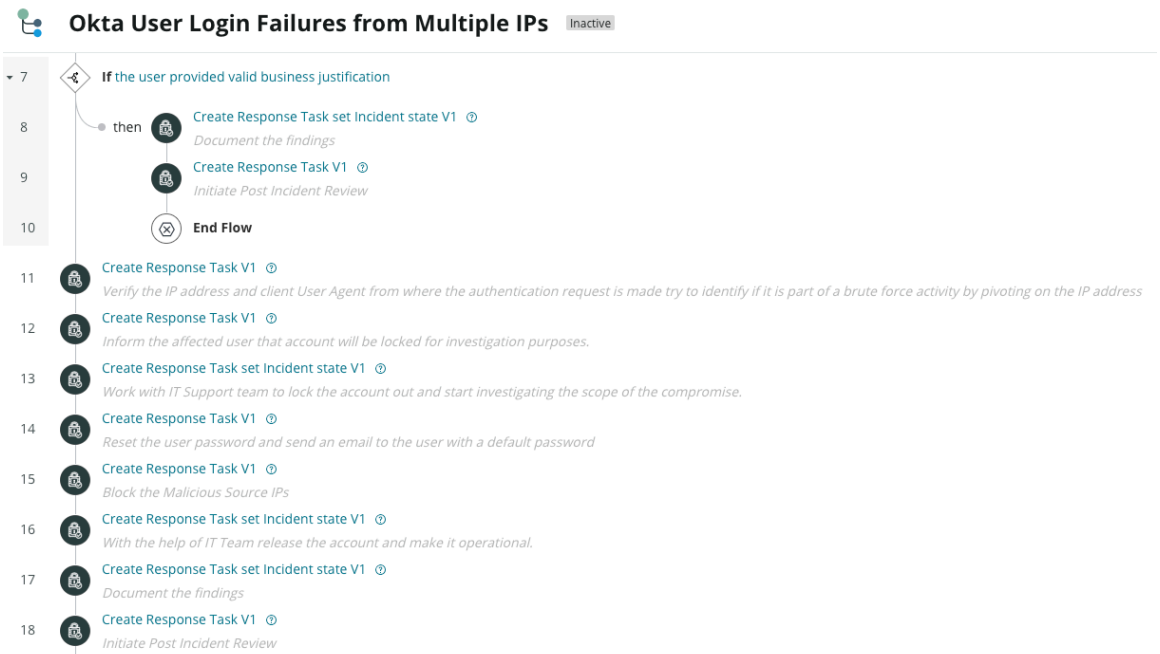
   b. Na Ação 9, crie uma resposta para iniciar uma análise pós-incidente.
   Na Ação 10, o fluxo termina.

7. Na Ação 11, verifique o endereço IP e o agente do usuário cliente de onde a solicitação de autenticação é feita e tente identificar se ela faz parte de uma atividade de força bruta girando no endereço IP.
8. Na Ação 12, informe ao usuário afetado que a conta será bloqueada para fins de investigação.
   Você pode usar o modelo de e-mail fornecido para informar o usuário afetado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook Falhas de login de usuário do Okta de vários IPs



9. Na Ação 13, trabalhe com a equipe de suporte de TI para bloquear a conta e começar a investigar o escopo do comprometimento.
10. Na Ação 14, redefina a senha do usuário e envie um e-mail para o usuário com a senha padrão.
11. Na Ação 15, bloqueie os IPs de origem mal-intencionados.
12. Na Ação 16, obtenha ajuda da equipe de suporte de TI para liberar a conta e trazê-la de volta aos padrões operacionais.
13. Na Ação 17, documente as descobertas até o momento.
14. Na Ação 18, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para força bruta do ModSec por pico de IP

Este playbook fornece etapas de correção sistemática para investigar incidentes de tentativas de força bruta nas páginas de login de vários IPs detectados pelo ModSec. As condições do evento podem ser definidas na própria política ModSec e gerarão um alerta no Splunk quando o evento for criado no ModSec.

Este playbook ajuda a detectar contagens anormais de tráfego na página de login. Neste exemplo, duas rajadas sucessivas de mais de 50 ocorrências/minuto devem ser de um IP para a página de login, o que indica uma tentativa de força bruta de login.

Configurar força bruta do ModSec por playbook de Burst de IP

Use as etapas a seguir para configurar o playbook de força bruta do ModSec por IP Burst.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Verifique se você instalou o Spoke das Operações de segurança (*sn_sec_spoke*).

Tradução automática

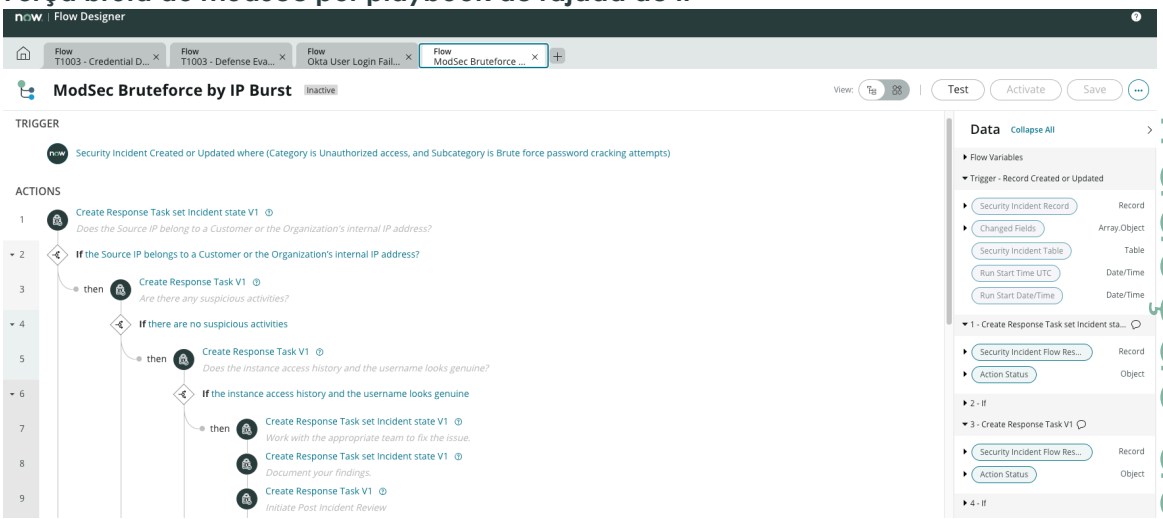
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook ModSec Bruteforce por IP Burst**.
3. Opcional: Crie uma cópia do fluxo do playbook ModSec Bruteforce by IP Burst e faça as modificações necessárias.

   (Optional) Para criar uma cópia do fluxo do playbook, selecione o ícone de menu mais ações (menu) e selecione **Copiar fluxo**. Execute esta etapa somente se você planeja personalizar ou fazer mudanças específicas no fluxo.

Força bruta do ModSec por playbook de rajada de IP



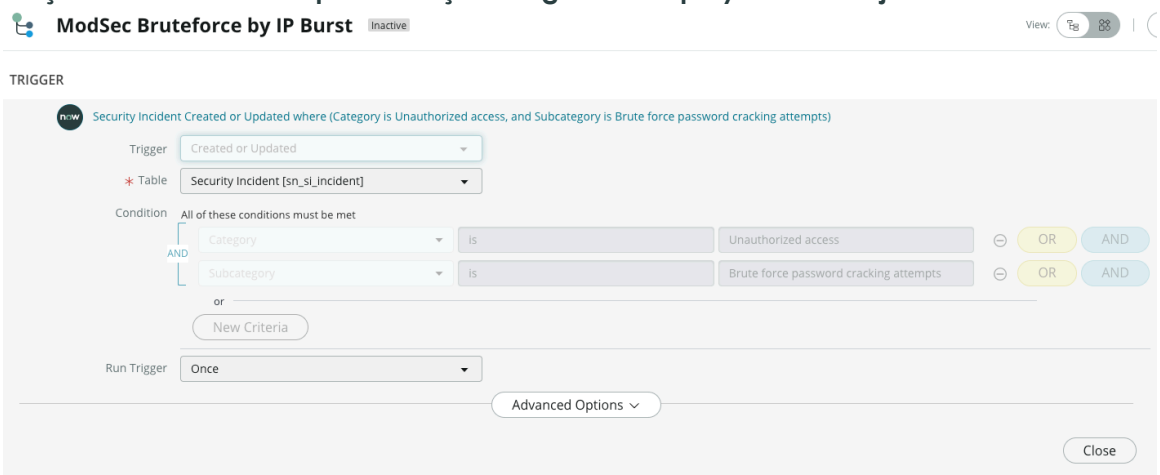
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. Defina uma **Condição do gatilho** para o playbook.
   Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A**categoria** é **Acesso não autorizado**.
- **A subcategoria** é **Tentativas de força bruta de quebra de senha**.

Força bruta do ModSec por condição de gatilho do playbook de rajada de IP



Use o playbook de Força bruta do ModSec por Burst de IP

Use este playbook para investigar incidentes de tentativas de força bruta nas páginas de login de vários IPs detectados pelo ModSec. As etapas a seguir fornecem instruções passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook de força bruta do ModSec por IP Burst.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1 verifique se o IP de origem pertence a um cliente ou ao endereço IP interno da organização.
2. Na Ação 2, se o IP de origem pertencer a um cliente ou ao endereço IP interno da organização, execute as seguintes etapas:

Força bruta do ModSec por playbook de rajada de IP

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 3, verifique se houve atividades suspeitas.

- Verifique a atividade do IP de origem nos últimos dias. Se o IP tiver tráfego insignificante, isso indica um ataque real.
- Verifique os nomes de usuário de aplicação. Por exemplo, verifique se os nomes de usuário estão organizados em ordem alfabética.
- Procure nomes de contas genéricas envolvidas. Por exemplo, admin, sysadmin, root, administrador e outros nomes de conta de aplicação.

Se não houver atividades suspeitas, o fluxo será encerrado.

b. Na Ação 4, se houver atividades suspeitas, na Ação 5, verifique se o histórico de acesso à instância e o nome de usuário parecem verdadeiros.

Verifique os logs *Appnode* em busca de indicações de falha. Pode haver eventos de falha de SAML, SSO ou LDAP, o que pode ser devido a um problema operacional.

Se o histórico de acesso à instância e o nome de usuário não parecerem verdadeiros, o fluxo será encerrado.

c. Na Ação 6, se o histórico de acesso à instância e o nome de usuário parecerem verdadeiros, execute as seguintes etapas:

i. Na Ação 7, coordene com a equipe apropriada para corrigir o problema.

ii. Na Ação 8, documente as descobertas até o momento.

iii. Na Ação 9, conclua a revisão pós-incidente antes de fechar a tarefa.

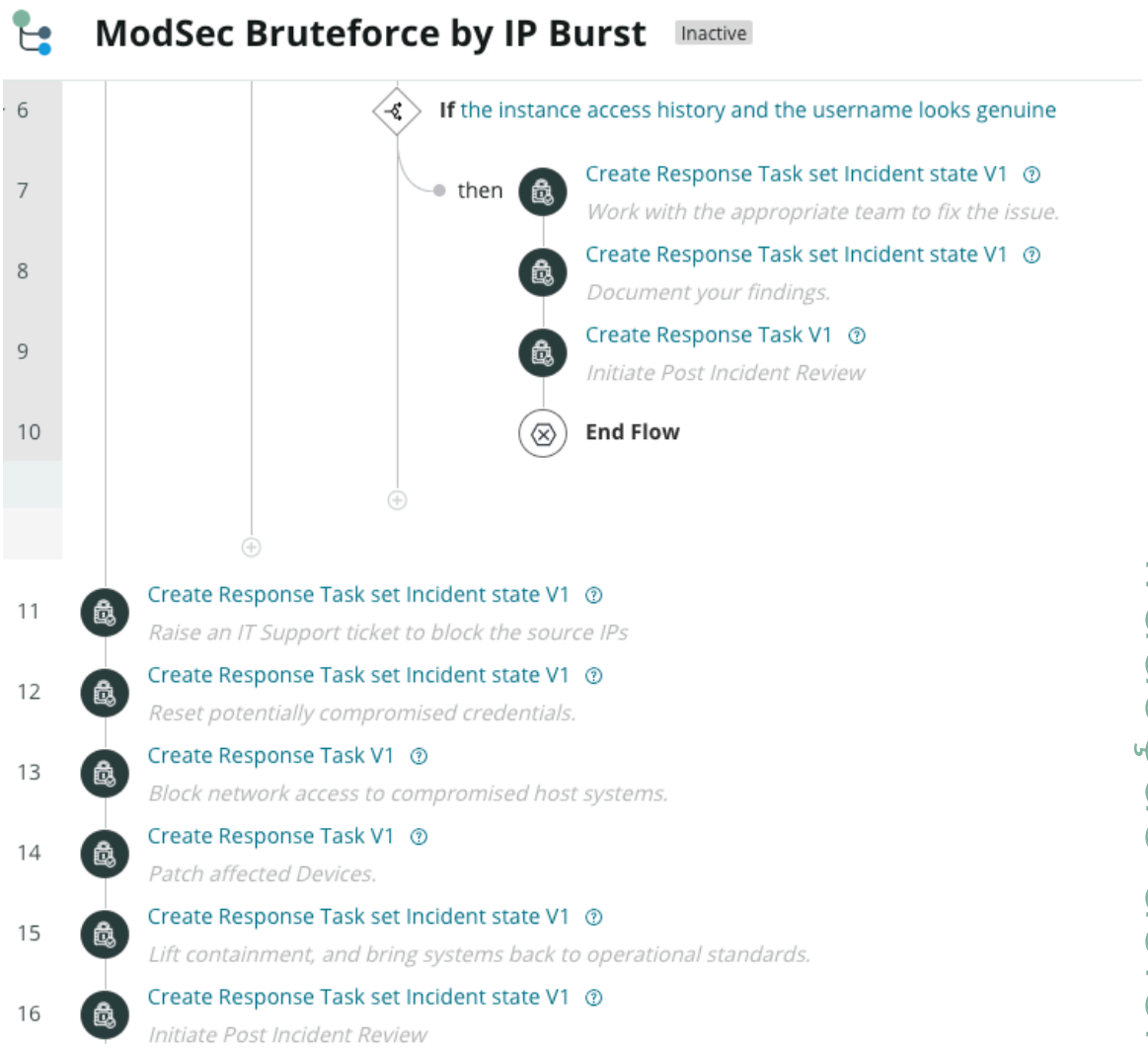
Na Ação 10, o fluxo termina.

3. Se o IP de origem não pertencer a um cliente ou ao endereço IP interno da organização, na Ação 11, gere um tíquete de suporte de TI para bloquear os IPs de origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar o playbook de Força bruta do ModSec por Burst de IP



4. Na Ação 12, redefina as credenciais potencialmente comprometidas.

5. Na Ação 13, bloqueie o acesso à rede para sistemas host comprometidos.

6. Na Ação 14, corrija os dispositivos afetados.

7. Na Ação 15, remova a contenção e restaure os sistemas aos padrões operacionais.

8. Na Ação 16, conclua a revisão pós-incidente antes de fechar a tarefa.

Ações do playbook do Security Incident Response

Esta seção descreve as ações fornecidas na biblioteca de ações do Flow Designer.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
Adicionar um marcador de segurança ao incidente de segurança	Use esta ação para adicionar um marcador de segurança automaticamente usando a lógica do Flow Designer.	Se o fluxo detectar um IOC, o marcador de **IOC detectado** poderá ser adicionado automaticamente usando esta ação. **Fluxo**:	• Entrada: incidente de segurança, marcador de segurança • Saída: não aplicável
Adicionar observáveis ao incidente de segurança	Use esta ação para adicionar observáveis a um incidente de segurança selecionado. • Por padrão, a lista de observáveis é separada pelo delimitador de vírgula (,), mas isso pode ser modificado. Você pode especificar outro caractere especial único como delimitador. Ao adicionar observáveis, o tipo (URL, endereço IP, hash) é definido automaticamente. • Quando os observáveis são adicionados ao incidente de segurança, o tipo (URL, endereço IP, hash) é definido automaticamente. • Quando os observáveis estão sendo adicionados, a opção Filtrar observáveis da lista de permitidos identifica os observáveis da lista de permitidos e não os adiciona à lista relacionada de observáveis		• Entrada: ◦ incidente de segurança ◦ observáveis ◦ delimitador ◦ filtrar observáveis da lista de permitidos e publicar anotação de atividade • Saída: não aplicável

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
	do incidente de segurança. Uma atividade automatizada do sistema (resposta) é adicionada para indicar que esses observáveis foram removidos.		
Obter usuários afetados (listas relacionadas) de vários incidentes de segurança V1	Recupera todos os usuários afetados listados na lista relacionada Usuários afetados para os incidentes de segurança especificados.	Você pode ter incidentes de segurança primários com vários incidentes de segurança secundários. Use esta ação para acumular usuários afetados de todos os incidentes de segurança secundários para os incidentes de segurança primários correspondentes. Somente usuários afetados exclusivos são acumulados e todas as duplicatas são eliminadas.	• Entrada: incidentes de segurança • Saída: ◦ usuário afetado ◦ contagem
Obter usuários afetados de vários incidentes de segurança	Recupera o usuário primário afetado pelo incidente de segurança especificado. Não inclui os usuários afetados da lista relacionada Usuários afetados.	• Ao investigar um incidente de segurança de phishing, envie um e-mail para os usuários primários afetados (que relataram o incidente de phishing) para confirmar se algum dos usuários clicou nos links maliciosos no e-mail de phishing. • Atualize a gravidade do incidente de segurança primário ou a pontuação de risco com base	• Entrada: incidentes de segurança • Saída: ◦ usuários afetados ◦ contagem

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
		na contagem de usuários primários afetados.	
Obter usuários afetados (lista relacionada) de um incidente de segurança	Recupera todos os usuários afetados listados na lista relacionada Usuários afetados para um incidente de segurança especificado.		• Entrada: incidentes de segurança • Saída: ◦ usuários afetados ◦ contagem
Adicionar usuários afetados ao incidente de segurança	Adiciona todos os usuários afetados a um incidente de segurança.	Suponha que você tenha um incidente de segurança primário com vários incidentes de segurança secundários. Você pode usar esta ação para acumular usuários afetados de todos os incidentes de segurança secundários para o incidente de segurança primário correspondente. Somente usuários afetados exclusivos são acumulados e todas as duplicatas são eliminadas.	• Entrada: ◦ incidente de segurança ◦ usuário • Saída: não aplicável
Obter itens de configuração dos usuários afetados	Recupera os itens de configuração (ICs) de todos os usuários afetados.	Em cenários de phishing ou malware, você pode usar esta ação para atualizar a lista relacionada de itens de configuração (IC) afetados e investigar os ICs. Você pode atualizar a pontuação de gravidade ou risco do incidente de segurança com base no número de ICs identificados.	• Entrada: usuários • Saída: ◦ itens de configuração ◦ contagem

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
Obter todos os incidentes de segurança secundários para um incidente de segurança	Recupera todos os incidentes de segurança secundários relacionados a um incidente de segurança primário específico.	Cenário de exemplo: use esta ação para: • Atualize o status dos incidentes de segurança secundários quando o status dos incidentes de segurança primários correspondentes for atualizado. • Atualize a pontuação de gravidade ou risco do incidente de segurança automaticamente com base no número de incidentes de segurança secundários.	• Entrada: ◦ incidente de segurança ◦ estado do incidente • Saída: ◦ incidente de segurança secundário ◦ contagem
Obter itens de configuração para os observáveis (tipo de endereço IP)	Recupera todos os itens de configuração (ICs) para observáveis do tipo endereço IP.	Um observável de endereço IP pode ser associado a um item de configuração. Por exemplo, o endereço IP de um servidor. Se você usar esta ação, poderá recuperar informações do servidor.	• Entrada: endereço IP do observável • Saída: ◦ itens de configuração ◦ contagem
É um observável malicioso	Confirma a presença de um ou mais observáveis maliciosos em um conjunto de observáveis.	Depois que a pesquisa de ameaças for concluída e você identificar a presença de observáveis mal-intencionados, poderá aumentar a pontuação de gravidade ou risco de um incidente de segurança.	• Entrada: incidente de segurança • Saída: mal-intencionado (verdadeiro/falso)
Enviar e-mail para confirmar a interação do usuário	Envia e-mail em resposta a uma resposta do usuário.	Se um usuário tentar fazer login várias vezes em uma aplicação e falhar,	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
		o resultado será um cenário de falha de login. Nesse caso, um e-mail é enviado ao usuário para confirmar se ele tentou fazer login ou não. Dependendo da resposta do usuário (sim ou não), diferentes ações podem ser realizadas. **Fluxo**: playbook manual de login com falha	
Remover do filtro observáveis da lista de permitidos	Use esta ação para permitir observáveis de lista de um determinado conjunto de observáveis.	Você pode identificar determinados observáveis que podem ser ignorados em um conjunto de observáveis. Esses observáveis não serão levados em conta ao resolver o incidente de segurança.	• Entrada: incidente de segurança • Saída: ◦ observáveis da lista permitida ◦ contagem
Redefinir senha para usuários afetados	Use esta ação para redefinir a senha dos usuários afetados.	Se uma conta de usuário tiver sido invadida ou um usuário solicitar que uma senha seja redefinida, um e-mail será enviado ao usuário para redefinir a senha. **Fluxo**: playbook manual de login com falha.	
Obter grupo de usuários para o usuário afetado	Recupera os detalhes do grupo de usuários afetados.	Em uma organização, se dois ou mais usuários relatarem e-mails de phishing, você poderá descobrir o grupo ao qual pertencem e identificar se mais usuários foram afetados	• Entrada: usuário • Saída: ◦ grupos de usuários ◦ contagem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Emissão de relatórios do Security Incident Response

Os gerentes de segurança podem identificar áreas de preocupação usando interfaces gráficas de alto nível.

Explorador do Security Incident Response para acesso

Você pode acessar o painel do Security Incident Response Explorer para exibir a atividade de incidente de segurança para identificar instantaneamente as áreas de preocupação e resolver problemas rapidamente.

Antes de Iniciar

Funções necessárias:

- sn_si.admin (para gravar)
- sn_si_basic (para ler)

Procedimento

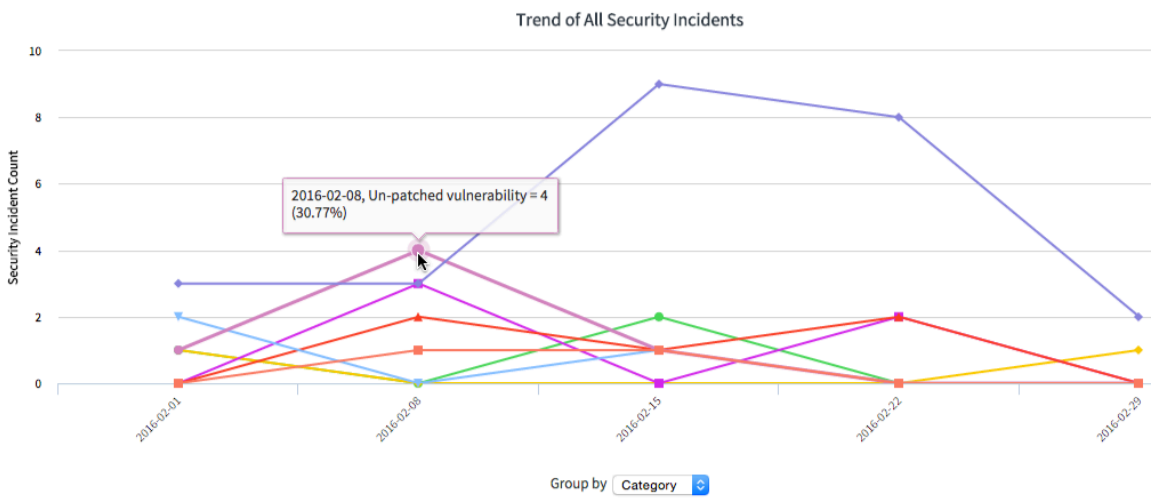
1. Navegar até **Todos** > **Autoatendimento** > **Página inicial** ou navegue até **Autoatendimento** > **Painéis**.
2. Escolha o Explorador de incidentes de segurança na lista de relatórios.

Security Incident Response Visão geral

A visão geral Security Incident Response fornece uma exibição executiva da atividade de incidente de segurança, fornecendo tendências e relatórios e detalhamentos de dados específicos.

O módulo Visão geral exibe informações do incidente de segurança que são personalizadas para a função do usuário. Você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados, mapa térmico e assim por diante) para exibir dados gerais específicos dessa parte. Veja a imagem a seguir. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Tendência de todos os incidentes de segurança



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral do gerenciador de Incidentes de segurança

Usuários com as funções de Administrador de incidentes de segurança e Gerente de incidentes de segurança exibem a Visão geral do Gerenciador de incidentes de segurança. Ele contém os seguintes relatórios no sistema de base.

Relatórios de visão geral do Gerenciador de incidentes de segurança

Nome	Visual	Descrição
Incidentes de segurança críticas da equipe	Pontuação única	O número de incidentes de segurança críticos atribuídos à equipe.
Incidentes de alta segurança da equipe	Pontuação única	O número de incidentes de alta segurança atribuídos à equipe.
ANS que expiram em 24 horas	Pontuação única	O número de SLAs que expiram nas próximas 24 horas.
Risco versus gravidade	Mapa Térmico	A distribuição de incidentes de segurança atribuídos à equipe por risco e gravidade.
Incidentes de segurança por classe de IC, últimos 3 meses	Gráfico de barras	A contagem de incidentes de segurança atribuídos à equipe por classe de item de configuração.
Tendência de todos os incidentes de segurança	Tendência	Representa graficamente a contagem do número de incidentes de segurança recebidos por categoria ou prioridade.
Incidentes de segurança de acesso não autorizado	Gráfico de barras	Exibe os tipos de categorias de incidentes de segurança recebidos ao longo do tempo.
Tempo médio de contenção	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança.
Tempo médio de contenção crítica	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança críticos.
Tempo médio de identidade	Pontuação única	O tempo médio necessário para identificar todos os incidentes de segurança.

Visão Geral de Análise de Segurança

Usuários com a função de Analista de incidentes de segurança exibem a Visão geral do Analista de segurança. Ele contém os seguintes relatórios no sistema de base.

Relatórios de visão geral do analista de segurança

Nome	Visual	Descrição
Meu trabalho de prioridade crítica	Pontuação única	O número de incidentes de segurança críticos atribuídos a mim.
Meu trabalho de alta prioridade	Pontuação única	O número de incidentes de alta segurança atribuídos a mim.
Meus ANS que expiram em 24 horas	Pontuação única	O número de SLAs atribuídos a mim que expiram nas próximas 24 horas.
Incidentes de segurança atribuídos a mim	Gráfico de barras	Incidentes de segurança atribuídos a mim por estado ou categoria de incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do analista de segurança

Nome	Visual	Descrição
Trabalho atribuído a mim por tipo	Gráfico de barras	Tarefas de segurança (incidentes, tarefas ou solicitações) atribuídas a mim por tipo ou prioridade.
Incidentes de segurança, solicitações e tarefas atribuídos a mim	Lista	Uma lista de todos os incidentes de segurança, solicitações de segurança e tarefas atribuídas a mim.
Local do incidente de segurança	Mapa	Localização regional dos incidentes de segurança.
Contagem	Mapa	Número de incidentes de segurança por região.
Contagem mínima/ máxima	Barra de Espectro de Cores	Os números mínimo e máximo de incidentes de segurança por região representados por uma barra de espetro de cores.
Percentual de contagem	Mapa	Percentual da contagem total de incidentes por região.

Visão geral do CISO de incidentes de segurança com análise de incidentes de segurança ativada

Quando o plug-in Análise de incidente de segurança é ativado, os usuários com as funções de CISO de incidentes de segurança e Administrador do sistema visualizam a Visão geral do CISO de incidentes de segurança. Os seguintes relatórios do CISO são fornecidos no sistema de base.

Relatórios de visão geral do CISO de incidentes de segurança (com a Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Novos Incidentes de segurança nesta semana	Pontuação única	O número de novos incidentes de segurança recebidos na semana atual.
Incidentes de segurança encerrados nesta semana	Pontuação única	O número de incidentes de segurança encerrados na semana atual.
Novos incidentes de segurança (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança abertos nos últimos 7 dias.
Incidentes de segurança encerrados (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança encerrados nos últimos 7 dias.
Novos incidentes de segurança diários versus incidentes de segurança encerrados	Tendência	Contagens de incidentes de segurança novos e encerrados ao longo do tempo por dia.
Novos incidentes de segurança semanais versus incidentes de segurança encerrados	Tendência	Incidentes de segurança novos e encerrados ao longo do tempo por semana.
Código de fechamento de incidentes de segurança	Tendência	Contagem total de códigos de fechamento ao longo do tempo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do CISO de incidentes de segurança (com a Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Impacto de Incidente de segurança nos negócios	Mapa de Árvore	Serviços de negócio com incidentes de segurança com agrupamentos disponíveis por importância para os negócios.
Tempo Médio para Conter (Por Semana)	Tendência	O tempo médio de 7 dias necessário para conter um incidente de segurança ao longo do tempo.
Tempo Médio para Eliminar (Por Semana)	Tendência	O tempo médio de 7 dias necessário para erradicar um incidente de segurança ao longo do tempo.
Tempo médio de identidade (por semana)	Tendência	O tempo médio de 7 dias necessário para identificar um incidente de segurança ao longo do tempo.
Local do incidente de segurança	Mapa	Localização regional dos incidentes de segurança.
Contagem	Mapa	Número de incidentes de segurança por região.
Contagem mínima/máxima	Barra de Espectro de Cores	Os números mínimo e máximo de incidentes de segurança por região representados por uma barra de espetro de cores.
Percentual de contagem	Mapa	Percentual da contagem total de incidentes por região.

Visão geral do CISO de incidentes de segurança sem a Análise de incidentes de segurança ativada

Quando o plug-in Análise de incidente de segurança não está ativado, os usuários com as funções de CISO de incidentes de segurança e Administrador do sistema visualizam a Visão geral do relatório de CISO de incidentes de segurança. Os seguintes relatórios do CISO são fornecidos no sistema de base.

Relatórios de visão geral do CISO de incidentes de segurança (sem a Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Novos Incidentes de segurança nesta semana	Pontuação única	O número de novos incidentes de segurança abertos na semana atual.
Incidentes de segurança encerrados nesta semana	Pontuação única	O número de incidentes de segurança encerrados na semana atual.
Novos incidentes de segurança (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança abertos nos últimos 7 dias.
Incidentes de segurança encerrados (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança encerrados nos últimos 7 dias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do CISO de incidentes de segurança (sem a Análise de incidentes de segurança ativada)

Nome	Visual	Descrição
Novos incidentes de segurança semanalmente	Tendência	Os novos incidentes de segurança são abertos semanalmente.
Incidentes de segurança encerrados semanalmente	Tendência	Os incidentes de segurança são encerrados semanalmente.
Códigos de fechamento de Incidentes de segurança	Tendência	Códigos de fechamento de incidente de segurança ao longo do tempo.
Serviços de negócio com incidentes de segurança - Impacto nos negócios	Mapa de Árvore	Serviços de negócio com incidentes de segurança com agrupamentos disponíveis por importância para os negócios.
Tempo médio de contenção	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança.
Tempo médio de contenção crítica	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança críticos.
Tempo médio de identidade	Pontuação única	O tempo médio necessário para identificar todos os incidentes de segurança.

Nota: O sistema base Security Incident Response inclui Soluções de Análise de desempenho para exibir painéis de práticas recomendadas pré-configurados. Os painéis apresentam métricas importantes para analisar seu processo de Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto. Para obter mais informações e instruções de instalação, consulte Security Incident Response Soluções Análise da plataforma e relatórios.

Mapa de incidentes de segurança

O mapa de incidentes de segurança fornece dados por localização geográfica. O mapa-múndi é realçado em todas as áreas em que ocorre um incidente. Quando o plug-in Análise de incidente de segurança está ativado, você pode adicionar o mapa de incidentes de segurança à visão geral Security Incident Response. Depois de adicionado, você pode configurar o mapa modificando os filtros do mapa.

Adicionar mapa à visão geral de Security Incident Response

Você pode adicionar o mapa à visão geral Security Incident Response para exibir dados de incidentes de segurança por localização geográfica. Um mapa permite que você faça uma busca detalhada nas informações de incidentes de segurança por local.

Antes de Iniciar

Função necessária: sn_si.admin

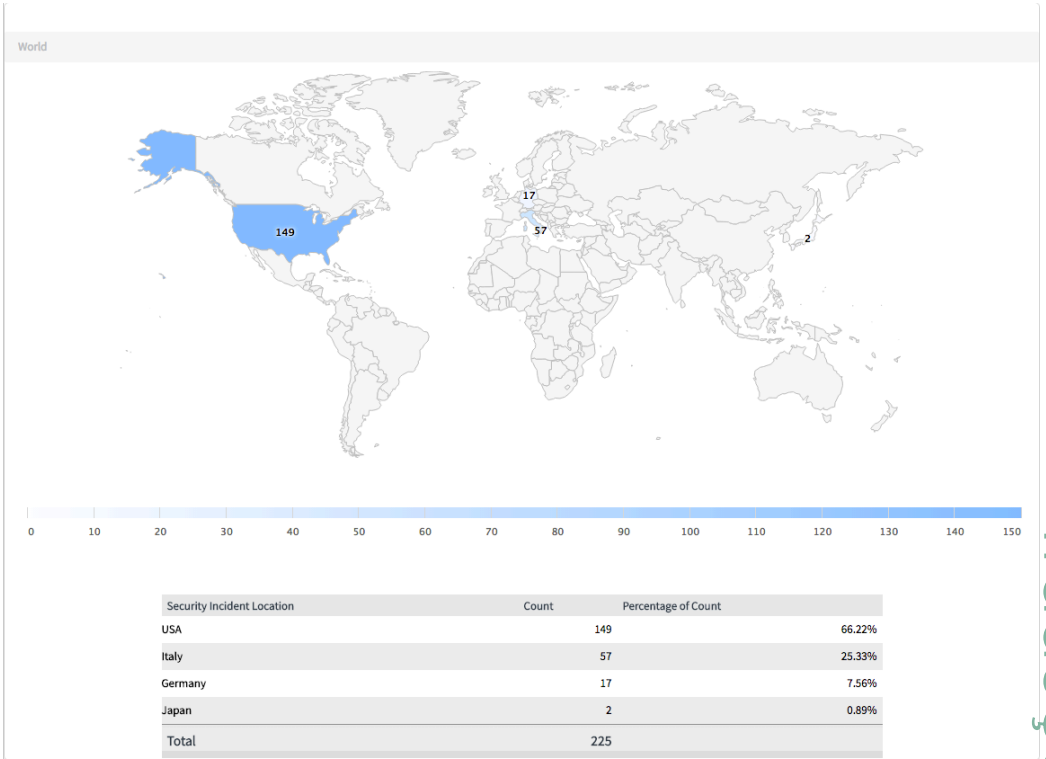
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Visão geral**.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Na primeira caixa de seleção, clique em **Relatórios**.
4. Na segunda caixa de seleção, clique em **Incidente de segurança**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na terceira caixa de seleção, clique em **Mapa de incidente de segurança**.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. Na parte inferior da tela, clique no local na tela que você deseja adicionar ao relatório.

7. Feche a caixa **Adicionar conteúdo**.

Modificar mapa de incidentes de segurança

Os administradores no domínio global podem modificar como o mapa de incidentes de segurança lida com incidentes de segurança usando filtros.

Antes de Iniciar

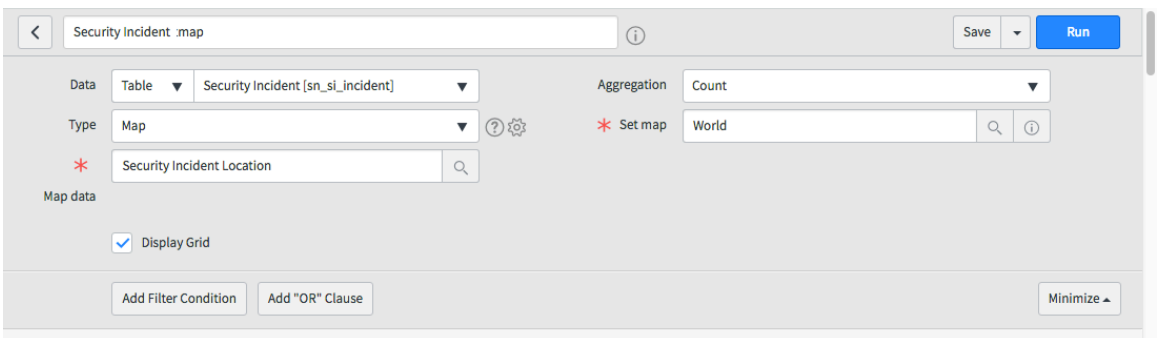
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Relatórios** > **Administração** > **Todos**.

2. Pesquise **o mapa de incidentes de segurança**.

3. Clique **em Editar relatório**.



4. Clique em **Adicionar condição de filtro** para adicionar ou editar filtros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Executar** para ver as mudanças aplicadas.
6. Clique em **Salvar**.

Mapas de árvore de incidentes de segurança

Quando o plug-in Análise de incidente de segurança está ativado, você pode adicionar os mapas de árvore em tempo real do incidente de segurança - impacto do serviço e incidente de segurança - à visão geral Security Incident Response. Depois que eles forem adicionados, você poderá configurar os mapas de árvore modificando as categorias e os indicadores do mapa de árvore.

Adicionar mapas de árvore à visão geral do Security Incident Response

Os mapas de árvore exibem dados hierárquicos (estruturados em árvore) como um conjunto de retângulos aninhados. Cada ramificação da árvore recebe um retângulo, que é lado a lado com retângulos menores que representam sub-ramificações. Os mapas de árvore permitem exibir informações de incidentes de segurança de forma dinâmica e envolvente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Visão geral**.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Na primeira caixa de seleção, clique em Mapa de **árvore**.
4. Na segunda caixa de seleção, selecione o mapa de árvore que deseja inserir na lista a seguir:
   - Incidente de segurança - Impacto no serviço
   - Incidente de segurança - Tempo real
   - Incidente de segurança - Impacto nos negócios
   - Significância da vulnerabilidade

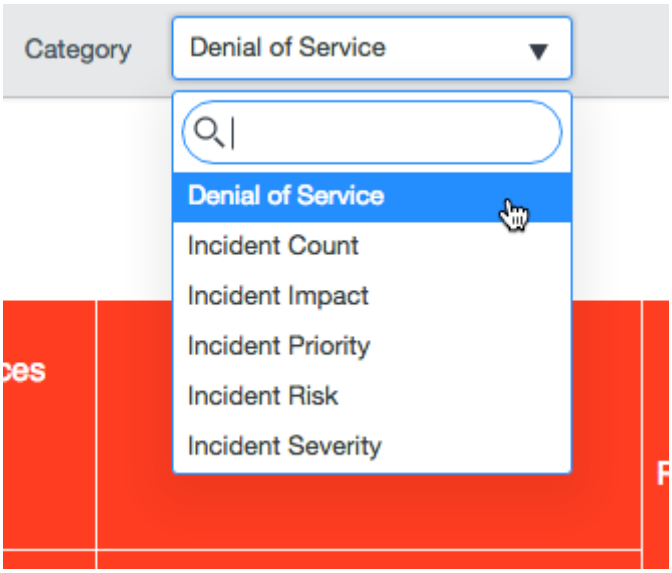
   Nota: O mapa de árvore do Impacto nos negócios aparece na página inicial Security Incident Response por padrão. Os mapas de árvore Impacto do serviço e Tempo real exigem que o plug-in Análise de incidentes de segurança esteja ativado.

5. Na terceira caixa de seleção, selecione o nível de granularidade das informações que você deseja recuperar para o mapa de árvore selecionado.

   Nota: Para o mapa de árvore Incidente de segurança - Impacto do serviço, selecione **Incidente de segurança** na terceira caixa de seleção. Esta seleção fornece uma lista suspensa com várias categorias de dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na parte inferior da tela, clique no local na tela em que você deseja adicionar o medidor.
7. Feche a caixa **Adicionar conteúdo**.

Criar ou atualizar uma categoria de mapa de árvore

Você pode modificar as categorias predefinidas para os mapas de árvore de incidentes de segurança ou criar categorias conforme necessário.

Antes de Iniciar

Função necessária: sn_si.admin

Os mapas de árvore usam a análise de desempenho como fonte de dados. O módulo Performance Analytics requer um plug-in separado.

Por Que e Quando Desempenhar Esta Tarefa

No sistema base, as categorias de mapa de árvore, como Risco de incidente, Negação de serviço e Gravidade de incidente, estão incluídas. Você pode modificar essas categorias ou definir mais categorias conforme necessário.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração**e abra a definição de mapa de árvore para a qual você deseja configurar categorias:
   - **Definição da emissão de relatórios de criticidade do serviço**
   - **Definição em tempo real**
2. Opcional: Mude o nome da definição do mapa de árvore.
   No sistema base, o nome padrão para a definição do mapa de árvore de impacto do serviço é **Incidente de segurança**. O nome padrão para a definição do mapa de árvore em tempo real é **Incidente de segurança - Tempo real**.
3. A menos que você esteja usando um mapa de árvore personalizado, não altere o valor do **Grupo de indicadores do PA**.
4. Para desativar a definição do mapa de árvore, desmarque a caixa de seleção **Ativo**.
   Se, por exemplo, você desativar a categoria de negação de serviço no painel de impacto do sistema, essa categoria de mapa de árvore não estará disponível.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na lista relacionada **Categorias** de mapa de árvore, selecione uma categoria para modificar ou clique em **Novo** para criar uma nova categoria.
6. Preencha os campos.

Formulário Categoria de mapa de árvore

Campo	Descrição
Nome	O nome que é exibido para a categoria na lista **Categorias** acima do mapa de árvore.
Ordem	A ordem em que a categoria aparece na lista **Categorias** acima do mapa de árvore.
Mapa de Árvore	O nome do mapa de árvore que usa esta categoria.
Cor	A cor exibida para esta categoria no mapa de árvore.
Ativo	Selecione para ativar esta categoria.
Descrição	Uma descrição da categoria.
Visível para todas as funções	Selecione para tornar esta categoria visível para todos os usuários, independentemente de sua função.
Funções	Se você não marcou a caixa de seleção **Visível por todas as funções**, selecione as funções capazes de exibir esta categoria.

7. Clique em **Enviar** ou **Atualizar**.

Criar ou atualizar um indicador de mapa de árvore

Você pode modificar os indicadores predefinidos para uma categoria de mapa de árvore ou criar novos indicadores. Para cada indicador, você pode configurar sua fonte de dados e especificar como as listas de incidentes de segurança são abertas a partir dos mapas de árvore exibidos com o indicador.

Antes de Iniciar

Função necessária: sn_si.admin

Os mapas de árvore usam a análise de desempenho como fonte de dados. O módulo Performance Analytics requer um plug-in separado.

Procedimento

1. Abra a definição de mapa de árvore para a qual você deseja configurar indicadores.

Definição de mapa de árvore	Ação
Mapa de árvore de impacto do serviço	Navegar até **Incidente de segurança** > **Administração** > **Definição de Impacto de Serviço**.
Mapa de árvore em tempo real	Navegar até **Incidente de segurança** > **Administração** > **Definição em tempo real**.

2. Na lista relacionada **Categorias** de mapa de árvore, selecione a categoria para a qual você deseja configurar indicadores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista relacionada **Indicadores** de mapa de árvore, selecione um indicador para modificar ou clique em **Novo** para criar um novo indicador.
4. Preencha os campos.

Formulário de indicador de mapa de árvore

Campo	Descrição
Nome	O nome que é exibido para o indicador na lista **Indicadores** no painel de impacto do serviço.
Descrição resumida	Uma descrição que é exibida para o indicador na lista **Indicadores** acima do mapa de árvore.
Limite do resultado	O número máximo de resultados permitidos. O limite superior é 100.
Precisão do resultado	O número de dígitos a serem exibidos após a vírgula decimal. Este campo é exibido somente para a definição de mapa de árvore em tempo real.
Ativo	Marque a caixa para ativar este indicador.
Categoria	O nome da categoria inserido na tela anterior.
Direção	Indica se o bloco no mapa de árvore está minimizado ou maximizado. Este campo é exibido somente para a definição de mapa de árvore em tempo real.
Unidade	A unidade de medida a ser usada para a métrica. Este campo é exibido somente para a definição em tempo real.
Intervalo de atualização automática	Com que frequência atualizar o mapa de árvore.
Ordem	A ordem em que o indicador aparece na lista de **Indicadores** acima do mapa de árvore.

5. Clique na guia **Configuração de fonte de dados** e configure uma das seguintes opções de fonte de dados para o indicador.

Opção	Ação
Análise de desempenho	Selecione **Performance Analytics** no campo **Fonte de dados** e faça as seguintes entradas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Ação
	◦ **Indicador:** o indicador usado para agrupar os dados do PA. ◦ Detalhamento**padrão:** o detalhamento padrão usado para dividir o indicador do PA selecionado em várias partes.
Script personalizado	Selecione **Script personalizado** no campo **Fonte de dados**. Em seguida, use o editor de HTML para personalizar o script conforme necessário. O resultado da execução do script deve ser uma matriz para que as informações sejam exibidas no mapa de árvore.
Condições da consulta	Selecione **Condição de consulta** no campo **Fonte de dados** e faça as seguintes entradas: ◦ Tabela de**consulta:** a tabela base a ser consultada. ◦ Tipo de**agregado:** o tipo de agregado (SUM, COUNT, AVG, MIN, MAX) a ser usado. ◦ **Campo agregado:** o campo a ser usado pela consulta. ◦ **Agrupar por:** o campo para classificar os dados consultados. **Nota:** Para aprimorar a consulta, clique em **Adicionar condição de filtro** e **Adicionar cláusula "OR"**.

6. Clique na guia **Clique** de referência e especifique como as listas de incidentes de segurança são abertas no mapa de árvore.
   a. No campo **Clique no tipo de navegação de URL**, selecione se deseja que a lista de incidentes de segurança seja aberta em uma nova janela, na mesma janela ou em uma caixa de diálogo.
   b. Opcional: No campo **Clicar por meio de script de URL**, modifique o script de exemplo, se necessário.
7. Clique em **Enviar** ou **Atualizar**.

Adicionar gráficos de significância de vulnerabilidade a uma visão geral

Se o plug-in Resposta a vulnerabilidades estiver ativado, você poderá adicionar gráficos de definição de significância de vulnerabilidade e outras visualizações à Visão geral.

Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até a página Visão geral à qual você deseja adicionar o medidor de significância de vulnerabilidade.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Nas três caixas de seleção, faça as seleções dependendo do medidor (mapa de árvore ou relatório de pontuação) que você deseja adicionar:
   - Para adicionar o mapa de árvore de significância da vulnerabilidade, faça estas seleções:
     - Mapa de Árvore
     - Significância da vulnerabilidade
     - Significância da vulnerabilidade
   - Para adicionar o relatório de pontuação de significância da vulnerabilidade, faça estas seleções:
     - Análise de desempenho
     - Pontuação
     - Serviços com significância de vulnerabilidade
4. Clique no local na tela em que você deseja adicionar o medidor.
5. Feche a caixa **Adicionar conteúdo**.

Gestão de incidentes graves de segurança

A aplicação ServiceNow® Gestão de incidentes graves de segurança rastreia o andamento de Incidente grave de segurança (MSI) desde a descoberta até a análise, propõe, promove e vincula incidentes de segurança e fechamento.

Gestão de incidentes graves de segurança

Explorar	Configurar	Integrar
Saiba mais sobre como analistas, administradores e gerentes usam a Gestão de incidentes de segurança graves (MSIM)	Planejar e configurar sua implementação	Estenda as capacidades do MSIM integrando com outras Microsoft aplicações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Administrar	Uso	Relatórios de Status
Tarefas de administração sobre como marcar registros de incidentes e configurar rótulos	Propor, promover, vincular e rejeitar registros de incidentes de segurança graves por meio da gestão de espaço	Monitorar tarefas relacionadas a incidentes e melhorar processos por meio de métricas, gráficos de tendências e relatórios
Capacidades adicionais		
Configurar informações para acumular registros		

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Solicitar um aplicativo Operações de segurança na Store

Se você é um novo cliente [Operações de segurança em Rome ou mais tarde, visite o ServiceNow Store site para exibir os aplicativos disponíveis e informações sobre como enviar solicitações para a loja.

Mais recursos

Visite o Gestão de incidentes graves de segurança fórum no ServiceNow Community.

Explorando a Gestão de incidentes graves de segurança

Explore Gestão de incidentes graves de segurança para entender como a aplicação funciona em termos de acompanhamento de incidentes de segurança críticos de alta prioridade, que são identificados como uma ameaça à organização.

Use esta seção para aprender os principais recursos e várias funções envolvidas no trabalho com registros de incidentes de segurança graves. Esta seção também ajuda a entender como começar a usar a aplicação, os pré-requisitos e os plug-ins necessários para trabalhar com a aplicação.

Gestão de incidentes graves de segurança

Rastreie e gerencie várias atividades que normalmente fazem parte da resolução de um incidente de segurança grave por meio de Gestão de incidentes graves de segurança. Por meio de um espaço intuitivo, os gerentes de incidentes e aqueles que trabalham em um incidente podem propor e promover incidentes a incidentes graves, rastrear atividades de incidentes de segurança graves e colaborar facilmente com colegas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

As capacidades de gestão de incidentes de segurança graves funcionam em conjunto com as capacidades de produto de resposta a incidentes de segurança existentes. Isso inclui a capacidade de um analista de segurança escalar um incidente de segurança padrão para um incidente de segurança grave, para que os novos recursos do produto estejam disponíveis para oferecer suporte ao processo de correção.

Depois de instalar em sua instância ServiceNow, um analista de incidentes de segurança pode:

- Proponha um incidente de segurança ao candidato a incidente de segurança grave para iniciar um processo de revisão sobre a necessidade de criar um incidente de segurança grave.
- Promova diretamente um incidente de segurança a um incidente de segurança grave sem a necessidade de um processo de revisão adicional.
- Rejeitar um incidente de segurança que é proposto como um incidente de segurança grave (MSI).
- Vincule um incidente de segurança como um incidente secundário ao incidente de segurança grave (MSI) para que todos os incidentes de segurança possam ser trabalhados.

Principais recursos

A Gestão de incidentes de segurança graves (MSIM) melhora o processo de correção de incidentes de segurança graves com os seguintes recursos:

- Espaço dedicado para gerenciar incidentes de segurança graves projetado para a função de usuário de gerente de incidentes de segurança graves.
- Organize tarefas de resposta em vários incidentes de segurança "secundários".
- Automatize a criação de pastas de colaboração e canais de comunicação de bate-papo após a criação de um incidente de segurança grave, bem como o arquivamento como parte do fechamento do incidente.
- Componente do explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de uma integração Microsoft SharePoint.
- Gerenciador de canal de bate-papo e componentes de fluxo de atividades para gerenciar comunicações em vários grupos funcionais, de segurança e de TI por meio de uma integração Microsoft Teams.

Componentes do espaço

O produto Gestão de incidentes graves de segurança contém vários novos componentes de espaço e páginas de interface do usuário que oferecem a funcionalidade de recursos principais:

- Espaço dedicado para gerenciar incidentes de segurança graves projetados especificamente para a função de usuário de gerente de incidentes de segurança graves.
- Organize tarefas de resposta em vários incidentes de segurança secundários.
- Automatize a criação de pastas de colaboração e canais de comunicação de bate-papo após a criação de um incidente de segurança grave, bem como o arquivamento como parte do fechamento do incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Componente do explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de uma integração Microsoft SharePoint.
- Gerenciador de canal de bate-papo e componentes de fluxo de atividades para gerenciar comunicações em vários grupos funcionais, de segurança e de TI por meio de uma integração Microsoft Teams.

Versões compatíveis da Gestão de incidentes de segurança graves

Gestão de incidentes graves de segurança (MSIM) requer a versão Now Platform® Rome.

Este recurso é compatível com Microsoft Teams, que é um espaço centrado no bate-papo no pacote Microsoft Office 365. Anteriormente Microsoft Teams era uma instalação separada de Microsoft Office 365 aplicações.

Versões da Now Platform compatíveis

Este recurso é compatível com Rome e versões posteriores.

As aplicações Operações de segurança seguintes são os plug-ins Security Incident Response padrão que provavelmente serão instalados para a maioria dos usuários se eles já estiverem usando Security Incident Response (SIR). Se não estiver instalado, você deverá instalar e ativar de ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem mencionada para garantir uma instalação sem problemas:

1. Security Incident Response: com.snc.si_dep é o plug-in dependente. A instalação deste plug-in ativa as outras aplicações das Operações de segurança.
2. Estrutura de integração de segurança
3. Security Support Common
4. Orquestração do Security Support Common

Para começar com MSIM

Revise as informações a seguir antes de começar a trabalhar com Gestão de incidentes graves de segurança.

Função necessária: sn_msi.workspace_admin.

Para facilitar a instalação e a configuração da aplicação Gestão de incidentes graves de segurança, talvez você precise verificar se os plug-ins a seguir estão ativados.

Importante: Um conjunto de atualizações (KB1289784) está disponível no Guia de início rápido da Gestão de incidentes de segurança graves para ajudar os usuários com uma configuração fácil. Você precisa importar o conjunto de atualizações após concluir a instalação da aplicação. Siga o procedimento detalhado no Guia de início rápido (Etapa 2) na seção Documentos de suporte na aplicação MSIM, que está na ServiceNow Store.

Pré-requisito

Tarefa	Descrição
Antes de começar com a aplicação, certifique-se de ter os plug-ins dependentes necessários.	Como primeira etapa, instale:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisito

Tarefa	Descrição
	• Instalador do ServiceNow IntegrationHub (com.glide.hub.integrations) • ServiceNow® Integration Hub Tempo de execução (com.glide.hub.integration.runtime). • ServiceNow® Integration Hub Etapa de ação - REST (com.glide.hub.action_step.rest) • ServiceNow® Integration Hub Modelo de ação - Fluxo de dados (com.glide.hub.action_type.datastream) • ServiceNow® Integration Hub Flow Designer - Entradas dinâmicas (com.glide.hub.dynamic_inputs) **Nota:** Se você não tiver os privilégios necessários para qualquer um dos ServiceNow® Integration Hub plug-ins listados, crie um tíquete de suporte para instalar essas aplicações de pré-requisito.
Verifique se você tem o acesso necessário para instalar o Microsoft SharePoint Spoke e o Microsoft Teams Graph Spoke. **Nota:** As listadas acima são as aplicações dependentes primárias para começar com Gestão de incidentes graves de segurança.	Antes de instalar o Microsoft SharePoint Spoke e o Microsoft Teams Graph Spoke, certifique-se de ter o acesso necessário às aplicações ServiceNow Integration Hub. **Nota:** Microsoft SharePoint Spoke e Microsoft Teams Graph] Spoke são aplicações dependentes de ServiceNow® Integration Hub aplicações.

Check-list para configuração de MSIM

Antes de usar a aplicação ServiceNow® Gestão de incidentes graves de segurança (MSIM), baixe a aplicação do ServiceNow® Store.

Acompanhe o andamento da configuração, instalação e configuração na tabela a seguir.

Nota: As funções atribuídas à aplicação Gestão de incidentes graves de segurança são listadas nas seções seguintes. Para obter mais informações, consulte Gestão de incidentes graves de segurança funções.

Use a check-list a seguir para orientá-lo nas etapas de ponta a ponta para instalar e configurar a aplicação Gestão de incidentes graves de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se a aplicação Gestão de incidentes graves de segurança está instalada e ativada a partir do ServiceNow® Store.	Gestão de incidentes graves de segurança v1.1.1 está disponível em ServiceNow® Store. Siga estas instruções: download de uma aplicação do ServiceNow Store.
Verifique se as seguintes aplicações estão instaladas na ordem fornecida.	As seguintes aplicações serão instaladas por padrão depois que você instalar a aplicação Gestão de incidentes graves de segurança na versão atual da aplicação: • File Explorer Core para Operações de segurança v1.1.1 • Microsoft SharePoint File Explorer Conector para Operações de segurança v1.1.1 • File Explorer Componente para Operações de segurança v1.0.0 • Microsoft Teams Conector de bate-papo para Operações de segurança v1.0.0 • Bate-papo principal para Operações de segurança v1.0.0 • Incidente grave de segurança Resposta v1.1.1 • Cartão do EVAM do Collab Chat para o espaço MSIM v1.0.0 (esta aplicação é configurada somente para as visualizações de IU no plano de fundo da aplicação para o espaço Gestão de incidentes graves de segurança) • Componente de IU do organizador de tarefas para o espaço Gestão de incidentes graves de segurança 1.0.0 • Security Incident Response v12.8.1
Verifique se as funções de usuário estão atribuídas a Incidente grave de segurança, conforme apropriado.	A seguir estão as funções envolvidas em todo o ciclo de vida do incidente do Incidente grave de segurança processo de correção: • Administrador do MSI [sn_msi.workspace_admin] • Gerente do MSI [sn_msi.workspace_manager] • Respondente MSI [sn_msi.workspace_responder

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	Para obter informações mais detalhadas sobre cada função, consulte Gestão de incidentes graves de segurança funções.
Verifique se você definiu com sucesso a configuração Microsoft SharePoint v1.0.0.	Microsoft SharePoint gerencia sites, pastas, arquivos, grupos e usuários em Microsoft SharePoint. Adicione dados Microsoft SharePoint à sua instância ServiceNow®. Para fazer isso, você precisa configurar as conexões Graph e Rest. Para obter informações, consulte a documentação do Spoke doMicrosoft SharePoint v1.1.2 sobre como configurar as conexões REST e Graph. Estabeleça a conexão Graph e REST para se conectar à sua instância [ServiceNow® de Microsoft SharePoint.
Verifique se você criou um site Microsoft SharePoint para criar uma biblioteca de documentos.	Crie um site Microsoft SharePoint, se necessário, ou você pode usar um site existente para criar nossa biblioteca de documentos.
Verifique se você criou uma biblioteca de documentos no site Microsoft SharePoint.	Crie uma biblioteca de documentos dedicada em um site Microsoft SharePoint novo ou existente.
Verifique se as permissões necessárias foram fornecidas aos usuários e atribuídas aos grupos de usuários necessários no Microsoft SharePoint.	Gerencie o acesso do site Microsoft SharePoint a diferentes usuários e grupos de usuários.
Verifique se você criou e configurou a Unidade Microsoft SharePoint e as definições de configuração necessárias.	Para verificar as configurações da unidade, configure Microsoft SharePoint o Conector do Explorador de Arquivos, Ações de Pasta e Arquivo e Modelos de Pasta: • Configurar o Explorador de Arquivos Repositório Unidade: cria conexão da instância Microsoft SharePoint para ServiceNow®. • Definir configurações de ação de pasta e arquivo: configure e controle as ações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	individuais de pasta e arquivo exibidas no componente do explorador de arquivos. • Criar modelos de pasta: configure para criar pastas exclusivas para diferentes tipos de incidentes de segurança graves.
Verifique se você estabeleceu com sucesso uma conexão com a aplicação Conector de bate-papo do Microsoft Teams.	Para estabelecer a conexão da aplicação Conector de bate-papo do Microsoft Teams com a instância ServiceNow®, siga o procedimento explicado aqui: Estabelecer conexão de gráficos do MS Teams em Now Platform.
Verifique se você configurou o Microsoft Teams com a instância Now Platform® e criou conexões e configurações de credenciais.	Para verificar a configuração [Microsoft Teams com a instância ServiceNow®, siga o procedimento conforme explicado aqui: • Estabelecer conexão de gráficos do MS Teams em Now Platform • Criar um modelo de canal de bate-papo
Verifique se as definições Administração de incidentes de segurança graves - Configuração foram bem-sucedidas.	Como administrador do MSI, você deve ser capaz de: • determine se os analistas de segurança podem propor e promover o incidente e vincular outros incidentes de segurança. • habilite ou desabilite as notificações quando um incidente for proposto ou promovido. Capacidade de editar mensagens de modelo padrão. • configure marcadores de segurança que aparecem na interface do analista de segurança para diferenciar os incidentes que foram propostos como candidatos a incidentes de segurança graves ou promovidos a incidentes de segurança graves.
Verifique se as configurações Administração de incidentes de segurança graves - Notificações foram bem-sucedidas.	Como administrador do MSI, acione notificações por e-mail quando um incidente de segurança for proposto e enviado para todos os usuários e grupos que estão configurados para a lista de notificações. Para obter mais informações, consulte Definir preferências de notificação para MSIM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de incidentes graves de segurança funções

Atribua funções para garantir que os usuários possam executar todas as ações necessárias na aplicação MSIM.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
Administrador do MSI	sn_msi.workspace_admin	Posso instalar e configurar Gestão de incidentes graves e definir as aplicações dependentes, como File Explorer (FE), configuração do Microsoft Teams e canal de bate-papo, configuração do espaço e configuração da administração do MSI: configurações e notificações. Como configurar: • Componente do Explorador de Arquivos (FE): ◦ Configure o repositório de arquivos. ◦ Configure ações de arquivo e pasta, que são fornecidas no componente Explorador de Arquivos da guia Colaboração no espaço de Gestão de incidentes de segurança graves. ◦ Crie as pastas e subpastas raiz e forneça acesso às subpastas. • Gestão de canal de bate-papo ◦ Ative e configure Microsoft Teams validando a conexão Microsoft Teams. ◦ Crie equipes de bate-papo e canais de bate-papo, adicione usuários e atribua usuários aos vários grupos de usuários. • Administração do MSI:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
		◦ Configurações: configure as ações dos analistas de segurança, as notificações enviadas quando os incidentes são propostos e promovidos e exiba marcadores para os incidentes de segurança. ◦ Notificações: automatize o processo de notificação por e-mail e as notificações do usuário quando um incidente de segurança for proposto ou promovido como um incidente de segurança grave.
Gerenciador do MSI	sn_msi.workspace_manager	• Exiba o acesso à página de definições de configuração da gestão de incidentes de segurança graves. Restringido de modificar qualquer uma das definições de configuração. • Exiba e edite dados de registro de incidentes nas guias **Detalhes**, **Colaboração**e **Organizador de tarefas** do espaço Gestão de incidentes graves. • Promova o incidente de segurança a um incidente de segurança grave. • Configure as ações de arquivo e pastas disponíveis no componente do Explorador de Arquivos na guia **Colaboração** do espaço Gestão de incidentes graves.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
		• Vinculando e desvinculando registros adicionais de incidentes de segurança graves do espaço.
Respondente do MSI	sn_msi.workspace_responder	• Função opcional para exibir, editar e responder a incidentes de segurança graves no **Detalhes** e **Tarefas** guias do espaço Gestão de incidentes graves. • Vinculando e desvinculando registros adicionais de incidentes de segurança graves do espaço.

Integrar Gestão de incidentes graves de segurança

Amplie os recursos de Gestão de incidentes graves de segurança e conecte-se à instância Now Platform, integrando com Microsoft aplicações.

Importante: Um conjunto de atualizações (KB1289784) está disponível no Guia de início rápido da Gestão de incidentes de segurança graves para ajudar os usuários com uma configuração fácil. Você precisa importar o conjunto de atualizações após concluir a instalação da aplicação. Siga o procedimento detalhado no Guia de início rápido (Etapa 2) na seção Documentos de suporte na aplicação MSIM, que está na ServiceNow Store.

Configurar Microsoft SharePoint biblioteca de documentos

Revise a configuração necessária que precisa ser feita no Microsoft SharePoint.

Antes de Iniciar

Verifique se o procedimento de configuração a seguir foi concluído.

Função necessária: administrador do sistema, sn_msi.workspace_admin

Procedimento

1. Crie uma nova biblioteca de documentos em um site Microsoft SharePoint novo ou existente e use esse mesmo site ao definir a configuração do repositório de arquivos Gestão de incidentes graves de segurança.
2. Registre uma aplicação com Microsoft para estabelecer uma conexão e se comunicar com Microsoft SharePoint usando Microsoft SharePoint REST API.
   O registro da aplicação estabelece uma conexão entre a aplicação e a Microsoft. Para obter mais informações, consulte Configuração de acesso somente de aplicativo ao SharePoint no portal docs.microsoft.com.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Existem duas maneiras de registrar uma aplicação com Microsoft SharePoint:

a. Conceder acesso via app do Azure AD - Somente

b. Conceder acesso usando Microsoft SharePoint Somente app

> **Importante:** Conceder acesso usando o aplicativo Microsoft SharePoint somente é uma abordagem legada, mas muito relevante e fácil de configurar.

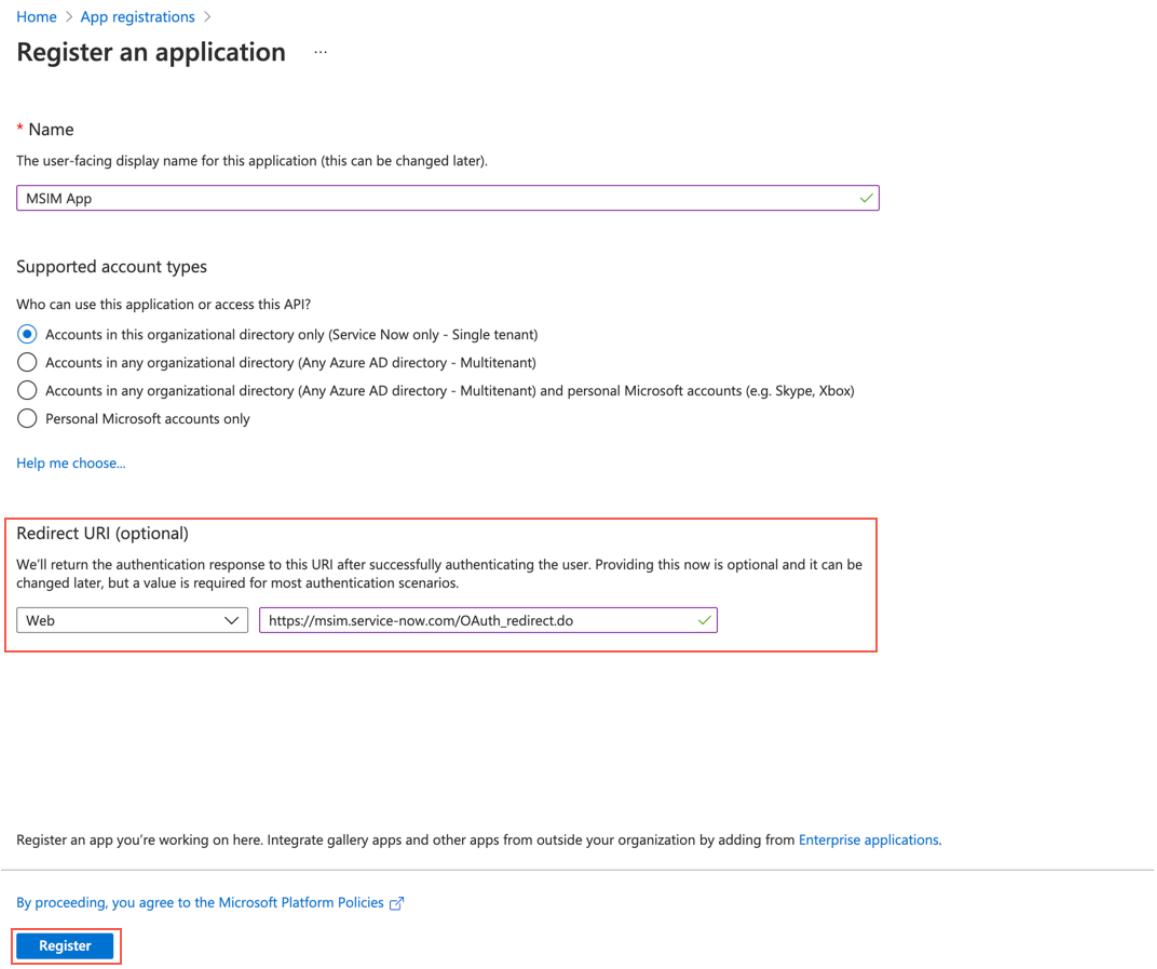
Use o ID do cliente e o segredo do cliente gerados na etapa acima ao configurar a conexão REST para o conector do Explorador de arquivos Microsoft SharePoint.

3. Registre mais um app com Microsoft para se comunicar com Microsoft SharePoint usando as APIs do Microsoft Graph.
Para obter mais informações, consulte Registrar uma aplicação na plataforma Microsoft Identity. **Registrar uma nova aplicação no Azure com a instância da Now Platform**

a. Entre no portal do Azure usando sua conta Microsoft.

b. Siga as instruções descritas no portal da Microsoft.

c. Forneça Now Platform® URL de redirecionamento de instância no campo URL de redirecionamento permitido.
Por exemplo, `msim.service-now.com/OAuth_redirect.do`



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

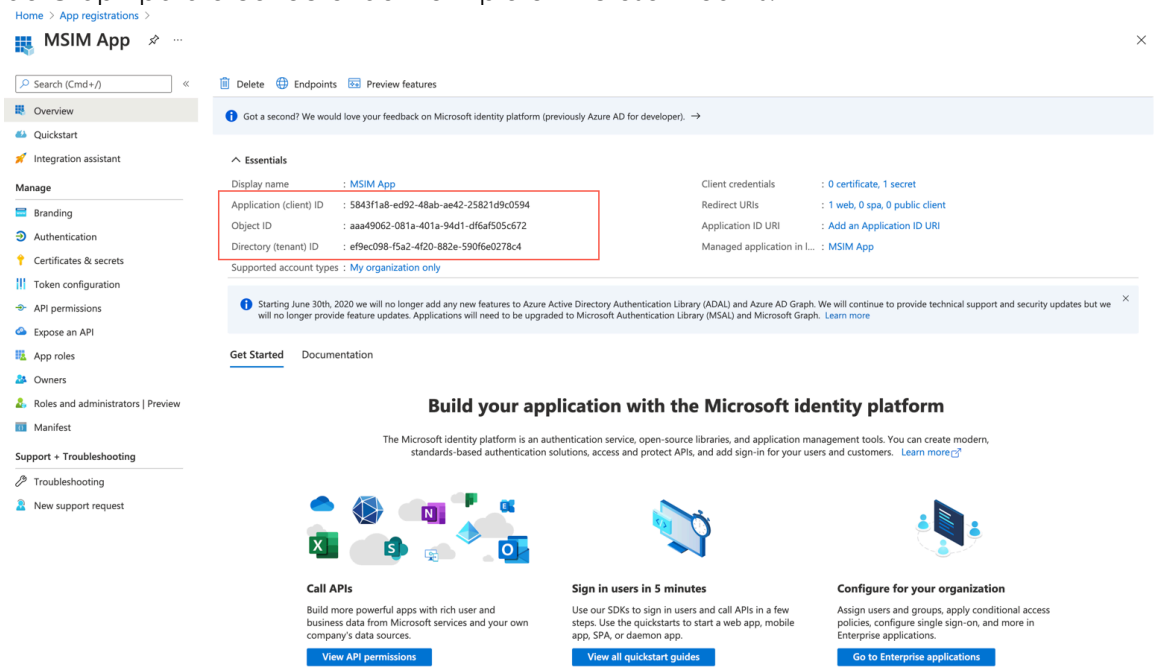
d. **Registrar** a aplicação.

e. Navegue até a seção **Certificados e segredos** e crie um novo segredo do cliente.

> **Nota:** Você também pode carregar um certificado de cliente e certificar-se de copiar e armazenar o valor de impressão digital gerado.

f. Copie e armazene o segredo do cliente gerado em algum lugar, pois ele é necessário ao configurar o registro da aplicação OAuth na instância ServiceNow®.

4. Em **Permissões de API**, adicione a permissão do Microsoft Graph:
   a. Clique **em Adicionar uma permissão**.
   b. Selecione **Microsoft Graph**.
   c. Selecione **Permissões delegadas**.
   d. Na lista **Sites**, selecione a permissão **Sites.ReadWrite.All**.
   e. Na lista **Usuário**, selecione Permissão **User.Read**.
   f. Clique **em Adicionar permissões**.
5. Em **Permissões de API**, adicione a permissão do SharePoint:
   a. Clique **em Adicionar uma permissão**.
   b. Selecione **SharePoint**.
   c. Selecione **Permissões da aplicação**.
   d. Na lista **Sites**, selecione a permissão **Sites.FullControl.All**.
   e. Clique **em Adicionar permissões**.
6. Depois de adicionar permissões, clique em **Conceder consentimento ao administrador**.
7. Use os mesmos valores de ID de cliente e segredo do cliente gerados a partir deste registro de aplicação (que está disponível na seção Visão geral) ao configurar a conexão do Graph para o conector do File Explorer Microsoft Teams.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estabelecer conexões gráficas e REST em Now Platform

Configure as conexões Graph e REST na instância Now Platform para se comunicar com Microsoft SharePoint.

Integre a instância [Now Platform e Microsoft SharePoint criando uma aplicação OAuth personalizada em Microsoft SharePoint para autenticar solicitações da Now Platform.

Configurar conexão REST para MS SharePoint

Configure a conexão REST na instância Now Platform para se comunicar com Microsoft SharePoint.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Configure um novo registro de locatário e selecione **MicrosoftSharepointOnline** como o registro de alias.
   Para obter mais informações, consulte Definir locatários do Microsoft SharePoint .
2. Para configurar a conexão e o alias de credencial do **MicrosoftSharepointOnline**, Configurar registro de conexão do Microsoft SharePoint Online .
3. Selecione o registro de locatário criado na etapa 2 acima como: **Conexão REST** ao preencher o formulário **Configuração do repositório de arquivos**.

Configurar a conexão do Graph para MS SharePoint

Configure a conexão Graph na instância Now Platform para se comunicar com Microsoft SharePoint.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Para configurar o alias de conexão e credencial do gráfico usando o segredo do cliente, consulte Configurar registro de conexão do Microsoft SharePoint Online .
   Siga as etapas abaixo para configurar a conexão do gráfico e o alias de credencial usando o certificado do cliente.

   Nota: Por padrão, o Provedor JWT, a Chave JWT e o Certificado, que estão configurados na conexão REST anterior, serão usados aqui neste procedimento. Para obter mais informações, consulte Configurar conexão REST para MS SharePoint.

   a. Navegar até **Todos** > **Conexões e Credenciais** > **Aliases de conexões e credenciais**.

   b. Abra o registro **MicrosoftSharePointGraph**.

   c. Clique no link relacionado **Criar nova conexão e credencial**.

   d. No formulário, preencha estes detalhes.

Campo	Descrição
Nome da entidade OAuth	Nome para identificar o registro da aplicação OAuth.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID do cliente OAuth	ID de cliente
Segredo do cliente OAuth	Você pode inserir qualquer valor. **Nota:** Isso não é importante, pois você usará a autenticação baseada em certificados.
URL de autorização do OAuth	URL de autorização neste formato: `https://login.microsoftonline.com/`<tenant-id> /oauth2/v2.0/authorize?response_mode=query
URL do token Oauth	URL do token neste formato: `https://login.microsoftonline.com/`<tenant-id> /oauth2/v2.0/token
URL de revogação do token	URL de revogação do token neste formato: `https://login.microsoftonline.com/`<tenant-id> /oauth2/v2.0/token .
URL de redirecionamento do OAuth	ServiceNow URL de redirecionamento neste formato: `https://empipaas.service-now.com/oauth_redirect.do`

Nota: Você pode alterar os valores padrão de acordo com seus requisitos.

e. Clique em **Criar e obter token do OAuth**.
Uma mensagem de erro é exibida solicitando 401- não autorizado.

f. Recarregue o formulário e abra o registro na lista relacionada **Conexões**.

g. Insira o valor de **impressão digital** codificado em Base64 no atributo **Valor** de impressão digital codificado na seção **Atributos**.

Nota: O valor de **impressão digital** é um valor hexadecimal. Você pode usar uma ferramenta de conversão de hexadecimal para base64 (de hexadecimal para base64) para codificar o valor de **impressão digital** para um valor de base64.

h. Navegar até **Sistema OAuth** > **Registro de aplicações**.

i. Abra o registro que tem o mesmo nome de **Nome da Entidade OAuth**, que é a etapa d neste mesmo procedimento.

j. Modifique o script da API OAuth para: **OAuthUtilJWTFESPGraph**

k. Navegar até **Conexões e Credenciais** > **Credenciais**.

l. Abra o registro: **Credencial do Microsoft SharePoint Graph**.

m. Clique em **Obter token OAuth** na seção Links relacionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Atualize o escopo da entidade OAuth.

   a. Navegar até **Sistema OAuth** > **Registro de aplicações**.

   b. Abra o registro da aplicação OAuth gerado na Etapa 1.

   c. Selecione a lista relacionada **Escopos de Entidade OAuth**.

   d. Substitua o campo de **escopo do OAuth** pelo seguinte valor **offline_access** :

   ```
   https://graph.microsoft.com/Sites.ReadWrite.All
   ```

   Nota: Você pode ignorar a etapa 2 e passar para a próxima, se estiver adicionando um certificado de cliente.

3. Configure um novo registro de locatário e selecione o registro de alias conforme criado na Etapa 1.
   Para obter mais informações, consulte Definir locatários do Microsoft SharePoint .
4. Selecione o registro de locatário criado na etapa 3 como: **Conexão do Graph** ao preencher o formulário Configuração do repositório de arquivos.

Estabelecer conexão de gráficos do MS Teams em Now Platform

Integre a instância Microsoft TeamsNow Platform e a conta [] estabelecendo uma conexão Microsoft Teams Graph.

Antes de Iniciar

Se quiser, você pode usar a mesma aplicação que criou para o SharePoint para estabelecer a conexão do Microsoft Teams Graph.

Função necessária: administrador, administrador do Azure

Registrar uma nova aplicação no Azure para conexão do Graph do Microsoft Teams

Procedimento

1. Entre no portal do Azure usando sua conta Microsoft.
2. Navegar até **Serviços do Azure** > **Registro da aplicação** > **Novo registro**.
3. Insira o nome da aplicação.
   Por exemplo, Microsoft Teams Graph.
4. Selecione a respectiva opção de **Tipos de conta compatíveis,** conforme aplicável à sua organização.
   Por exemplo, selecione a opção **Contas somente neste diretório organizacional (somente Service Now - locatário único)**.

   Nota: Para obter informações sobre os tipos de conta compatíveis, consulte Registrar uma aplicação na plataforma Microsoft Identity .

5. Selecione Tipo de **web** na lista suspensa em Redirecionar URL.
6. Insira Now Platform URL de redirecionamento de instância no campo URL de redirecionamento permitido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, https://<<InstanceName> >.service-now.com/oauth_redirect.do

7. Clique **em Registrar** para registrar sua nova aplicação e certifique-se de que a página com a seção **Visão geral** seja exibida.

Como usar certificados para autenticação

Solicite um token de acesso com uma credencial de certificado.

Antes de Iniciar

1. Você pode usar um certificado autoassinado ou um certificado emitido pela CA. Você pode criar um certificado autoassinado executando o script do PowerShell conforme descrito emConfiguração de um aplicativo do Azure AD para acesso somente ao aplicativo . O script gera dois arquivos: arquivo .PFX e arquivo .CER.

   Nota: Certifique-se de estar ciente da senha usada para criptografar a chave privada para gerar o arquivo .PFX e o arquivo .CER.

2. Use o arquivo .PFX para criar um arquivo Java Key Store (JKS).

   Nota: Certifique-se de estar ciente da senha usada para gerar o arquivo JKS a partir do arquivo .PFX.

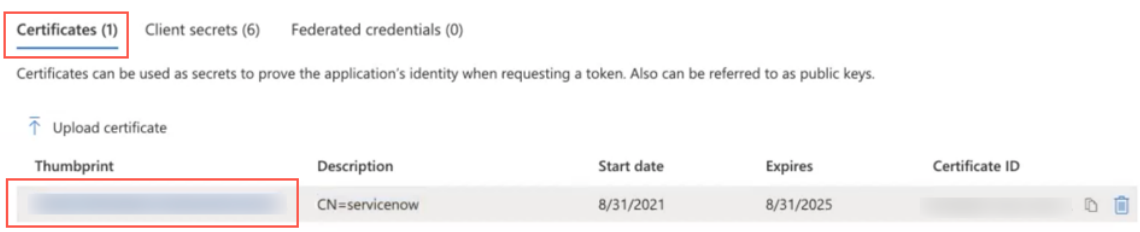
Função necessária: administrador

Procedimento

1. Navegue até **Registros de aplicações** no portal do Azure AD.
2. Clique em **Certificados e segredos** na seção **Gerenciar**.
3. Na guia **Certificados**, clique em **Carregar certificado**.
4. No formulário, preencha estes valores.

Campo	Descrição
Carregar um certificado (chave pública) com um dos seguintes tipos de arquivo: .cer, .pem, .crt	Arquivo .CER que você gerou usando o script do PowerShell.
Descrição	Descrição do certificado.

5. Clique em **Adicionar**.
   O certificado é carregado e seus detalhes são exibidos na guia **Certificados**.
6. Copie o valor da **impressão digital** do certificado carregado.
   O valor de **impressão digital** é um valor hexadecimal.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Codifique o valor de **impressão digital** para um valor Base64 e registre o valor para uso posterior.

   Nota: Você pode usar uma ferramenta de conversão de hexadecimal para Base64 (Hex para Base64) para codificar o valor de **impressão digital** para um valor de Base64.

Anexar um certificado Java Key Store para MS Teams

Habilite a autenticação de token de Concessão de Portador JWT anexando um certificado Java Key Store (JKS) válido.

Antes de Iniciar

Faça login na instância da ServiceNow para executar o procedimento a seguir.

- Certificado Java Key Store válido
- Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Certificados**.
2. Abra o registro **Certificado do conector do Microsoft Teams**.
   Certifique-se de usar somente **o certificado do conector do Microsoft Teams** do registro padrão.
3. Insira a senha associada ao arquivo JKS em Senha do **armazenamento de chaves**.
4. Clique no ícone de anexos (ícone de) e anexe o certificado JKS que você gerou.
   Para obter mais informações, consulte Configurar a aplicação OAuth no Microsoft Azure .
5. Clique **em Validar armazenamentos/certificados**.
6. Clique em **Atualizar**.

Configurar a chave de assinatura JWT para MS Teams

Crie uma chave de assinatura JWT (JSON Web Token) para atribuir ao seu certificado Java Key Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **OAuth de Sistema** > **Chaves de JWT**.
2. Abra o registro do **Conector do Microsoft Teams JWT**.
3. Insira a senha usada para criptografar a chave privada para gerar os arquivos .PFX e .CER em **Senha da chave de assinatura**.
4. Clique em **Atualizar**.

Configurar o provedor JWT para MS Teams

Adicione um provedor JWT (JSON Web Token) à sua instância da ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Copie e registre o valor da ID da **aplicação (cliente) e da IDdo diretório (locatário)** da aplicação que você registrou no portal do Azure.

- Função necessária: administrador

Procedimento

1. Navegar até **OAuth de Sistema** > **Provedores JWT**.
2. Abra o registro do **Provedor JWT do conector do MS Teams**.
3. Insira valores para **iss**, **sub**e **aud** na lista relacionada Declarações padrão.

Campo	Valor
aud	URL do Microsoft Online neste formato: `https://login.microsoftonline.com/`<tenant-id> /oauth2/token . Substituir<tenant-id> com o valor de `ID de diretório (locatário)` da sua aplicação registrado no portal do Azure.
iss	**ID da aplicação (cliente)** da aplicação que você registrou no portal do Azure.
sub	**ID da aplicação (cliente)** da aplicação que você registrou no portal do Azure.

4. Clique em **Atualizar**.

Estabeleça uma conexão usando certificados

Estabeleça uma conexão entre a aplicação de gráficos do Microsoft Teams recém-criada usando certificados.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Conexões e Credenciais** > **Aliases de conexões e credenciais**.
2. Abra **o Spoke do Microsoft Teams**.
3. Modifique o valor do campo **Modelo de configuração: MSIM Microsoft Teams ConnectorAuthorization Code Template** e salve o formulário.

> **Nota:** Este modelo contém a permissão de API delegada necessária para a integração do MSTeams.

4. Na seção Links relacionados, clique em Criar **nova conexão e credencial**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Qualquer nome exclusivo.
URL de Conexão	URL de conexão. Por exemplo, https://graph.microsoft.com
Versão da API	Versão da API. Por exemplo, v1.0
URL de Autorização	https://login.microsoftonline.com/<<tenant ID> /oauth2/v2.0/autorizar
URL de Token	https://login.microsoftonline.com/<<tenant ID> /oauth2/v2.0/token
URL de revogação do token	https://login.microsoftonline.com/<<tenant ID> /oauth2/v2.0/revogar
ID do cliente OAuth	ID do cliente.
Segredo do cliente OAuth	Você pode inserir qualquer valor. **Nota:** Isso não é importante, pois você usará a autenticação baseada em certificados.

5. Clique **em Criar e obter token OAuth**.
   Uma mensagem de erro é exibida solicitando 401- não autorizado.
6. Recarregue o formulário e abra o registro na lista relacionada Conexões.
7. Insira o valor da **impressão digital** codificada em Base64 no atributo **Impressão digital do certificado codificado** na seção **Atributos**.

   Nota: O valor de impressão digital é um valor hexadecimal. Você pode usar uma ferramenta de conversão de hexadecimal para base64 (de hexadecimal para base64) para codificar o valor de impressão digital para um valor de base64.

8. Navegar até **OAuth de Sistema** > **Registro de aplicações**
9. Abra o registro **do código de autorização do conector do Microsoft Teams do MSIM**.
10. Modifique o script da API do OAuth: **OAuthUtilJWTMSTeamsConnector**.
11. Navegar até **Conexões e Credenciais** > **Credenciais**.
12. Abra o registro **MSIM Credencial do conector do Microsoft Teams**.
13. Em Links relacionados, clique em **Obter token OAuth**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Em caso de sucesso, as seguintes permissões de API são adicionadas à aplicação do Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Usando o valor do segredo do cliente

Use o valor de segredo do cliente para configurar o registro da aplicação Graph.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Registros de aplicações** no portal do Azure AD.
2. Clique em **Certificados e segredos** na seção **Gerenciar**.
3. Clique **em Novo segredo do cliente**.
4. Copie e anote o segredo do cliente criado no campo **Valor**.

Estabelecer uma conexão usando o segredo do cliente

Estabeleça uma conexão entre a aplicação de gráficos do Microsoft Teams recém-criada com a instância Now Platform.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Conexões e Credenciais** > **Aliases de conexões e credenciais**.
2. Abra **o Spoke do Microsoft Teams**.
3. Modifique o valor do campo **Modelo de configuração: MSIM Microsoft Teams ConnectorAuthorization Code Template** e salve o formulário.

   Nota: Este modelo contém a permissão de API delegada necessária para a integração do MSTeams.

4. Na seção Links relacionados, clique em Criar **nova conexão e credencial**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Qualquer nome exclusivo.
URL de Conexão	URL de conexão. Por exemplo, https://graph.microsoft.com
Versão da API	Versão da API. Por exemplo, v1.0
URL de Autorização	https://login.microsoftonline.com/<<tenant ID> /oauth2/v2.0/autorizar
URL de Token	https://login.microsoftonline.com/<<tenant ID> /oauth2/v2.0/token
URL de revogação do token	https://login.microsoftonline.com/<<tenant ID> /oauth2/v2.0/revogar
ID do cliente OAuth	ID do cliente.
Segredo do cliente OAuth	Segredo do cliente.

5. Clique **em Criar e obter token OAuth**.
   Em caso de sucesso, as seguintes permissões de API são adicionadas à aplicação do Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Tradução automática

Ativar o conector de bate-papo do MS Teams para o usuário do Spoke do MS Teams

Se você for um usuário existente, siga o procedimento nesta seção para ativar o conector de bate-papo do Microsoft Teams.

Antes de Iniciar

Função necessária: administrador

Procedimento

Se você já é um usuário do Microsoft Teams Graph Spoke, siga as etapas abaixo:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Navegue até sua aplicação registrada no portal do Azure que é usada pelo Spoke do Microsoft Teams Graph.
- Navegue até a seção **Permissões de API** para configurar as permissões de API necessárias.
- Clique **em Adicionar uma permissão**.
- Selecione **Microsoft Graph**.
- Para usar a aplicação Conector do Microsoft Teams, você precisa adicionar mais duas permissões delegadas à sua aplicação no portal do Azure: "ChannelMember.ReadWrite.All" e "TeamMember.ReadWrite.All".
- Depois de adicionar as permissões necessárias acima, clique em **Conceder consentimento ao administrador**.

Configure o MS Teams na instância da Now Platform para um usuário existente:

- Navegue até **Aliases de conexão e credencial**.
- Selecione o registro **Spoke do Microsoft Teams**, conforme mostrado na imagem abaixo.
- Selecione o registro de credencial associado ao Spoke do Microsoft Teams.
- Clique **em Obter token OAuth**. Uma mensagem de confirmação exibe que o token de atualização do OAuth está disponível.

Como usuário existente, você concluiu a integração da aplicação do conector de bate-papo do Microsoft Teams com a Graph API do Microsoft Teams.

Gestão de incidentes graves de segurança Integração de chamada em conferência

Com a integração de chamadas em conferência Gestão de incidentes graves de segurança, você pode colaborar com seus clientes e agentes colegas para resolver problemas do cliente usando as opções de compartilhamento de vídeo e tela em Microsoft Teams, Cisco Webexou Zoom da aplicação MSIM.

A integração de chamada em conferência Gestão de incidentes graves de segurança permite que você integre o canal de comunicação de conferência com o canal de comunicação Notify, gerenciando e iniciando uma reunião Microsoft Teams, Cisco Webexou Zoom diretamente da aplicação Gestão de incidentes graves de segurança.

Como um gerente do MSI, você pode usar a integração de chamada em conferência do MSIM para iniciar Microsoft Teams, Cisco Webex ou Zoom reuniões. Integre a Gestão de incidentes graves de segurança Chamada em conferência com os provedores de serviço de terceiros como um canal de comunicação para se encontrar com as partes interessadas a fim de resolver os incidentes de segurança graves.

Principais recursos

A integração da Chamada em conferência de gestão Incidente grave de segurança fornece os seguintes recursos principais:

- Os gerentes do MSI podem iniciar uma chamada em conferência Microsoft Teams, Cisco Webexou Zoom diretamente do incidente de segurança grave.
- Convidar participantes adicionais para a chamada.
- Exibir gravações de chamadas e detalhes do bate-papo.
- Envia convites para os participantes por e-mail e Microsoft Teams bate-papo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como iniciar uma chamada em conferência

Inicie uma chamada em conferência a partir de uma tarefa ou de uma segurança principal convidando um ou mais usuários para ingressar em uma chamada em conferência.
A chamada em conferência iniciaria somente quando pelo menos dois participantes ingressem.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Verifique se você fez o seguinte na instância ServiceNow® :

- Instalado e ativado o plug-in Notify (com.snc.notify).
- Instalado o app Notify Componentes de IU para espaços configuráveis.
- Instalou e ativou o plug-in Visual Task Board (com.devsnc.snb_vtb).

Para obter mais informações, consulte Solicitação de IntegrationHub .

Por Que e Quando Desempenhar Esta Tarefa

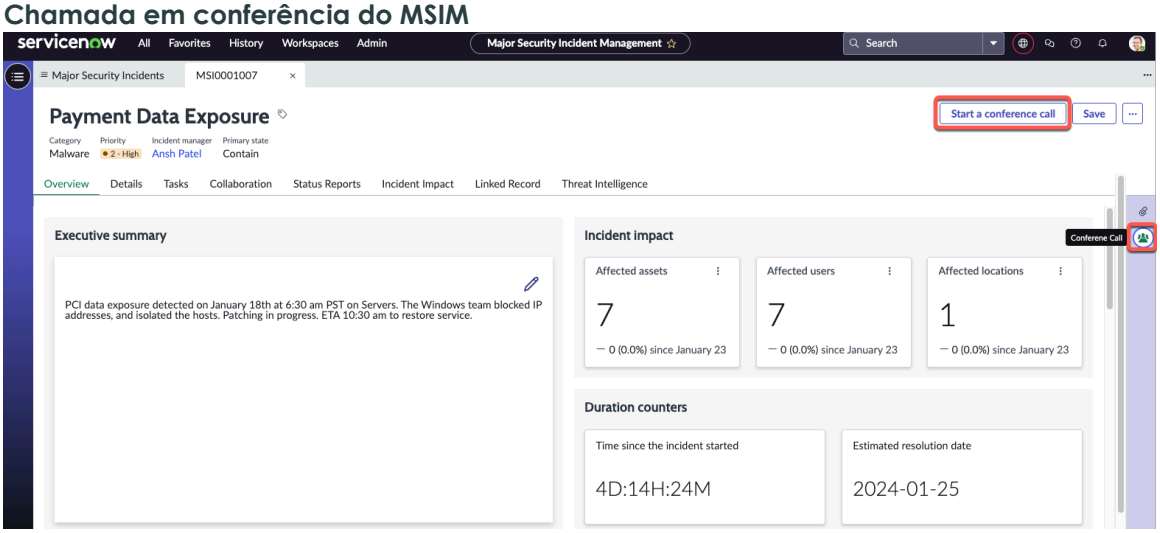
Os participantes da chamada podem incluir o seguinte:

- Usuários que receberam responsabilidades específicas.
- Contatos ad hoc ou sob demanda
- Outros contatos de terceiros

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione a ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência selecionando o ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.

Chamada em conferência do MSIM



5. No campo Ponte de conferência, escolha uma **Ponte de conferência da** qual você deseja se conectar.
   Por exemplo, Microsoft Team, Zoom ou Cisco Webex.

Tradução automática

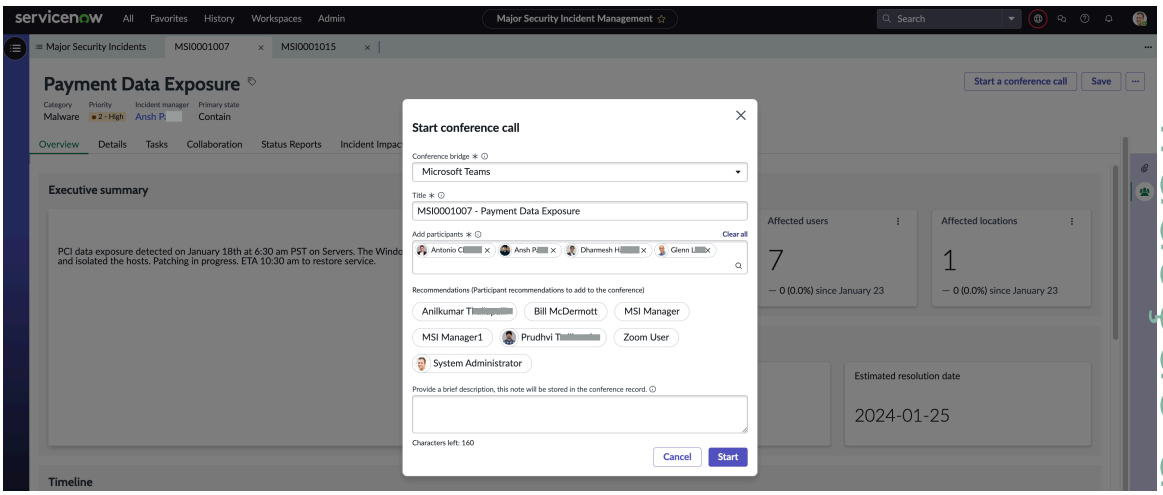
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. No campo Título, forneça um título que descreva o motivo da chamada em conferência.
7. No campo Adicionar participantes, selecione os participantes da chamada em conferência.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência.

   O usuário (host) que inicia a chamada em conferência é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

   Nota: Verifique se os participantes selecionados têm um endereço de e-mail válido.

Como iniciar uma chamada em conferência



8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição que você fornecer será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, selecione **Iniciar**.
   A chamada em conferência começa na ponte de conferência selecionada. Todos os participantes são notificados por e-mail e também por meio da respectiva ponte de conferência selecionada.
10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência.
    Os participantes podem usar o link da notificação por e-mail ou a notificação da ponte de conferência selecionada para ingressar na chamada.
11. Abra o incidente de segurança grave associado para exibir os detalhes da chamada em conferência.
    Quando o participante final sair da conferência, a chamada em conferência será encerrada ou selecione **Encerrar chamada** para encerrar a chamada em conferência.

Como adicionar participantes a uma chamada em conferência

Adicione participantes a uma chamada em conferência usando a opção de pesquisa no pop-up **Iniciar chamada em conferência** para localizar e adicionar os participantes necessários. Você também pode adicionar participantes selecionando-os na lista Recomendações, que fornece recomendações de participantes para adicionar à chamada em conferência.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

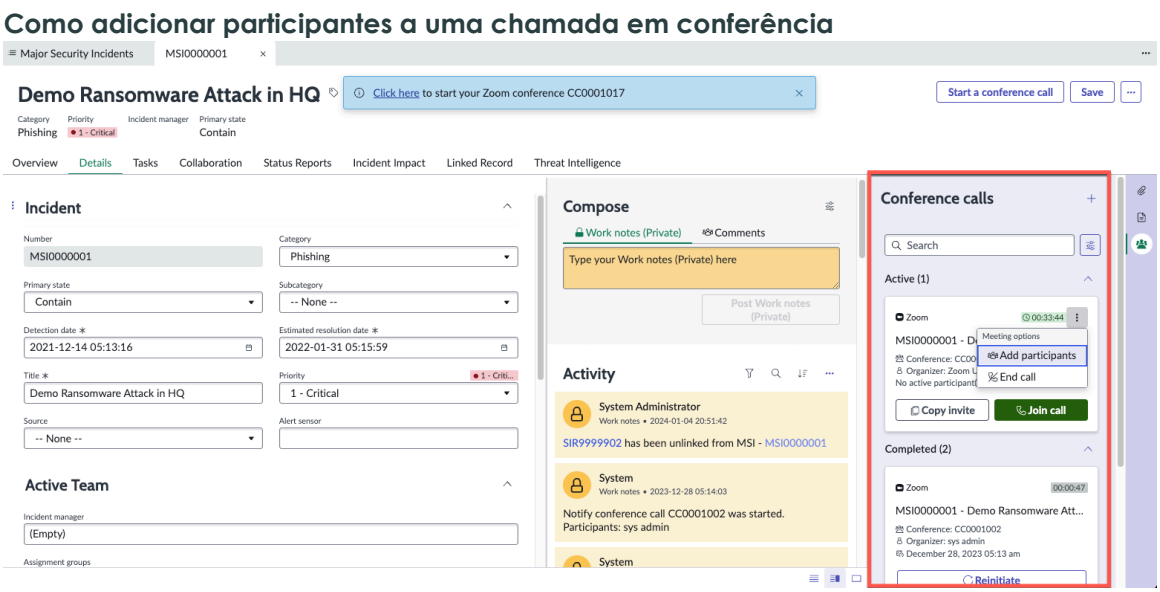
O usuário (host) que inicia a chamada em conferência é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista Recomendações.

Os participantes da chamada podem incluir o seguinte:

- Usuários que receberam responsabilidades específicas.
- Contatos ad hoc ou sob demanda
- Outros contatos de terceiros

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione o ícone de no menu de contexto direito para exibir os detalhes das chamadas em conferência.
   Isso inclui detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.
4. Selecione ao lado da chamada em conferência ativa e selecione a opção **Adicionar participantes**.



5. Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência.
6. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Todos os participantes são notificados por e-mail e também por meio da respectiva ponte de conferência selecionada. Os participantes podem usar o link da notificação por e-mail ou a notificação da ponte de conferência selecionada para ingressar na chamada.

7. Como alternativa, você pode adicionar participantes selecionando a opção **Copiar convite** na seção Chamadas em conferência no menu de contexto direito e pode compartilhar com os participantes necessários.

Silenciar participantes em uma chamada em conferência

Como gerente do MSI ou host de chamada em conferência, você tem a opção de silenciar um participante específico ou todos os participantes da chamada em conferência.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Antes de iniciar este procedimento, verifique se há uma chamada em conferência ativa com um ou mais participantes.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione o ícone de no menu de contexto direito para exibir os detalhes das chamadas em conferência.
4. Selecione **Ingressar na chamada** na ponte de conferência ativa.
5. Depois de ingressar na chamada em conferência, selecione um participante que você deseja silenciar e selecione **Mudo** na ponte de conferência.
6. Para silenciar todos os participantes na chamada em conferência, selecione **Participantes** nos controles da reunião e selecione **Silenciar tudo**.

Exibir detalhes da chamada em conferência

As chamadas em conferência são listadas como atividades do sistema na seção Atividade do incidente de segurança grave e também listadas na lista relacionada de Chamadas em conferência. Você pode exibir detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada e participantes ativos e inativos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

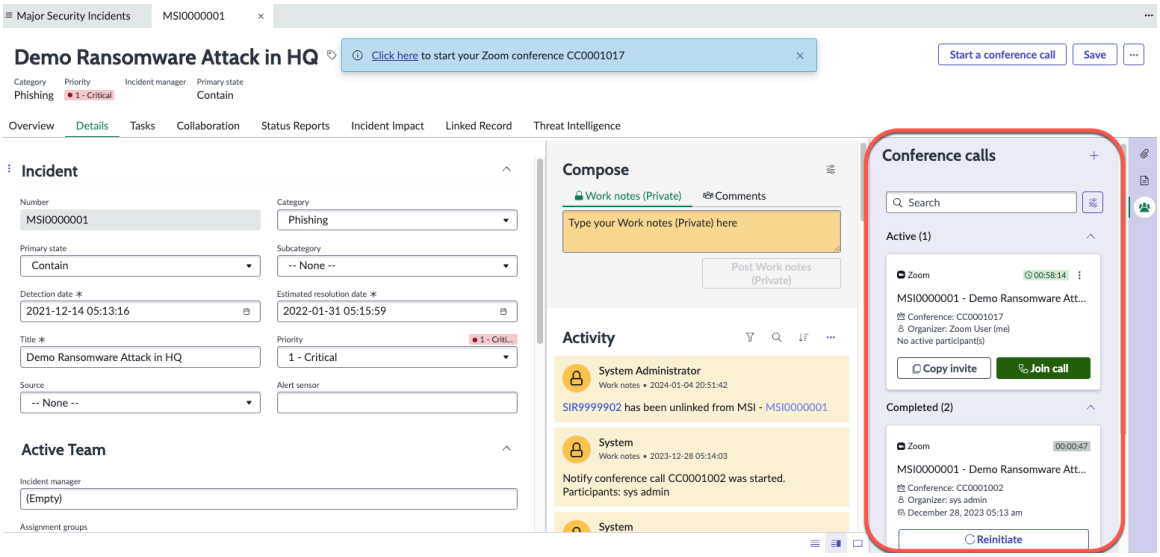
Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione o ícone de no menu de contexto direito para exibir os detalhes das chamadas em conferência.
   Isso inclui detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir detalhes da chamada em conferência



4. Você pode usar a opção de pesquisa para procurar uma chamada em conferência específica.
   Pode haver várias chamadas para o mesmo incidente de segurança grave.

5. Para adicionar participantes a uma chamada em conferência, selecione ⋮ ao lado da chamada ativa chamada em conferência e selecione a opção **Adicionar participantes**.
6. Você também pode adicionar participantes usando a opção **Copiar convite** e compartilhando o link com os participantes necessários.
7. Para ingressar em uma chamada em conferência, navegue até a seção Ativo e selecione a opção **Ingressar na chamada** da chamada em conferência necessária.
8. Para encerrar uma chamada em conferência, selecione ⋮ ao lado da chamada em conferência ativa e selecione a opção **Encerrar chamada**.
9. Para reiniciar uma chamada em conferência, navegue até a seção Concluído e selecione a opção **Reiniciar** da chamada em conferência necessária.

Integrar chamadas em conferência do MSIM com Microsoft Teams

A integração de chamada em conferência Microsoft Teams permite que você gerencie e inicie uma chamada em conferência Microsoft Teams diretamente de um incidente de segurança grave.

Principais recursos

- Inicie e encerre Microsoft Teams chamadas em conferência diretamente de incidentes de segurança graves ou de uma tarefa do workbench de segurança principal.
- Gerencie uma Microsoft Teams chamada em conferência adicionando ou removendo participantes.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins Integration Hub em sua instância ServiceNow.

- Notify plug-in (com.snc.notify)
- Microsoft Teams Plug-in Spoke de comunicações (sn_msteams_com_spk).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Plug-in de mapeamento de usuário do Azure Active Directory (sn_now_azure).
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

- Para configurar a integração da Chamada em conferência do MSIM Microsoft Teams usando o aplicativo pré-configurado, consulte Integre o app pré-publicado do conector do Notify ao Microsoft Teams .
- Para configurar a integração da Chamada em conferência do MSIM Microsoft Teams usando o aplicativo autoconfigurado, consulte Integração deapp autoconfigurado do conector do Notify [com Microsoft Teams .

Usar a integração de chamada em conferência do MSIM Microsoft Teams

As etapas a seguir mostram como você pode gerenciar e iniciar uma chamada em conferência Microsoft Teams diretamente de um incidente de segurança grave.

Antes de Iniciar

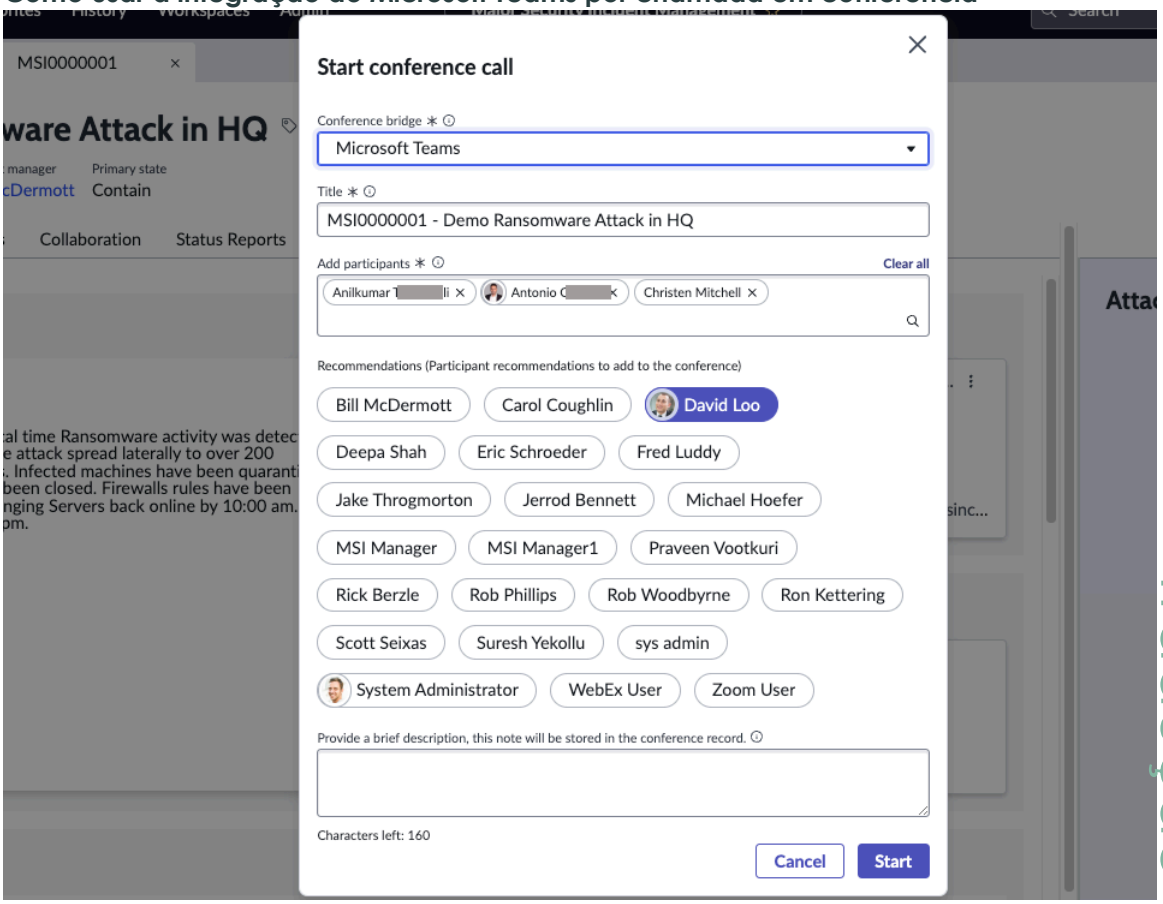
Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione a ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência selecionando o ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha **o Microsoft Teams** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Microsoft Teams.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Microsoft Teams.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência do Microsoft Teams.

   O usuário (host) que inicia a chamada em conferência do Microsoft Teams é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

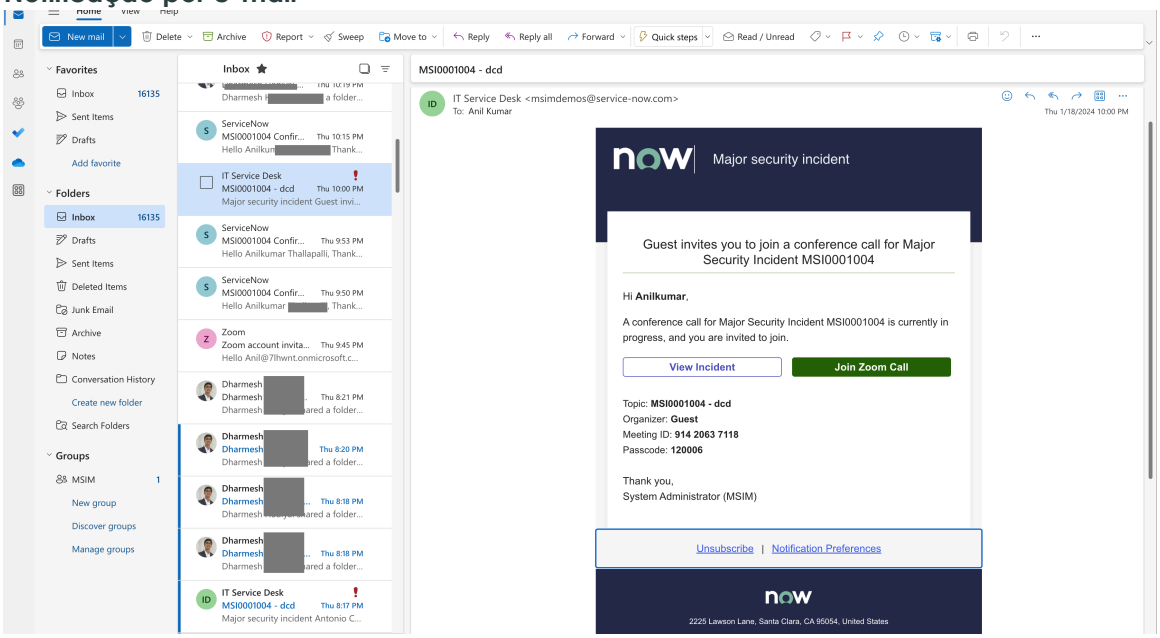
   Nota: Verifique se os participantes selecionados têm um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição que você fornecer será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, selecione **Iniciar**.
   A chamada em conferência começa no aplicativo Microsoft Teams. Todos os participantes são notificados por e-mail do aplicativo MSIM e a outra notificação é enviada por meio de um bot no aplicativo Microsoft Teams.
10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência no aplicativo Microsoft Teams.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Microsoft Teams para ingressar na chamada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificação por e-mail



11. Abra o incidente de segurança grave associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sair da chamada, a chamada em conferência será encerrada ou selecione **Encerrar chamada** na seção Chamada em conferência para encerrar a chamada em conferência.

Integrar chamadas em conferência do MSIM com Zoom

A integração de chamada em conferência Zoom permite que você gerencie e inicie uma chamada em conferência Zoom diretamente de um incidente de segurança grave.

Principais recursos

- Inicie e encerre Zoom reuniões diretamente de qualquer registro de tarefa, como um incidente de segurança grave, uma mudança ou até mesmo do workbench de incidente grave.
- Gerencie Zoom reuniões adicionando ou removendo participantes.
- Rastreie e relate os detalhes da reunião, como a duração da reunião e os participantes, para análise posterior.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins Integration Hub em sua instância ServiceNow.

- Notify plug-in (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notify Zoom (sn_notify_zoom)
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração

Para configurar a integração da Chamada em conferência MSIM Zoom usando o canal de comunicação Notify, consulte Configuração do conector Notify para Zoom no Notify .

Usar a integração de chamada em conferência do MSIM Zoom

As etapas a seguir mostram como você pode gerenciar e iniciar uma chamada em conferência Zoom diretamente de um incidente de segurança grave.

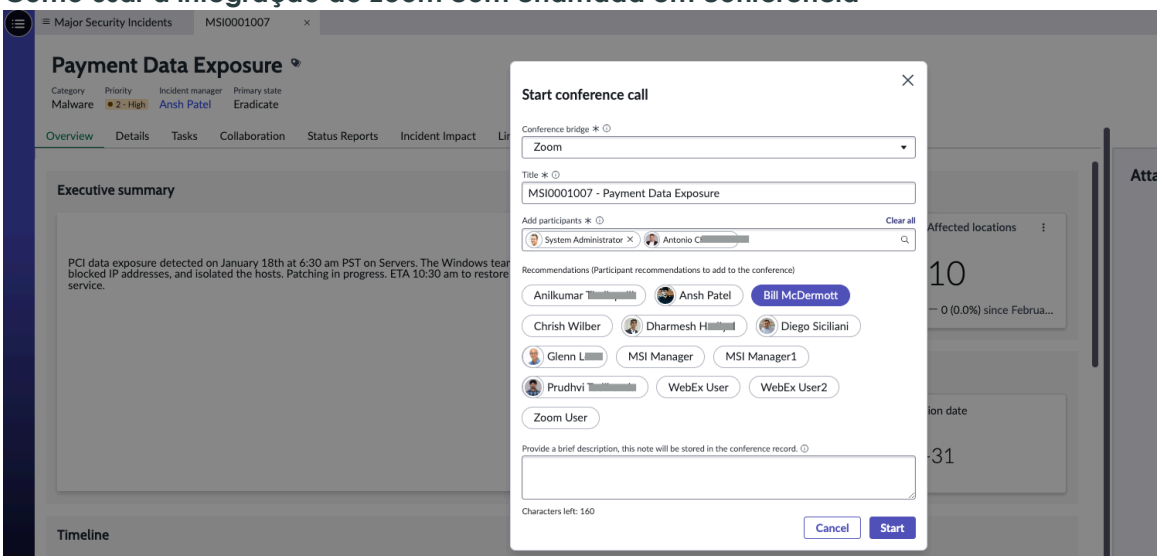
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Clique na ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência clicando no ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha o **Zoom** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Zoom.

Como usar a integração do Zoom com chamada em conferência



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Zoom.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência do Zoom.

   O usuário (host) que inicia a chamada em conferência do Zoom é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

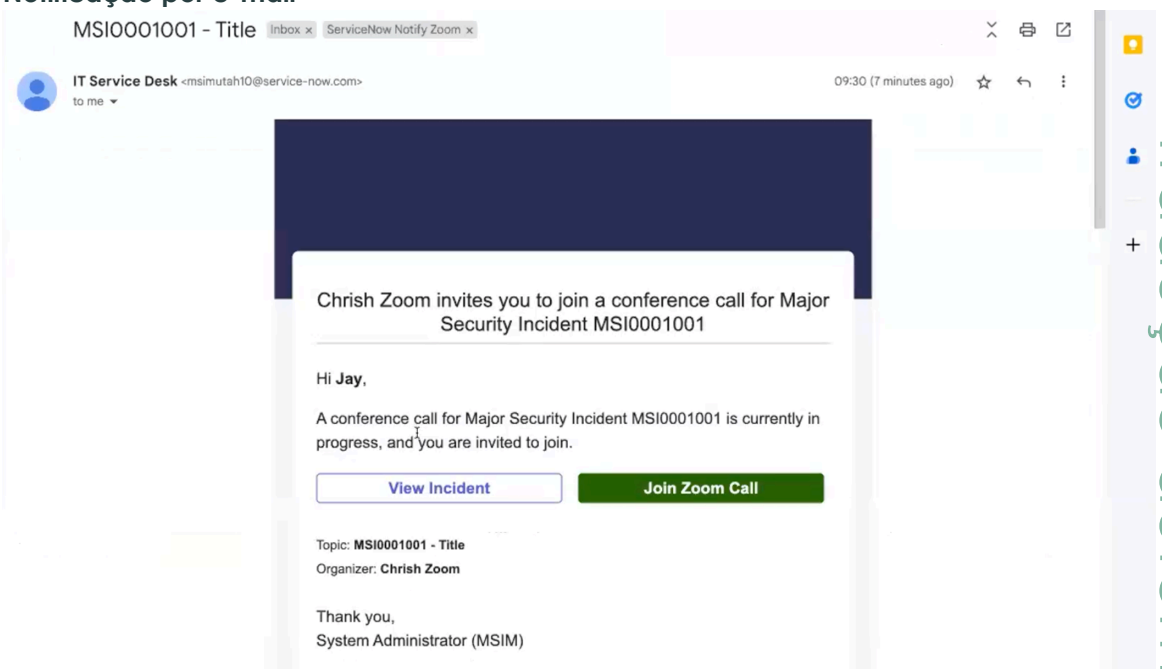
Nota: Verifique se os participantes selecionados têm um endereço de e-mail válido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição que você fornecer será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, clique em **Iniciar**.
   A chamada em conferência começa no aplicativo Zoom. Todos os participantes são notificados por meio de dois e-mails, um e-mail é enviado aos participantes do aplicativo MSIM e o outro e-mail é enviado da ponte de conferência do Zoom.
10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência no aplicativo Zoom.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Zoom para ingressar na chamada.

Notificação por e-mail



11. Abra o incidente de segurança grave associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sair da chamada, a chamada em conferência será encerrada ou selecione **Encerrar chamada** na seção Chamada em conferência para encerrar a chamada em conferência.

    Se a chamada em conferência foi gravada, a gravação estará disponível na seção Chamada em conferência do incidente de segurança grave associado após algum tempo.

Integrar chamadas em conferência do MSIM com Cisco Webex

A integração de chamada em conferência do MSIM Cisco Webex permite que você gerencie e inicie uma chamada em conferência Cisco Webex diretamente de um incidente de segurança grave.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

- Inicie e encerre Cisco Webex reuniões diretamente a partir dos incidentes de segurança graves.
- Gerencie uma Cisco Webex reunião adicionando ou removendo participantes.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins Integration Hub em sua instância ServiceNow.

- Notify plug-in (com.snc.notify)
- Notify Cisco Webex Conector (sn_notify_webex)
- Cisco Webex Spoke do Teams (sn_cisco_teams_spk)
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

Para configurar a integração da Chamada em conferência MSIM Cisco Webex usando o canal de comunicação Notify, consulte Configuração do Notify Cisco Webex Connector .

Use a integração de Chamadas em conferência Cisco Webex

As etapas a seguir mostram como você pode gerenciar e iniciar uma chamada em conferência Cisco Webex diretamente de um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

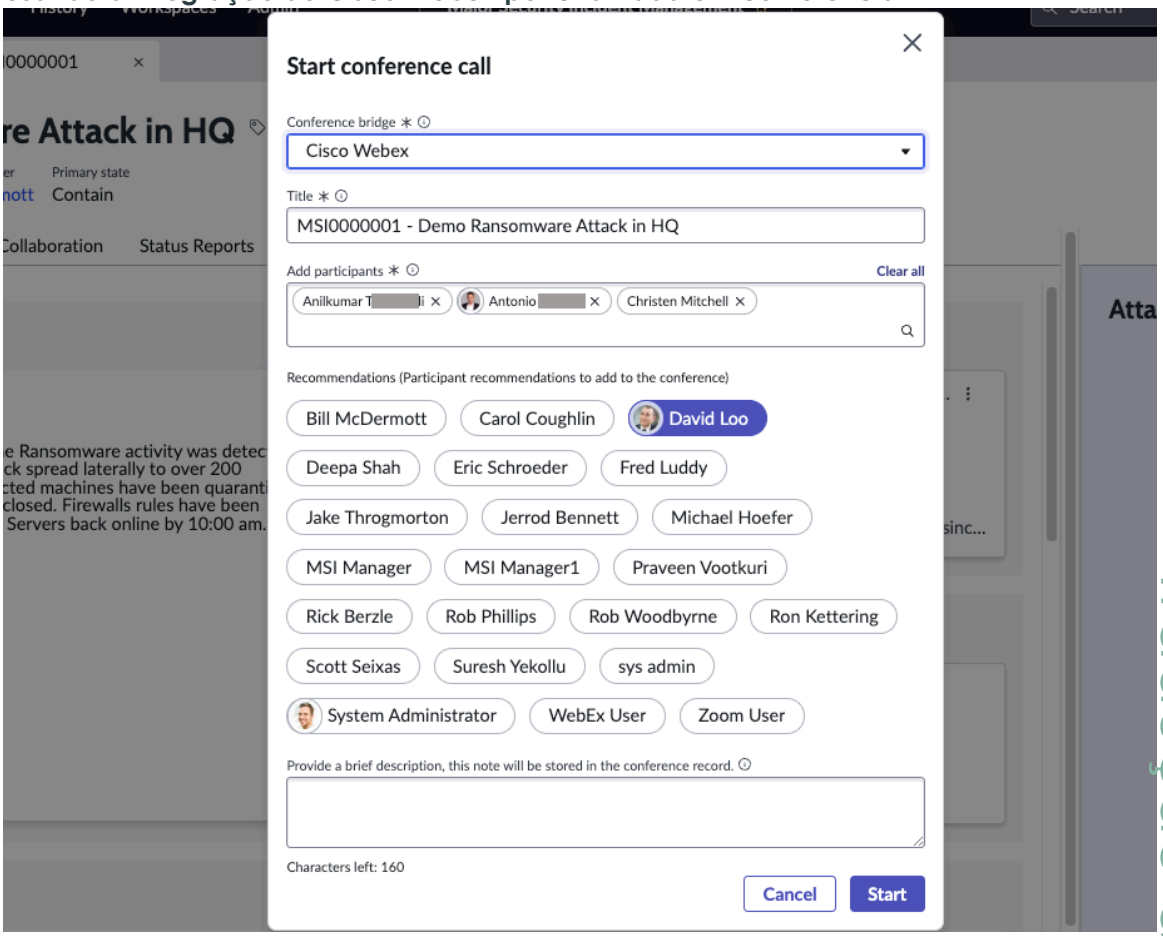
Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione a ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência selecionando o ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha **Cisco Webex** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Cisco Webex.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando a integração do Cisco Webex por chamada em conferência



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Cisco Webex.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência do Cisco Webex.

   O usuário (host) que inicia a chamada em conferência do Cisco Webex é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

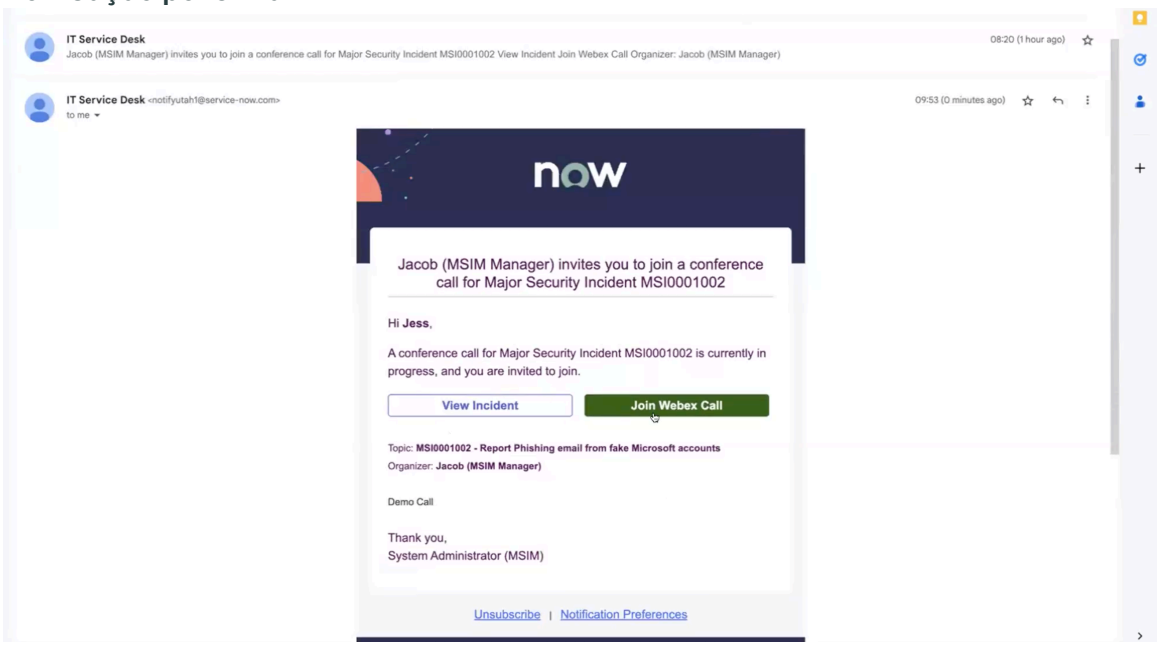
   Nota: Verifique se os participantes selecionados têm um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição que você fornecer será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, selecione **Iniciar**.
   A chamada em conferência começa no aplicativo Cisco Webex. Todos os participantes são notificados por meio de dois e-mails, um e-mail é enviado aos participantes do aplicativo MSIM e o outro e-mail é enviado da ponte de conferência do Cisco Webex.
10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência no aplicativo Cisco Webex.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Cisco Webex para ingressar na chamada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificação por e-mail



11. Abra o incidente de segurança grave associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sair da chamada, a chamada em conferência será encerrada ou selecione **Encerrar chamada** na seção Chamada em conferência para encerrar a chamada em conferência.

    Se a chamada em conferência foi gravada, a gravação estará disponível na seção Chamada em conferência do incidente de segurança grave associado após algum tempo.

Configuração da Gestão de incidentes graves de segurança

Instale e configure a aplicação Gestão de incidentes graves de segurança.

Importante:

- Para começar rapidamente com a configuração Gestão de incidentes graves de segurança, consulte o Guia de início rápido da Gestão de incidentes de segurança graves (MSIM) na ServiceNow Store.
- Depois de instalar o app Gestão de incidentes graves de segurança, certifique-se de importar o conjunto de atualizações em KB1289784 para carregar os arquivos parcialmente pré-configurados.

Use esta seção para saber como definir as configurações necessárias para trabalhar com registros Incidente grave de segurança, integrando com outras aplicações Microsoft externas para estabelecer conexões com a instância ServiceNow.

Configurar componente do File Explorer

O componente do espaço do Explorador de arquivos organiza e rastreia a coleção de artefatos (arquivos) relacionados a um incidente de segurança grave. Ele foi projetado para oferecer suporte à integração com qualquer provedor de hospedagem de arquivos de terceiros, como Microsoft SharePoint no espaço Gestão de incidentes graves de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- File Explorer Componente: fornece uma interface gráfica do usuário para exibir o sistema de arquivos e permite que os usuários executem operações de arquivo.
- File Explorer Núcleo: fornece uma camada de abstração que permite que o componente do File Explorer exiba o sistema de arquivos e execute várias operações de arquivo sem saber nada sobre o conector subjacente que é usado para se comunicar com repositórios externos.
- File Explorer Microsoft SharePoint Aplicação do conector: fornece os módulos de implementação necessários para rastrear e buscar metadados de arquivos/pastas de uma biblioteca de documentos Microsoft SharePoint e executar operações de arquivo.

O componente File Explorer Core fornece uma infraestrutura de base necessária para que as diferentes aplicações do conector de compartilhamento de arquivos definam suas propriedades de conexão.

Você deve instalar e configurar a unidade do repositório de arquivos e o provedor do repositório de arquivos adicionando as propriedades de conexão para extrair os metadados dos arquivos de um local do provedor de hospedagem de arquivos.

Para esta versão atual do File Explorer, essas instruções incluem a configuração e a assinatura de um arquivo de recuperação de metadados, como Microsoft SharePoint, atualizações de arquivo e pasta, operações de arquivo e registro em log da atividade de arquivo. Uma biblioteca de documentos Microsoft SharePoint designada e a configuração da unidade relacionada serão necessárias para criar pastas individuais específicas para um incidente de segurança grave.

File Explorer também permite aplicações de conector como Microsoft SharePoint. Você pode usar este exemplo para configurar suas implementações de operação de arquivo, como **Baixar** ou **Renomear** As ações de pasta e arquivo serão habilitadas no componente do espaço do Explorador de Arquivos. Essas ações são habilitadas e executadas usando os subfluxos do Flow Designer integrado. Para obter mais informações, consulte Configurações de ação de pasta e arquivo.

File Explorer configuração inclui a seguinte configuração:

- Configurar o Explorador de Arquivos Repositório Unidade
- Definir configurações de ação de pasta e arquivo
- Criar modelos de pasta

Introdução ao Explorador de arquivos

Revise as informações a seguir antes de começar a trabalhar com o componente File Explorer.

Revise as informações a seguir antes de começar a estabelecer a conexão com Microsoft SharePoint, criar ações de pasta e arquivo e criar modelos de pasta para o componente do explorador de arquivos.

Pré-requisitos

Nome	Descrição
Microsoft SharePoint spoke, versão 2.0.2 para ServiceNow® IntegrationHub.	Use o ID do plug-in **sn_sp_spoke** para pesquisar e instalar o Microsoft SharePoint spoke.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

Nome	Descrição
	A instalação deste plug-in fornece fluxos e ações para automatizar a colaboração, a gestão de documentos e os direitos de acesso do usuário em Microsoft SharePoint.
Componente do File Explorer v1.1.0	Use o ID do plug-in **sn_file_explorer** para pesquisar e instalar o componente File Explorer v1.1.0 A instalação deste plug-in fornece uma interface gráfica do usuário para navegar pelo sistema de arquivos, que está disponível no explorador de arquivos core.
File Explorer Core para Operações de segurança v1.1.1	Use o ID do plug-in **sn_fe** para pesquisar e instalar o File Explorer Core. A instalação deste plug-in fornece a infraestrutura de base para integração com qualquer provedor de hospedagem de arquivos de terceiros.
Microsoft SharePoint Conector do explorador de arquivos para Operações de segurança v1.1.1	Use o ID do plug-in **sn_fe_sharepoint** para pesquisar e instalar o Microsoft SharePoint File Explorer Connector. A instalação deste plug-in gerenciará os Microsoft SharePoint arquivos/pastas usando o Explorador de arquivos.

Configurar o Explorador de Arquivos Repositório Unidade

O conector Microsoft SharePoint fornece vários recursos a serem implementados nos recursos do Explorador de Arquivos Microsoft SharePoint, gerenciando e rastreando os metadados do arquivo.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança grave** > **Explorador de arquivos** > **Configuração do repositório de arquivos**.
2. Preencha os seguintes campos conforme descrito na tabela a seguir:

Nome do Campo	Descrição do Campo
Nome	Nome do registro do repositório de arquivos que identifica o uso. Por exemplo, MSIM.
Provedor	Nome do provedor que é o provedor do repositório de hospedagem do arquivo de terceiros. Por exemplo,Microsoft SharePoint.

Tradução automática

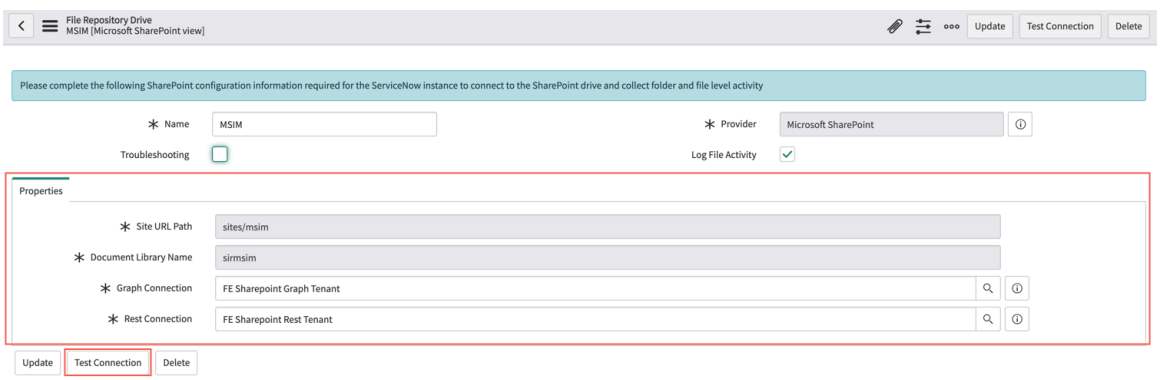
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição do Campo
Propriedades	
Caminho de URL de site	Insira uma URL Microsoft SharePoint com um caminho de site específico. Forneça somente o caminho relativo para o site e uma URL de site completa pode não ser necessária. Por exemplo, Sites/MSIM.
Nome da Biblioteca de Documentos	Crie uma biblioteca de documentos no site Microsoft SharePoint e forneça o mesmo nome de biblioteca de documentos aqui. Esta seria a mesma biblioteca de documentos que você criou na configuração da Unidade do Conector Microsoft SharePoint.
Conexão do Graph	Selecione o registro de locatário do Explorador de arquivos Graph. Para obter mais informações sobre a configuração de conexão de locatário, consulte Spoke do Microsoft SharePoint .
Conexão REST	Selecione o registro de locatário REST do Explorador de arquivos. Para obter mais informações sobre a configuração de conexão de locatário, consulte Spoke do Microsoft SharePoint .

3. Selecione **Salvar**.
4. Clicar **Testar conexão** para testar a conexão e validar as propriedades de configuração da unidade do repositório de arquivos.

   Nota: Antes de **ativar** o repositório de arquivos, certifique-se de que a biblioteca de documentos correspondente em Microsoft SharePoint não tenha dados de pasta ou arquivo.

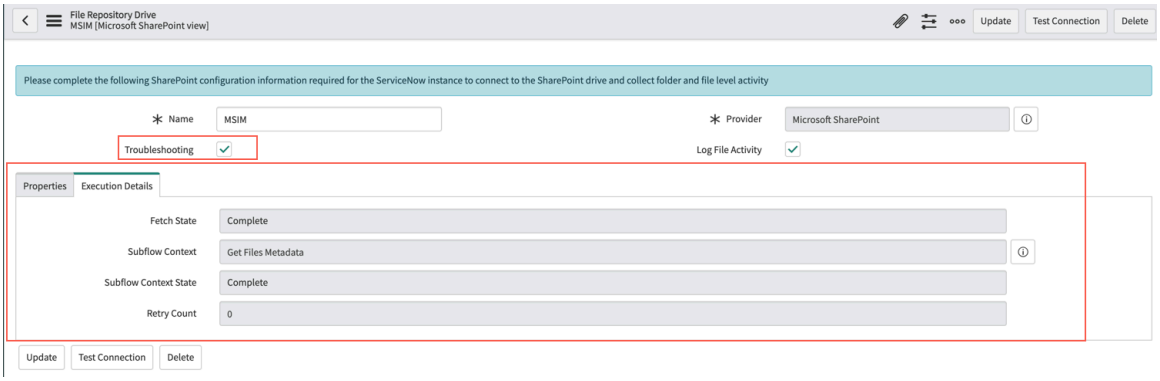
5. Clique em **Ativar** para ativar o repositório de arquivos.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Marque a caixa de seleção **Solução** de problemas para verificar os **Detalhes de execução** do repositório de arquivos e verificar o **Buscar estado** está concluído e certifique-se de que Microsoft SharePoint As assinaturas da unidade estejam criadas e o estado esteja concluído.



Nota: Usando o botão **Testar conexão**, o Administrador do MSI ou o Gerenciador do MSI só podem validar a configuração do repositório de arquivos.

Definir configurações de ação de pasta e arquivo

Configure as ações de pasta e arquivo que você deseja habilitar no componente do Explorador de Arquivos no espaço de Gestão de incidentes de segurança graves, usando a página de configuração Configurações de ação de pasta e arquivo. Como administrador do MSI, você pode controlar as ações individuais de pasta e arquivo exibidas no componente do explorador de arquivos.

Antes de Iniciar

A seguir estão as capacidades de operações de arquivo implementadas no componente do explorador de arquivos usando o ServiceNow® Flow Designer:

Capacidades de operações de arquivo

Operação de arquivo	Descrição
Abrir em Microsoft SharePoint	Abre uma nova guia do navegador para exibir Microsoft SharePoint exibição de arquivo da biblioteca de documentos
Criar pasta	Capacidade de criar pastas ad hoc adicionais após a criação do incidente de segurança grave.
Renomear pasta	Capacidade de renomear as pastas criadas.
Mover arquivo	Permite que você mova arquivos entre pastas no componente Explorador de Arquivos do espaço, resultando na movimentação de arquivos em Microsoft SharePoint
Localizar arquivo	Mostra o local da pasta ao usar o **Recentes** exibição do Explorador de Arquivos.
Exclusão de arquivo	Exclua o arquivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidades de operações de arquivo

Operação de arquivo	Descrição
Excluir pasta	Exclua a pasta.
Baixar arquivo	Baixa o arquivo na guia do navegador existente do Espaço do MSIM para exibição rápida.
Renomear arquivo	Renomeia o arquivo.

Nota:

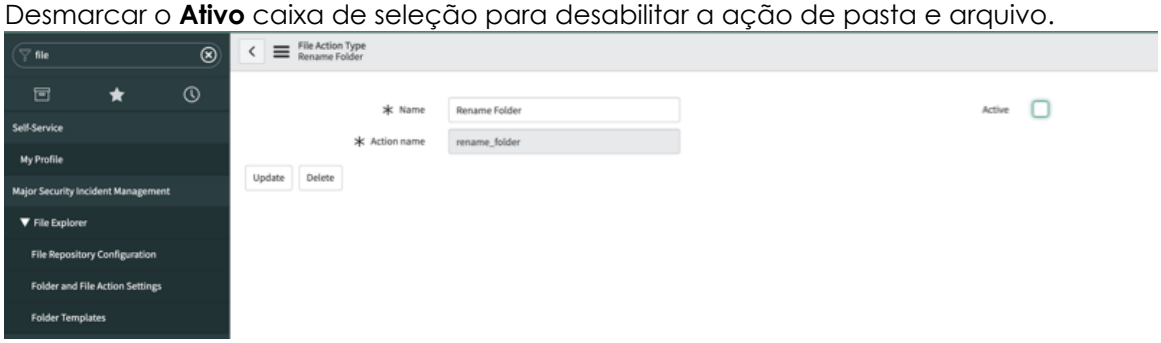
1. Todas as ações listadas estão habilitadas por padrão. Você precisará editar o **Configurações de ação de arquivo** se você não quiser que determinadas ações sejam exibidas. No momento, todas as configurações são globais para todos os usuários, , o que significa que não há capacidade de habilitar ações para um subconjunto dos usuários que têm uma função específica.
2. **Revogar acesso do usuário** e **Adicionar permissão** ações são ações relacionadas ao sistema. É recomendável não modificar essas ações de arquivo.

O seguinte exemplo de procedimento descreve uma das capacidades de operações de arquivoies para desabilitar qualquer ação específica de pasta e arquivo durante a configuração do Repositório do Explorador de Arquivos. Este procedimento é aplicável a todas as outras ações que podem precisar ser editadas:

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Explorador de arquivos** > **Configurações de ação de pasta e arquivo**.
2. Selecione o registro desejado para habilitar ou desabilitar a ação de pasta ou arquivo, respectivamente.
3. Desmarcar o **Ativo** caixa de seleção para desabilitar a ação de pasta e arquivo.

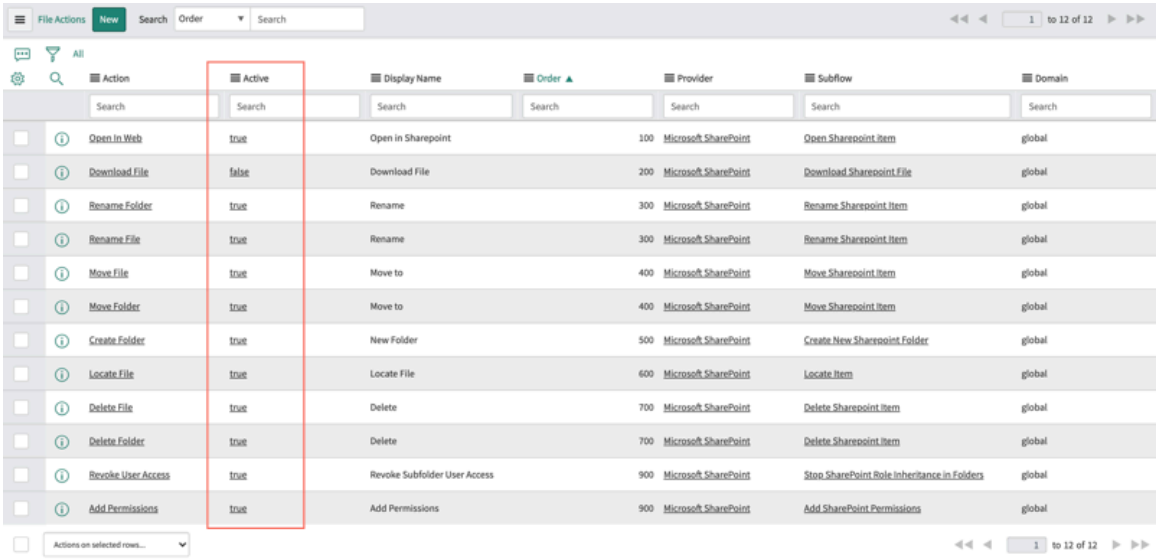


Tradução automática

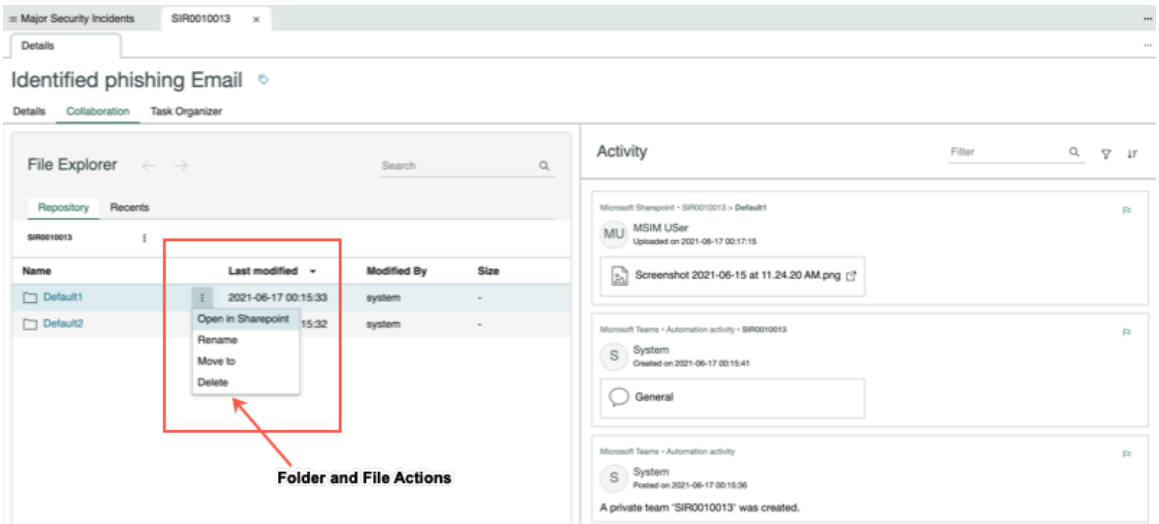
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. **Atualize** o registro da unidade.

Nota: Você também pode executar a ação de arquivo diretamente na lista de operações de arquivo exibidas, escolhendo o **Ativo** valores de coluna como Verdadeiro ou Falso.



Se a ação de arquivo realizada estiver desabilitada, a ação não será exibida no **Colaborações** guia do **Gestão de incidentes graves de segurança** espaço.



Criar modelos de pasta

Use modelos de pasta para criar automaticamente pastas exclusivas para diferentes tipos de incidentes de segurança graves. Os modelos de pasta no Componente do Explorador de Arquivos são usados para criar uma estrutura de pastas base para o incidente de segurança no Microsoft SharePoint.

Antes de Iniciar

Como administrador do MSI, você define a estrutura de pastas inicial necessária para permitir a colaboração entre diferentes grupos de respondentes do incidente e atribui privilégios de acesso apropriados em um nível de subpasta. Várias configurações podem ser criadas para diferentes tipos Incidente grave de segurança usando um construtor de condições para valores de campo Incidente grave de segurança específicos, o que inclui permitir o acesso a diferentes usuários e grupos de usuários em cada nível de subpasta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esses modelos de pasta são usados por todos os incidentes de segurança graves que atendem às condições especificadas no Construtor de condições. É recomendável que você considere o uso de variáveis de campo de incidente, como o número do incidente ou a categoria, para criar nomes de pasta raiz exclusivos que diferenciem um conjunto de subpastas com nomes de pasta comuns para um incidente de segurança grave de pastas semelhantes com esses nomes que fazem parte de um incidente de segurança grave diferente.

A configuração definida de Modelos de pasta é aplicada ao incidente de segurança grave somente quando a condição é atendida.

Nota: Uma configuração do sistema de base (sem subpastas) é aplicada a todos os incidentes de segurança. Você pode editar esta configuração padrão para incluir subpastas específicas ou criar uma nova configuração com base em um conjunto especificado de valores de campo de incidente de segurança grave. Por exemplo, categoria = atividade de código mal-intencionado.

Função necessária: sn_msi.workspace_admin

Procedimento

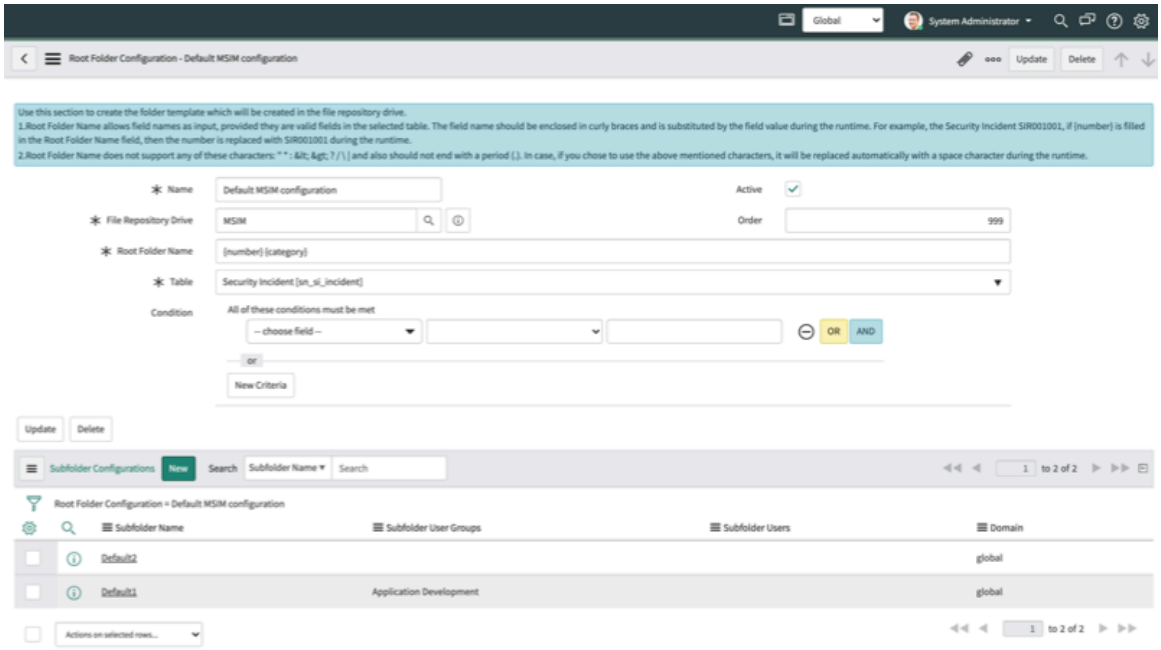
1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Explorador de arquivos** > **Modelos de pasta**.
2. Clicar **Novo** para configuração da pasta raiz.
3. No formulário, preencha os campos.

Nome do Campo	Descrição
Nome	Nome do modelo de pasta.
Unidade de repositório de arquivos	
Nome da pasta raiz	Nome da pasta raiz que aparecerá em Microsoft SharePoint, bem como no Explorador de arquivos e provavelmente deve incluir variáveis de campo de incidente, como o número e a categoria do incidente de segurança grave, para que um incidente de segurança grave possa ser diferenciado de outro.
Tabela	

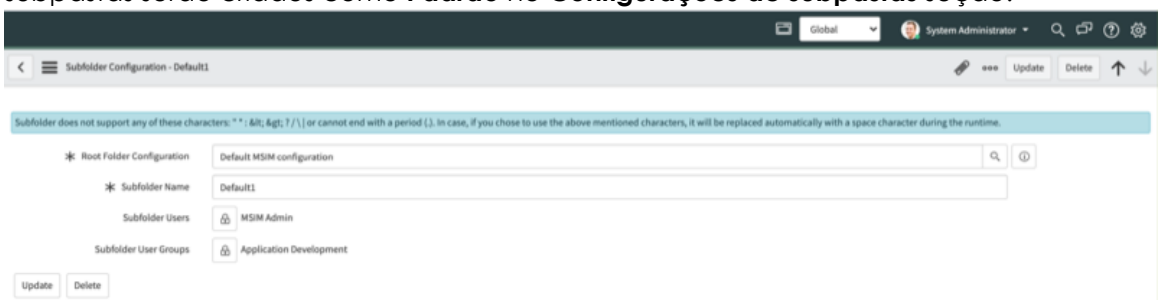
4. Definir o incidente de segurança **Condição** valores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. **Atualizar** o registro.
   As subpastas são criadas com os valores definidos.
6. Clique na **subpasta**desejada.
   Se você não criar uma subpasta com um nome apropriado, os nomes das subpastas serão criados como **Padrão** no **Configurações de subpastas** seção.



A mesma estrutura de pastas será criada automaticamente em Microsoft SharePoint usando os mesmos privilégios de acesso configurados em **Modelos de pasta** página.

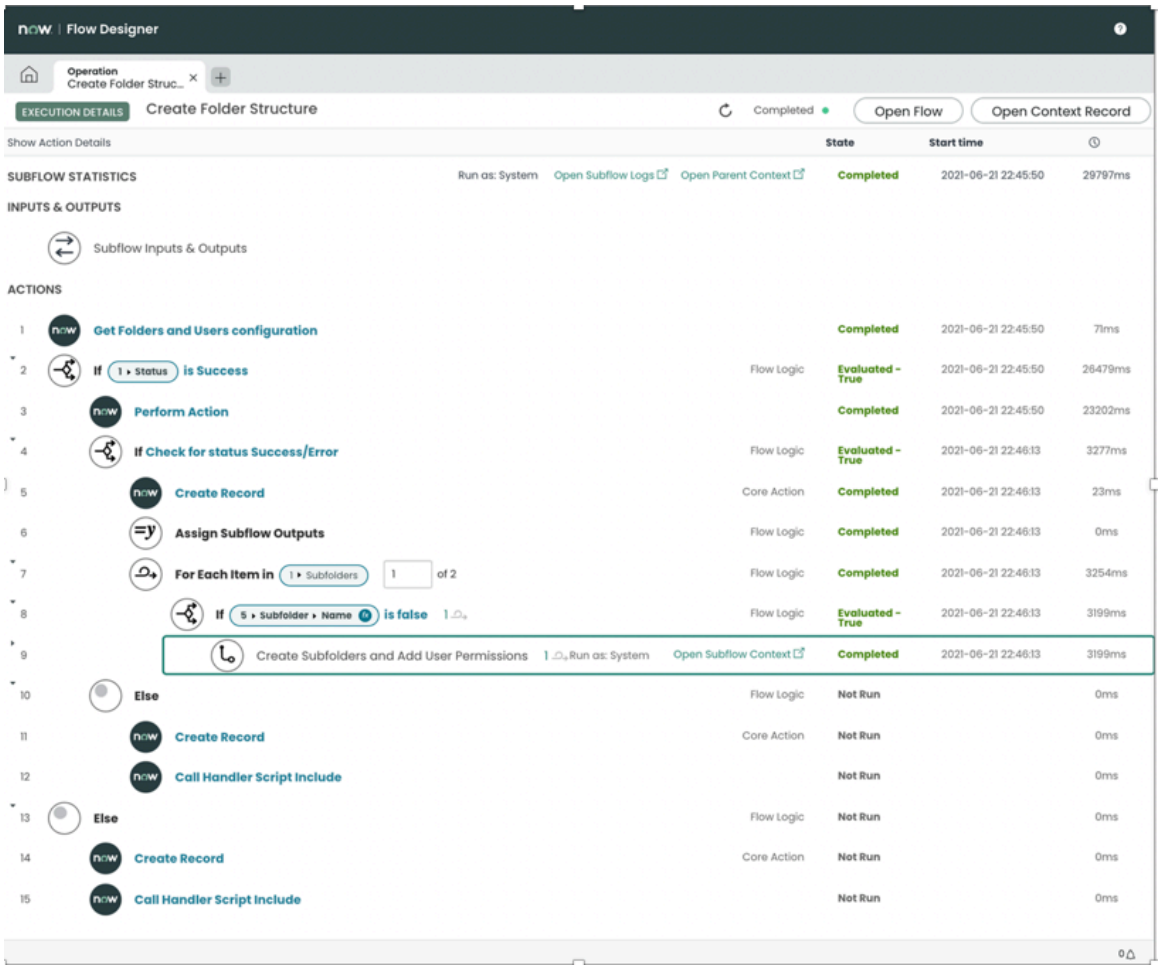
Nota:

- **O nome da pasta raiz** permite nomes de variáveis de campo como entrada, desde que sejam campos válidos na tabela selecionada. O nome do campo deve estar entre chaves e é substituído pelo valor do campo durante o tempo de execução do fluxo. Por exemplo, o incidente de segurança SIR001001, se a variável {number} estiver configurada no campo **Nome da pasta raiz**, o número será substituído por SIR001001 durante o tempo de execução.
- **Nome da pasta raiz** não é compatível com nenhum destes caracteres: " * : < > ? / \ | e também não deve terminar com um ponto (.). Se você usar os caracteres mencionados acima, eles serão substituídos automaticamente por um caractere de espaço durante o tempo de execução.
- Se o nome da **pasta raiz** e da **subpasta** exceder o limite definido (256 caracteres), o nome da pasta será truncado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está a execução do tempo de execução do subfluxo Criar estrutura de pastas:



File Explorer Fluxo de atividades no espaço

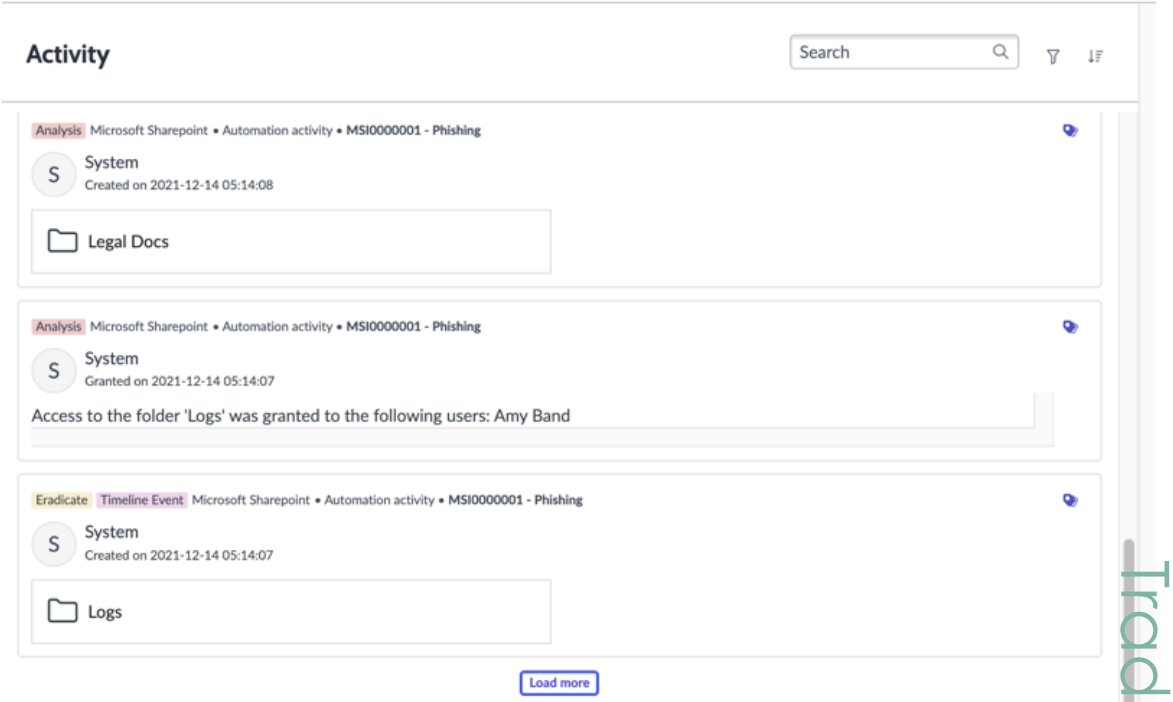
Use a seção Explorador de arquivos do espaço Gestão de incidentes graves de segurança para exibir as pastas e arquivos, a sequência em que foram criados na biblioteca de documentos Microsoft SharePoint.

O fluxo de atividades lista todas as publicações de atividades de automação sempre que houver qualquer atividade de pasta e arquivo ou logs que ocorrerem durante a resolução Incidente grave de segurança. A estrutura do fluxo de atividades está alinhada no mesmo formato da biblioteca Microsoft SharePoint, que mostra as pastas que foram criadas e quais usuários ou grupos de usuários foram atribuídos a essas pastas.

O fluxo de atividades permite que os gerentes do espaço e outros usuários ou grupos de usuários se comuniquem e colaborem com eficácia, listem as atividades que foram realizadas em Microsoft SharePoint pastas e arquivos, monitorem o status do incidente, publiquem as anotações ou adicionem comentários adicionais. têm no registro do incidente. Os gerentes

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do espaço podem selecionar e trabalhar com base na última atividade



atualizada.

Solução de problemas File Explorer

A seção de solução de problemas pode ajudar a resolver alguns dos problemas técnicos que você pode encontrar ao configurar o componente File Explorer.

Consulte a seção a seguir sobre trabalhos agendados, propriedades do sistema e File Explorer subfluxos do Flow Designer em detalhes.

Trabalhos agendados para File Explorer

Trabalhos agendados são trabalhos automatizados que são executados para processar as notificações de Microsoft SharePoint, ingerir os metadados dos arquivos na instância ServiceNow e renovar as assinaturas do repositório de arquivos em uma programação recorrente.

Trabalhos agendados são trabalhos automatizados que são executados em segundo plano para:

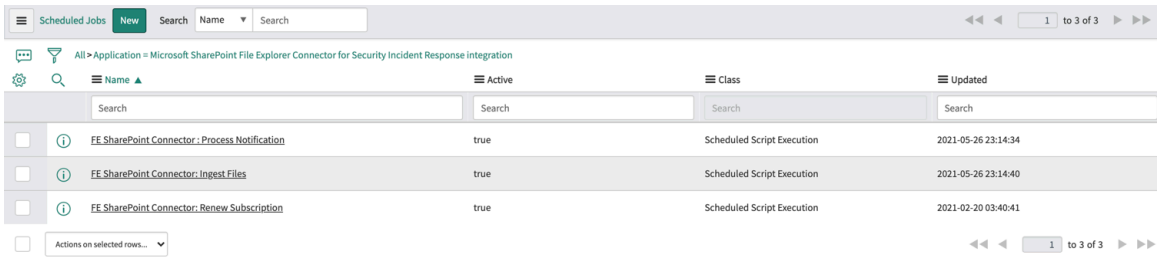
- processar as notificações do Microsoft Microsoft SharePoint.
- ingerir os metadados dos arquivos na instância Now Platform.
- renove a assinatura com a biblioteca de documentos Microsoft SharePoint para receber notificações.

Trabalho	Descrição
Microsoft SharePoint File Explorer Conector: processar notificação	É executado a cada 30 segundos e é responsável pela leitura das notificações, o que indica que ocorreu qualquer mudança na biblioteca de documentos inscrita e marca o estado das unidades (sn_fe_file_repo_drive) como pendente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
Microsoft SharePoint File Explorer Conector: ingerir arquivos	É executado a cada 30 segundos e é o principal responsável pelo processamento das unidades (sn_fe_file_repo_drive) que estão no estado pendente e extrai as mudanças do arquivo delta da biblioteca de documentos Microsoft SharePoint configurada desde a última extração.
Microsoft SharePoint File Explorer: renovar assinatura	É executado a cada 10 minutos e é responsável por renovar a assinatura da biblioteca de documentos Microsoft SharePoint um dia antes da data de vencimento. Normalmente, essas assinaturas expiram em 30 dias.



Propriedades do sistema do Explorador de arquivos disponíveis

A seguir estão as propriedades do sistema do conector do Explorador de Arquivos Microsoft SharePoint disponíveis.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_fe_sharepoint.max_retry_count	Controla a frequência de tentativas que a aplicação do conector Microsoft SharePoint tentou extrair a unidade com falha ou renovar a assinatura com falha. O valor de frequência padrão é definido como 50.
sn_fe_sharepoint.retry_after_seconds	Intervalo de tempo entre cada tentativa de extrair a unidade com falha ou renovar a assinatura. O valor padrão é definido como 900 segundos ou 15 minutos.
sn_fe_sharepoint.max_subscription_expiration_period	Período máximo de expiração da assinatura em número de dias para Microsoft SharePoint. O período de expiração padrão é definido como 30 dias.

File Explorer Subfluxos do Flow Designer

A seguir estão os subfluxos do Flow Designer que são instalados com o conector Microsoft SharePoint File Explorer.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Subfluxos

Nome	Descrição
Adicionar Microsoft SharePoint permissões	Concede permissão de edição de uma pasta específica a usuários específicos.
Criar assinatura de unidade	Assina com uma biblioteca de documentos Microsoft SharePoint configurada para receber notificações sobre quaisquer atualizações ocorridas na biblioteca de documentos.
Criar nova pasta Microsoft SharePoint	Cria uma nova pasta Microsoft SharePoint em uma determinada pasta primária.
Excluir Microsoft SharePoint item	Exclui Microsoft SharePoint arquivos e pastas.
Baixar Microsoft SharePoint arquivo	Retorna a URL de download de Microsoft SharePoint arquivos
Obter metadados de arquivos	Assina e extrai as mudanças da biblioteca de documentos Microsoft SharePoint.
Mover item Microsoft SharePoint	Move os Microsoft SharePoint arquivos/ pastas para a pasta de destino
Abrir Microsoft SharePoint item	Retorna o URL da Web de Microsoft SharePoint arquivo/pasta a ser aberto em um navegador.
Renovar assinatura da unidade	Renova a assinatura com Microsoft SharePoint biblioteca de documentos.
Criar estrutura de pastas	Segue as configurações do modelo de pasta e cria a estrutura de pastas na biblioteca de documentos Microsoft SharePoint.

Como configurar o Microsoft Teams

Integre e colabore facilmente com Microsoft Teams para resolver Incidente grave de segurança para exibir e filtrar atividades de bate-papo de colaboração.

Configurar e assinar um ambiente de bate-papo Microsoft Teams, recuperar conversas de bate-papo de dentro de canais especificados e arquivar a Equipe e os canais associados estão incluídos como parte do processo de fechamento do incidente. Um ambiente Microsoft Teams designado e uma configuração de API Microsoft Teams Graph relacionada são necessários para criar canais individuais específicos para um Incidente grave de segurança.

Para configurar o Microsoft Teams, ative o Teams como o provedor de bate-papo. Você pode criar canais de bate-papo para as várias partes interessadas e grupos que se comunicam sobre atividades e rastrear conversas de bate-papo para resolver o Incidente grave de segurança. A configuração do Microsoft Teams e da API do Microsoft Graph inclui:

- Estabelecer conexão de gráficos do MS Teams em Now Platform
- Ativar o MS Teams como um provedor de bate-papo
- Criar um modelo de canal de bate-papo
- Exibir atividade de mensagem de bate-papo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para começar com Microsoft Teams

Revise as informações a seguir antes de começar a trabalhar com Microsoft Teams como uma aplicação conectora.

Certifique-se de que os plug-ins a seguir estejam instalados antes de começar a estabelecer, ativar e validar Microsoft Teams configurar conexões.

Plug-ins necessários

Nome	Descrição
Integração de bate-papo com Gestão de incidentes de segurança	Use o ID do plug-in **sn_chat_collab_core** para pesquisar e instalar o Microsoft Teams bate-papo. A instalação deste plug-in permite rastrear a atividade de bate-papo para aplicações de terceiros, como o Microsoft Teams (ou Slack e outras aplicações de bate-papo de terceiros).
Conector de bate-papo do Microsoft Teams para Gestão de incidentes de segurança	Use a ID do plug-in **sn_ms_teams_connector** para pesquisar e instalar o Conector de bate-papo do Microsoft Teams para Gestão de incidentes de segurança graves. A instalação deste plug-in permite rastrear as atividades de bate-papo usando o componente de colaboração específico para Microsoft Teams.
Microsoft Teams Spoke do Graph	A instalação deste plug-in estabelece uma conexão de spoke do Graph com Microsoft Teams. Para obter mais informações, consulte Spoke do Microsoft Teams Graph

Ativar o MS Teams como um provedor de bate-papo

Ative Microsoft Teams validando a conexão Microsoft Teams.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Depois que a conexão é ativada e validada, uma mensagem informativa é exibida informando que a conexão do provedor foi validada com sucesso. Você pode modificar a configuração do canal adicionando e removendo usuários e, possivelmente, adicionando mais canais ou renomeando os canais existentes.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Configuração do provedor de bate-papo**.
2. Selecione **o registro do Microsoft Teams**.
3. Clique **em Validar conexão**.
   Uma mensagem de confirmação exibe que a conexão do provedor foi validada com sucesso.
4. Marque a caixa de seleção **Ativo** para ativar o registro do provedor.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma mensagem de confirmação exibe que a conexão do provedor foi validada com sucesso.

5. **Salve** o formulário depois de ativar a configuração do provedor de bate-papo. Com esta conexão entre o Microsoft Teams e a instância Now Platform, a instância foi estabelecida com sucesso.

Criar um modelo de canal de bate-papo

Configure equipes de bate-papo e modelos de canal para criar equipes de bate-papo e canais para colaborar, rastrear conversas de bate-papo e adicionar usuários e grupos de usuários a esses canais de bate-papo. Esses modelos de canal são criados no Microsoft Teams quando um incidente de segurança grave é promovido.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Modelos de canal**.
2. No formulário Configuração do canal de bate-papo, clique em **Novo** no cabeçalho do formulário.
3. No formulário, preencha os campos.

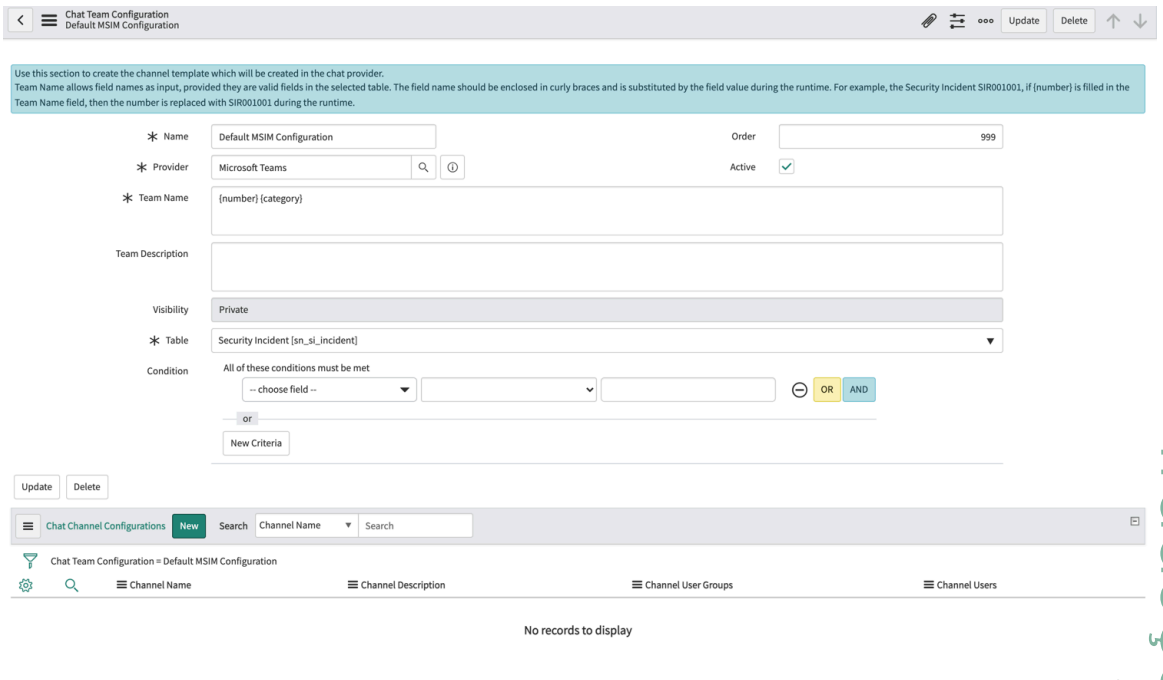
Formulário Configuração da equipe de bate-papo

Campo	Descrição
Nome	Nome da pasta.
Provedor	Microsoft Teams.
Nome da Equipe	Nome da equipe, por exemplo, no formato {number}-{category}. **Nota:** O nome da equipe fornecido aqui será usado em todos os registros de incidentes de segurança graves. Para garantir que o nome real do Microsoft Teams seja exibido na aplicação MS Teams e tenha um valor de nome exclusivo para diferentes incidentes de segurança graves, é recomendável usar um valor de campo de incidente exclusivo, como o número do incidente - {number}. Conforme mostrado no exemplo de captura de tela, o {number} seguido por um separador '-' e a variável de campo {category} forneceriam um número exclusivo e uma descrição do incidente de segurança grave para o qual o Microsoft Teams foi criado, por exemplo, {number} - {categoria}.
Descrição da equipe	Descrição opcional da equipe.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela	Incidente de segurança grave (sn_msi_incident).



4. Clique em **Enviar**.
5. Navegue até a seção Configuração do canal de bate-papo.
6. Clicar **Novo** para criar uma nova configuração de canal de bate-papo.
7. Insira o **Configuração da equipe de bate-papo** e **Nome do Canal**.

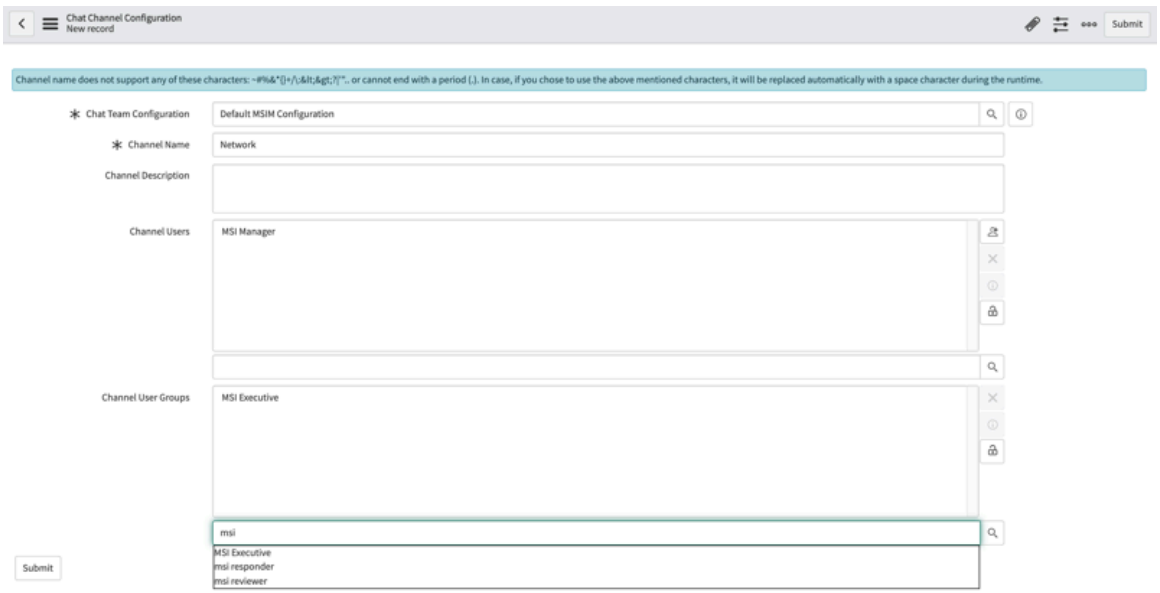
   Nota: O novo canal que você criou aqui também será o nome do seu canal no Microsoft Teams. Você pode pesquisar o mesmo canal e adicionar suas conversas.

8. Adicionar o **Usuários do canal** e **Grupos de usuários do canal** na lista de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. **Enviar** o novo registro de configuração do canal de bate-papo.



Resultados

O canal de bate-papo agora foi criado e os usuários estão atribuídos a esses grupos de canais de bate-papo. Você pode exibir as atividades de bate-papo de colaboração em Microsoft Teams e no fluxo de atividades de Colaboração do Espaço do MSIM com a estrutura de hierarquia do canal de bate-papo organizado conforme definido na configuração do provedor do Canal de bate-papo.

Exibir atividade de mensagem de bate-papo

A atividade de mensagem de bate-papo é registrada e exibida na guia Colaboração do espaço de Gestão de incidentes de segurança graves.

A atividade de mensagem de bate-papo inclui todas as conversas de bate-papo ocorridas entre os participantes, diferentes grupos de usuários.

Solução de problemas do conector de bate-papo do MS Teams para MSIM

Consulte a seção de solução de problemas do conector de bate-papo do Microsoft Teams sobre trabalhos agendados, propriedades do sistema e subfluxos do Flow Designer do Microsoft Teams.

Em qualquer caso, verifique os trabalhos agendados do processo do conector de bate-papo se você não vir as mensagens do bate-papo de colaboração publicadas no Microsoft Team e no fluxo de atividades de colaboração externo do espaço do MSIM.

Trabalhos agendados para Microsoft Teams

Trabalhos agendados são trabalhos automatizados que são executados para processar as notificações do conector de bate-papo Microsoft Teams e renovar as assinaturas do Microsoft Teams em uma programação recorrente.

Função necessária: administrador

- **Conector de bate-papo do MS Teams: processar notificação**

  Para cada evento de mensagem de bate-papo, será recebida uma notificação que terá o ID do recurso e a notificação que estão armazenados em uma tabela. Um

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

trabalho programado é executado a cada 30 segundos para selecionar notificações não processadas e consultar a API do Microsoft Teams para obter o conteúdo real da mensagem, que é armazenado em uma tabela diferente.

- **Conector de bate-papo do MS Teams: renovar assinaturas**

  Para cada canal da equipe, são criadas assinaturas para receber notificações sobre eventos criados, atualizados e excluídos. Esta assinatura fica ativa por apenas 60 minutos. As assinaturas são renovadas a cada 25 minutos por meio do trabalho de programação Conector do Microsoft Teams: Renovar notificação.

Microsoft Teams Fluxo funcional do conector de bate-papo

Veja esta seção para entender os Microsoft Teams subfluxos do Flow Designer usados para administrar a criação de canais de bate-papo e o acesso do usuário a partir do incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

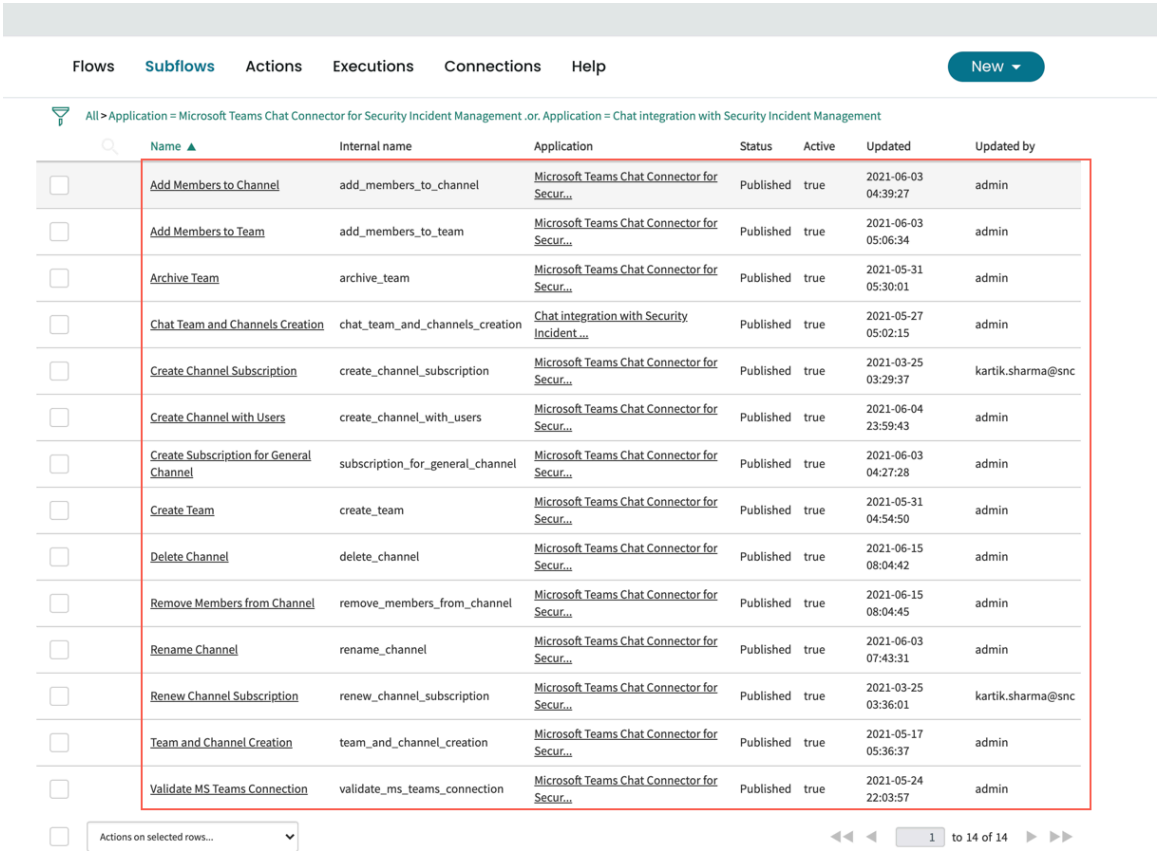
Procedimento

1. Navegar até **Todos** > **Flow Designer**.
2. Adicionar membros ao canal
3. Adicionar membros à equipe
4. Arquivar equipe
5. Criação de equipe e canais de bate-papo
6. Criar assinatura de canal
7. Criar canal com usuários
8. Criar assinatura para canal geral
9. Criar Equipe
10. Excluir canal
11. Remover membros do canal
12. Renomear canal
13. Renovar assinatura de canal
14. Criação de equipe e canal

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

15. Validar conexão do MS Teams



Configurar o conector de bate-papo do Slack para incidentes de segurança graves

Integre e colabore com Slack para resolver o incidente de segurança grave para exibir e filtrar atividades de bate-papo de colaboração.

Configurar e assinar um ambiente de bate-papo Slack, recuperar conversas de bate-papo de dentro de canais especificados e arquivar o Slack e os canais associados estão incluídos como parte do processo de fechamento do incidente. Um ambiente Slack designado e uma configuração de API Slack relacionada são necessários para criar canais individuais específicos para um Incidente grave de segurança.

Para configurar o Slack, ative o Slack como o provedor de bate-papo. Você pode criar canais de bate-papo para as várias partes interessadas e grupos que se comunicam sobre atividades e rastrear conversas de bate-papo para resolver o Incidente grave de segurança. A configuração das APIs Slack e Slack inclui:

- Introdução à configuração do conector de bate-papo do Slack
- Ativar o Slack como um provedor de canal
- Criar um modelo de canal de bate-papo para Slack
- Exibir atividades de mensagem de bate-papo no Slack

Introdução à configuração do conector de bate-papo do Slack

Revise as informações a seguir antes de começar a trabalhar com Slack como uma aplicação conectora.

Certifique-se de que os plug-ins a seguir estejam instalados antes de começar a estabelecer, ativar e validar Slack configurar conexões.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-ins necessários

Nome	Descrição
Slack Conector de bate-papo para Gestão de incidentes de segurança	Use o ID do plug-in **sn_slack_connector** para pesquisar e instalar o Slack Conector para Gestão de incidentes de segurança graves. A instalação deste plug-in permite rastrear as atividades de bate-papo usando o componente de colaboração específico para Slack.
Slack spoke	A instalação deste plug-in estabelece uma conexão de spoke com Slack. Para obter mais informações, consulte Slack Spoke .

Criar um modelo de canal de bate-papo para Slack

Configure equipes de bate-papo e modelos de canal para criar equipes de bate-papo e canais para colaborar, rastrear conversas de bate-papo e adicionar usuários e grupos de usuários a esses canais de bate-papo. Esses modelos de canal são criados em Slack quando um incidente de segurança grave é promovido.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa
O novo canal que você criar será o nome do seu canal em Slack. Você pode pesquisar o mesmo canal e adicionar suas conversas.

Procedimento
1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Modelos de canal**.
2. Selecione **Configuração do canal do Slack** para exibir os detalhes de configuração do Slack.
3. Marque a caixa de seleção **Ativo** para ativar a configuração do canal de bate-papo do Slack.
4. No campo Nome da equipe, forneça o número do MSI e o nome do código.

   Por padrão, todos os canais do Slack serão prefixados com o número do incidente. Por exemplo, `MSI000000 - {nome do canal}`. Você pode alterar o prefixo para qualquer campo de sua escolha neste formato: `{field_name}`.

   Nota: O nome da equipe fornecido aqui será usado em todos os registros de incidentes de segurança graves. Para verificar se o Slack real é exibido na aplicação Slack e tem um valor de nome exclusivo para diferentes incidentes de segurança graves, é recomendável usar um valor de campo de incidente, que seja exclusivo, como `MSI000000 - {nome do canal}`.

5. Clique com o botão direito do mouse na configuração e selecione **Salvar**.
6. Navegue até a seção Configuração do canal de bate-papo.
7. Selecionar **Novo** para criar uma nova configuração de canal de bate-papo.
8. No formulário, preencha os campos.

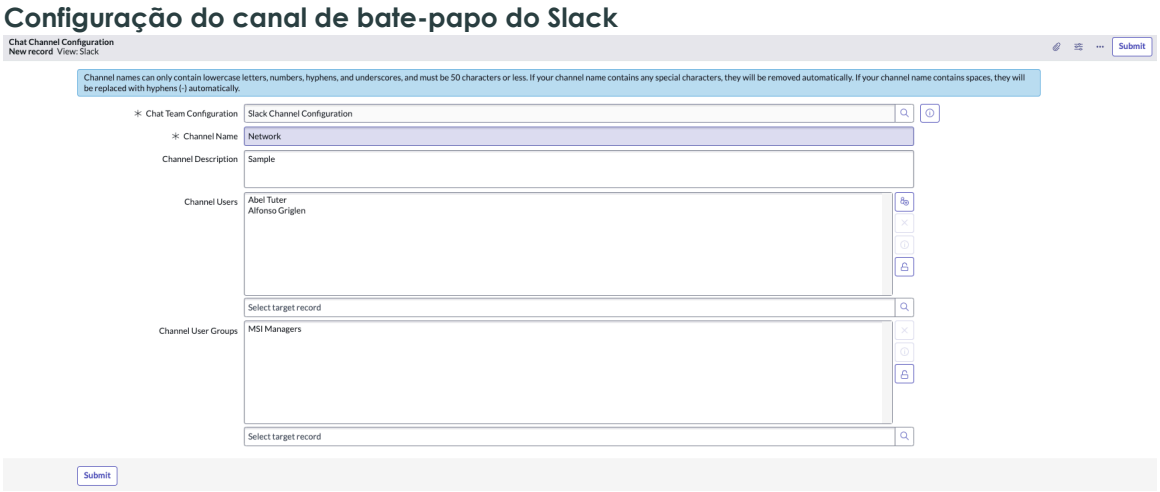
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Configuração da equipe de bate-papo	Nome da configuração da equipe de bate-papo. Por exemplo, configuração de canal do Slack.
Nome do Canal	Nome do canal. Por exemplo, jurídico. **Nota:** ◦ Os nomes de canal podem conter apenas letras minúsculas, números, hifens e sublinhados e devem ter 50 caracteres ou menos. Se o nome do canal contiver caracteres especiais, eles serão removidos automaticamente. Se o nome do canal contiver espaços, eles serão substituídos automaticamente por hifens (-). ◦ O novo canal criado aqui também será o nome do canal em Slack. Você pode pesquisar o mesmo canal e adicionar suas conversas.
Descrição do Canal	Descrição exclusiva do canal.
Usuários do canal	Selecione o ícone **Desbloquear usuários do canal** e adicione os usuários que podem acessar este canal na lista de pesquisa. Selecione o ícone **Bloquear usuários do canal** para bloquear a lista selecionada de usuários do canal.
Grupos de usuários do canal	Selecione o ícone **Desbloquear grupos de usuários do canal** e adicione os grupos de usuários que podem acessar este canal na lista de pesquisa. Você também pode usar o ícone **Adicionar-me** para adicionar a si mesmo. Selecione o ícone Bloquear **grupos de usuários do canal** para bloquear a lista selecionada de grupos de usuários do canal.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Selecione **Enviar**.

Resultados

O canal de bate-papo agora foi criado e os usuários estão atribuídos a esses grupos de canais de bate-papo. Você pode exibir as atividades de bate-papo de colaboração em Slack e no fluxo de atividades de Colaboração do Espaço do MSIM com a estrutura de hierarquia do canal de bate-papo organizado conforme definido na configuração do provedor do Canal de bate-papo.

Ativar o Slack como um provedor de canal

Ative Slack validando a conexão Slack.

Antes de Iniciar

Função necessária:

- sn_msi.workspace_admin — Gravação
- sn_msi.chat_collab_provider — Leitura

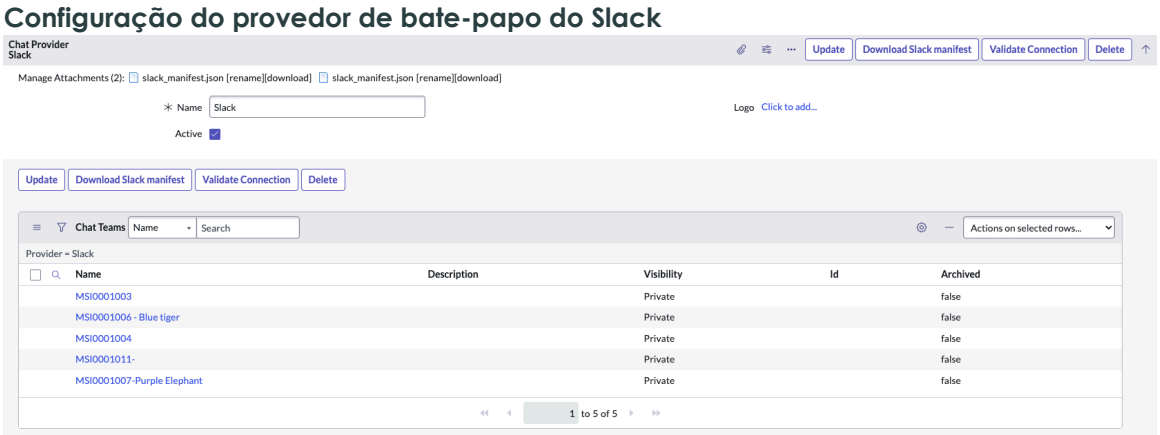
Depois que a conexão é ativada e validada, uma mensagem informativa é exibida informando que a conexão do provedor foi validada com sucesso. Você pode modificar a configuração do canal adicionando e removendo usuários e, possivelmente, adicionando mais canais ou renomeando os canais existentes.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Configuração do provedor de bate-papo**.
2. Selecione **Slack** para abrir a configuração do provedor de bate-papo do Slack.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Selecione **Baixar manifesto do Slack** para baixar o arquivo `slack_manifest.json`.
   O arquivo `slack_manifest.json` contém a configuração completa para a configuração do Slack e permite que você configure o Slack automaticamente. Você precisa carregar este arquivo JSON na configuração do Slack.
4. Abra o arquivo `slack_manifest.json` e execute as seguintes etapas:

   a. Acesse a URL `api.slack.com/apps` no navegador da Web.

   b. Selecione a ação **Criar novo app**.

   c. No pop-up Criar um app, escolha a opção **De manifesto de um app**.

   d. No pop-up Escolha um espaço para desenvolver seu app, escolha um espaço na lista e selecione **Avançar**.
   Por exemplo, MSIM Slack Workspace.

   e. No pop-up Inserir manifesto do app abaixo, selecione a guia **JSON** e copie e cole o código do arquivo `slack_manifest.json`.

   f. Selecione **Avançar**.

   g. No pop-up Revisar resumo e criar seu app, selecione **Criar**.
   Agora, seu app foi criado.

   h. Na página Informações básicas, selecione **Instalar no espaço**.
   O bot de integração do Slack solicita sua permissão para acessar o espaço do Slack do MSIM.

   i. Selecionar **Permitir**.

   j. Na seção Credenciais da aplicação, preencha os detalhes navegando de volta para a instância da ServiceNow.

   k. Selecionar **Todos** > **Configurações do Slack**.
   Você precisa da função sn_msi.workspace_admin para esta ação.

   l. Selecione uma propriedade de **Segredo de assinatura**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

m. Copie o segredo da assinatura e cole-o na seção Credenciais do app do Slack.

n. Na instância da ServiceNow, navegue até **Todos** > **Flow Designer**.

o. Navegar até **Conexões** > **Slack** > **Exibir detalhes** > **Configurar**.

p. No formulário, preencha os campos.

Campo	Descrição
Nome da conexão	Nome desta conexão. Por exemplo, Slack.
URL de Conexão	URL desta conexão. Por exemplo, https://slack.com
Nome da Credencial	Nome das credenciais. Por exemplo, Credenciais do Slack.
Nome do OAuth	Nome do OAuth. Por exemplo, OAuth do Slack.
ID do cliente OAuth	O ID de cliente que foi gerado para a conta que você criou no Slack.
Segredo do cliente OAuth	O segredo do cliente da conta que você criou no Slack.
URL de redirecionamento do OAuth	Nome da instância de redirecionamento do OAuth. Por exemplo, msimslack.service-now.com/oauth_redirect.do

q. Selecione **Configurar e obter token do OAuth**.
O bot de integração do Slack solicita sua permissão para acessar o espaço do Slack do MSIM.

r. Selecionar **Permitir**.
O token de acesso OAuth está disponível e expirará em<YYYY-MM-DD><HH:MM:SS> .

5. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Configuração do provedor de bate-papo**.
6. Marque a caixa de seleção **Ativo** para ativar o registro do provedor de bate-papo.
7. Selecione **Validar conexão** para testar a conexão.
Uma mensagem de confirmação exibe que a conexão do provedor foi validada com sucesso.
8. Clique com o botão direito do mouse no registro e selecione **Salvar**.
Depois disso, a conexão entre o Slack e a instância Now Platform é estabelecida com sucesso.
9. Navegar até **api.slack.com/apps** > **Recursos** > **OAuth e permissões**.

a. Verifique se todos os escopos estão corretos.

b. Navegar até **Recursos** > **Assinaturas de evento**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. No campo URL da solicitação, selecione **Repetir**.
Você pode ver uma mensagem verificada.

d. Selecione **Salvar**.

Exibir atividades de mensagem de bate-papo no Slack

A atividade de mensagem de bate-papo é registrada e exibida na guia Colaboração do espaço de Gestão de incidentes de segurança graves.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa
A atividade de mensagem de bate-papo inclui todas as conversas de bate-papo ocorridas entre os participantes, diferentes grupos de usuários. Para obter mais informações, consulte Gerenciar comunicações de canais de bate-papo usando o Slack.

Administração do Gestão de incidentes graves de segurança

Planeje e configure a sua implementação do Gestão de incidentes graves de segurança.

Você pode configurar os seguintes aspectos da administração de Gestão de incidentes graves de segurança :

Habilitar proposta, promoção e vinculação de incidentes de segurança graves

Permita que os usuários decidam propor ou promover incidentes como incidentes de segurança graves. Rastreie facilmente todos os incidentes relacionados a um incidente de segurança grave, permitindo que os incidentes de segurança sejam vinculados ao incidente primário ou secundário.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento
1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Permita que os usuários proponham um incidente de segurança a um incidente de segurança grave marcando a caixa de seleção **Propor** incidente de segurança grave na seção Ações do espaço SIR/VR.
3. Permita que os usuários promovam um incidente de segurança a um incidente de segurança grave marcando a caixa de seleção **Promover a** incidente de segurança grave.
4. Habilite a vinculação de um incidente de segurança a um incidente de segurança grave para que eles possam ser rastreados juntos marcando a caixa de seleção **Vincular ao** incidente de segurança grave.
5. Selecione **Atualizar**.

Marcar incidentes de segurança como incidentes de segurança graves

Marque ou rotule os incidentes de segurança ou registros vulneráveis a um incidente de segurança grave quando o incidente for proposto ou promovido. Se um incidente de segurança for proposto, o registro do incidente será chamado de candidato a incidente de segurança grave. Quando uma segurança é promovida, o registro do incidente é referido como Incidente de segurança grave com o estado Aceito.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Habilite a caixa de seleção **Exibir rótulos** para rotular o candidato a incidente proposto como incidente de segurança grave selecionando o campo de pesquisa **Nome do rótulo - Propor como candidato** e selecione Candidato a incidente de segurança grave na seção **Rótulos do espaço SIR/VR**.
3. Habilite a caixa de seleção **Exibir rótulos** para rotular o candidato a incidente promovido como incidente de segurança grave selecionando o campo de pesquisa **Nome do rótulo - Promoção a** incidente de segurança grave e selecione Incidente de segurança grave na seção **Rótulos do espaço SIR/VR**.
4. Selecione **Atualizar**.

Configurar rótulos para incidentes de segurança graves

Configure rótulos na gestão de incidentes de segurança graves para criar rótulos personalizados e filtrar as atividades e tarefas de colaboração externas no fluxo de atividades. Os diferentes tipos de rótulos implementados são rótulos de estado e rótulos de linha do tempo.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Habilite a caixa de seleção **Exibir rótulos** para habilitar a rotulagem de diferentes estados de incidente, como Análise, Conter, Eliminar, Recuperar, Revisar, Evento da linha do tempo na seção **Rótulos do espaço do MSIM (Exibir em atividades e tarefas de colaboração)**.
3. Selecione **Atualizar**.

Configurar rótulos para incidentes de segurança graves

Configure diferentes tipos de rótulos para filtrar melhor e também indicar os estados do incidente. Os rótulos de incidentes de segurança graves fornecem a flexibilidade para rotular as atividades e tarefas de colaboração dos registros de incidentes.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Você pode marcar ou desmarcar os rótulos usando o ícone de rótulos que está disponível na seção Fluxo de atividades da seção Colaboração e organizador de tarefas do espaço do MSIM.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Rótulos do ISG**.
2. Clique em **Novo** para criar um novo rótulo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha o formulário com **Nome dorótulo e Cor do rótulo**.
4. Clique **em Criar rótulo**.
5. Como parte do sistema de base, a seguir estão os rótulos configurados para cada estado de incidente e você não pode modificar o nome ou a cor do rótulo:
   - Análise
   - Contém
   - Erradicar
   - Revisão
   - Recuperar
   - Evento da linha do tempo

Nota: Você pode modificar os rótulos personalizados e suas propriedades.

Configurar categorias de linha do tempo para incidentes de segurança graves

Configure e atribua categorias de Linha do tempo, como Ameaça, Resposta ou Personalizado, aos seus incidentes de segurança graves usando a seção Linha do tempo na guia Visão geral.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Categorias da linha do tempo**.
   As seguintes categorias de linha do tempo são fornecidas como parte do sistema de base:
   - **Personalizado**.
   - **Resposta**.
   - **Ameaça**.
2. Para modificar uma categoria de evento de linha do tempo existente, execute as seguintes etapas:
   a. Selecione uma categoria de evento de linha do tempo na lista.
   b. Você pode modificar o nome da categoria de evento da linha do tempo.
   c. Você pode modificar a Cor do evento e selecionar outra cor para a categoria de evento da Linha do tempo.
   d. Selecione **Atualizar**.
3. Para criar uma nova categoria de evento de linha do tempo, execute as seguintes etapas:
   a. Selecione **Novo**.
   b. No campo Nome, insira um nome para a categoria de evento da Linha do tempo.
   c. No campo Cor do evento, escolha uma cor para a categoria da linha do tempo do evento usando a lista suspensa.
   d. Selecione **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir preferências de notificação para MSIM

Automatize o processo de notificação por e-mail e notifique os usuários quando um incidente de segurança for proposto ou promovido a um candidato a incidente de segurança grave.

Função necessária: sn_msi.workspace_admin.

As notificações são acionadas somente quando um incidente de segurança é proposto e enviado a todos os usuários e grupos que estão configurados para a lista de notificações. Por padrão, a notificação por e-mail é recebida pelo usuário que propôs o incidente de segurança como um candidato a incidente de segurança grave.

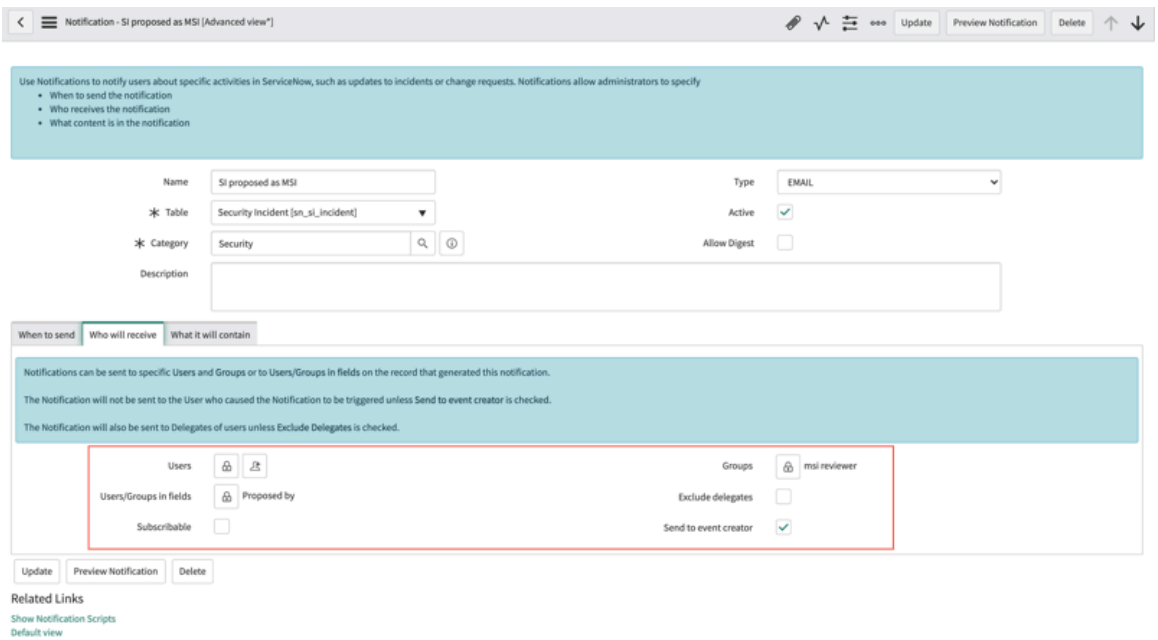
Notificação: incidente de segurança proposto (SI) como incidente de segurança grave (MSI)

Quem receberá:

- Por padrão, **Revisores do MSI** O nome do grupo foi criado e qualquer usuário adicionado a este grupo terá o privilégio de ser um **Gerente do MSIM** e os usuários desse grupo receberão os e-mails de notificação.
- Qualquer usuário específico adicionado ao **Usuários** A lista também receberá os e-mails de notificação.

O que ele conterá:

Se você quiser modificar o conteúdo do e-mail, como o corpo do e-mail, que inclui o HTML do Assunto ou da Mensagem, você deve ter o acesso à função de Administrador do Sistema ou atribuído como Administrador do Sistema e não um Administrador do MSI.



Notificação: incidente de segurança promovido (SI) como incidente de segurança grave (MSI)

Esta notificação é acionada quando um incidente de segurança é promovido e quando o Explorador de arquivos e a estrutura de base Microsoft Teams são criados. Por padrão, esta notificação é recebida pelo usuário que promoveu o incidente de segurança a um incidente de segurança grave.

Quem receberá

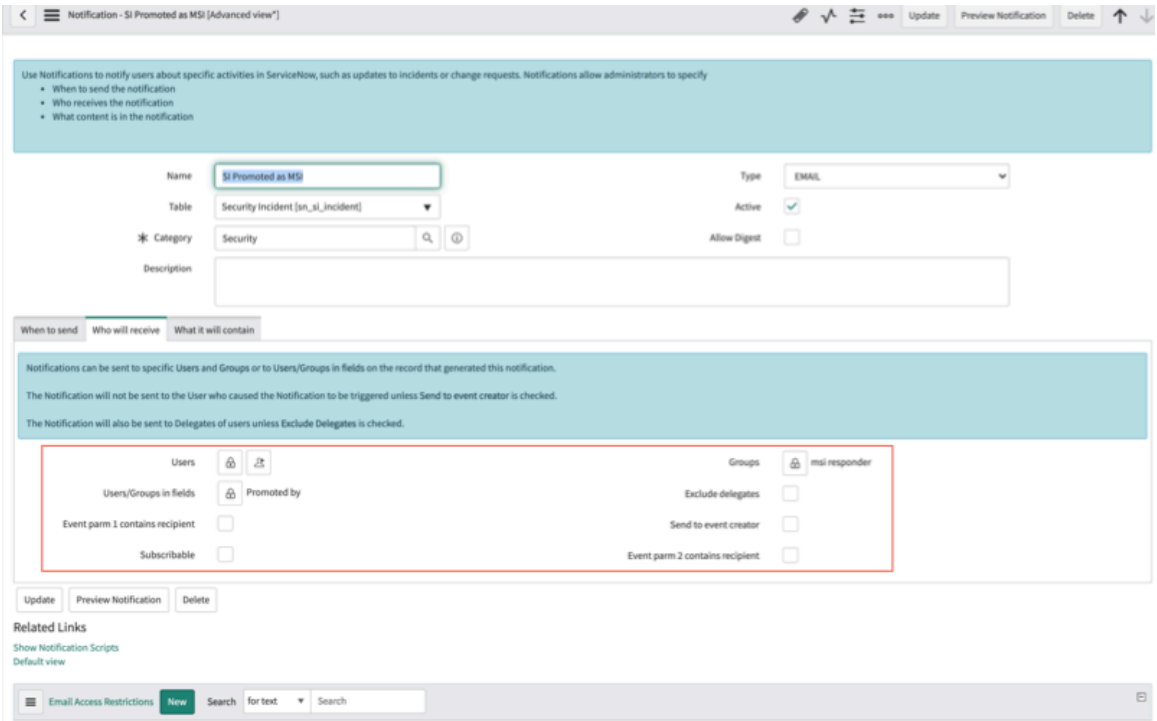
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Por padrão, um **Grupo** por nome **Respondente do MSI** foi criado e qualquer usuário adicionado a este grupo terá o privilégio de ter **Respondente do MSIM** A função e todos os usuários desse grupo receberão o e-mail de notificação.
- Qualquer usuário específico adicionado ao **Usuários** A lista também receberá os e-mails de notificação.

O que isso conterá

Se você quiser modificar o conteúdo do e-mail, como o corpo do e-mail, que inclui o HTML do Assunto ou da Mensagem, você deve ter o acesso à função de Administrador do Sistema ou atribuído como Administrador do Sistema e não um Administrador do MSI.



Configurar atividades de fechamento do ISG

Estabeleça ações que ocorrerão automaticamente quando um incidente de segurança grave for encerrado. Aumente a segurança arquivando e removendo automaticamente o acesso a pastas que contêm informações de resolução.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Arquivar comunicações de bate-papo relacionadas a resolver o incidente marcando a caixa de seleção **Arquivar canais de colaboração** na seção Ações de fechamento automatizadas.
3. Remova pastas que contêm material relacionado à resolução do incidente marcando a caixa de seleção **Remover pastas de colaboração**.
4. Selecione **Atualizar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de incidentes graves de segurança espaço

Gestão de incidentes graves de segurança fornece um espaço dedicado para gerenciar incidentes de segurança graves projetados especificamente para o gerente Incidente grave de segurança.

Colabore facilmente em atividades que ajudam a resolver incidentes de segurança graves compartilhando e exibindo arquivos e pastas, exibindo e atualizando tarefas de incidente e se comunicando com aqueles que trabalham no incidente por meio de canais de bate-papo dedicados.

A Gestão de incidentes de segurança graves (MSIM) fornece um mecanismo para rastrear e resolver incidentes de segurança graves. O MSIM funciona em conjunto com os recursos existentes do produto de resposta a incidentes e vulnerabilidades de segurança e melhora o processo de correção de incidentes de segurança graves com os seguintes recursos:

- Espaço dedicado para gerenciar incidentes de segurança graves projetados especificamente para a função de usuário de gerente de incidentes de segurança graves.
- Organize tarefas de resposta a incidentes de segurança graves, incluindo tarefas rastreadas em incidentes de segurança vinculados e grupos de vulnerabilidades.
- Automatize a criação de pastas de colaboração e canais de comunicação de bate-papo quando um incidente de segurança grave for criado, bem como o arquivamento como parte do fechamento do incidente.
- Componente do explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de uma integração Microsoft SharePoint.
- Gerenciador de canal de bate-papo e componentes de fluxo de atividades para gerenciar comunicações em vários grupos funcionais, de segurança e de TI por meio de uma integração Microsoft Teams.
- Relatórios resumidos de métricas de progresso e impacto de incidentes de segurança graves, incluindo acúmulo de ativos afetados, usuários, locais e recursos de equipe, bem como a linha do tempo de marcos de incidentes significativos.

Use o Espaço do MSIM para rastrear e resolver incidentes de segurança graves:

1. Exiba os gráficos de tendências e o andamento do incidente de segurança grave.
2. Rastreie e organize a atividade de arquivos do Microsoft SharePoint por meio do Espaço do MSIM.
3. Rastreie e organize a atividade de bate-papo do Microsoft Teams por meio do Espaço do MSIM.
4. Exiba e atualize os detalhes do incidente por meio do Espaço do MSIM.
5. Filtrar atividades de colaboração no fluxo de atividades do Espaço do MSIM.

Como usar o Gestão de incidentes graves de segurança

Os gerentes podem usar o espaço Gestão de incidentes graves de segurança para exibir os registros de incidentes propostos, promovidos, vinculados e rejeitados e rastrear suas atividades relacionadas.

Propor, promover e vincular registros de incidentes

Proponha ou promova incidentes de segurança como incidentes de segurança graves quando os incidentes forem identificados como ameaças críticas à organização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que a Gestão de incidentes de segurança graves estiver instalada na instância ServiceNow, você poderá lidar com a transição de incidentes de segurança para incidentes graves da seguinte forma:

- Proponha um incidente de segurança ao candidato a incidente de segurança grave para iniciar um processo de revisão.
- Promova diretamente um incidente de segurança a um incidente de segurança grave sem um processo de revisão.
- Rejeitar um incidente de segurança proposto como um incidente de segurança grave.

Você também pode vincular um incidente de segurança como um incidente secundário ao incidente de segurança grave para que todos os incidentes de segurança relacionados possam ser rastreados juntos.

Propor como um Incidente grave de segurança

Proponha um incidente de segurança a um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Listas**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja propor como um incidente de segurança grave.
3. Selecione o ícone **Mais ações** e selecione **Propor como incidente de segurança grave**.
4. Na caixa de diálogo Propor como incidente de segurança grave, preencha os campos.
   a. **Data de detecção**: data em que o incidente de segurança grave foi criado ou proposto pela primeira vez.
   b. **Justificativa**: forneça a justificativa para propor o incidente.
   c. **Impacto potencial**: indique o impacto do incidente.
5. Selecione **Propor**.

Resultados

O incidente é proposto e ocorrem as seguintes ações:

- No registro de incidente de segurança, uma mensagem de faixa de verificação é exibida e o marcador de Incidente de segurança grave definido é exibido.
- O registro aparece na lista relacionada Incidente de segurança grave no registro de incidente, com o estado listado como Proposto e na lista Candidatos ao espaço do MSIM.
- A seção Atividade no Espaço do MSIM mostra que o incidente de segurança foi proposto para ser promovido como um incidente de segurança grave.
- Uma mensagem é enviada para aqueles na lista de notificação definida que contém um link para o registro do incidente e a guia Detalhes do incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Promover para um Incidente grave de segurança

Promova um incidente de segurança a um incidente de segurança grave ou rejeite propostas promovidas por meio do espaço Gestão de incidentes graves de segurança (MSIM).

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Incidentes de segurança** > **Listas**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja promover como incidente de segurança grave.
   Revise os detalhes do incidente de segurança na seção Detalhes ou exiba detalhes estendidos no registro do incidente em uma guia separada clicando em **Exibir mais detalhes**.
3. Selecione o ícone **Mais ações** e selecione **Promover a incidente de segurança grave**.
4. Na caixa de diálogo Promover incidente de segurança grave, preencha os campos.

   a. **Data de detecção**: data em que o incidente de segurança grave foi criado ou proposto pela primeira vez.

   b. Data de**resolução estimada : a data**de resolução estimada até quando o incidente de segurança grave deve ser resolvido.

   c. **Nome**do código : selecione o nome do código para o incidente de segurança grave. Por exemplo, Tigre azul.

   d. **Categoria**: selecione a categoria do incidente de segurança grave. Por exemplo, configuração incorreta.

   e. **Justificativa**: forneça a justificativa para propor o incidente.

   f. **Impacto potencial**: indique o impacto do incidente.

5. Selecione **Propor**.
6. Promova o incidente de segurança ou rejeite a proposta de promoção.
   - Para promover o incidente, clique em **Promover a incidente de segurança grave**.
   - Para rejeitar a proposta de promoção, clique em **Rejeitar como incidente de segurança grave**.
7. Selecione **Salvar**.

Resultados

- Se você rejeitou a proposta de promoção, o incidente não será promovido e a entrada do incidente será movida para a guia Rejeitado.
- Se você promoveu o incidente, a entrada do incidente será movida para a guia Abrir e o registro de segurança exibirá um marcador indicando que se trata de um incidente de segurança grave.
- A decisão é listada na seção Atividade do Espaço do MSIM.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que um incidente é promovido, a configuração padrão é aplicada.

- Uma estrutura de pastas é criada com base na configuração do modelo de pasta.
- Os canais de bate-papo são criados com base na configuração de canais.
- Uma mensagem de e-mail é enviada aos usuários designados. A notificação padrão contém um link para o incidente de segurança grave e os detalhes do incidente. Os usuários designados agora também têm acesso aos recursos de colaboração, portanto, a notificação também inclui o nome do Microsoft Team e um link para pastas do Microsoft SharePoint relacionadas ao incidente.

Vincular a Incidente grave de segurança

Vincule incidentes de segurança a um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja vincular ao incidente de segurança grave.
3. Selecione o ícone **Ações adicionais** e escolha **Vincular ao incidente de segurança grave**.
4. Selecione o incidente de segurança grave ao qual você deseja vincular.
   a. Na caixa de diálogo, selecione o ícone Pesquisar usando lista.
   b. Selecione o incidente de segurança grave ao qual você deseja vincular.
   c. Selecione **OK**.
5. Selecione **Propor**.

Resultados

A proposta é enviada e ocorrem as seguintes ações:

- No registro de incidente de segurança, uma mensagem de faixa de verificação é exibida e o marcador de Incidente de segurança grave definido aparece ao lado do campo **Selecionar marcador de segurança**.
- Na guia **Detalhes** do incidente de segurança grave em Gestão de incidentes graves de segurança, a lista suspensa do número de registro inclui ambos os incidentes.
- O registro aparece na lista relacionada de Incidente de segurança grave do registro de incidente, com o estado listado como Proposto.
- Uma mensagem é enviada para aqueles na lista de notificação definida que contém um link para o registro do incidente e a guia Detalhes do incidente.
- A seção **Atividade** no Espaço do MSIM mostra que o incidente de segurança foi adicionado como um incidente de segurança secundário ao incidente de segurança grave com um link.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar a exibição de lista do MSI no espaço do MSIM

Com a exibição de lista no espaço do MSIM, você pode exibir incidentes de segurança graves propostos, promovidos e rejeitados.

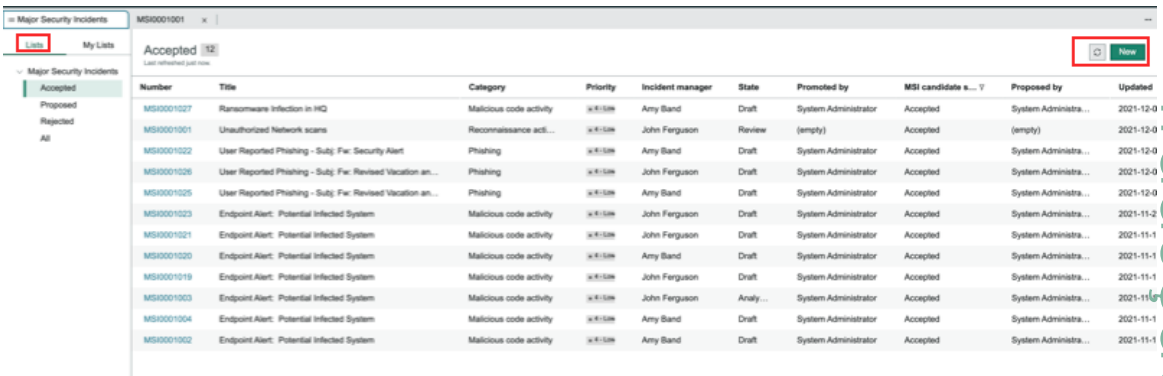
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Você também pode criar novos incidentes usando o botão **Novo** disponível no canto superior direito do espaço.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Espaço do MSIM**.
2. Selecione a guia Listas para exibir a exibição de Listas.



3. Selecione **Minhas listas** para criar sua própria lista de incidentes de segurança graves.
4. Consulte a tabela a seguir para saber o que você pode fazer na exibição de lista:

Tarefa	Descrição
Minhas listas	Crie novas listas de registros do MSI e exiba as listas que você criou.
Definir filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo uma: ◦ Mostrar correspondência — Exibe somente itens que correspondem ao item selecionado na coluna. ◦ Remover do filtro - Filtra os itens da coluna que correspondem ao item selecionado na respectiva coluna.
Atualizar lista	Atualize as listas e exiba as listas completas que foram atualizadas.
Novo	Crie um novo registro de MSI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir Incidente grave de segurança métricas de impacto

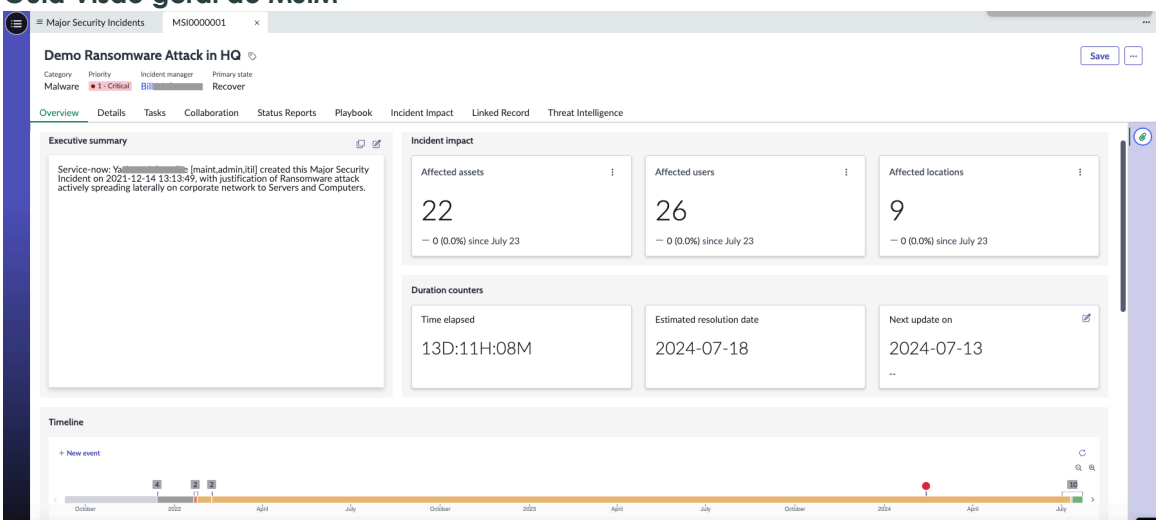
Fornece relatórios resumidos atualizados do impacto e do andamento de incidentes de segurança graves, que é um aspecto importante do gerenciamento de um incidente de segurança grave usando o novo espaço.

A guia **Visão geral** fornece as métricas relevantes para gerenciar o escopo e o andamento do incidente, incluindo um acúmulo de ativos afetados, usuários, locais e recursos da equipe, bem como a linha do tempo de marcos de incidentes significativos.

A linha do tempo fornece uma exibição horizontal dos principais eventos e marcos que ocorreram como parte da resolução específica do incidente de segurança grave. O componente da linha do tempo é exibido na parte superior de todas as guias do espaço de Gestão de incidentes graves de segurança com a capacidade de recolher e expandir para exibição conforme necessário. Os dados de eventos representados serão atualizados e atualizados sempre que eventos de marco designados ou marcos forem adicionados ou atualizados.

Cada evento ou marco é indicado com uma opção de tipo de evento de linha do tempo diferente para identificar o número e o tipo de eventos ou marcos. Por exemplo, atualizações de registro do NOW, atividades de colaboração. Além disso, o período de intervalo de tempo para os diferentes estados de incidente de segurança grave é rastreado automaticamente e exibido usando intervalos codificados por cores exibidos junto com a duração de cada estado de incidente.

Guia Visão geral do MSIM



Resumo executivo e impacto do incidente

Tarefa	Descrição
Resumo executivo	Um breve resumo do incidente de segurança grave junto com o nome de usuário, a função do usuário e os detalhes do carimbo de data/hora. • Você pode modificar o Resumo executivo selecionando o ícone **Editar**. Depois de fazer as mudanças necessárias, selecione a opção **Atualizar**. • Para copiar o Resumo executivo e colá-lo em um incidente de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo executivo e impacto do incidente

Tarefa	Descrição
	grave, selecione o ícone **Copiar** e cole o resumo no incidente de segurança grave necessário.
Impacto do incidente	Esses componentes exibem os recursos afetados com base em um acúmulo de todas as tarefas ativas e incidentes vinculados a ativos, usuários, locais e membros da equipe atribuídos identificados. Os recursos afetados são: • **Ativos afetados** • **Usuários afetados** • **Locais afetados** A seleção dos valores numéricos permite que você faça uma busca detalhada e navegue até os ativos afetados, usuários e detalhes do local e exibe as tarefas relacionadas na guia **Impacto do incidente** do espaço. Com base no link do tipo de impacto do incidente selecionado, os detalhes do incidente relacionado, como tipo de tarefa e sua descrição, grupo de atribuição e estado do incidente, são exibidos no **Impacto do incidente** guia do espaço do MSIM.
Contadores de duração	Esses componentes exibem a duração do incidente de segurança grave. Os recursos afetados são: • **Tempo decorrido**: exibe o tempo decorrido a partir do momento em que o incidente de segurança grave é detectado. • Data de**resolução estimada**: exibe a data de resolução estimada até quando o incidente de segurança grave deve ser resolvido. • **Próxima atualização em**: data e hora da próxima atualização para resolver o incidente de segurança grave. Por exemplo, 17h EST em 25 de março de 2024.

Tradução automática

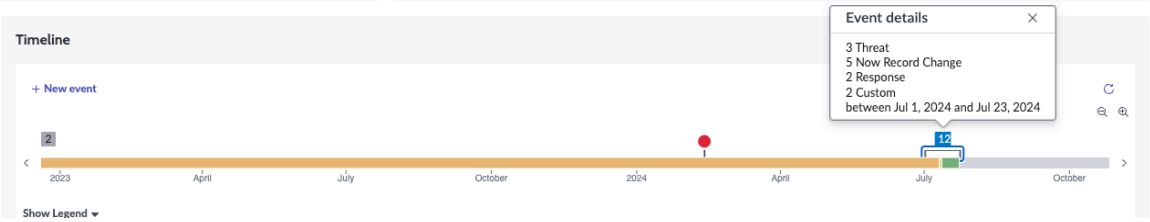
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo executivo e impacto do incidente

Tarefa	Descrição
	Você pode modificar a **Próxima atualização em** selecionando o ícone **Editar**. Selecione a nova data e hora e selecione **Atualizar**.

Você pode habilitar ou desabilitar a exibição de determinados tipos de evento para indicadores de linha do tempo e intervalos de linha do tempo usando os botões de alternância de filtro.

Linha do tempo



Consulte a tabela a seguir para obter recursos adicionais disponíveis com o componente da linha do tempo.

Capacidades adicionais do componente da linha do tempo

Tarefa	Descrição
Novo evento	Cria novos eventos personalizados e associa esses eventos ao registro do MSI. Isso ajuda a criar eventos para datas passadas e futuras que podem não ser capturados por meio de uma tarefa rotulada, mudança de estado de registro ou atividade de colaboração rotulada, que são exibidos por padrão na linha do tempo.
Atualização	Atualiza os eventos da linha do tempo para exibir as atualizações mais recentes.
Indicadores da linha do tempo	Lista os vários tipos de eventos, como mudanças de campo do Now Record, atividades de colaboração rotuladas e outros (personalizados), junto com os ícones e o número total de eventos que ocorreram em relação a cada indicador de tipo de evento. O indicador deslizante permite habilitar ou desabilitar todos os eventos para um tipo de evento específico.
Mostrar legenda	Selecione para exibir a legenda suspensa com diferentes tipos de indicadores de linha do tempo.
Barra de andamento da linha do tempo	Exibe o andamento geral do incidente por meio de eventos ou marcos de linha do tempo designados que ocorreram dentro dos diferentes intervalos de linha do tempo exibidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidades adicionais do componente da linha do tempo

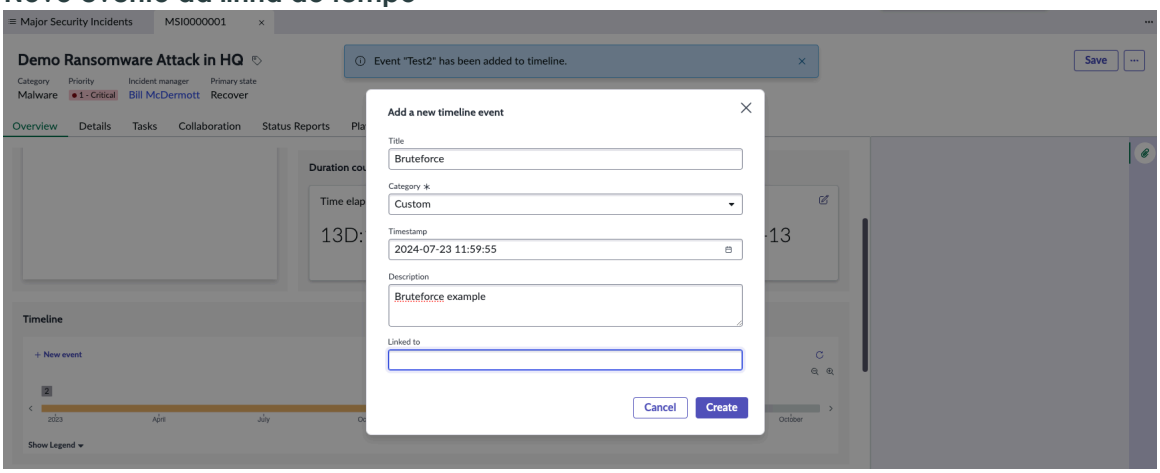
Tarefa	Descrição
	Você também pode vincular um tipo de evento a uma categoria de evento. Depois de vinculá-lo, os detalhes do evento são atualizados em ambos os locais da linha do tempo.
Intervalos de linha do tempo	Exibe vários tipos de estado de incidentes e duração conforme o incidente progride ao longo de todo o ciclo de vida do incidente de segurança grave. Habilite ou desabilite um evento específico com base no estado do incidente.

Criar um evento de linha do tempo

Para criar um novo evento de linha do tempo, execute as seguintes etapas:

1. Na guia Visão geral, navegue até a seção **Linha** do tempo.
2. Selecionar **+ Novo evento**.
3. No pop-up Adicionar um novo evento de linha do tempo, preencha os campos.

Novo evento da linha do tempo



Tarefa	Descrição
Título	Insira o título do evento da linha do tempo.
Categoria	Selecione uma categoria para o evento da linha do tempo. As categorias a seguir são fornecidas como parte do sistema de base e você pode escolher uma com base em seus requisitos. ◦ **Personalizado**. ◦ **Resposta**. ◦ **Ameaça**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Para adicionar ou configurar uma categoria de evento de linha do tempo, consulte Configurar categorias de linha do tempo para incidentes de segurança graves.
Carimbo de data/hora	Selecione a data e a hora do evento da linha do tempo usando o calendário de carimbo de data/hora. Você pode adicionar eventos à Linha do tempo antes e depois da data de início.
Descrição	Forneça uma breve descrição sobre o evento da linha do tempo.
Vinculados a	Opção para vincular o evento da linha do tempo a um registro de incidente de segurança grave.

4. Selecionar **Criar**.
5. Você pode usar os ícones **Ampliar** e **Reduzir** para ampliar ou reduzir a barra de andamento da linha do tempo, o que inclui a exibição de eventos individuais quando os números são exibidos para representar vários eventos próximos.

   Você também pode adicionar o nível de zoom padrão para mostrar todos os eventos.
6. Selecione o ícone **Atualizar** para exibir os eventos da linha do tempo mais recentes.

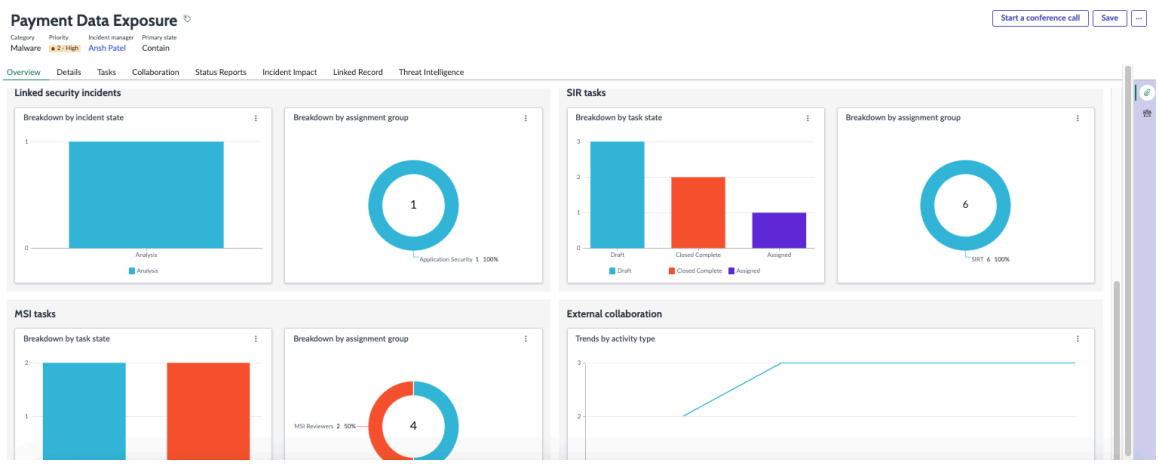
Exibir Incidente grave de segurança gráficos de tendências

Exiba as métricas de andamento do impacto do incidente de segurança grave visualizadas como gráficos de barras.

Além da linha do tempo do incidente e das visualizações do gráfico de tendências de andamento, o **Visão geral** A guia fornece métricas de impacto relevantes para gerenciar o escopo de mudança do incidente, incluindo o acúmulo de ativos afetados, usuários, locais e recursos da equipe.

As contagens exibidas nos componentes de visualização são baseadas em tarefas ativas em incidentes vinculados do Security Incident Response (SIR). Conforme as tarefas são abertas e fechadas, essas contagens mudam em termos da natureza e do volume da atividade restante planejada para o incidente de segurança grave para representar as tendências mostradas nos componentes de visualização do gráfico de tendências.

Métricas de impacto da guia Visão geral do MSIM



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte a tabela a seguir para ver as ações de IU que você pode executar a partir do **Visão geral** seção:

Seções de IU de visão geral

Título	Descrição
Hora	Exibe o período em número total de dias a partir do momento em que o incidente de segurança grave está ativo. O tempo é calculado com base em **Data de detecção** inserido no **Detalhes** guia do espaço. A data de detecção geralmente é capturada inicialmente quando o incidente de segurança grave foi criado ou proposto pela primeira vez. Sempre que esta data for modificada, a hora será calculada automaticamente, atualizada e exibida no formato dias: horas: minutos, por exemplo, 20D: 13H: 58M. **Data de resolução estimada**: a data em que a data de resolução do incidente está estimada para ser resolvida. Essa data geralmente é capturada inicialmente quando o incidente de segurança grave foi criado ou promovido pela primeira vez. A data é atualizada e atualizada com base na data estimada fornecida no **Detalhes** guia do espaço. Se a data estimada não for fornecida na seção Detalhes, esta seção exibirá "hífen" sem nenhum valor de data.
Equipe ativa	Exibe as diferentes equipes de resposta e membros de cada equipe que estão trabalhando ativamente no incidente de segurança grave e nas tarefas relacionadas. **Equipe ativa** tendência: exibe o gráfico de tendências de cada equipe e dos membros da equipe que estão trabalhando ativamente no incidente de segurança grave e nas tarefas relacionadas em intervalos regulares. **Nota:** Exiba os grupos ativos atribuídos no **Detalhes** guia do espaço.
Incidentes de SIR vinculados	**Por estado do incidente**: exibe a distribuição de incidentes de segurança vinculados com base em um estado de incidente,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de IU de visão geral

Título	Descrição
	como Análise, Conter, Eliminar, Recuperar ou Revisar. **Tendências por estado do incidente**: indica ainda a exibição de tendências de como o número de incidentes vinculados está progredindo com base no estado do incidente. A seleção de cada link de estado de incidente permite que você navegue e exiba os detalhes do incidente de segurança vinculado diretamente no **SI/VI vinculado** guia do espaço. Esta seção é atualizada e atualizada automaticamente sempre que ocorrem mudanças nos incidentes subjacentes.
Tarefas de SIR	Exibe os totais de tarefas ativas que estão vinculadas ao registro do MSI por meio de incidentes de SIR. • **Por estado da tarefa**: exibe as tarefas de resposta do incidente com base no estado do incidente, como Rascunho, Atribuído, Trabalho em andamento, Encerrado concluído. Este gráfico de distribuição permite um detalhamento de distribuição adicional por grupos de atribuição. Selecionar cada estado de tarefa permite que você exiba uma lista filtrada por estado de tarefa de incidente no **Tarefas** guia do espaço. A exibição filtrada permite exibir e atualizar detalhes de tarefas individuais. • **Tarefas em andamento por rótulo do estado do incidente**: exibe tarefas e grupos ativos com base no rótulo de estado do incidente que deve ser aplicado nos componentes do Organizador de tarefas. Esses rótulos padrão têm valores como Análise, Conter, Eliminar, Recuperar ou Revisar para indicar a natureza da tarefa envolvida. • **Atrasado**: exibe as tarefas de resposta a incidentes de segurança que estão ativas e ultrapassaram a data de vencimento. Você pode exibir os detalhes de todas as tarefas atrasadas selecionando a Contagem total de atrasos e fazendo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de IU de visão geral

Título	Descrição
	com que ela navegue automaticamente até a guia Tarefas. • **Tendências por estado da tarefa**: exibe a tendência de andamento do trabalho em andamento e das tarefas de resposta encerradas ao longo da duração do incidente. **Nota:** O gráfico do gráfico de tendências recupera os dados mais recentes com base no trabalho agendado. Você pode configurar ou modificar o intervalo de tempo de recuperação de dados conforme necessário.
Tarefas do MSI	Exibe as tarefas ativas no total, que foram criadas diretamente no registro do MSI (e não são tarefas de resposta vinculadas): **Por estado da tarefa:** Exiba as tarefas criadas por incidentes de segurança graves, as tarefas atribuídas e suas informações relacionadas. Selecionar cada estado de tarefa permite que você exiba uma lista filtrada por estado de tarefa de incidente no **Tarefas** guia do espaço. A exibição filtrada permitirá exibir e atualizar detalhes de tarefas individuais.
Colaboração externa	Exibe as atividades de colaboração no total para todas as atividades de colaboração rotuladas do fluxo de atividades de colaboração: • **Por rótulo de estado do incidente:**Exiba os dados de atividades de colaboração de incidentes que são coordenados com arquivos e pastas Microsoft Teams e Microsoft SharePoint e são rotulados usando rótulos de estado de incidente, como Análise, Conter, Eliminar ou Recuperar na guia **Colaboração** do espaço. • **Tendências por tipo de atividade**: exibe o gráfico de tendências para o número de Microsoft Teams e Microsoft SharePoint atividades de arquivos e pastas ao longo da duração do incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizar Incidente grave de segurança detalhes

Exiba e atualize detalhes específicos relacionados ao incidente de segurança grave, como Detalhes do registro do incidente, participantes ativos da equipe e o log de atividades correspondente.

Todos os detalhes relacionados ao incidente de segurança grave são exibidos com várias seções de formulário na guia **Detalhes** do espaço. Exibe os detalhes, como Detalhes do registro do incidente, Participantes ativos da equipe e o log de atividades correspondente. Você também pode exibir os incidentes de SIR vinculados, os detalhes do registro do grupo de vulnerabilidade e a capacidade de transmitir uma publicação de atividade para todos os registros de incidentes vinculados.

A guia Detalhes contém principalmente:

1. Campos de formulário de incidente de segurança grave e seções de IU relacionadas ao incidente.
2. Fluxo de atividades

A tabela a seguir fornece os detalhes dos campos do formulário de incidente de segurança grave:

Seções de formulário de incidente de segurança grave

Campo	Descrição
Incidente	
Número	Número do incidente de segurança grave.
Estado principal	O estado primário do incidente de segurança grave.
Data de detecção	A data em que o incidente de segurança grave foi criado ou proposto pela primeira vez. Sempre que você modifica a data de detecção na guia Detalhes, a data e a hora do MSI são calculadas, atualizadas e exibidas automaticamente na **Hora** > **Tempo desde o início do incidente** seção na seção **Visão geral** do espaço.
Título	Título do incidente de segurança grave.
Nome do código	Nome do código para o incidente de segurança grave. Por exemplo, Tigre azul.
Próxima atualização em	A data e a hora da próxima atualização para resolver o incidente de segurança grave. Por exemplo, 17h EST em 25 de março de 2024.
Categoria	Categoria do incidente de segurança grave.
Subcategoria	Tipo de subcategoria do incidente de segurança grave.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de formulário de incidente de segurança grave

Campo	Descrição
Data de resolução estimada	A data em que a data de resolução do incidente está estimada para ser resolvida. A data estimada é a data em que o incidente de segurança grave foi criado ou promovido pela primeira vez.
Prioridade	Prioridade do incidente de segurança grave.
Sensor de alerta	Sensor de alerta do incidente de segurança grave. Por exemplo, Phishing relatado pelo usuário.
Origem	Origem do incidente de segurança grave.
Equipe ativa	
Gestão de incidentes	Nome do gerente de incidentes.
Grupos de atribuição	Indica as diferentes equipes de resposta e membros da equipe de cada equipe que estão trabalhando ativamente no incidente de segurança grave.
Candidato	
Estado do candidato a ISG	Indica o estado do candidato a incidente de segurança grave, como proposto ou promovido. Se o incidente for promovido, o estado será exibido como Aceito.
Promovido por	Usuário que promoveu o incidente de segurança grave.
Promovido	Data em que o incidente de segurança grave foi promovido.
Justificativa	Justificativa do incidente de segurança grave. A justificativa deve incluir o número do MSI e o nome do código.
Impacto potencial	O possível impacto e a gravidade do incidente de segurança grave. O impacto potencial deve incluir o número do MSI e o nome do código.
Restrição	
Impor restrição	Selecione esta opção para impor restrições a determinados incidentes de segurança graves. Você pode impor restrições para limitar a exibição ou modificar o acesso somente a determinados usuários ou grupos. Para obter mais informações, consulte Restringir o acesso a determinados incidentes de segurança graves.
Membros permitidos	Lista de usuários que podem acessar o incidente de segurança grave.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de formulário de incidente de segurança grave

Campo	Descrição
Grupos permitidos	Lista de grupos que podem acessar o incidente de segurança grave.
Outras ações	
Anexo	Todos os anexos relacionados ao incidente de segurança grave. Selecione **Selecionar** opção para adicionar anexos ao incidente.
Chamada em conferência	Use chamadas em conferência com os provedores de serviço de terceiros como um canal de comunicação para se encontrar com as partes interessadas a fim de resolver os incidentes de segurança graves. Para obter mais informações, consulte Gestão de incidentes graves de segurança Integração de chamada em conferência.

Atividade:

Use a seção Atividade para adicionar anotações de trabalho e comentários e publicar sua atividade de forma privada e também adicionar comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade ou as anotações de trabalho adicionadas na seção Atividade.

Nota: Clique no link **Mostrar mais** detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

Você define suas preferências para exibir as atividades relacionadas, como:

1. **Filtros**: selecione o ícone **Conjuntos** de filtros para definir filtros.

   Defina filtros para exibir as conversas de atividade, como atividades adicionadas nas anotações de trabalho, e-mail, linha do tempo e quaisquer comentários adicionais.

2. **Sinalizado**: clique no ícone Sinalizado para **sinalizar** as atividades.

   Sinalize todas as conversas de atividade importantes para você revisitar rapidamente quando necessário.

Restringir o acesso a determinados incidentes de segurança graves

Gerencie quem pode exibir ou modificar incidentes de segurança graves que contêm informações confidenciais. Você pode impor restrições de incidentes de segurança graves para determinar quem tem acesso para exibir ou modificar determinados registros de incidentes de segurança graves e listas relacionadas e limitar o acesso de leitura ou gravação somente a determinados usuários ou grupos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

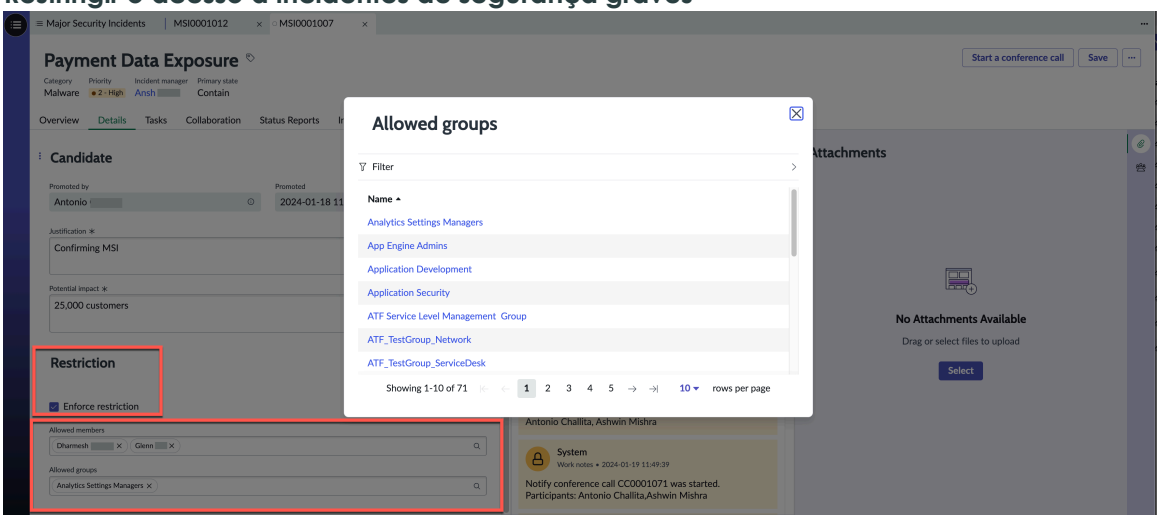
As restrições de incidentes de segurança graves permitem que você oculte incidentes de segurança graves críticos para que não sejam acessados ou modificados por todos os usuários ou grupos em uma organização específica. Essas restrições permitem que você forneça uma maneira mais granular de controlar os incidentes de segurança graves que um usuário ou grupo pode exibir ou modificar. Você pode impor uma restrição de incidente de segurança grave marcando a caixa de seleção **Impor restrição** e selecionando os usuários ou grupos com permissão para exibir ou modificar o incidente de segurança grave específico.

Depois de impor a restrição em incidentes de segurança graves ou listas relacionadas a determinados usuários ou grupos, todos os usuários ou grupos restantes em sua organização não poderão exibir ou modificar esses incidentes de segurança graves ou listas relacionadas.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Detalhes**.
5. Role para baixo e selecione a seção **Restrição**.
6. Marque a caixa de seleção **Impor restrição** para habilitar a restrição do incidente de segurança grave.

Restringir o acesso a incidentes de segurança graves



7. No campo Membros permitidos, selecione os usuários que podem exibir ou modificar o incidente de segurança grave usando a opção Pesquisar.
8. No campo Grupos permitidos, selecione os grupos que podem exibir ou modificar o incidente de segurança grave usando a opção Pesquisar.

> **Nota:** Depois que a caixa de seleção **Impor restrição** estiver habilitada para o incidente de segurança grave, somente sn_msi.workspace_manager e membros ou grupos permitidos terão acesso para exibir ou modificar o incidente de segurança grave.

9. Selecione **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vincular registros adicionais a Incidente grave de segurança

No espaço, use a funcionalidade de vinculação de registros para vincular todos os registros de incidentes de segurança relacionados e seus incidentes de segurança secundários, tarefas de correção da Resposta a vulnerabilidades e casos de segurança da inteligência contra ameaças a um registro Incidente grave de segurança (MSI).

Antes de Iniciar

Função necessária: sn_msi.workspace_manager e sn_msi.workspace_responder

Procedimento

1. Navegar até **Resposta a incidentes graves de segurança** > **Espaço do MSIM**.
2. Navegue até a exibição **Listas**, que é exibida no painel esquerdo do espaço.
3. Clique em **Aceito** para selecionar os registros de incidentes de segurança graves promovidos.
4. Selecione o registro de incidente que precisa ser vinculado e que não está no estado Fechado na lista de registros promovidos.
5. Clique na guia **Registros vinculados**.
   Uma lista suspensa é fornecida para selecionar outras tabelas de registros vinculados. A seção Registros vinculados exibe os registros vinculados e seus registros relacionados, que foram vinculados ao incidente de segurança grave.
6. Selecione a exibição de tabela desejada, como Incidentes de segurança, Tarefas de correção (itens vulneráveis) ou Caso de segurança na lista.
   Com base na exibição da tabela de registros do tipo de seleção, os registros vinculados aos registros de incidentes de segurança graves são exibidos.
7. Vincule um registro que não esteja vinculado a nenhum registro do MSI e esteja no estado **Aberto** selecionando o registro e clicando em **Vincular registro** no canto superior direito da página.

   Nota: Você não pode vincular um registro de incidente a um registro do MSI se ele estiver no estado **Fechado**.

8. Selecione o registro a ser vinculado e clique em **Vincular**.
   Uma mensagem de confirmação exibe que o registro foi vinculado com sucesso e que o acúmulo de registros relacionados será processado em segundo plano.

   Nota: Depois que um registro é vinculado, a exibição de lista é atualizada automaticamente e lista a lista atualizada de registros de incidentes.

Informações relacionadas

Desvincular registros de Incidente grave de segurança

Desvincular registros de Incidente grave de segurança

Usando o espaço de Gestão de incidentes de segurança graves, desvincule os registros de incidentes de segurança graves da seção Registros vinculados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager e sn_msi.workspace_responder

Nota: Você só pode desvincular um único registro de cada vez. Depois de desvincular um registro, as informações acumuladas relacionadas serão removidas das seções Impacto do incidente e Inteligência contra ameaças no espaço e a ação não poderá ser desfeita.

Tradução automática

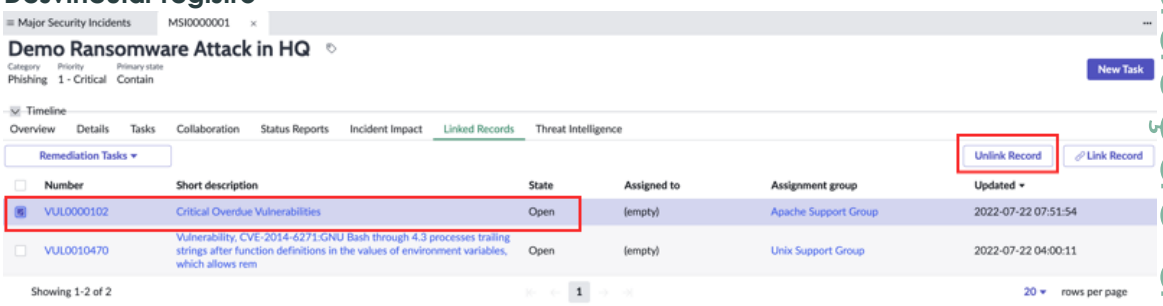
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre registros de acúmulo, consulte Estrutura de Rollup para MSIM.

Procedimento

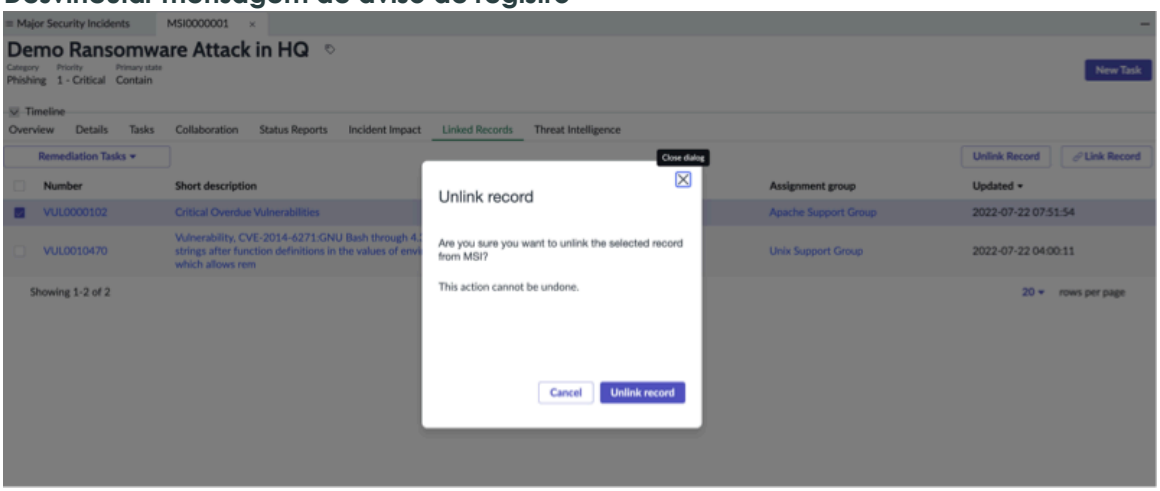
1. Navegar até **Resposta a incidentes graves de segurança** > **Espaço do MSIM**.
2. Navegue até Exibição de **listas**, que é exibida no painel esquerdo do espaço.
3. Clique em **Aceito** para selecionar os registros de incidentes de segurança graves promovidos.
4. Clique na guia **Registros vinculados**.
   Esta seção exibe os registros vinculados e os registros relacionados, que estão vinculados ao incidente de segurança grave.
5. Selecione a exibição de tabela desejada, como Incidentes de segurança, Tarefas de correção (itens vulneráveis) ou Caso de segurança.
6. Selecione o registro a ser desvinculado na exibição de lista de registros.
7. Clique **em Desvincular registro**.

Desvincular registro



8. Uma mensagem de aviso será exibida perguntando se você deseja desvincular o registro selecionado do MSI.

Desvincular mensagem de aviso de registro



9. Clique **em Desvincular registro**.
   O registro está desvinculado e, uma vez desvinculado, as mudanças não podem ser revertidas. A exibição de lista de registros vinculados será atualizada após a desvinculação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Configurar registros vinculados no Gestão de incidentes graves de segurança

Configurar registros de acúmulo no Gestão de incidentes graves de segurança

Gerenciar tarefas em um Incidente grave de segurança

A guia Tarefa permite rastrear e gerenciar todas as tarefas associadas a um incidente de segurança grave no espaço do MSIM. Você pode exibir as várias tarefas usando o Visual Task Board padrão (exibição Kanban) ou a exibição de lista.

O sn_msi.workspace_manager pode fazer o seguinte na guia Tarefas:

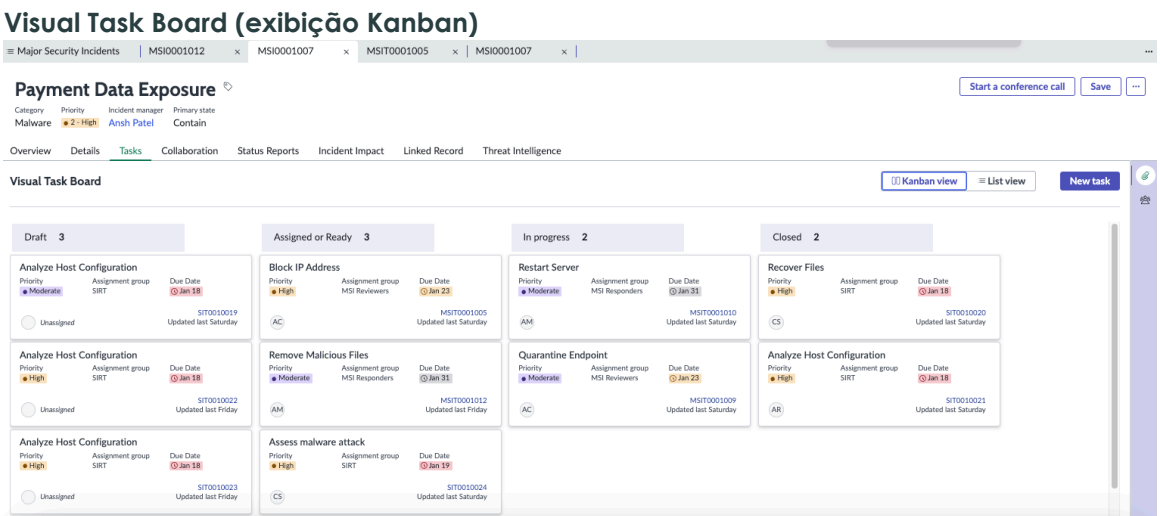
- Criar uma tarefa
- Modificar tarefas
- Exibir e atribuir tarefas a si mesmo ou a outras pessoas
- Excluir tarefas

Nota: Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente após instalar o aplicativo MSIM.

A guia Tarefas exibe os detalhes de todas as tarefas associadas a um incidente de segurança grave. A guia Tarefa oferece suporte a duas exibições:

- **Visual Task Board (exibição Kanban)**:

  Exiba e atualize vários registros de tarefa, que aparecem como cartões no Visual Task Board que podem ser movidos entre raias com base no status das tarefas no incidente de segurança grave.

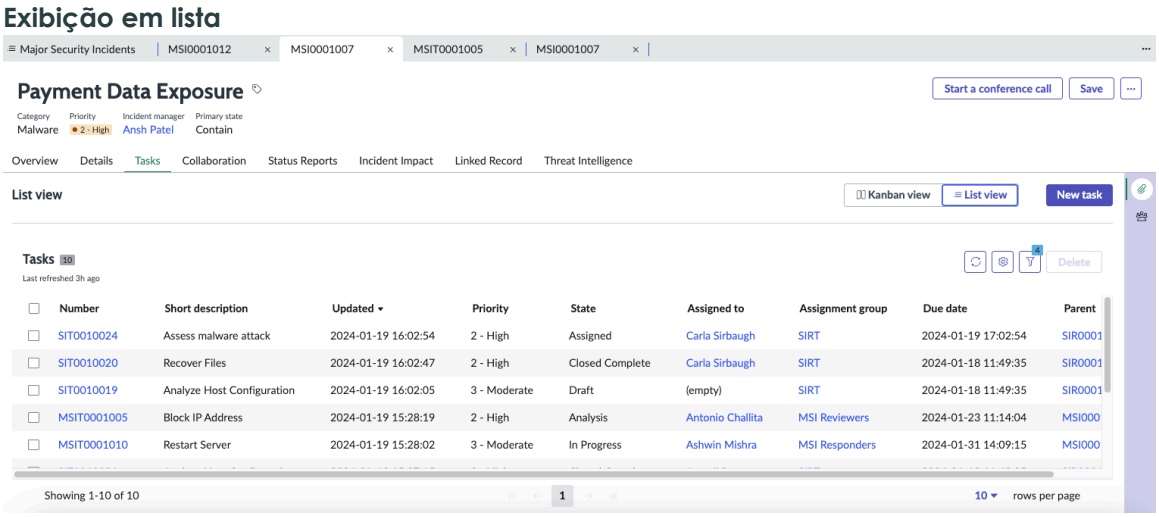


- **Exibição de lista**:

  Exiba e atualize vários registros de tarefa usando na forma de listas. Usando essas categorias de lista e filtros, você pode encontrar e rastrear rapidamente as tarefas nas quais precisa trabalhar em um incidente de segurança grave.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As atividades rotuladas são resumidas e exibidas na seção Visão geral do incidente de segurança grave. Um gráfico de tendências está disponível na seção Visão geral para exibir o estado das atividades da tarefa consolidada.

Gerenciar tarefas usando o Visual Task Board

Rastreie e gerencie todas as tarefas associadas a um incidente de segurança grave usando o Visual Task Board (exibição Kanban).

Você pode usar o Visual Task Board para mover os cartões passo a passo entre raias como Rascunho, Atribuído ou Pronto, Em andamento e Encerrado, dependendo do status das tarefas. Um fluxo de atividades no quadro exibe a atividade recente para rastrear facilmente as mudanças de tarefa. Você pode adicionar cartões de tarefa de qualquer tabela que estenda a tarefa para rastrear rapidamente atualizações e editar incidentes de segurança graves diretamente do quadro.

Criar uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota: Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente após instalar o aplicativo MSIM.

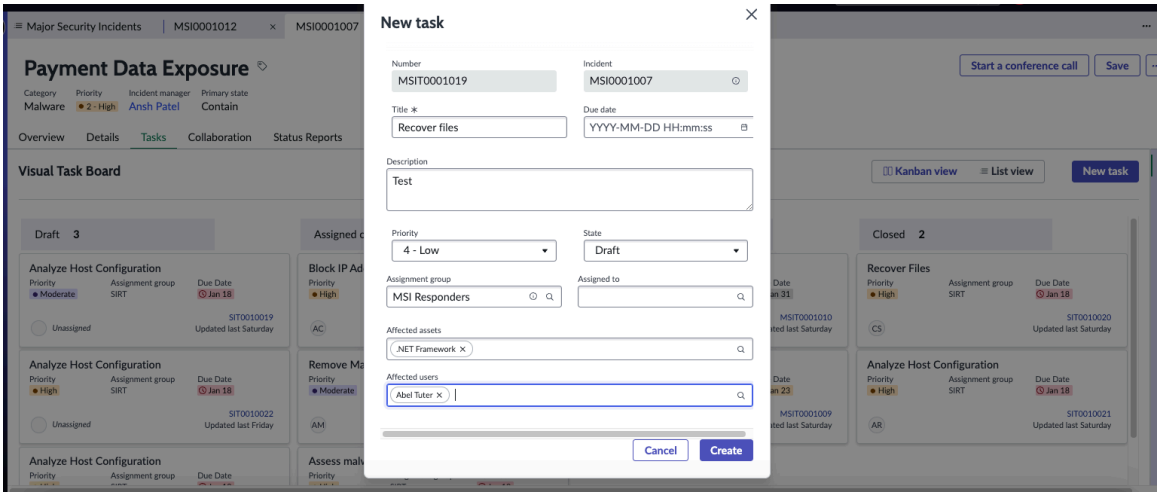
Os gerentes do MSI podem criar uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma tarefa usando o Visual Task Board



5. Selecione **Exibição Kanban**e escolha **Nova tarefa**.

6. No formulário, preencha os campos.

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a conclusão da tarefa. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa é executada. A prioridade pode ser um dos seguintes valores: ◦ **Nenhum(a)** ◦ **1-Crítico** ◦ **2 - Alta** ◦ **3 - Moderada** ◦ **4 - Baixo** ◦ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ◦ **Rascunho** ◦ **Análise**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Em andamento** ◦ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione **Criar** para criar a tarefa.

Exibir e modificar uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota: Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente após instalar o aplicativo MSIM.

Os gerentes do MSI podem exibir os detalhes de uma tarefa e as informações da atividade dos respondentes do MSI e modificar uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas** e escolha a **exibição Kanban**.
5. Escolha o cartão de tarefa desejado em uma das raias para exibir os detalhes da tarefa.

   O cartão de tarefa pode estar em uma das raias: Rascunho, Atribuído ou Pronto, Em andamento ou Encerrado.

6. Na seção Informações da tarefa, você pode modificar os seguintes detalhes:

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a conclusão da tarefa. Selecione uma data usando

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa é executada. A prioridade pode ser um dos seguintes valores: ◦ **Nenhum(a)** ◦ **1-Crítico** ◦ **2 - Alta** ◦ **3 - Moderada** ◦ **4 - Baixo** ◦ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ◦ **Rascunho** ◦ **Análise** ◦ **Em andamento** ◦ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

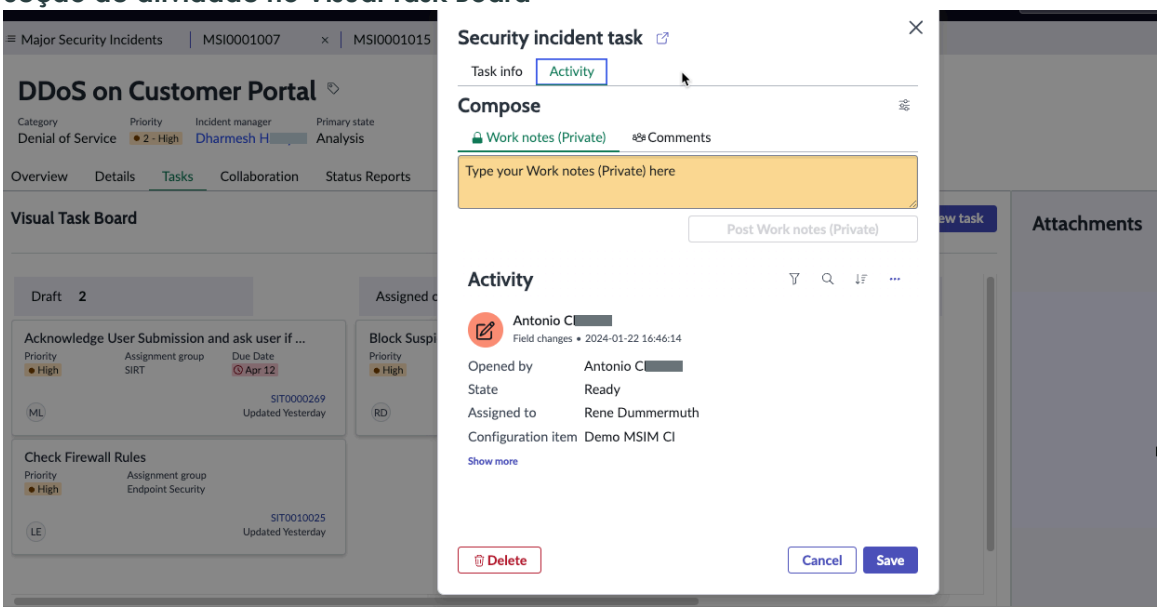
Tradução automática

7. Selecione a seção **Atividade** para exibir os detalhes da atividade dos respondentes do MSI.

   Use a seção Atividade para adicionar anotações de trabalho e comentários e publicar sua atividade de forma privada e também adicionar comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade ou as anotações de trabalho adicionadas na seção Atividade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção de atividade no Visual Task Board



Nota: Selecione o link **Mostrar mais** detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

8. Selecione **Salvar** para atualizar as informações da tarefa.

   As informações da tarefa são atualizadas instantaneamente.

Excluir uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota: Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente após instalar o aplicativo MSIM.

O Gerenciador do MSI pode excluir uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas** e escolha a **exibição Kanban**
5. Escolha o cartão de tarefa que você deseja excluir.
6. No pop-up Tarefa de incidente de segurança grave, selecione a opção **Excluir**.

   O pop-up Excluir tarefa aparece solicitando que você confirme a exclusão da tarefa.

7. Selecione **Excluir**.

Gerenciar tarefas usando a exibição de lista

Rastreie e gerencie todas as tarefas associadas a um incidente de segurança grave usando a exibição de lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A exibição de lista mostra os detalhes de todas as tarefas associadas ao incidente de segurança grave, como número da tarefa, prioridade, estado atual, atribuído a, grupo atribuído. Usando essas categorias de lista e filtros, você pode encontrar e rastrear rapidamente as tarefas necessárias nas quais precisa trabalhar em um incidente de segurança grave.

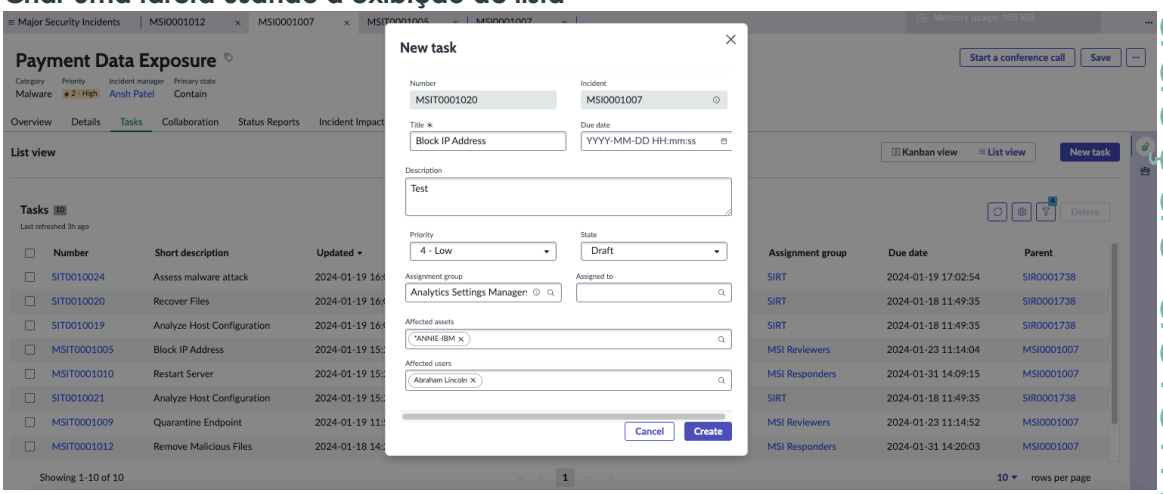
Criar uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Os gerentes do MSI podem criar uma tarefa na exibição de lista usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas**.

Criar uma tarefa usando a exibição de lista



5. Selecione **Exibição de lista**e escolha **Nova tarefa**.
6. No formulário, preencha os campos.

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a conclusão da tarefa. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa é executada. A prioridade pode ser um dos seguintes valores: ◦ **Nenhum(a)** ◦ **1-Crítico** ◦ **2 - Alta** ◦ **3 - Moderada** ◦ **4 - Baixo** ◦ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ◦ **Rascunho** ◦ **Análise** ◦ **Em andamento** ◦ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione **Criar** para criar a tarefa.

Exibir e modificar uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Os gerentes do MSI podem exibir os detalhes de uma tarefa e as informações de atividade dos respondentes do MSI e modificar uma tarefa na exibição de lista usando as etapas a seguir

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas** e escolha **Exibição de lista**.
5. Escolha a Tarefa desejada na exibição de lista para exibir os detalhes da tarefa.
6. Na seção Informações da tarefa, você pode modificar os seguintes detalhes:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a conclusão da tarefa. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa é executada. A prioridade pode ser um dos seguintes valores: ◦ **Nenhum(a)** ◦ **1-Crítico** ◦ **2 - Alta** ◦ **3 - Moderada** ◦ **4 - Baixo** ◦ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ◦ **Rascunho** ◦ **Análise** ◦ **Em andamento** ◦ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

Tradução automática

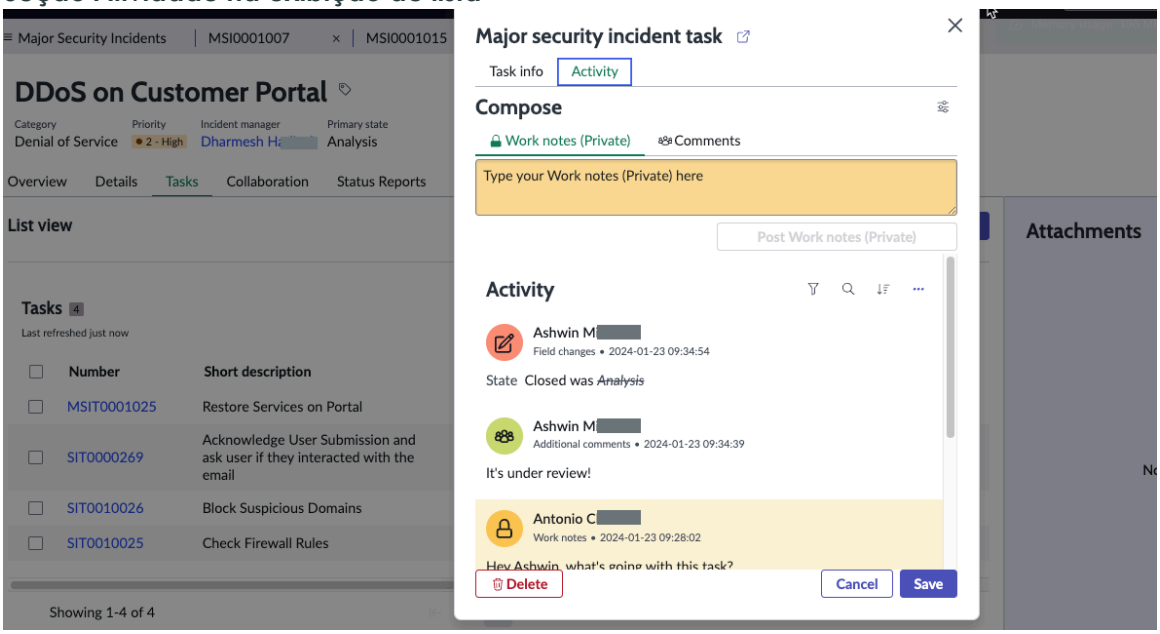
7. Selecione a seção **Atividade** para exibir os detalhes da atividade dos respondentes do MSI.

   Use a seção Atividade para adicionar anotações de trabalho e comentários e publicar sua atividade de forma privada e também adicionar comentários adicionais conforme

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade ou as anotações de trabalho adicionadas na seção Atividade.

Seção Atividade na exibição de lista



Nota: Selecione o link **Mostrar mais** detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

8. Selecione **Salvar** para atualizar as informações da tarefa.

   As informações da tarefa são atualizadas instantaneamente.

9. Você também pode executar as seguintes ações na exibição de lista:
   a. Selecione o ícone **Atualizar** para atualizar a lista de tarefas na exibição de lista.
   b. Selecione o ícone **Configurações** e use a opção **Editar colunas** para modificar a lista de colunas que aparecem na exibição de lista. Use a opção **Redefinir larguras** para redefinir as larguras das colunas.

Excluir uma tarefa usando a Exibição de lista

Função necessária: sn_msi.workspace_manager.

O Gerenciador do MSI pode excluir uma tarefa na exibição de lista usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas**.
5. Selecione **Exibição de lista**.
6. Escolha uma tarefa que você deseja excluir da lista.
7. No pop-up Tarefa de incidente de segurança grave, selecione a opção **Excluir**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O pop-up Excluir tarefa aparece solicitando que você confirme a exclusão da tarefa.

8. Selecione **Excluir**.

Rastreie a atividade de colaboração por meio do espaço MSIM

Rastreie atividades de bate-papo e arquivo relacionadas à resolução de incidentes de segurança graves por meio do Espaço do MSIM.

As atividades são coordenadas usando o bate-papo Microsoft SharePointMicrosoft Teams e arquivos e pastas [] e, em seguida, publicadas de volta no Incidente grave de segurança por meio de integrações.

Depois que o Microsoft Teams e o Microsoft SharePoint estiverem integrados ao Gestão de incidentes graves de segurança, você poderá usar o espaço MSIM para rastrear a colaboração entre usuários de resposta a incidentes e outros grupos que estão contribuindo para a resolução de um incidente de segurança grave. Todas as atualizações nas pastas e arquivos de colaboração em Microsoft SharePoint são sincronizadas com o MSIM Workspace File Explorer e também refletidas nos componentes do Fluxo de atividades.

Quando um incidente de segurança é promovido a incidente de segurança grave:

1. Uma estrutura de pastas será criada em Microsoft SharePoint com base na configuração do modelo de pasta. A mesma estrutura de pastas será refletida no componente File Explorer do espaço.
2. Uma equipe com vários canais é criada na aplicação Microsoft Teams, e o mesmo será refletido no componente de gestão de bate-papo do espaço.

Função necessária: sn_msi.workspace_manager.

Interagir com arquivos e pastas

O Explorador de arquivos exibe o sistema de arquivos para que você possa exibir e interagir com arquivos e pastas relacionados à resolução do incidente.

Exibe o arquivo e as pastas que são capturados no Microsoft SharePoint para um incidente de segurança específico. Essas pastas serão criadas automaticamente no Microsoft SharePoint para esse incidente de segurança grave. Você pode usar essas pastas criadas padrão para carregar arquivos de suporte, se necessário. Você pode renomear, mover ou excluir esses arquivos e pastas conforme necessário.

Além disso, sempre que você carregar um arquivo em qualquer uma das pastas, a atividade correspondente a essas pastas será automaticamente associada às pastas do Explorador de arquivos na guia Colaboração e a atividade será registrada e exibida na seção Atividade da Gestão de incidentes de segurança graves Espaço.

Nota: Na guia **Colaboração**, o registro de incidente é anexado ao arquivo primário no SharePoint com um número de incidente e categoria de incidente exclusivos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. **Exibição do repositório**: lista os arquivos e as pastas listados no Microsoft SharePoint para esse incidente de segurança específico. Para cada arquivo ou pasta, a exibição do repositório exibe o Nome, Modificado por, Última modificação e o Tamanho será exibido.

Exibição do repositório

Campo	Descrição
Abrir no SharePoint	Selecione esta opção disponível ao lado do seu incidente de segurança grave. Clique no link para selecionar e exibir a estrutura de pastas no Microsoft SharePoint.
Nova pasta	Selecione esta opção para criar uma nova pasta conforme necessário. Depois de criar uma nova pasta, a mesma pasta nova é criada e associada ao Microsoft SharePoint, por padrão.

2. **Recentes**: exibe todos os logs de atividades recentes. Esses logs incluem suas atividades do SharePoint e do Explorador de arquivos. As atividades recentes geralmente são seus arquivos de suporte, que incluem a pasta primária.

   A seguir está o procedimento para **localizar o arquivo de log:**

   a. Selecione o respectivo arquivo para exibir os detalhes.

   b. Clique **em Localizar arquivo**.

   Nota: A navegação e os detalhes do arquivo primário e das pastas primárias são exibidos na seção de exibição de lista **Recentes**. Você pode abrir o mesmo arquivo no seu SharePoint. Sempre que você carrega os arquivos de log relacionados ou quaisquer atividades, todos esses arquivos e atividades são exibidos no SharePoint e no Explorador de arquivos.

Gerenciar comunicações de canais de bate-papo usando o Microsoft Teams

O Gerenciador de canal de bate-papo exibe o Microsoft Teams com vários canais criados na aplicação Microsoft Teams com base em uma configuração de modelo.

Esses canais configurados são refletidos no componente de gestão de bate-papo junto com os usuários e grupos de usuários atribuídos a eles. O Gerenciador de canal de bate-papo permite que você execute o seguinte:

- **Gerenciar canais de bate-papo**
- **Renomear equipe**
- **Gerenciar membros da equipe**

A equipe e os canais são criados com base na configuração do canal de bate-papo no Microsoft Teams.

Gerenciar canais de bate-papo

O Gerenciador de canal de bate-papo permite criar, editar ou excluir canais de bate-papo. Para gerenciar um canal de bate-papo no Microsoft Teams, execute as seguintes etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecione a guia **Colaboração**.
2. Navegar até **Gerenciador de canal de bate-papo** > **Criar novo canal**.
3. Adicione um novo **Nome do canal**, **Descrição**e selecione os **Membros** do canal.
4. Selecione **Criar**.

> **Nota:** Um novo registro de canal é criado na seção Canais do Microsoft Teams da aplicação Microsoft Teams e o mesmo registro será refletido no MSIM.

5. Para editar um canal de bate-papo, selecione um canal de bate-papo na lista do gerenciador de canal de bate-papo.
6. Você pode modificar o Nome do canal, a lista de membros e a lista de membros do grupo com base em seus requisitos.
7. Selecione **Salvar**.
8. Para excluir um canal de bate-papo, selecione um canal de bate-papo na lista do gerenciador de canal de bate-papo.
9. Selecione **Excluir canal**.

Renomear equipe

Para renomear uma equipe no Microsoft Teams, execute as seguintes etapas:

1. Selecione a guia **Colaboração**.
2. Navegar até **Gerenciador de canal de bate-papo** > **Renomear equipe**.
3. No campo Nome da equipe, renomeie a equipe de acordo com seus requisitos.
4. Selecione **Salvar**.

> **Nota:** Renomear o nome da equipe também renomeará o nome da equipe no Microsoft Teams.

Gerenciar membros da equipe

O Gerenciador de canal de bate-papo permite adicionar ou remover membros da equipe no Microsoft Teams. Você também pode adicionar membros por meio de grupos. Para gerenciar membros da equipe no Microsoft Teams, execute as seguintes etapas:

1. Selecione a guia **Colaboração**.
2. Navegar até **Gerenciador de canal de bate-papo** > **Gerenciar membros da equipe**.
3. No campo Membros, adicione ou remova membros da equipe de acordo com seus requisitos.
4. No campo Adicionar membros por meio de grupos, selecione os grupos que você deseja adicionar ao Microsoft Teams.

> **Nota:** Se os membros do grupo já estiverem na equipe, esses membros não serão adicionados.

5. Selecione **Salvar**.

   O Gerenciador de canal de bate-papo exibe os detalhes do total de membros da equipe e o número de novos membros que serão adicionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciar comunicações de canais de bate-papo usando o Slack

O Gerenciador de canal de bate-papo exibe o Slack com vários canais criados na aplicação Slack com base em uma configuração de modelo.

Esses canais configurados são refletidos no componente de gestão de bate-papo junto com os usuários e grupos de usuários atribuídos a eles. O Gerenciador de canal de bate-papo permite que você **gerencie canais de bate**-papo. A equipe e os canais são criados com base na configuração do canal de bate-papo no Slack.

Gerenciar canais de bate-papo

O Gerenciador de canal de bate-papo permite criar, editar ou excluir canais de bate-papo no Slack. Para gerenciar um canal de bate-papo, execute as seguintes etapas:

1. Selecione a guia **Colaboração**.
2. Navegar até **Gerenciador de canal de bate-papo** > **Criar novo canal**.
3. Adicione um novo **Nome do canal**, **Descrição**e selecione os **Membros** do canal.
4. Selecione **Criar**.

   Nota: Um novo registro de canal é criado na seção Canais do Slack da aplicação Slack e o mesmo registro será refletido no MSIM.

5. Para editar um canal de bate-papo, selecione um canal de bate-papo na lista do gerenciador de canal de bate-papo.
6. Você pode modificar o Nome do canal, a lista de membros e a lista de membros do grupo com base em seus requisitos.
7. Selecione **Salvar**.
8. Para excluir um canal de bate-papo, selecione um canal de bate-papo na lista do gerenciador de canal de bate-papo.
9. Selecione **Excluir canal**.

Gerenciar conversas do fluxo de atividades

Exibe todas as atividades, logs e status que foram realizados em Microsoft SharePoint, explorador de arquivos e Microsoft Teams.

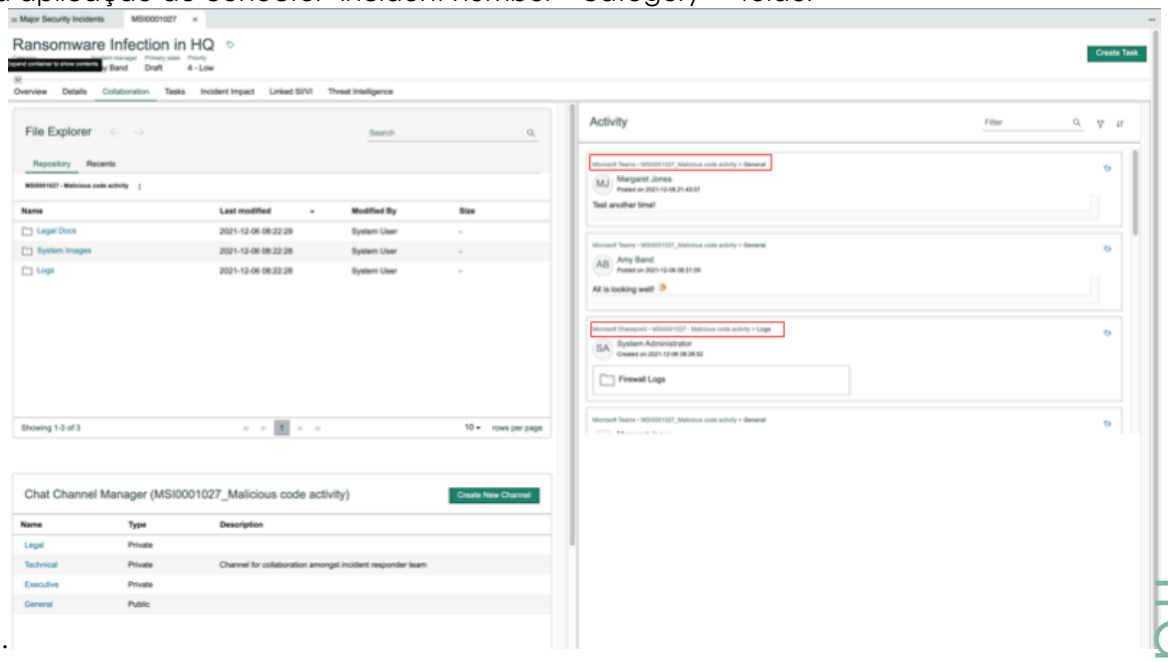
Se você quiser exibir qualquer atividade específica ou pesquisar os detalhes da atividade de colaboração que interagiram entre vários arquivos e pastas e também no Microsoft Teams, use a capacidade de filtro que é exibida no canto superior direito da seção Fluxo de atividades e localize o desejado detalhes da atividade.

Pastas e conversas de bate-papo compartilhadas com a Gestão de incidentes de segurança graves são refletidas como trilhas com a estrutura:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

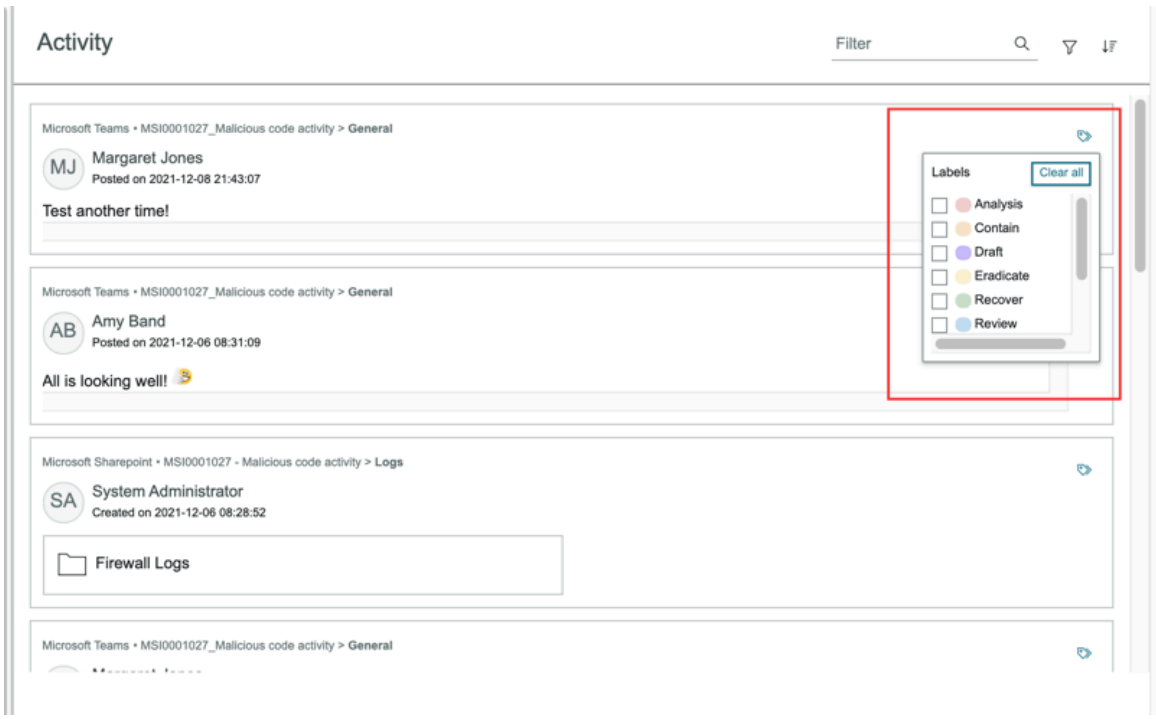
nome da aplicação do conector<incident number – category ><folder



name>).

Rotular as atividades:

1. Clique no ícone **Rótulo**.
2. Marque a caixa de seleção do respectivo rótulo de atividade de incidente, conforme mostrado na captura de tela abaixo.



3. As atividades rotuladas são codificadas por cores e representadas como gráfico de tendências de andamento na seção **Colaboração externa** do espaço.

Criar e distribuir MSIM relatórios de status

Como um gerente Incidente grave de segurança, você pode criar e distribuir os diferentes relatórios de status para diferentes partes interessadas em vários intervalos com base

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no modelo de relatório configurado ou em um relatório de status anterior ao longo da resolução do incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Você pode visualizar os elementos de dados do relatório de resumo configurados anteriormente, adicionar texto ou resumo adicional, remover componentes de relatório individuais conforme necessário e verificar a precisão e a integridade do relatório antes de distribuí-lo para diferentes partes interessadas.

Crie os relatórios de status selecionando o modelo de relatório desejado que foi configurado inicialmente na página Configuração de modelos de relatório do MSI.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Selecione o respectivo registro de MSI promovido.
4. Selecione a guia **Relatórios de status**.
   A guia Relatórios de status contém três tipos diferentes de subseções, como abaixo.

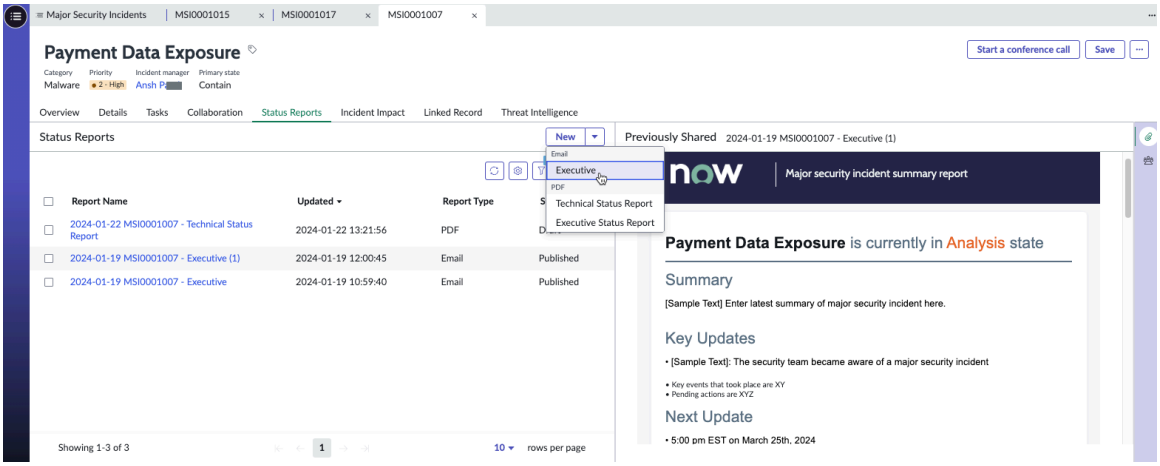
Campo	Descrição
Nome de relatório	Nome do modelo de relatório de status. **Nota:** A exibição Relatórios de status lista os modelos de relatório predefinidos existentes que estão disponíveis como parte do sistema de base para a persona em questão. Por exemplo, relatórios de status executivo por e-mail (compatível com dispositivos móveis), relatórios de status técnico e relatórios de status executivo como PDFs.
Atualizado em	A data em que o modelo de relatório foi atualizado pela última vez.
Tipo de relatório	Tipo de relatório de status. O relatório de status pode estar em um dos seguintes tipos: ◦ PDF ◦ E-mail
Estado	Estado dos relatórios de status. Os relatórios de status podem estar em um dos seguintes estados: ◦ Rascunho ◦ Em fila ◦ Publicado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione o tipo de relatório de status que você deseja exibir ou selecione **Novo** para criar um relatório de status.

Guia Relatórios de status do MSIM



6. Escolha um dos seguintes tipos de relatório de status na lista.
   - Relatórios de status de e-mail**executivo** que são compatíveis com dispositivos móveis.
   - PDF**do relatório de status técnico**
   - PDF**do relatório de status executivo**

   Nota: Quando você seleciona qualquer modelo de relatório desejado, a visualização do relatório selecionado é gerada imediatamente no painel direito. Você pode exibir o relatório de status selecionado do MSI.

7. No modelo de relatório de status de e-mail executivo, preencha as seções com os detalhes do relatório de status.

Seção de relatório	Descrição
Atualizações	Forneça um resumo da atualização de status. Esta seção contém o seguinte: ◦ **Resumo do MSI**: forneça um breve resumo do incidente de segurança grave. ◦ **Acrescentar texto do último relatório compartilhado**: selecione esta opção para acrescentar o texto do último relatório compartilhado.
Explicação	Adicione uma explicação sobre o que mudou desde a última atualização de status. Esta seção contém o seguinte: ◦ **Atualizações**importantes: forneça atualizações importantes, como o que a equipe de segurança deve saber sobre o incidente de segurança grave, nomeie os principais eventos que ocorreram e liste todas as ações pendentes. ◦ **Próxima atualização**: forneça a data e a hora da próxima atualização para resolver o incidente de segurança grave. Por exemplo, 17h EST em 25 de março de 2024.

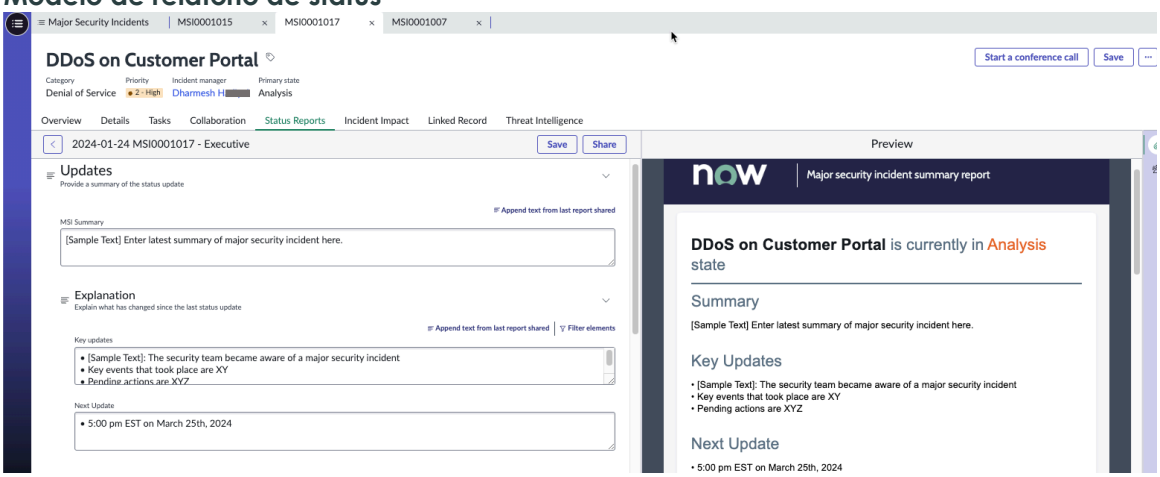
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção de relatório	Descrição
	◦ **Acrescentar texto do último relatório compartilhado**: selecione esta opção para acrescentar o texto do último relatório compartilhado. ◦ **Elementos de filtro**: selecione os elementos do relatório a serem incluídos no relatório. Por exemplo, Atualizações de chave ou Próximas atualizações.
Informações adicionais	Forneça detalhes específicos relevantes para a atualização de status.
Visualizações	Selecione as visualizações que melhor ajudam a comunicar a atualização de status. ◦ **Impacto do incidente**: selecione as métricas de impacto do incidente, como Ativos afetados, Local afetado, Usuários afetados que estão relacionados à atualização de status. ◦ **Elementos de filtro**: selecione os elementos do relatório a serem incluídos no relatório. Por exemplo, Impacto do incidente.
Listas	Selecione listas de registros que fornecem contexto para a atualização de status. ◦ **Registros vinculados**: selecione os registros que estão vinculados à atualização de status do incidente de segurança grave. Por exemplo, Incidente de segurança vinculado. ◦ **Elementos de filtro**: selecione os elementos do relatório a serem incluídos no relatório. Por exemplo, Registros vinculados.

Nota: As opções que você selecionou na seção Relatórios de status são as mesmas opções que são renderizadas no relatório de visualização.

Modelo de relatório de status



8. Selecione **Salvar** para salvar as atualizações feitas no relatório de status.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Selecione **Compartilhar** para compartilhar o relatório de status com partes interessadas internas e externas.
   A caixa de diálogo Compartilhar é exibida.

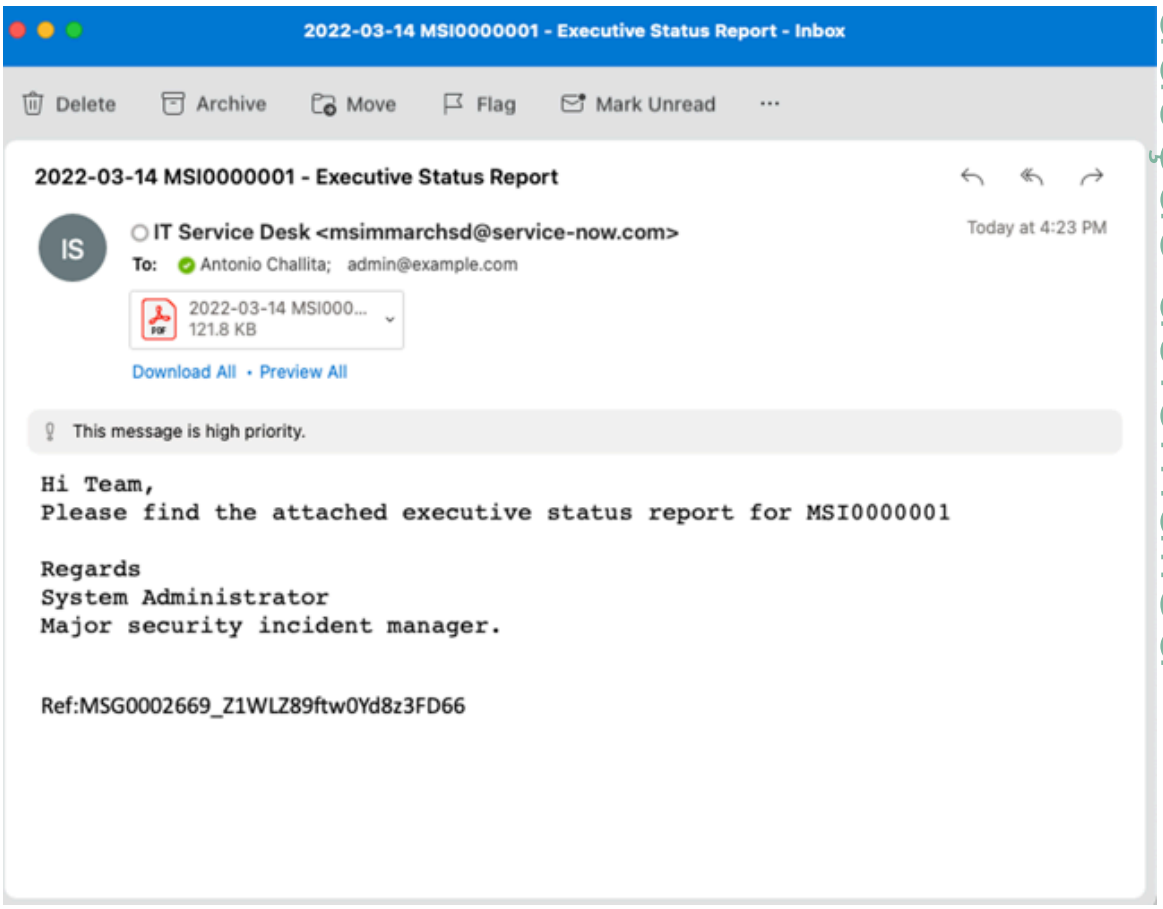
   a. No campo Assunto, insira o assunto do relatório de e-mail.

   b. No campo Adicionar destinatários internos, digite e selecione os destinatários do relatório de e-mail.

   c. No campo Adicionar destinatários externos, digite o e-mail ou DL dos destinatários para o relatório de e-mail.
   Você pode adicionar vários IDs de e-mail usando vírgula ou ponto-e-vírgula.

10. Selecione **Relatório de e-mail**.
    Um e-mail com o relatório de status em PDF anexado é enviado com sucesso ao destinatário em questão para que ele verifique.

Relatório de status - e-mail



11. Você também pode executar as seguintes ações na guia Relatórios de status:
    a. Use a ação **Atualizar** na exibição Relatórios de status para atualizar a lista de relatórios de status.
    b. Use a ação **Listar ações** na exibição Relatórios de status para editar colunas ou redefinir as larguras da lista de relatórios de status.
    c. Use a ação **Filtrar** na exibição Relatórios de status para filtrar os relatórios de status com base em determinadas condições.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Configurar Incidente grave de segurança relatórios de status

Gerenciando MSIM relatórios de status

Os relatórios de status fornecem gráficos de tendências pré-configurados com visualizações de dados acionáveis para melhorar os processos de operações de segurança, medir e analisar a linha do tempo de resolução, a contagem atrasada e o status de cada tarefa atribuída.

Configurar Incidente grave de segurança relatórios de status

Configure relatórios de incidentes de segurança graves para configurar e baixar os relatórios de acordo com as necessidades de negócio durante todo o ciclo de vida do processo de correção de registros de incidentes de segurança graves.

Você pode criar os modelos de relatório com um formato e layout específicos e personalizar esses relatórios de acordo com seus requisitos específicos usando o recurso Relatórios de status do espaço Gestão de incidentes graves de segurança.

Um usuário com a função sn_msi.workspace_manager pode criar e configurar os modelos de relatório que descrevem o tipo de informações de relatório que podem ser usadas para gerar todos os relatórios de status, que podem ser compartilhados com usuários específicos, como partes interessadas executivas, departamentos jurídicos e mapeá-los modelos para os registros de incidentes de segurança graves.

Para personalizar seus relatórios de status do MSI, você deve primeiro configurar os modelos de relatório usando **Modelos**de relatório . Com a ajuda de Modelos de relatório, você pode criar os tipos de modelo de relatório, definir os componentes de relatório para esses modelos de relatório, adicionar informações adicionais, criar dados visualizados para rastrear o escopo e as métricas de andamento, adicionar dados da lista relacionada e gerar os relatórios de status.

A seguir está descrito os campos padrão fornecidos em todos os tipos de modelo de relatório. Você pode configurar e formatar o modelo de relatório com base em seus requisitos usando seções, subseções e seus elementos:

Componentes do relatório de status

Tipo de componente	Descrição
Título do relatório	Título do tipo de relatório. Por exemplo, o formato padrão do tipo de relatório é: {Número de MSI} - {Relatório de parte interessada executiva} representado como MSI0001001: Relatório de parte interessada executiva.
Nome	Exibe o nome do usuário que gerou o relatório usando a seção Relatórios de status do espaço Gestão de incidentes de segurança graves.
Resumo	Exibe um breve resumo do relatório.
Data	Exibe a data em que o relatório é compartilhado com o destinatário em questão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Componentes do relatório de status

Tipo de componente	Descrição
Andamento	Exibe o escopo e as métricas de andamento, como incidentes de SIR vinculados, tarefas de resposta, tarefas suplementares, colaboração externa, componentes da linha do tempo e eventos recentes da linha do tempo.
Desafios	Esta seção exibe uma breve descrição dos desafios envolvidos em todo o processo de correção de incidentes de segurança graves.
Próximas etapas	Esta seção exibe uma breve descrição das próximas etapas envolvidas na resolução do incidente de segurança grave. Por exemplo, a subseção da equipe ativa no relatório da parte interessada executiva fornece as informações com a próxima etapa na atribuição da equipe que está envolvida na análise posterior do registro de incidente de segurança grave.
Outras personalizações	O modelo de relatório também oferece a capacidade de carregar o logotipo e personalizar os cabeçalhos e rodapés no relatório.

A seguir estão os tipos de categorias de relatório que podem ser configuradas e exibidas:

- E-mail**executivo**
- PDF**do relatório de status técnico**
- PDF**do relatório de status executivo**

Os relatórios acima estão configurados e disponíveis para o usuário selecionar, exibir e gerar o relatório no espaço de Gestão de incidentes de segurança graves.

Relatórios de status executivo otimizados para dispositivos móveis - e-mail

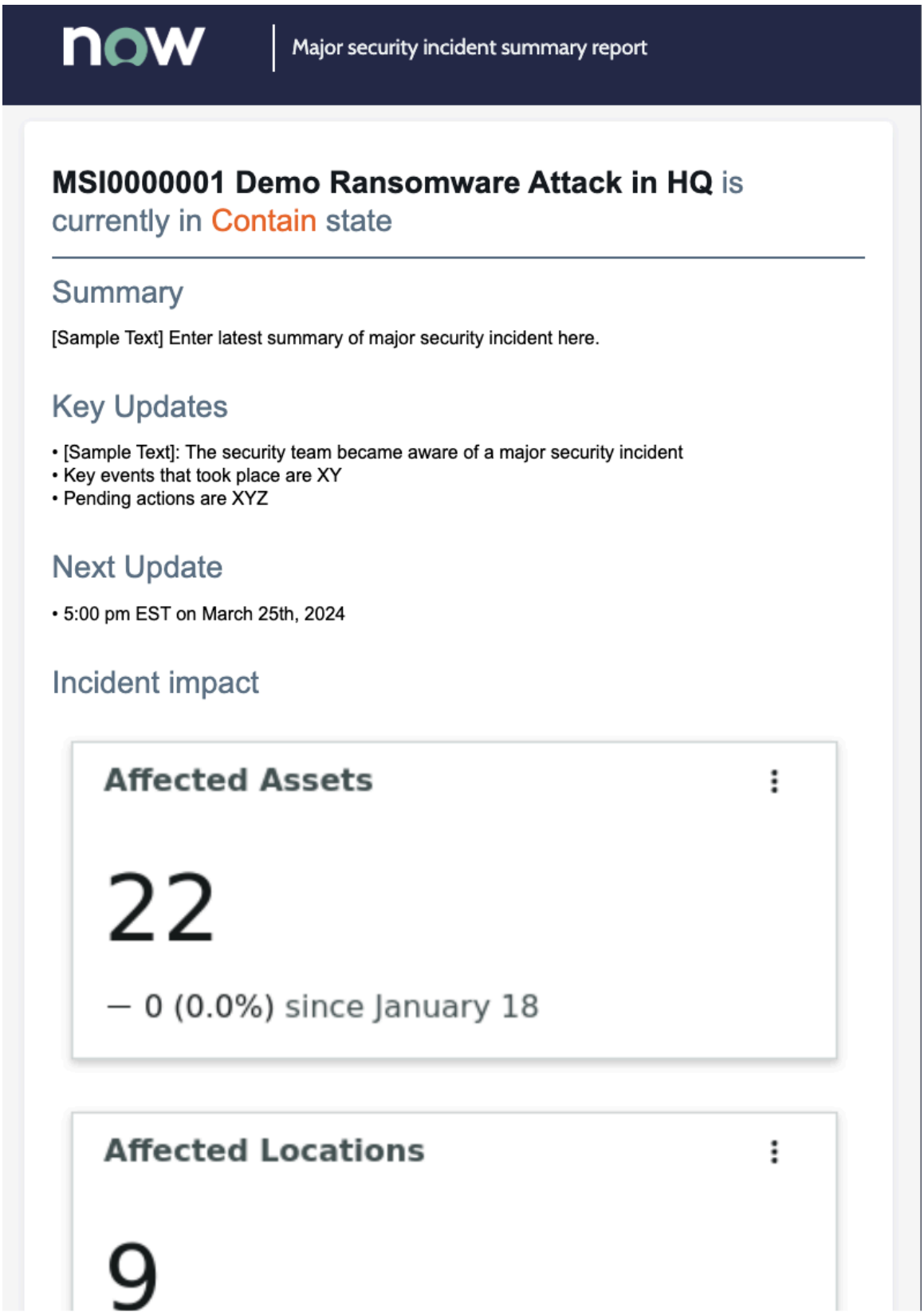
Os Relatórios de status executivo - E-mail são relatórios de status compatíveis com dispositivos móveis que são gerados no formato de e-mail. A seção de relatório inclui um resumo do relatório, coluna de duração do MSI, escopo/impacto do incidente, métricas de equipe ativa, métricas de andamento e componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico.

Personalize e configure os seguintes recursos de modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório de status de e-mail executivo é mostrado abaixo para sua referência.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

E-mail do relatório de status executivo



Tradução automática

Relatórios de status executivo - PDF

Os Relatórios de status executivo - PDF são relatórios de status gerados no formato PDF. A seção de relatório inclui um resumo do relatório, coluna de duração do MSI, escopo/ impacto do incidente, métricas de equipe ativa, métricas de andamento e componentes

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico.

Personalize e configure os seguintes recursos de modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório executivo é mostrado abaixo para sua referência.

PDF do relatório de status executivo

MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label
6

Figure 3. Response Tasks

Relatórios de status técnico - PDF

Os Relatórios de status técnicos - PDF são relatórios de status gerados no formato PDF. A seção de relatório inclui um resumo do relatório, coluna de duração do MSI, escopo/impacto do incidente, métricas de equipe ativa, métricas de andamento e componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico, atualizações de tarefa rotuladas e atividades rotuladas, com base no grupo de atribuição e no rótulo do marcador selecionado desde

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

quando o último relatório de status foi gerado e informações adicionais, como impacto do incidente e incidentes vinculados.

Personalize e configure o modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório técnico que mostra as informações adicionais, como o impacto do incidente, é ilustrado abaixo para sua referência, e a parte restante das informações do relatório é semelhante aos relatórios executivos.

Relatório de status técnico - PDF

As seções do modelo de relatório contêm várias subseções, que descrevem como você pode construir as subseções do relatório e seus elementos, como:

1. Identidade visual: Adicionar identidade visual aos seus modelos de relatório
2. Scripts de modelo: Usar scripts de modelo em seus modelos de relatório
3. Usar visualizações em modelos de relatório
4. Usar listas de relatórios em modelos de relatório

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um modelo de relatório

Crie vários modelos de relatório que podem ser aplicados aos incidentes de segurança graves e gerem um relatório de status. Você pode adicionar campos de formulário de resposta a incidentes graves de segurança padrão e personalizados ao modelo de relatório que pode ser percorrido por pontos. Além disso, você pode formatar e configurar o relatório com base em seus requisitos usando seções, subseções e seus elementos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode definir componentes de relatório para seus modelos de relatório e fornecer informações adicionais. Crie dados visualizados para rastrear o escopo e as métricas de andamento, adicionar dados da lista relacionada, visualizar e gerar ou compartilhar os relatórios de status.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Selecione **Novo** para criar um modelo de relatório.
4. No formulário Modelo de relatório, preencha os campos.

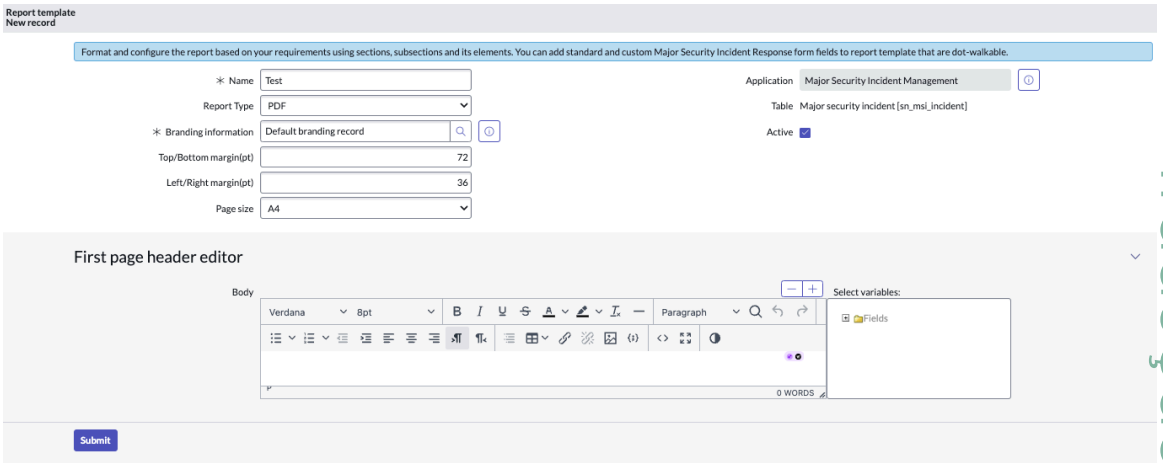
Campo	Descrição
Nome	Nome do modelo de relatório.
Informações de identidade visual	Selecione as informações de identidade visual do modelo de relatório, como logotipo, cabeçalho e texto do rodapé. Por exemplo, Registro de identidade visual padrão.
Tipo de relatório	Tipo de relatório de status. O relatório de status pode estar em um dos seguintes tipos: ◦ PDF ◦ E-mail
Tabela	Nome da tabela de modelo de relatório.
Margem superior/inferior	Defina os recuos das margens superior e inferior necessários ao gerar o relatório.
Margem Esquerda/Direita	Defina os recuos das margens esquerda e direita necessários ao gerar o relatório.
Tamanho da Página	O tamanho da página do seu modelo de relatório. Por exemplo, o tamanho padrão é A4.
Ativo	Marque a caixa de seleção do MSI Manager para gerar um relatório a partir do modelo que foi criado na seção **Modelo de relatórios**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar um relatório para esse tipo de modelo de relatório específico no espaço do MSIM.
Editor de cabeçalho da primeira página	Permite que você defina o corpo do modelo. Selecione as variáveis necessárias para adicionar à seção do editor de modelos.

Criar um modelo de relatório



5. **Envie** o novo registro de modelo de relatório.
   Um novo modelo de relatório é criado na página Modelos de relatórios.

Informações relacionadas

Criar e distribuir MSIM relatórios de status

Adicionar identidade visual aos seus modelos de relatório

Adicione identidade visual aos seus relatórios. Você pode adicionar imagem de cabeçalho e rodapé, texto de cabeçalho e rodapé. Você pode incluir essas informações de identidade visual em qualquer um dos tipos de modelo de relatório que deseja criar, exceto os dois relatórios predefinidos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

As principais considerações ao adicionar identidade visual aos modelos de relatório são as seguintes:

- Carregue a imagem do cabeçalho e do rodapé e alinhe a posição da imagem.
- O limite máximo de tamanho para a imagem do cabeçalho e rodapé é de 5 MB. Se o tamanho exceder o limite especificado, uma mensagem de erro "O formato da imagem não pode ser reconhecido" será exibida no incidente de segurança grave.
- Ajuste a altura da imagem do cabeçalho e do rodapé.
- O tamanho do texto do rodapé está limitado a 100 caracteres.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
2. Detalhar até **Modelo de relatório** > **Identidade visual**.
3. Selecione **Configurar**.
4. Selecione **Novo** para adicionar uma identidade visual ao seu modelo de relatório.
5. No formulário Modelo de identidade visual, preencha os campos.

Campo	Descrição
Nome	Nome do modelo de identidade visual.
Imagem do cabeçalho	Adicione uma imagem de cabeçalho para o modelo de identidade visual executando as seguintes etapas: **a.** Selecione **Clique para adicionar**. **b.** Selecione **Escolher arquivo** **c.** Escolha uma imagem do seu sistema e selecione **OK**.
Imagem do rodapé	Adicione uma imagem de rodapé para o modelo de identidade visual executando as seguintes etapas: **a.** Selecione **Clique para adicionar**. **b.** Selecione **Escolher arquivo** **c.** Escolha uma imagem do seu sistema e selecione **OK**.
Posição da imagem do cabeçalho	Selecione uma posição de imagem de cabeçalho para o modelo de identidade visual. Você pode escolher **Esquerda**, **Centralizado**ou **Direita**.
Posição da imagem do rodapé	Selecione uma posição de imagem de cabeçalho para o modelo de identidade visual. Você pode escolher **Superior à esquerda**, **Superior ao centro**, **Superior à direita**, **Inferior à esquerda**, **Inferior ao centro**ou **Inferior à direita**.
Altura da imagem do cabeçalho	Forneça um valor de altura (em pt) para a imagem do cabeçalho do modelo de identidade visual.
Altura da imagem do rodapé	Forneça um valor de altura (em pt) para a imagem do rodapé do modelo de identidade visual.
Texto do rodapé	Forneça um texto de rodapé para o modelo de identidade visual. Você pode incluir informações de classificação ou confidencialidade. Por exemplo, este e-mail está classificado como Confidencial, Somen-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	te interno ou Advogado do cliente privilegiado.
Posição do texto do rodapé	Selecione uma posição de texto de rodapé para o modelo de identidade visual. Você pode escolher **Superior à esquerda**, **Superior ao centro**, **Superior à direita**, **Inferior à esquerda**, **Inferior ao centro**ou **Inferior à direita**.

6. Selecione **Enviar**.
   Um novo modelo de identidade visual é criado na página Modelos de identidade visual.

Usar visualizações em modelos de relatório

Use widgets de relatório para definir e incluir elementos do Construtor de interface do usuário (UIB), como visualizações de dados, nos relatórios de status do MSIM.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Detalhar até **Modelo de relatório** > **Visualizações**.
3. Selecione **Configurar**.
   A seguir estão as visualizações UIB predefinidas como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Nome do widget	Descrição
Equipe ativa	Exibe a lista de equipes ativas envolvidas na resolução do MSI.
Ativos afetados	Exibe a lista de ativos afetados.
Locais afetados	Exibe a lista de locais afetados.
Usuários afetados	Exibe a lista de usuários afetados.
Gráfico de pizza da colaboração	Inclui as atividades de colaboração no gráfico de pizza.
Gráfico de tendência de colaboração	Exibe as atividades de colaboração como um gráfico de tendências.
Data de resolução estimada	Exibe a data de resolução estimada até quando o ISG deve ser resolvido.
Gráfico de barras dos incidentes vinculados	Exibe o gráfico de barras de incidentes vinculados.
Gráfico de tendências de incidentes vinculados	Exibe o gráfico de tendências de incidentes vinculados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do widget	Descrição
Gráfico de barras das tarefas de resposta do ISG	Exibe o gráfico de tarefas de resposta do MSI.
Gráfico de barras das tarefas de resposta	Exibe o gráfico de barras das tarefas de resposta.
Tarefas de resposta em andamento por rótulos	Exibe as tarefas de resposta em andamento por rótulos.
Tarefas de resposta atrasadas	Exibe o total de tarefas de resposta que estão atrasadas para fechamento.
Gráfico de tendências de tarefas de resposta	Exibe o gráfico de tendências das tarefas de resposta.
Tempo decorrido desde a detecção do incidente	Exibe o tempo decorrido desde o momento em que o incidente foi detectado.
Linha do tempo	Exibe a linha do tempo dos principais eventos e marcos que ocorreram como parte do incidente de segurança grave.

Informações relacionadas

Criar um elemento de tipo de visualização

Usar listas de relatórios em modelos de relatório

Use listas de relatório para definir e incluir os artefatos de lista relacionados para gerar listas no PDF com base nos registros de lista do MSI configurados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Detalhar até **Modelo de relatório** > **Listas**.
3. Selecione **Configurar**.
   A seção Listas de relatórios de status do MSI descreve como cada lista relacionada específica é afetada desde que o incidente foi criado. A seguir estão as Listas de Relatórios do MSI predefinidas como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Listas de relatórios do ISG	Descrição
Ativos afetados	A lista relacionada de ativos afetados é exibida no relatório de status.
Locais afetados	A lista relacionada de locais afetados é exibida no relatório de status.
Usuários afetados	A lista relacionada de usuários afetados é exibida no relatório de status.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas de relatórios do ISG	Descrição
Indicadores	A lista relacionada de indicadores exibidos no relatório de status.
Incidente de segurança vinculado	A lista relacionada à exibição de incidentes de segurança vinculados no relatório de status.
Observáveis	A lista relacionada de exibição de observáveis no relatório de status.

Informações relacionadas

Criar um elemento de tipo de lista

Usar scripts de modelo em seus modelos de relatório

Crie um script para incluir os dados das listas relacionadas, as operações de data e quaisquer outros dados que não sejam diretamente percorridos por pontos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar este script de modelo predefinido em seus modelos de relatório para incluir todos os dados relacionados depois que os modelos de relatório forem configurados e personalizados.

Crie um script de modelo para exibir os dados da lista relacionada no modelo de relatório. Se você quiser utilizar e preencher qualquer script de modelo, deverá adicionar o marcador de script do modelo de marcador como: `${template_script:script name}`.

Exemplo: `${template_script:msi_collab_cards}`

Nota: Você não pode excluir os scripts de modelo predefinidos. Uma mensagem de erro será exibida se um usuário com função de administrador tentar excluir um registro de script de modelo se ele estiver mapeado com qualquer modelo de relatório.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Detalhar até **Modelo de relatório** > **Scripts do Modelo**.
3. Selecione **Configurar**.
   A seguir estão os scripts de modelo predefinidos como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Nome do script do modelo	Descrição
data_atual_formatada	Retorna a data e hora locais atuais no formato DMMAAAA 00:00 AM ou PM. Por exemplo, 21 de janeiro de 2021 3:51 pm PST.
msi_active_team	Gere HTML para cartões de equipe ativos.
msi_collab_cards	Gere HTML para cartões de atividade de colaboração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do script do modelo	Descrição
msi_task_activities	Gere HTML para cartões de tarefa.
msi_timeline_events	Gere HTML para cartões de evento da linha do tempo.
si_afetados_usuários	Retorna os usuários afetados da lista relacionada em um formulário tabular.
si_assessments	Retorna os resultados da avaliação pós-incidente em um formulário tabular.
si_associated_phish_e-mails	Retorna os e-mails de phishing associados da lista relacionada em um formulário tabular.
si_associated_phish_headers	Retorna os cabeçalhos de phishing associados da lista relacionada em um formulário tabular.
si_business_criticality	Retorna o valor de criticalidade dos negócios codificado por cores.
si_maliciosos_observáveis	Retorna os observáveis maliciosos da lista relacionada em um formulário tabular.
si_observáveis	Retorna os observáveis da lista relacionada em um formulário tabular.
si_priority	Retorna um valor de prioridade codificado por cores.
si_response_tasks	Retorna as tarefas de resposta da lista relacionada em um formulário tabular.
si_time_to_identify	Retorna a duração gasta no estado Rascunho e Análise.
si_time_to_resolver	Retorna o tempo para resolver o incidente.

Nota: Você também pode criar seu próprio script de modelo para incluir os dados de listas relacionadas, operações de data e quaisquer outros dados que não sejam diretamente percorridos por pontos, além dos scripts de modelo listados.

Visualizar o modelo de relatório

Use a funcionalidade Visualizar para visualizar o modelo de relatório em tempo de design para gerar e compartilhar o relatório com outras partes interessadas durante o tempo de execução no espaço Gestão de incidentes graves de segurança.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Selecione o modelo de relatório desejado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione o Tipo de relatório como E- **mail** ou **PDF** com base em seus requisitos.
5. Selecione a ação **Salvar e visualizar relatório**.

   A caixa de diálogo Visualizar relatório é exibida.
6. Selecione um incidente de segurança grave usando a opção Pesquisar para visualizar um relatório com o modelo selecionado.
7. Selecione **Visualizar relatório**.
   O relatório gera uma visualização de acordo com a configuração do modelo selecionado. Se você selecionou o Tipo de relatório como E- **mail**, a visualização estará no formato de modelo de e-mail. Os relatórios de status no formato de e-mail são compatíveis com dispositivos móveis.

Criar um modelo de seção de relatório

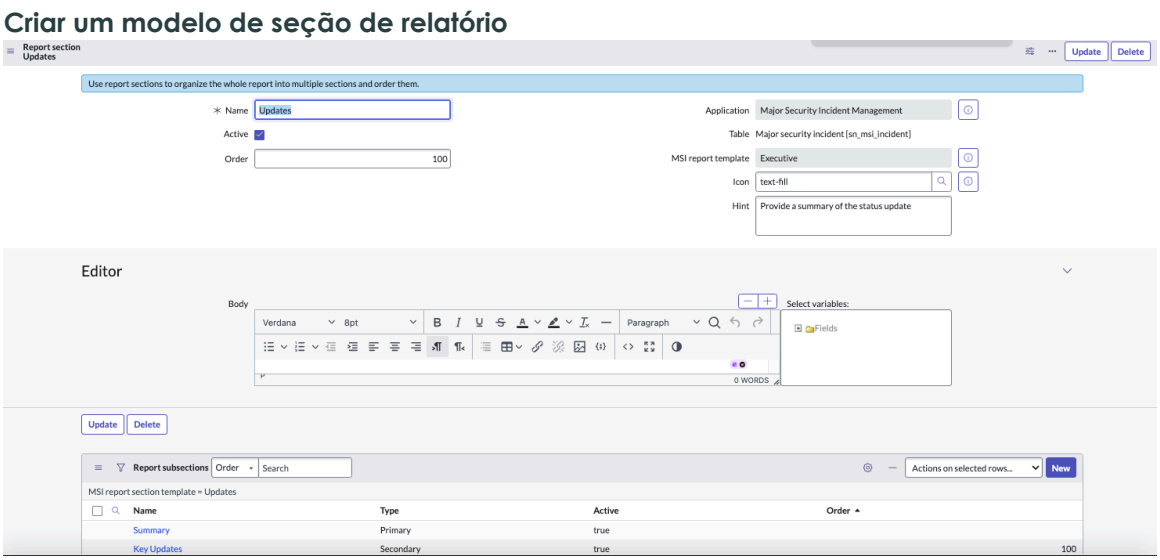
Um relatório pode ser dividido em várias seções. Use a seção Relatório para dividir o relatório em várias seções e reorganizá-las em ordem.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente.
4. Navegar até **Seções de relatório** > **Novo**.
   A nova página da seção de relatório é exibida.



5. No formulário Modelo de seção de relatório, preencha os campos.

Campo	Descrição
Nome	Nome da seção do modelo de relatório. Por exemplo, Resumo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela	Nome da tabela de modelo de relatório.
Ativo	Marque a caixa de seleção para criar uma seção de relatório para o modelo selecionado no espaço do MSIM. **Nota:** Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar uma seção de relatório para este modelo no espaço do MSIM.
Modelo de relatório do ISG	O nome do modelo de relatório do MSI para o qual o relatório é dividido em seções.
Ordem	A ordem na qual as seções do relatório serão renderizadas.
Ícone	Use o ícone para exibir ícones do sistema no relatório.
Dica	Use o texto de dica para orientar a criação do relatório. No relatório, o texto de dica é exibido sob o título da seção.
Editor - Corpo	Defina o corpo da seção do modelo. Você pode definir o corpo da seção selecionando os tokens ou variáveis personalizados no editor.

6. Salve e **envie** a nova seção de modelo de relatório.

Criar um modelo de subseção de relatório

Use a subseção de relatório para organizar ainda mais a seção em várias subseções e configurar seu alinhamento e posição usando os tipos disponíveis, como Painel lateral de texto, Primário e Secundário.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

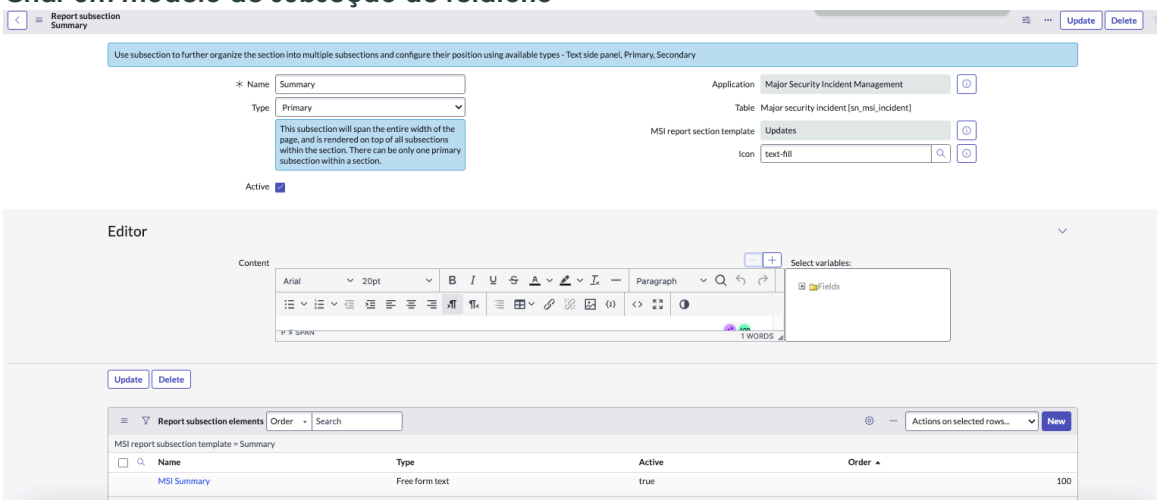
Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Navegar até **Subseções de relatório** > **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um modelo de subseção de relatório



6. No formulário de subseção Relatório, preencha os campos.

Campo	Descrição
Nome	Nome da subseção do modelo de relatório. Por exemplo, Escopo. **Nota:** As subseções existentes para os relatórios predefinidos são: Visão geral, Escopo, Andamento, Explicação. ◦ **Visão geral**: exibe a visão geral como uma subseção no relatório. ◦ **Escopo**: exibe os elementos de visualização no relatório, como contadores de duração, impacto do incidente, equipes ativas e tendência de equipes ativas. ◦ **Andamento**: exibe os elementos de visualização no relatório, como Gráficos de incidentes de segurança vinculados, Gráfico de tarefas de resposta e Gráficos de colaboração.
Tipo	O tipo de subseção do relatório. Os tipos disponíveis são: ◦ **Primário**: esta subseção abrange toda a largura da página e é renderizada sobre todas as subseções dentro da seção. Só pode haver uma subseção primária em uma seção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Secundário**: esta subseção abrange toda a largura da página, a menos que seja usada com o painel lateral de texto. ◦ **Painel lateral de texto**: esta subseção acompanha o painel secundário e oferece suporte somente ao texto.
Tabela	Nome da tabela de modelo de relatório.
Modelo de seção de relatório do ISG	O nome do modelo de relatório do MSI para o qual você está dividindo o relatório em seções.
Ordem	A ordem na qual as subseções do relatório serão renderizadas.
Ícone	Use o ícone para indicar ou realçar o contêiner de seção no formulário de configuração do tempo de execução do relatório.
Ativo	Marque a caixa de seleção para criar uma subseção de relatório para o modelo selecionado no espaço do MSIM. **Nota:** Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar uma subseção de relatório para este modelo no espaço do MSIM.
Editor - Conteúdo	Defina o conteúdo da subseção do modelo.

7. Salve e **envie** a nova seção de modelo de relatório.

Criar modelo de elemento de subseção de relatório

Use elementos de subseção para organizar ainda mais uma subseção em vários elementos. Os elementos de subseção ajudam a definir visualizações, listas e texto de forma livre de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

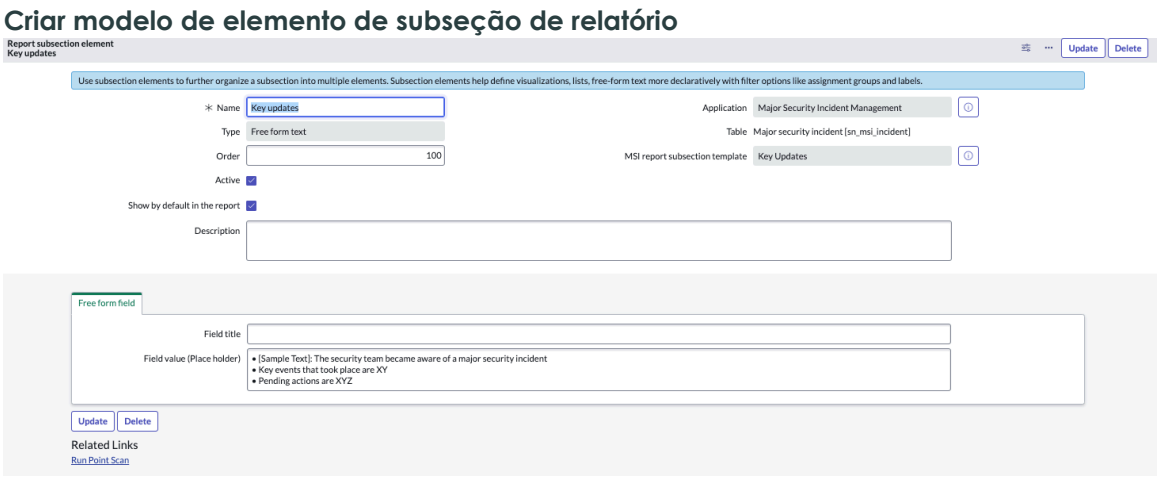
Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.



7. No formulário Elementos da subseção Relatório, preencha os campos.

Campo	Descrição
Nome	Nome do elemento de subseção do modelo de relatório. Por exemplo, Escopo. **Nota:** As subseções existentes para os relatórios predefinidos são: Contadores de duração, Impacto do incidente, Equipe ativa, Tendência da equipe ativa. ◦ **Contadores de duração**: exibe o contador de duração como um elemento de subseção, como o tempo estimado para resolver o incidente no relatório de status. ◦ **Impacto do incidente**: exibe os elementos de visualização no relatório, como os ativos afetados, os locais afetados e os usuários afetados. ◦ **Equipe ativa**: exibe os elementos de visualização no relatório, como o número de equipes ativas envolvidas no encerramento do incidente de segurança grave. ◦ **Tendência de equipe ativa:** descreve a tendência de equipes ativas em uma representação gráfica.
Tipo	O tipo de elemento de subseção de relatório. Os tipos disponíveis são: ◦ Texto de forma livre ◦ Visualização

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Personalizado ◦ Lista
Tabela	Nome da tabela de modelo de relatório.
Ativo	Marque a caixa de seleção para criar uma seção de relatório para o modelo selecionado no espaço do MSIM. **Nota:** Se a caixa de seleção estiver desmarcada, o MSI Manager não poderá criar uma seção de relatório para este modelo no espaço do MSIM.
Mostrar por padrão no relatório	Marque esta caixa de seleção se quiser incluir a seção no relatório para renderizar rapidamente os elementos.
Modelo de relatório do MSI	O nome do modelo de relatório do MSI para o qual você está dividindo o relatório em seções.
Ordem	A ordem na qual as seções do relatório serão renderizadas.
Descrição	Forneça uma descrição para o tipo de elemento de subseção.

8. Salve e **atualize** a nova seção de modelo de relatório.

Criar um elemento de tipo de forma livre

Crie um tipo de elemento de forma livre para definir o texto de forma livre de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **de campo de formulário livre**.
   Isso exibe a seção **Campo de forma livre**.
9. Na guia Forma livre, preencha os campos.

Campo	Descrição
Título do campo	Nome do título do campo. Por exemplo, Visão geral.
Valor do campo (espaço reservado)	Insira a descrição do valor do campo. Por exemplo, Aqui está um exemplo de texto de visão geral. `Fizemos um bom progresso na contenção de ativos afetados. No entanto, acabamos de descobrir que os invasores ainda estão invadindo os sistemas, incluindo o Windows. A contenção de ativos LINUS está em andamento, mas demorando mais do que o esperado. O novo dia de resolução estimado é 5 dias a partir de hoje.`

Criar um elemento de tipo de visualização

Crie um tipo de elemento de visualização para definir os elementos de visualização de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **Visualização**.
   Isso exibe a seção **Visualização**.
9. No formulário Visualização, preencha os campos.

Tradução automática

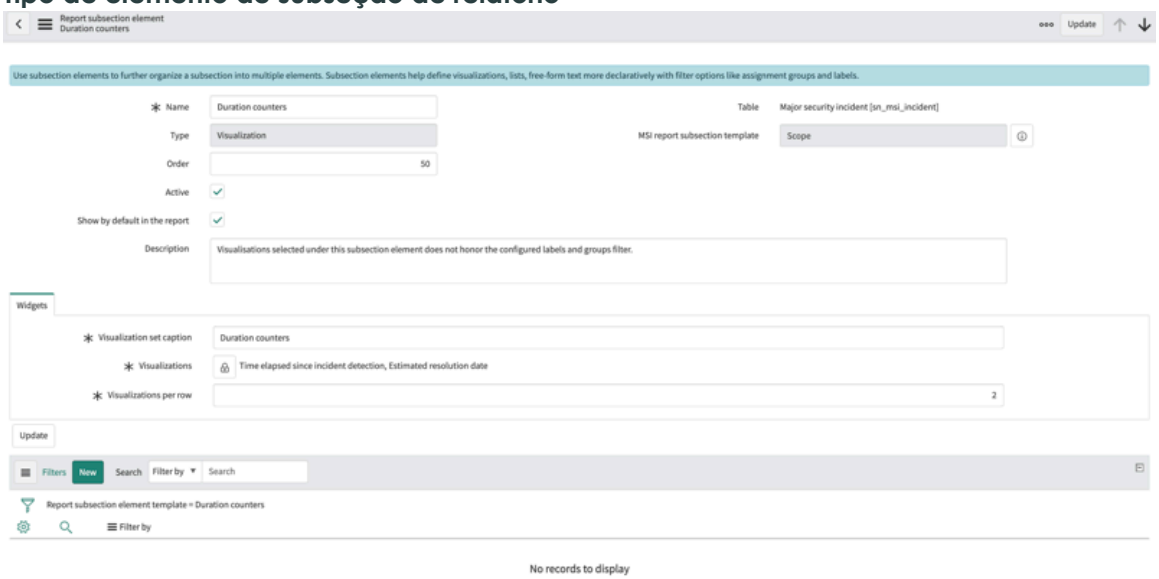
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Legenda do conjunto de visualizações	Insira o nome da legenda do conjunto de visualizações. Por exemplo, Contadores de duração.
Visualizações	Selecione o tipo de visualizações. Por exemplo, selecione Tempo decorrido desde a detecção do incidente, Data de resolução estimada para o tipo de subseção: Contadores de duração.
Visualizações por linha	Selecione o número de visualizações exibidas de acordo com cada linha.

10. Selecione **Enviar**.

Example: Tipo de elemento de subseção de modelo de relatório para um relatório de status técnico

Tipo de elemento de subseção de relatório



Criar um elemento de tipo de lista

Crie um elemento de tipo de lista, que define os elementos de lista relacionados de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **Lista**.
   Isso exibe a seção **Listas**.
9. No formulário Lista, preencha os campos.

Campo	Descrição
Listas	Nome das listas relacionadas associadas ao MSI. Por exemplo, Observáveis, Indicadores. Selecione uma lista usando a opção de pesquisa.

Criar um elemento de tipo personalizado

Crie um elemento de tipo de lista, que define os elementos de lista relacionados de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **Personalizado**.
   Isso exibe a seção **Conteúdo personalizado**.
9. No formulário Conteúdo personalizado, preencha os campos.

Campo	Descrição
Conteúdo dinâmico	Insira o conteúdo dinâmico, como os scripts de modelo.
Tempo de execução configurável	Marque esta caixa de seleção se o tipo de elemento personalizado for configurável em tempo de execução.

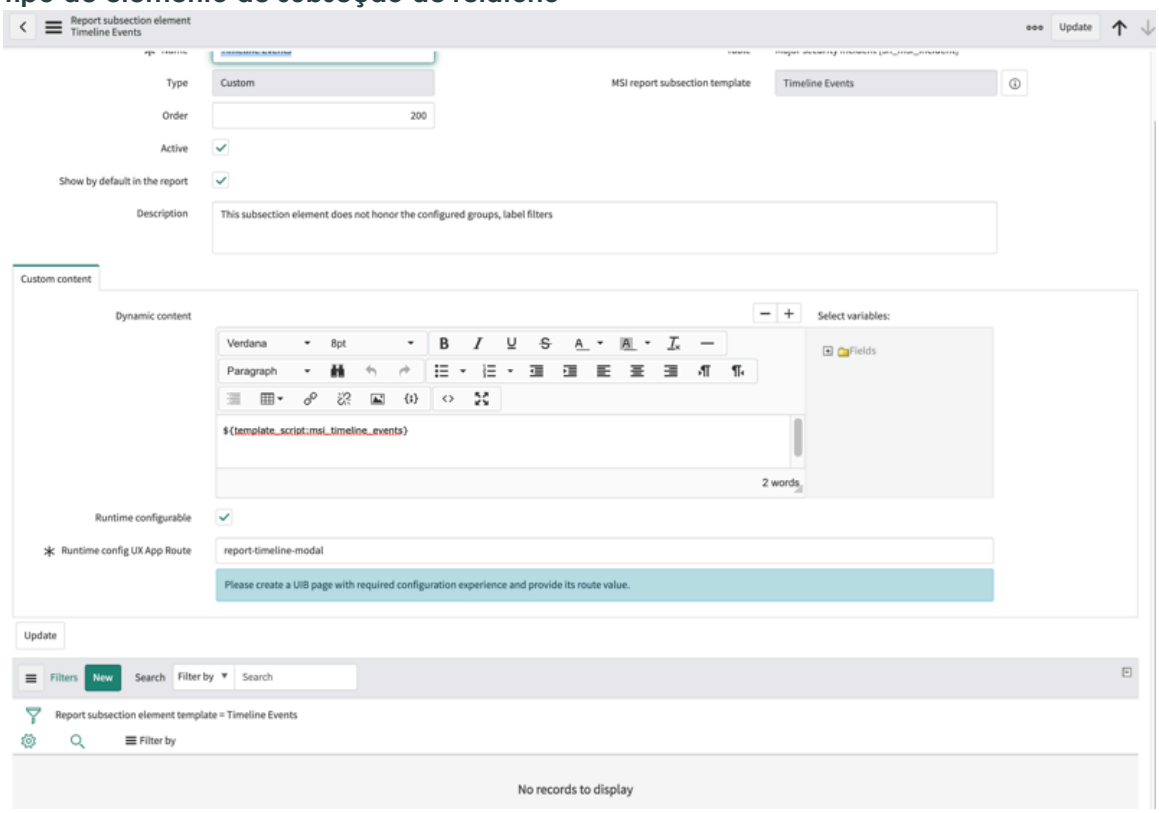
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Rota da aplicação UX de configuração de tempo de execução	Insira o valor de Rota do app de UX da configuração do tempo de execução quando uma página UIB for criada com a experiência de configuração necessária. **Nota:** Este campo aparece somente quando a opção **Tempo de execução configurável** está selecionada.

Example: A seguir está um exemplo do tipo de elemento de subseção do modelo de relatório para um relatório de status técnico

Tipo de elemento de subseção de relatório



Tradução automática

Adicionar propriedades do sistema

Adicione propriedades do sistema para controlar o comportamento da aplicação MSIM. A seguir estão as propriedades do sistema padrão que são introduzidas como parte dos Gestão de incidentes graves de segurança relatórios de status.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_msi.export_img	Use esta propriedade para controlar a exportação de imagens. O valor padrão está definido como ATIVADO.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_msi.export_img_log	Use esta propriedade para habilitar o login no console do navegador. O valor padrão está definido como DESLIGADO.
sn_msi.export_img_parallel_threshold	Use esta propriedade para controlar o número máximo de solicitações paralelas para gerar as imagens a partir das configurações do widget de relatório. O valor padrão é definido como 14.
sn_msi.img_export_log	Use esta propriedade para habilitar os logs do console no navegador.
sn_msi.img_export_poll_interval	Use esta propriedade para controlar o intervalo de tempo entre as pesquisas que verifica se a imagem foi gerada ou não. O tempo de intervalo de pesquisa padrão é definido como 3000 milissegundos.
sn_msi.export_poll_request_timeout	Use esta propriedade para controlar o tempo máximo em que o sistema pode pesquisar a imagem exportada. O valor padrão é 120.000 milissegundos.
sn_msi.msi_report_uib_element_js_path	Use esta propriedade para controlar o caminho genérico para capturar a imagem da parte da página do UIB.
sn_msi.report_default_style_objects	Use esta propriedade para mudar o CSS dos PDFs gerados, como tamanho da fonte, cor da fonte ou valor do campo. Por exemplo, se sn_msi.workspace_manager preferir mudar a cor da fonte do painel esquerdo do relatório de status do PDF gerado, o gerente do espaço poderá modificar a cor da fonte da propriedade do sistema e renderizar o PDF na exibição desejada.

Playbooks de gestão de incidentes graves de segurança

Você pode invocar o fluxo do playbook de Gestão de incidentes de segurança graves automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook é compatível somente com o Designer de automação de processos (PAD) criado. A Gestão de incidentes graves de segurança fornece o playbook de solicitação jurídica com o sistema de base.

Playbook para solicitação jurídica

O playbook de solicitação jurídica fornece orientação passo a passo sobre como você pode informar o departamento jurídico sobre o resumo mais recente de um MSI para que ele possa notificar a SEC no intervalo de tempo de 4 dias necessário para violações materiais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Como gerente de incidentes, você pode usar o playbook de solicitação jurídica para informar a equipe jurídica sobre o resumo mais recente de um MSI para que ela possa notificar a SEC sobre violações materiais. Você pode usar os modelos do Designer de automação de processos (PAD) para executar as etapas no playbook de solicitação jurídica e informar a equipe jurídica adequadamente.

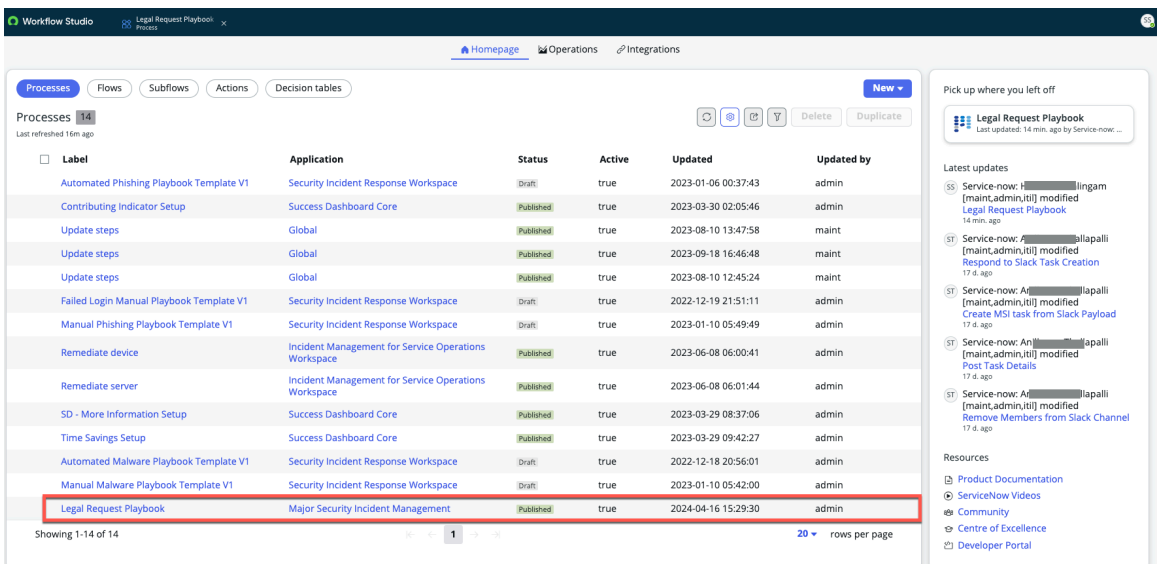
Este playbook pode ser usado se um incidente de segurança grave for criado ou atualizado. Você precisa ativar o playbook de solicitação jurídica no PAD e executar todas as tarefas, como analisar, conter, erradicar e revisar.

A seguir estão as raias da definição do processo e correspondem ao estado do incidente de segurança grave:

- Análise
- Contém
- Erradicar
- Revisão

Cada raia tem determinadas atividades dentro dela.

Playbook para solicitação jurídica



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você pode passar para a próxima. O status é refletido no painel esquerdo conforme você conclui tarefas e raias. Um Log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode editar qualquer campo ou selecionar **Concluir** para concluir o processo de criação do direito.

Criar processos para o playbook de solicitação jurídica

Use estas etapas para criar processos para o playbook de solicitação jurídica no Designer de automação de processos (PAD).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager.

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

   Por exemplo, Playbook de solicitação jurídica.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir suas condições de gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
7. Clique **em Ir para Designer**.
   A página do Designer de automação de processos é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova raia**.
   O painel de propriedades da raia é aberto no lado direito da IU.
9. No painel de propriedades da raia, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a raia seria executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra raia, clique em **Adicionar outra raia**.
    Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Eliminar e Revisar, respectivamente. No exemplo a seguir, a raia de **análise** começa imediatamente e não tem condição de execução. O início da**raia** de contenção após a conclusão da raia anterior e tem uma condição de execução que se baseia no resultado de uma atividade na raia anterior.
    Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.
12. Clique na **atividade Adicionar outro processo** em uma raia específica (por exemplo, Raia de análise).
    O pop-up Adicionar atividade é aberto.

    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.

13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de maneira semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.
14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar o playbook de solicitação jurídica

Use estas etapas para saber como você pode usar o playbook de solicitação jurídica no Espaço do MSIM e seus recursos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager.

Procedimento

1. No espaço do MSIM, abra um incidente de segurança grave.
2. Selecione a guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança grave.

   Nota: Se você não vir os playbooks listados, precisará acessar o PAD e permitir que eles o vejam na guia **Playbook**.

3. Selecione o **Playbook de solicitação jurídica**.
4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.
   Você tem a opção de alterá-lo de acordo com seus requisitos.
6. Da mesma forma, você pode clicar em Conter, Eliminar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Estrutura de Rollup para MSIM

Estende a capacidade de vincular os registros de origem do espaço Gestão de incidentes graves de segurança.

Visão geral

A Estrutura de Acúmulo torna o fluxo de acúmulo configurável e extensível. Use este modelo de estrutura para configurar as informações, que podem ser acumuladas para um incidente de segurança grave.

Anteriormente, sn_msi.workspace_manager era capaz de vincular os incidentes de segurança e itens vulneráveis que foram propostos ou promovidos como MSI. Depois de vincular o incidente de segurança ou item vulnerável, as informações foram acumuladas para um incidente de segurança grave. O tipo de informação que precisa ser acumulado foi codificado nos scripts.

Você pode usar o modelo de estrutura para configurar o fluxo de acúmulo, que oferece suporte aos seguintes recursos e também resolve os problemas existentes na aplicação:

O modelo da estrutura de acúmulo habilita o sn_msi.workspace_manager com os seguintes benefícios para:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adicione ou remova a vinculação, proponha ou promova capacidades de registro MSI em qualquer tabela, o que estende a tabela de tarefas.
- Controle o tipo de informações a serem acumuladas para MSI ao executar ações como vincular/propor/promover nos registros de incidentes.
- Suporte à vinculação, proposta ou promoção de incidentes de segurança, tarefas de correção e casos de segurança prontos para uso (OOTB) no ambiente clássico e no espaço Gestão de incidentes graves de segurança.

A estrutura de acúmulo exibe as configurações conforme explicado na tabela a seguir.

Configurações da Estrutura de Acúmulo

Nome	Descrição
Configuração de registro vinculada	Armazena as informações das tabelas de tarefas que podem ser usadas para vincular/promover/propor para Incidente grave de segurança.
Acumular configuração de registro	Captura as informações que podem ser acumuladas da tabela de tarefas quando as ações vincular/promover/propor são executadas.
Configuração de layout de lista	Controla os rótulos e o layout de lista de várias tabelas, conforme mostrado nas guias do espaço Gestão de incidentes graves de segurança, como Impacto do incidente, Registros vinculados e Inteligência contra ameaças.

Configurar registros vinculados no Gestão de incidentes graves de segurança

Use a configuração de registros vinculados para armazenar as informações das tabelas de tarefas que podem ser usadas para vincular/promover/propor para Incidente grave de segurança.

Função necessária: administrador e sn_msi.workspace_admin.

Nota: O administrador pode criar o registro e o administrador do espaço MSIM pode atualizar o registro.

Procedimento

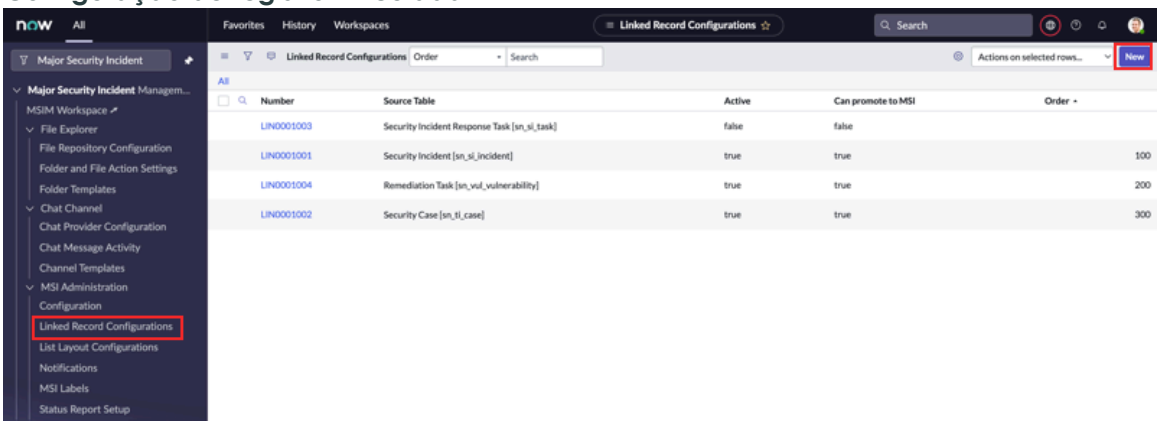
1. Navegar até **Gestão de incidentes graves de segurança** > **Configurações de registro vinculadas**.

   A página Configuração de registro vinculado é exibida.

Tradução automática

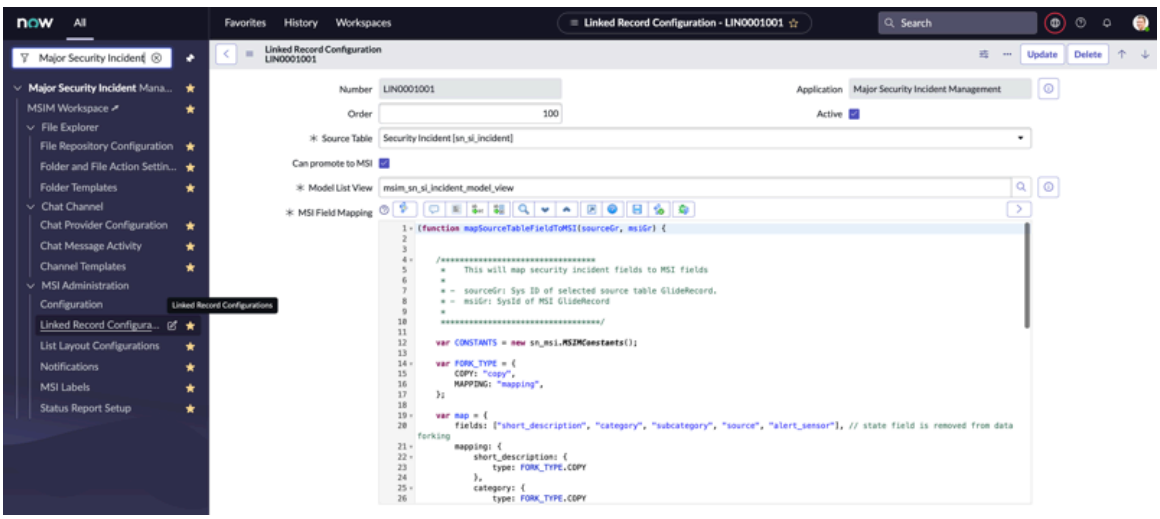
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de registro vinculada



2. Na página Configuração de registro vinculado, clique em **Novo**

Nota: Certifique-se de que a aplicação esteja no escopo Gestão de incidentes graves de segurança.



3. No formulário de configuração de registro, preencha os campos.

Descrições do Campo de Registros Vinculados

Campo	Descrição
Tabela de origem	Indica a tabela de tarefas que deve ser vinculada e acumulada para Incidente grave de segurança.
Ordem	Permite que você controle a ordem da tabela de origem atual no menu suspenso do espaço do MSIM. Abaixo está um exemplo da **ordem**. Consulte a imagem 1 abaixo, que é fornecida após esta tabela.
ListView do modelo	Selecione uma exibição que possa controlar o layout da lista que é mostrado na Lista do modal de registro vinculado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pode promover a MSI	Marque esta caixa de seleção para confirmar se o registro é primário. Abaixo está um exemplo da seleção da opção **Pode promover a MSI**. Consulte a imagem 2 a seguir, que é fornecida após esta tabela. Se esta caixa de seleção estiver marcada e o valor for verdadeiro, então: ◦ você pode propor e promover diretamente um registro de origem para Incidente grave de segurança usando as ações de ambiente clássicas com configurações adicionais. ◦ você pode vincular registros de origem a incidentes de segurança graves no ambiente clássico e no espaço MSIM. ◦ Gestão de incidentes graves de segurança A página de registros vinculados do espaço de trabalho exibe os registros da tabela de origem vinculada. **Nota:** Se um registro puder ser proposto/promovido diretamente como um Incidente grave de segurança, esse registro será primário. Por exemplo, na configuração da tabela de tarefas de resposta de segurança, o valor de **Pode promover para MSI** é falso, pois você não pode promover diretamente a tarefa de resposta de segurança para Incidente grave de segurança. Portanto, ele não aparece na lista suspensa da guia Registro vinculado ao espaço MSIM.
MSI Mapeamento de Campo	Escreva um script para mapear os campos de registro de origem para um incidente de segurança grave recém-criado quando o registro das tabelas de origem estiver no processo de ser proposto ou promovido. Este script é executado somente quando o valor **Pode promover para MSI** é verdadeiro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Imagem 1: Ordem de exibição da lista de registros vinculados

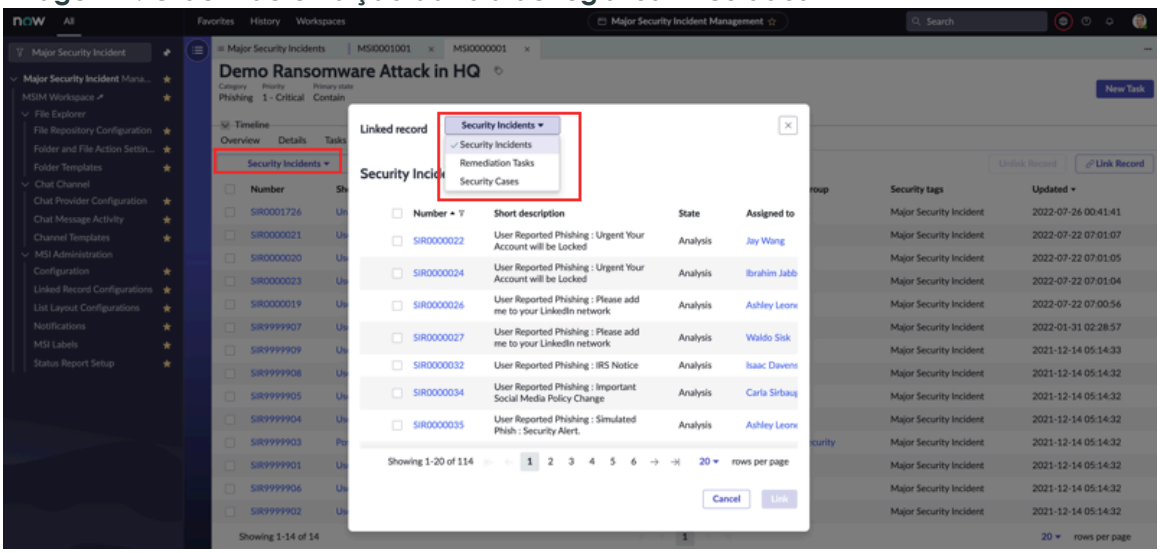
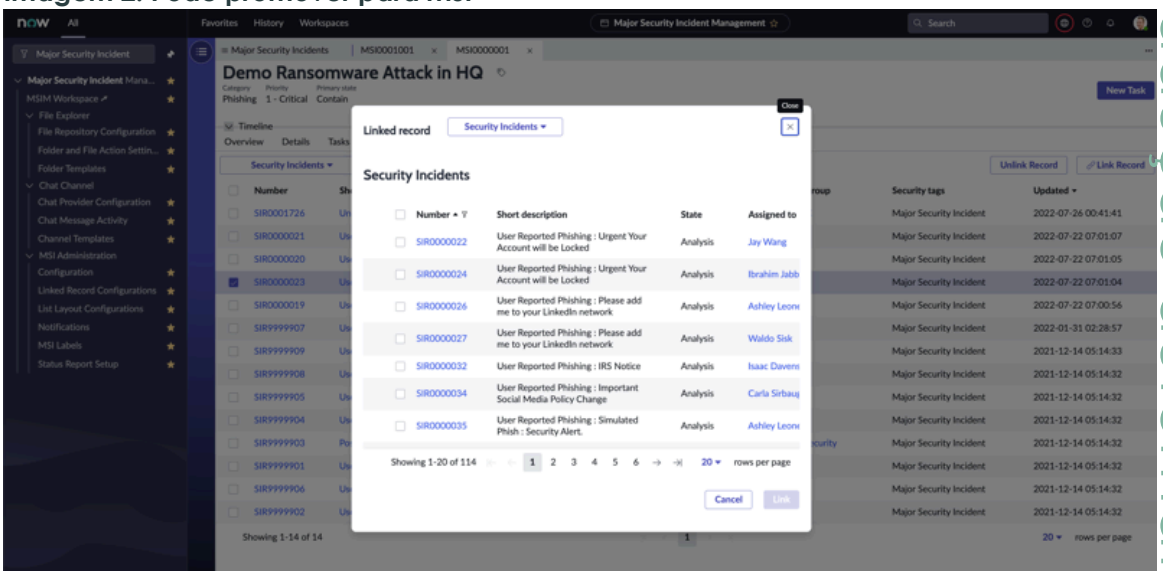


Imagem 2: Pode promover para MSI



Tradução automática

Configurar registros de acúmulo no Gestão de incidentes graves de segurança

Configure os registros de acúmulo em Gestão de incidentes graves de segurança para controlar as informações, que serão acumuladas quando o registro de origem for vinculado/proposto/promovido como incidentes de segurança graves.

Função necessária: administrador e sn_msi.workspace_admin.

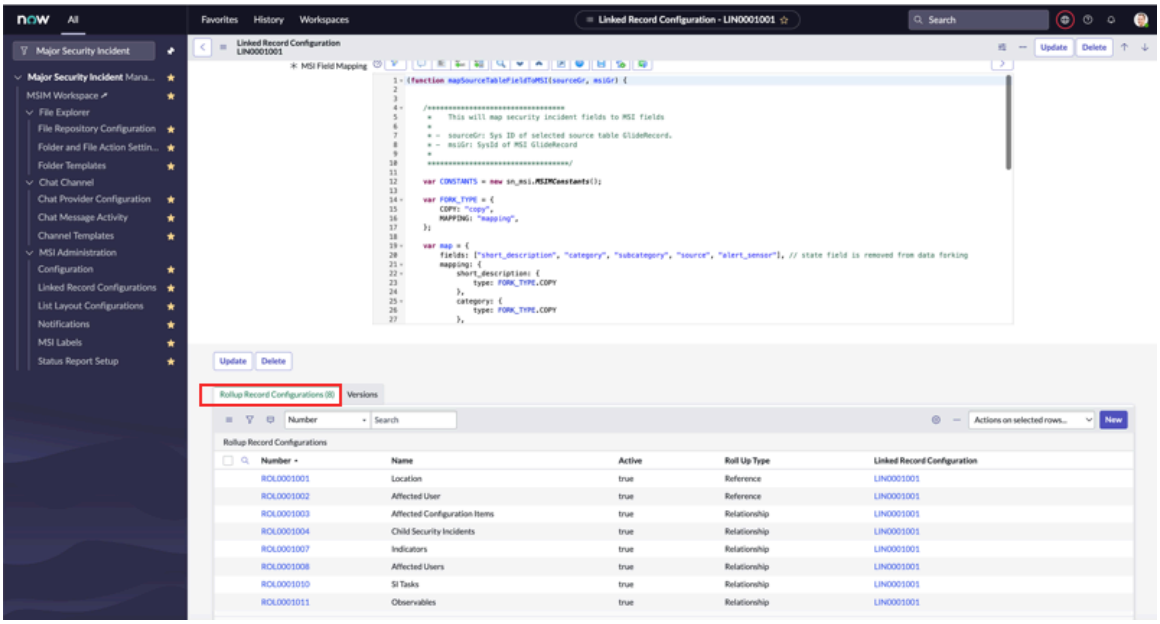
Nota: O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Procedimento

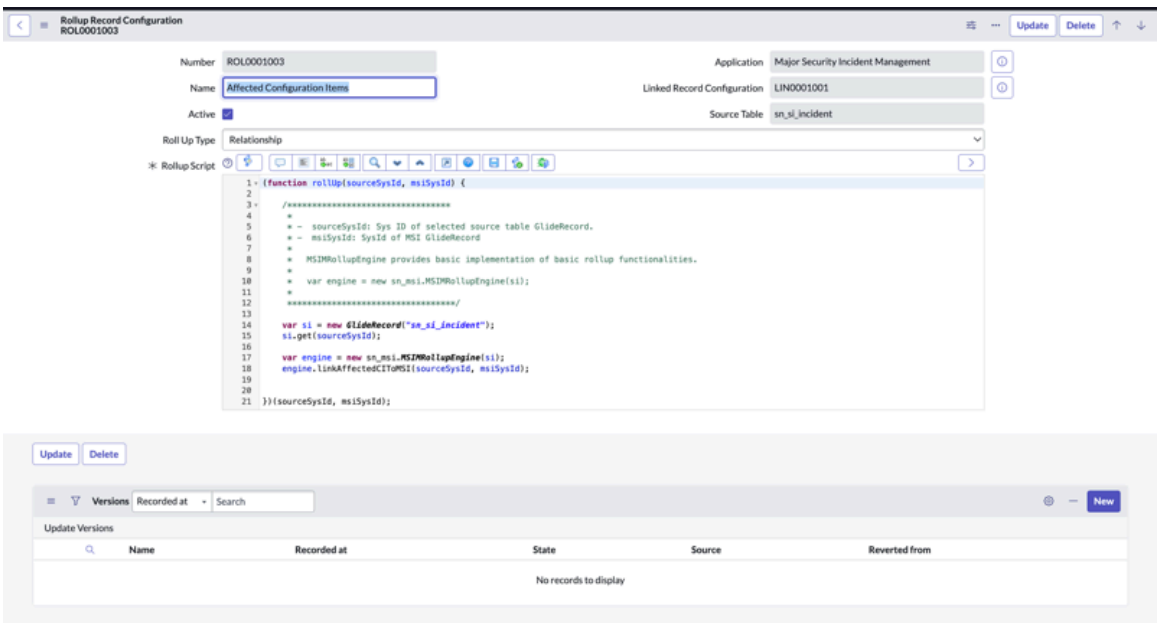
1. Navegar até **Resposta a incidentes graves de segurança** > **Configuração de registros vinculados**. A página Configurações de registro vinculado é exibida.
2. Selecione ou crie um novo registro vinculado e navegue até a seção **Acumular configuração de registro** na mesma página.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção Configuração de registro de acúmulo



3. Clique em **Nova**.



4. Na página de configuração, preencha os detalhes.

Acumular configuração de registro

Nome do Campo	Descrição do Campo
Nome	Indica o nome do registro de acúmulo.
Ativo	Marque esta caixa de seleção para implementar a configuração atual quando ocorrer o acúmulo do registro de origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição do Campo
Configuração de registro vinculada	Indica um número exclusivo, que se refere à configuração de registros vinculados primários e somente leitura.
Tabela de origem	O nome da tabela de origem usada na configuração do registro vinculado, que é somente leitura.
Tipo de Rollup	Descreve o tipo de informação que deve ser acumulada. ◦ **Relacionamento**: selecione esta opção se os dados precisarem estar presentes como uma lista relacionada. ◦ **Referência**: selecione esta opção se os dados estiverem presentes como um campo de referência no formulário da tabela de origem.
Script de acúmulo	Se o tipo de rollup for: **Relacionamento**, o campo **Script de Rollup** será habilitado, o que permite escrever um script e pode ser usado para acumular informações. Aqui, o script receberá as entradas que contêm informações do registro de origem e do incidente de segurança grave. O script deve ser capaz de encontrar as informações das tabelas de relacionamento e acumular para a tabela Registro vinculado (sn_msi_m2m_child).
Campo de origem	Se o tipo de acúmulo for: **Referência**, o **Campo de origem** estará disponível. Isso permite que você selecione o campo de referência Tabela de origem que contém as informações que precisam ser acumuladas.
Campo de destino	Se o tipo de acúmulo for: **Referência**, o **Campo de destino** estará disponível. Isso permite que você faça referência ao campo da tabela Registro vinculado (sn_msi_m2m_child) e armazenará os dados que estão presentes no campo de origem selecionado e no registro da tabela de origem.

Escrevendo script para rollup

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

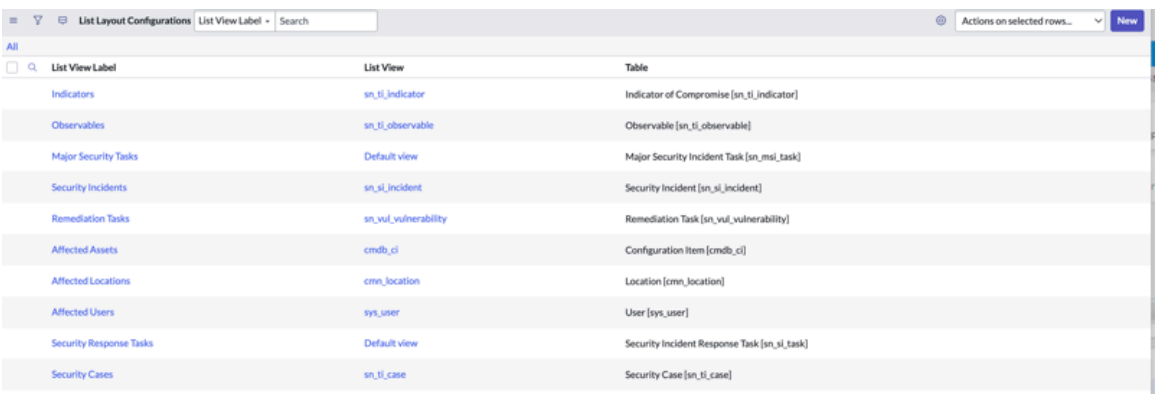
Nome	Descrição
Entradas	• sourceSysId: SYS ID do registro da tabela de origem que está sendo vinculado/proposto/promovido. • msiSysId: SYS ID do incidente de segurança grave ao qual o registro de origem está sendo vinculado/proposto/promovido.
Saída	Nenhum valor de retorno de saída.
Responsabilidade	O script deve acumular informações para a tabela Registro vinculado (sn_msi_m2m_child). • Use sourceSysID para consultar dados de ServiceNow tabelas de relacionamento. • Depois que os dados forem obtidos, acumule os dados em um registro vinculado (sn_msi_m2m_child) usando o utilitário MSIRollupEngine para acumular dados.

Configurar layout de lista no Gestão de incidentes graves de segurança

Configure o layout de lista para personalizar o layout e os rótulos usados no espaço Gestão de incidentes graves de segurança, como Impacto do incidente, Registros vinculados e guias de Inteligência contra ameaças.

Função necessária: administrador e sn_msi.workspace_admin.

Nota: O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.



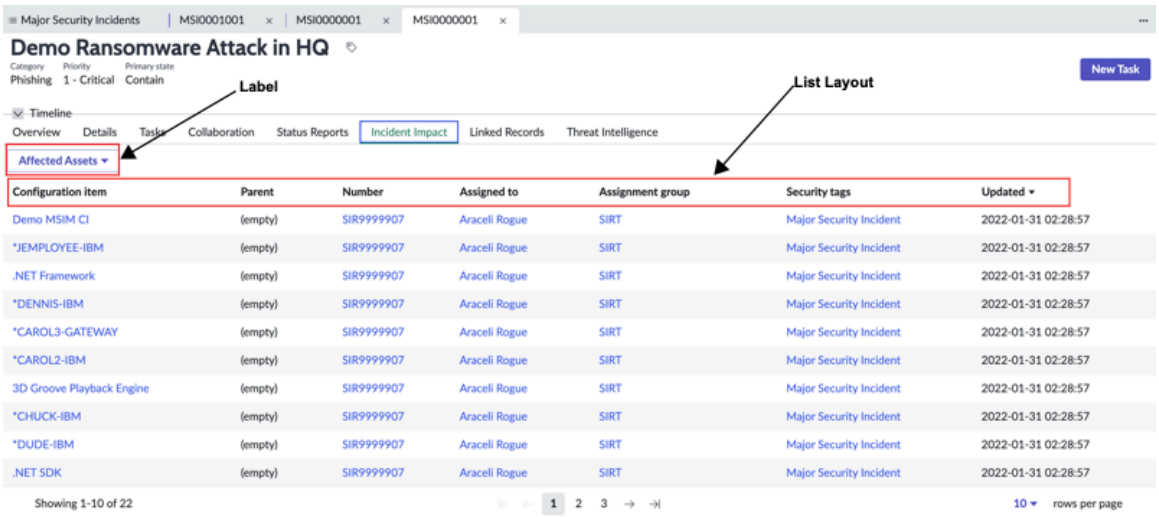
As configurações de layout de lista já foram enviadas para as tabelas conhecidas existentes mostradas no espaço Gestão de incidentes graves de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se você quiser renderizar a exibição personalizada das tabelas existentes, poderá atualizar o respectivo registro da tabela na configuração do layout de lista com a exibição de lista personalizada.
- Para novas tabelas de tarefas, você pode criar uma nova configuração de Layout de lista para renderizar a exibição de lista personalizada e os rótulos. Para obter um procedimento mais detalhado, consulte sobre como Etapa 4. Criar uma exibição para uma nova guia de registro vinculado para um caso de segurança



Exemplo de implementação de caso de uso de acúmulo para um caso de segurança

As etapas a seguir explicam um caso de uso de exemplo sobre como adicionar suporte para vincular/propor/promover para incidente de segurança grave para uma tabela de caso de segurança.

- Etapa 1. Criar configuração de registro vinculado para um caso de segurança
- Etapa 2. Criar uma exibição da janela modal de um caso de segurança
- Etapa 3. Criar ações de IU para a tabela de origem de um caso de segurança
- Etapa 4. Criar uma exibição para uma nova guia de registro vinculado para um caso de segurança
- Etapa 5. Adicionar listas de controle de acesso (ACLs) para usuários do espaço Gestão de incidentes graves de segurança
- Etapa 6. Criar regras de negócio para um caso de segurança
- Etapa 7. Criar configurações de registro de acúmulo

Etapa 1. Criar configuração de registro vinculado para um caso de segurança

Crie uma configuração de registro vinculado para um caso de segurança.

Antes de Iniciar
Função necessária: administrador e sn_msi.workspace_admin

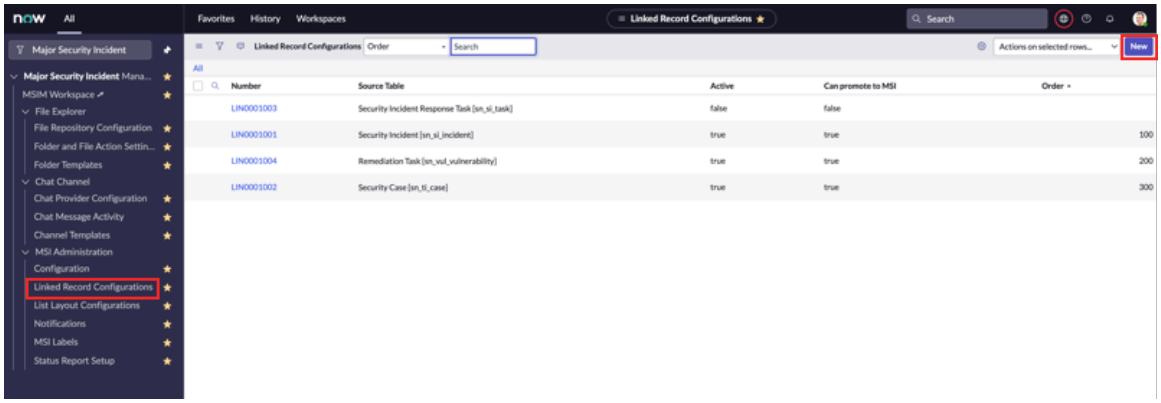
Nota: O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Tradução automática

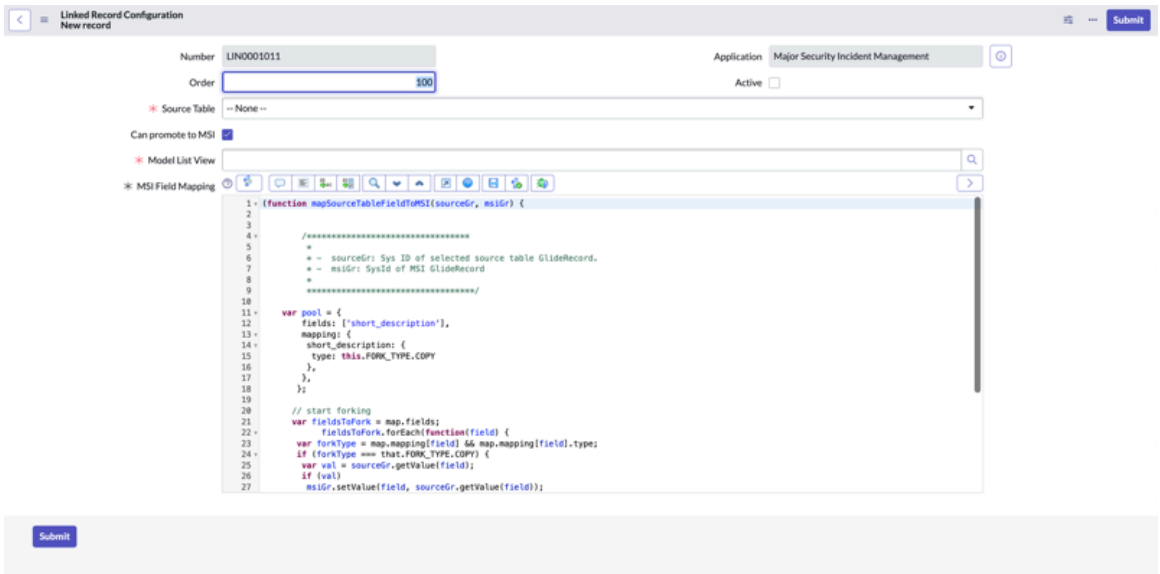
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Pesquise a configuração de registro vinculado na navegação à esquerda.
2. Clique em **Nova**.



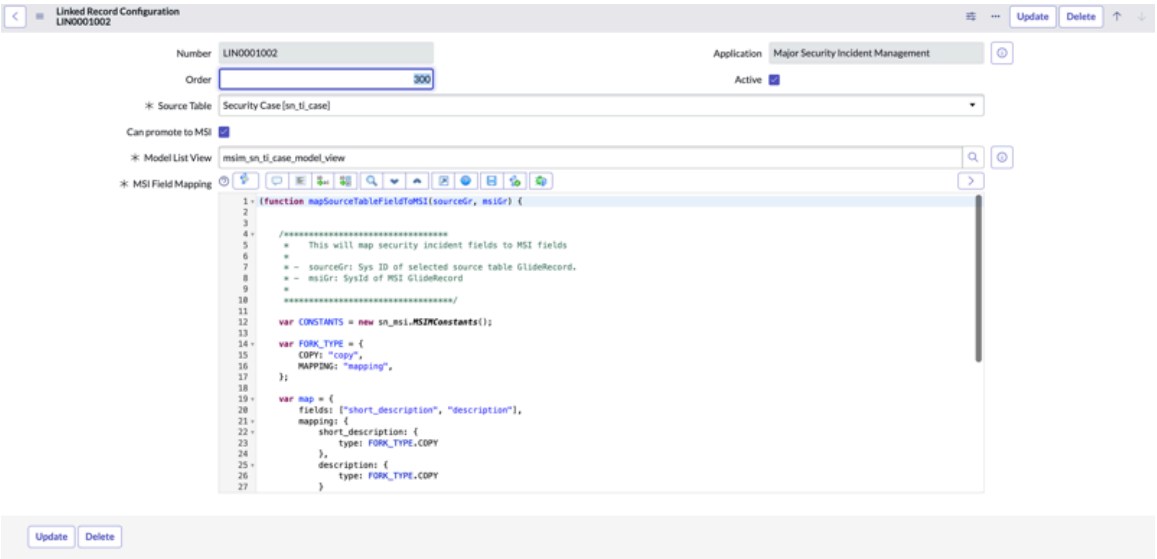
3. Preencha o formulário com as colunas necessárias e grave um script de mapeamento de campo.



4. Agora você criou uma configuração de registro vinculado para o caso de segurança adicionando os valores conforme descrito na tabela a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nome	Descrição
Tabela de origem	Caso de segurança (sn_ti_case). Neste exemplo, vincule/promova/proponha um caso de segurança como MSI.
Ordem	Valor de entrada: 300 **Nota:** A ordem mais baixa tem precedência sobre as ordens mais altas. Como um caso de segurança tem uma ordem superior ao incidente de segurança e à tarefa de correção, ele aparecerá na última sequência.
Pode promover para MSI	Verdadeiro, marque esta caixa de seleção para promover o caso de segurança para MSI.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: ◦ Vincule e desvincule registros de caso de segurança de incidentes de segurança graves no espaço Gestão de incidentes graves de segurança. Além disso, a funcionalidade Desvincular registro está visível somente para os registros vinculados. ▪ Isso habilitará o link, a promoção e a proposta do caso de segurança para o incidente de segurança grave usando ações de ambiente clássicas, mas essas ações de IU não estarão disponíveis prontas para uso. Cada ação de IU precisa ser criada manualmente. Para obter mais informações, consulte Etapa 3. Criar ações de IU para a tabela de origem de um caso de segurança. ▪ As ações de IU Vincular/ Promover/Propor estão disponíveis para Incidente de segurança, Tarefa de correção e Caso de segurança prontos para uso. ◦ A página de registro vinculada ao espaço do MSIM mostrará os registros de caso de segurança vinculados. Consulte a imagem abaixo 1 para exibir as opções disponíveis após marcar esta caixa de seleção.
Exibição de lista modal	msim_sn_ti_case_model_view **Nota:** Esta exibição contém campos e a ordem dos campos mostrados na exibição de lista no modal Vincular registro no espaço do MSIM. Para obter mais informações, consulte Etapa 2. Criar uma exibição da janela modal de um caso de segurança. Consulte a imagem abaixo 2 para exibir na página **Registros vinculados**.
Script de mapeamento de campo	Este script descreve os campos do registro das tabelas de origem que serão mapeados para o incidente de segurança grave recém-criado quando o registro

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	das tabelas de origem for proposto ou promovido. que receberá entradas: ◦ sourceGr: objeto de registro do glide de caso de segurança ◦ msiGr: objeto de registro de incidente de segurança grave O script lerá a descrição resumida do caso de segurança e a copiará como título para o incidente de segurança grave.

Imagem 1: Pode promover para MSI

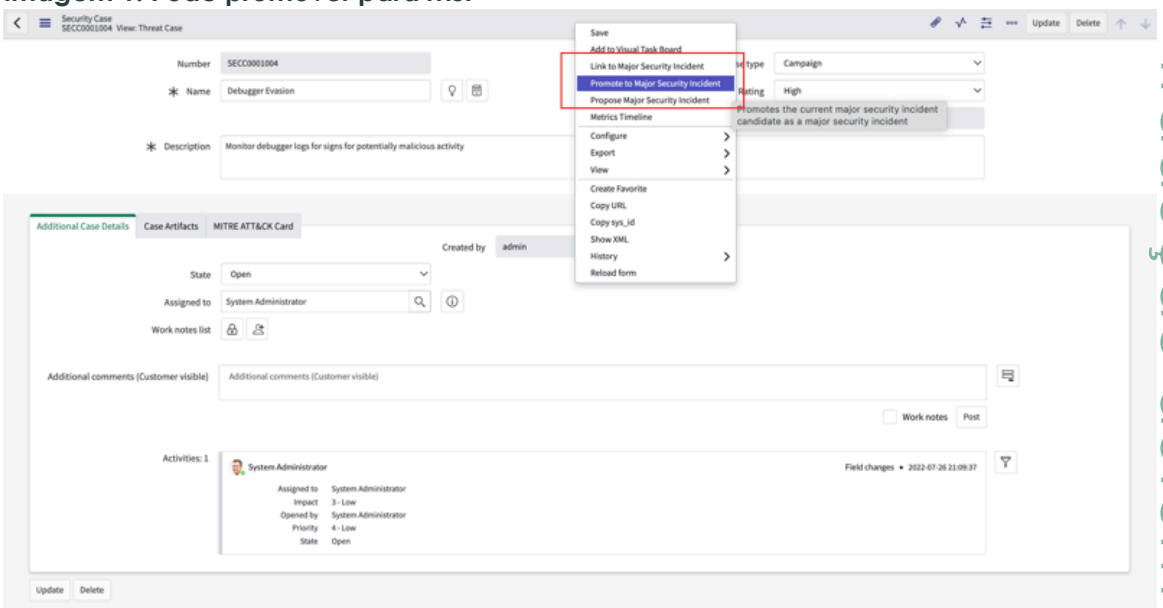
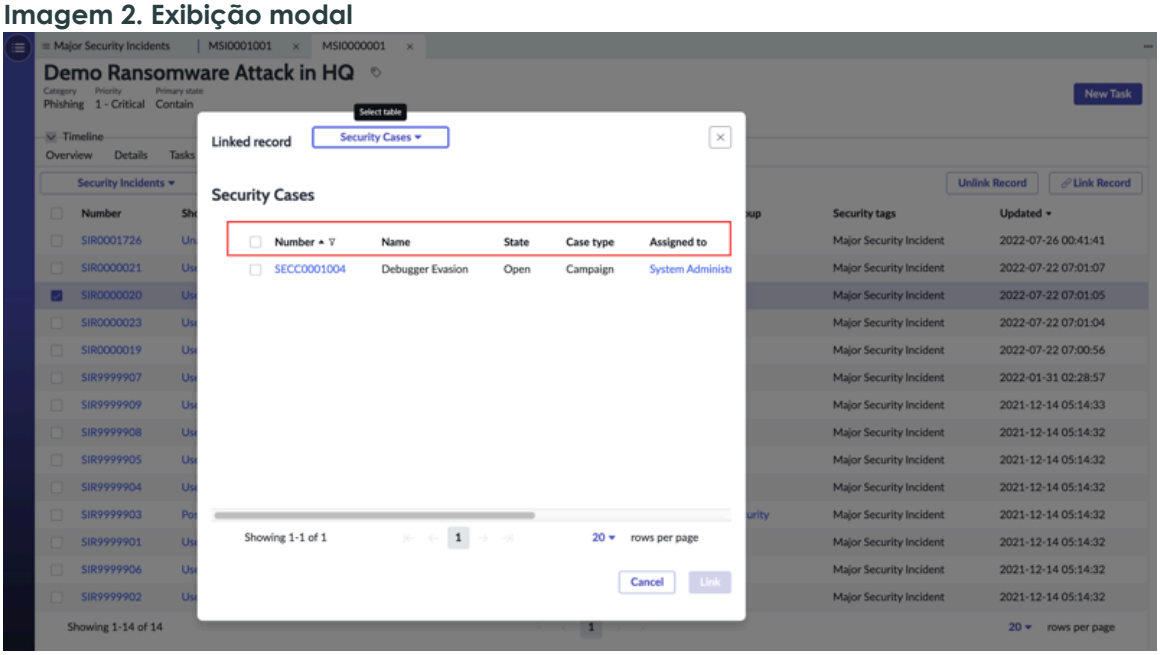


Imagem 2. Exibição modal



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Etapa 2. Criar uma exibição da janela modal de um caso de segurança

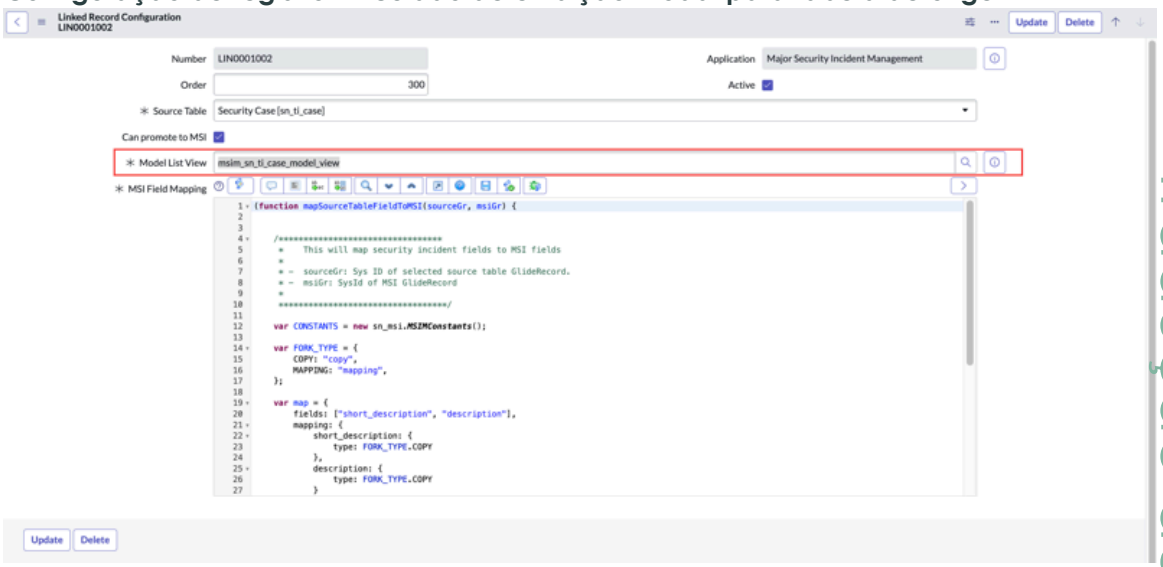
Crie uma exibição para a janela modal de um caso de segurança.

Antes de Iniciar

Consideração de chave:

- Por padrão, a lista modal de registro vinculada mostrará somente o layout de lista **Padrão**. Se você quiser personalizar o layout da lista, poderá fazer isso usando **Exibição personalizada** na Tabela de origem.
- Se você quiser renderizar a exibição personalizada, a exibição personalizada também deverá ser selecionada na Configuração de registro vinculado da Tabela de origem.

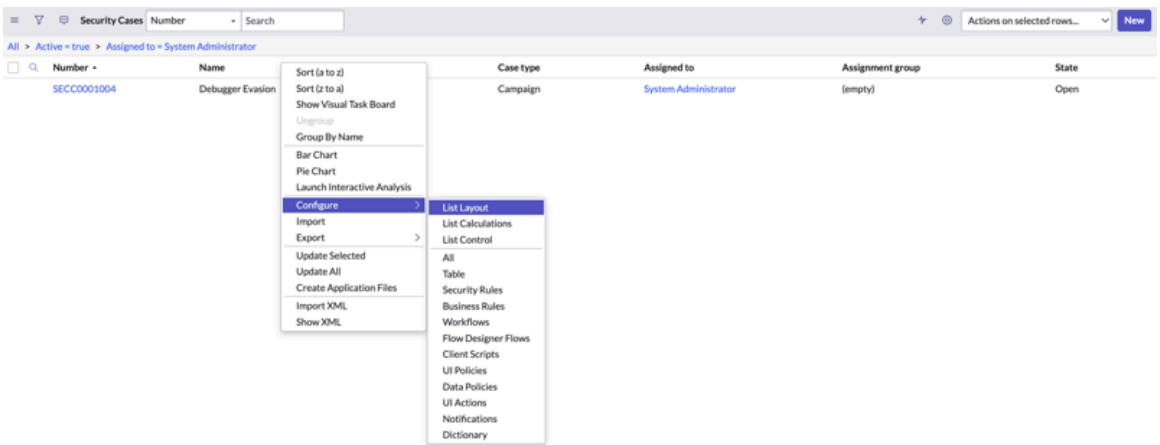
Configuração de registro vinculado de exibição modal para tabela de origem



Função necessária: administrador

Procedimento

1. Acesse a tabela de origem e clique em **Configurar** > **Layout de lista**.



2. Ir para **Exibição em lista** > **Nome de exibição**.
3. Clique em **Novo** na lista suspensa Nome da exibição e crie uma nova exibição, por exemplo, msim_sn_ti_case_modal_view.
4. Selecione a exibição recém-criada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de selecionado, você pode escolher os campos obrigatórios na lista Disponível.

5. Clique em **Salvar**.
6. Navegar até **Menu** > **Exibições** para verificar se a exibição foi renderizada corretamente.

Etapa 3. Criar ações de IU para a tabela de origem de um caso de segurança

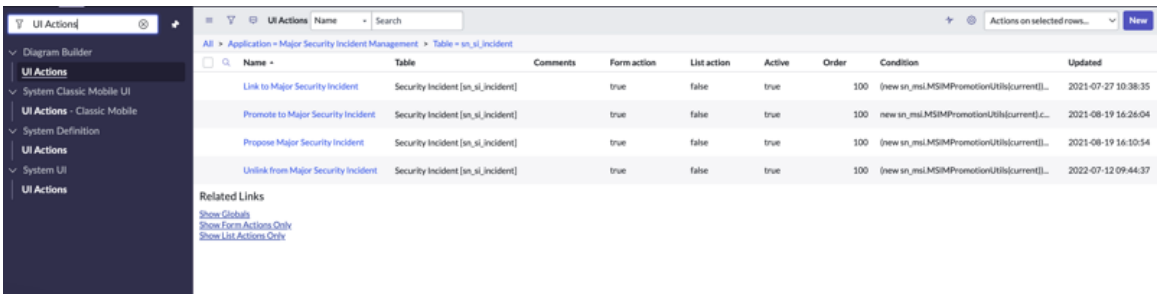
Crie ações de IU para a tabela de origem de um caso de segurança.

Antes de Iniciar

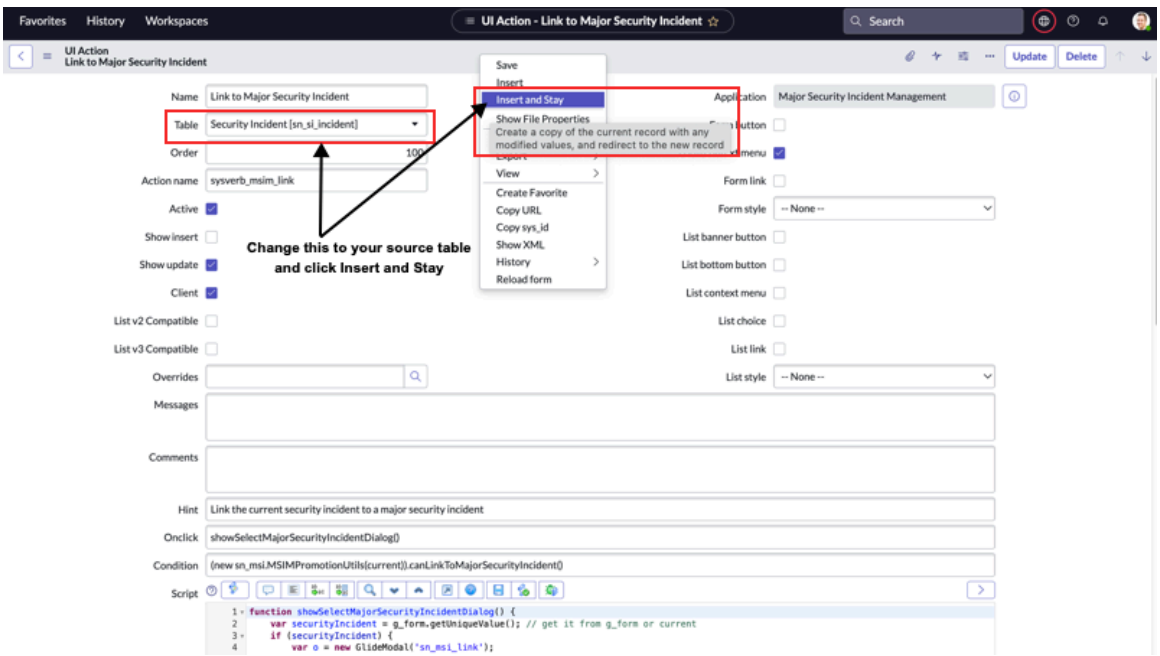
Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Ações de IU**.
2. Execute a opção Filtrar para filtrar a lista por **Aplicação**: Gestão de incidentes de segurança graves e **Tabela**: sn_si_incident.



3. Selecione cada ação de IU uma por uma e salve os detalhes da tabela de origem.



4. Repita as mesmas etapas acima para as seguintes ações de IU:
   - Link para o incidente de segurança grave
   - Incidente de segurança grave proposto
   - Desvincular de um incidente de segurança grave
   - Promover a incidente de segurança grave

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

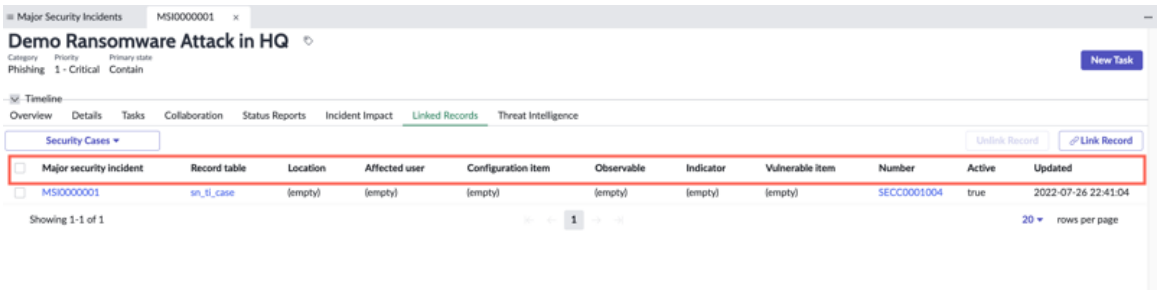
Etapa 4. Criar uma exibição para uma nova guia de registro vinculado para um caso de segurança

Personalize o layout de lista de uma tabela de casos de segurança quando ela for exibida na página Vincular registros com o espaço Gestão de incidentes graves de segurança.

Antes de Iniciar

Pré-requisitos:

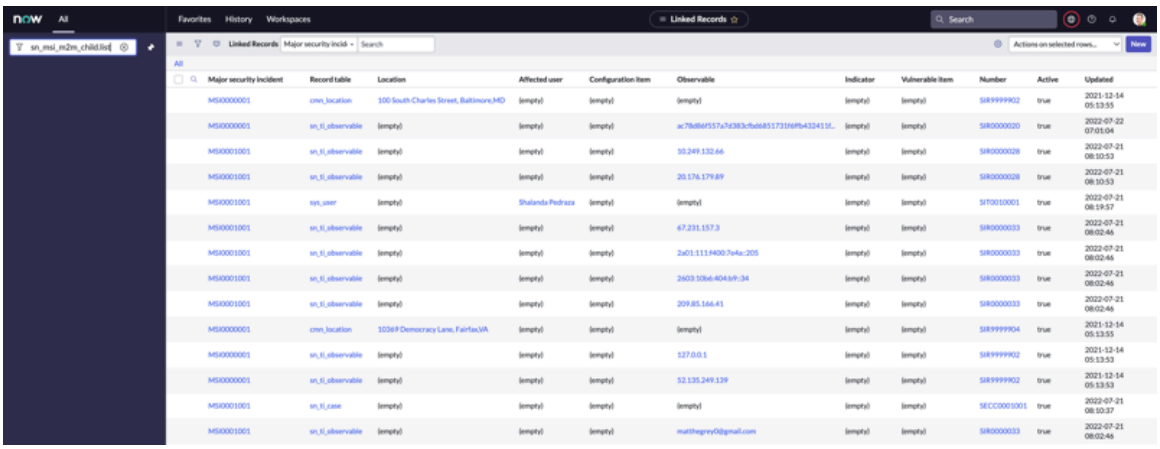
- Escolha a coluna que deve estar visível quando uma lista for renderizada para uma tabela de Caso de segurança.
- Escolha a ordem dos campos a serem exibidos na lista suspensa.



Função necessária: administrador

Procedimento

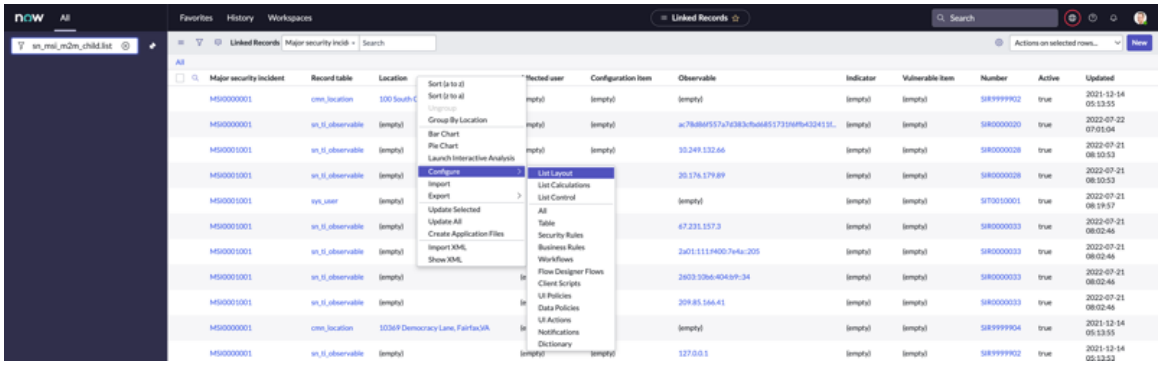
1. Pesquise **sn_msi_m2m_child.list** usando a navegação à esquerda.
   A tabela Registros vinculados é exibida.



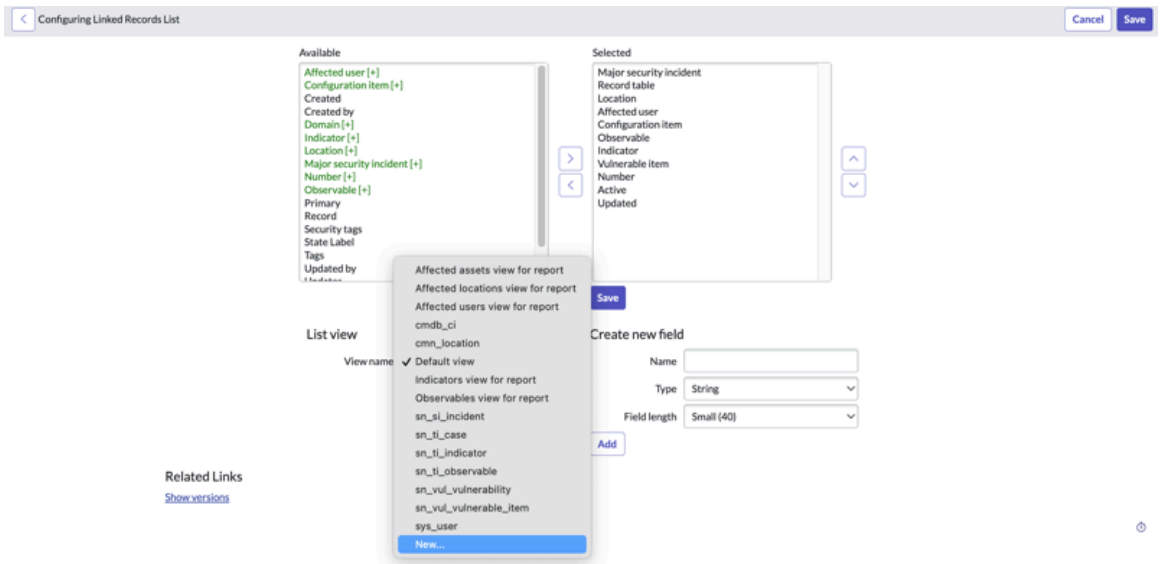
2. Clique com o botão direito do mouse no cabeçalho e selecione **Configurar** > **Layout de lista**.
   A página Configurando lista de registros vinculados é exibida.

Tradução automática

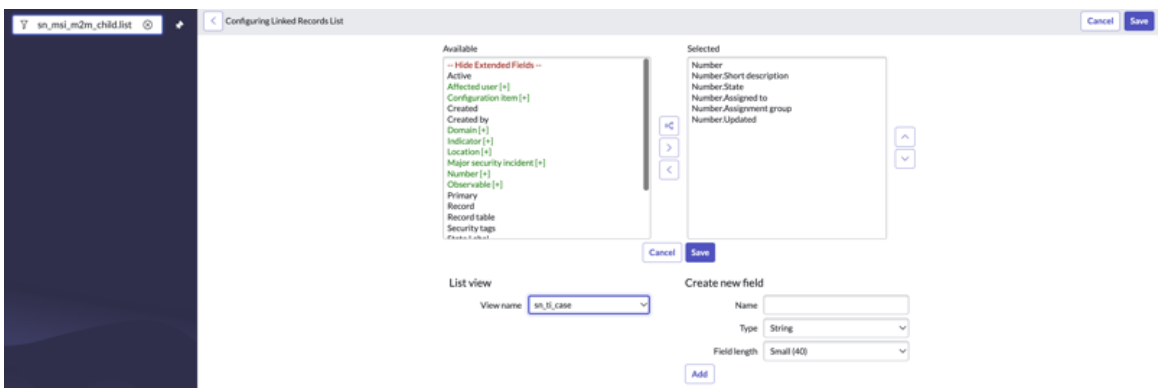
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Ir para **Exibição da lista** > **Nome de exibição**.
4. Selecione **Novo** na lista suspensa Exibir nome.



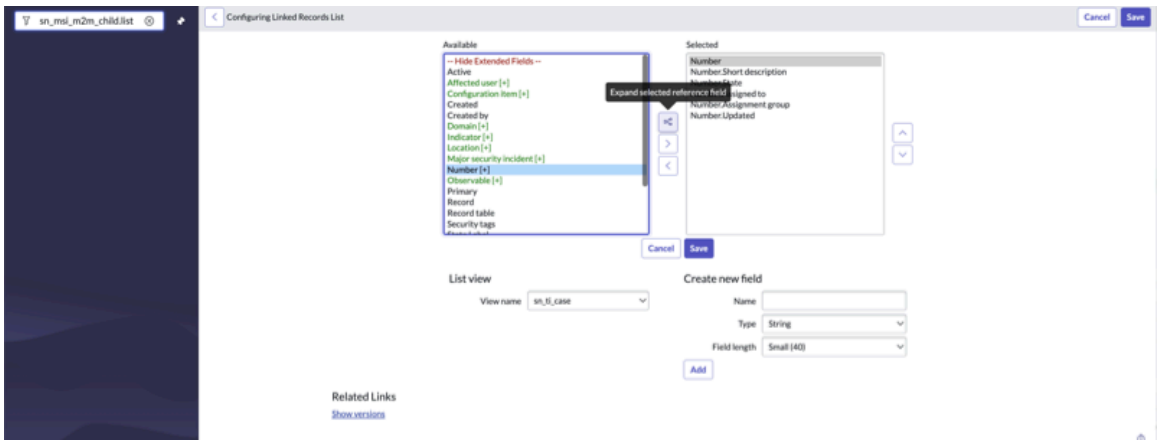
5. Selecione as colunas que serão renderizadas na exibição de lista do espaço.
   O registro de caso de segurança é armazenado na coluna **Número**. Para renderizar informações de um caso de segurança, você deve fazer referência com pontos na coluna **Número**.



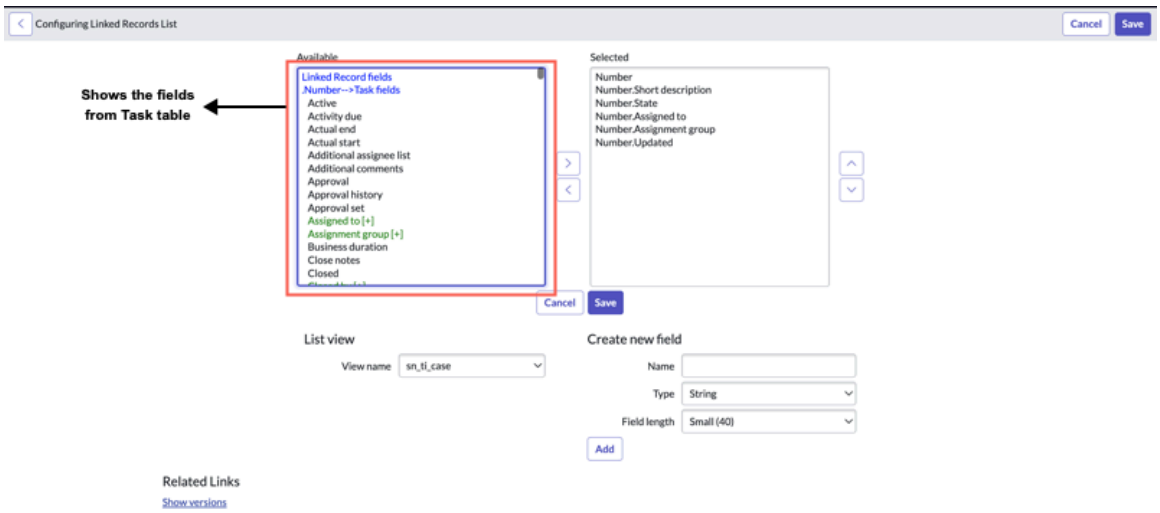
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para fazer referência com pontos, primeiro selecione a coluna **Número** na lista Disponível e clique em **Expandir campo de referência selecionado**.



b. Expanda as colunas de **Número** para selecionar e movê-las para a lista Selecionada.



c. Clique em **Salvar** para salvar e criar uma exibição.

6. A próxima etapa é renderizar a exibição criada no espaço Gestão de incidentes graves de segurança, você precisa criar uma **configuração de layout de lista**.

a. Pesquise a **configuração de layout de lista** usando a navegação à esquerda.

b. Clicar **Administração do MSI** > **Configurações de layout de lista**.

c. Clique em **Novo** para criar uma nova configuração.

d. Selecione a tabela de origem na coluna Tabela e selecione a exibição recém-criada no campo Exibição de lista.

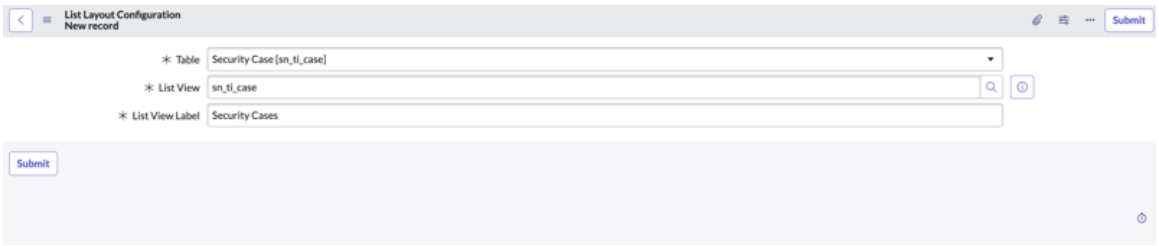
e. O rótulo **Exibição de lista** permite que você controle os rótulos quando a mesma tabela de origem é renderizada no espaço Gestão de incidentes graves de segurança.

f. Salve o registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Depois que o registro for salvo, navegue até o espaço Gestão de incidentes graves de segurança para exibir a exibição de lista renderizada e o rótulo no espaço.



Etapa 5. Adicionar listas de controle de acesso (ACLs) para usuários do espaço Gestão de incidentes graves de segurança

Adicione listas de controle de acesso (ACLs) para usuários do espaço Gestão de incidentes graves de segurança.

Antes de Iniciar

Função necessária: administrador

Nota: As permissões necessárias para vincular e desvincular capacidades são controladas pela função sn_msi.linkedsivi_read.

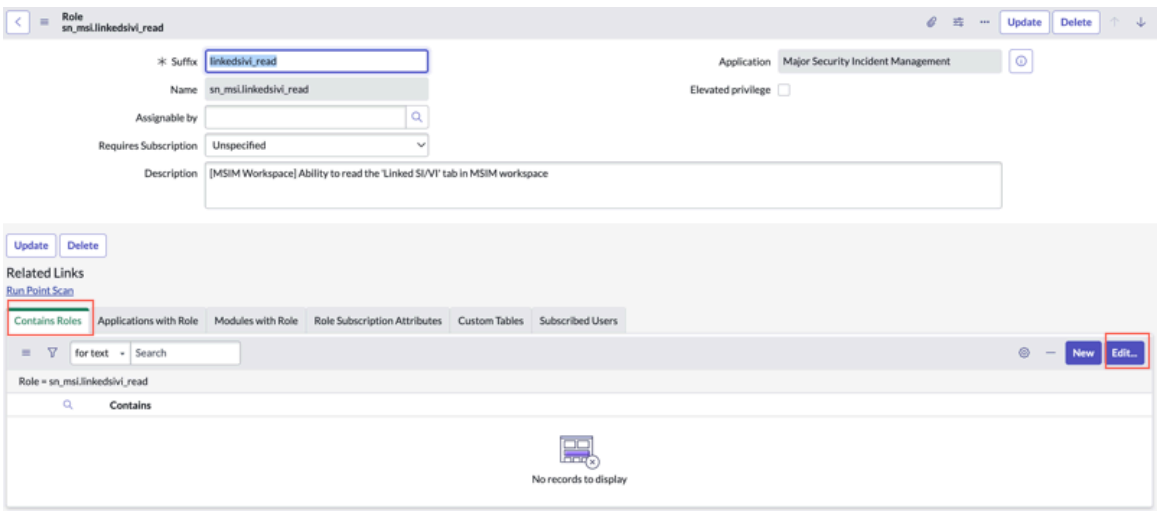
Gestão de incidentes graves de segurança persona contém a função sn_msi.linkedsivi_read.

1. sn_msi.workspace_admin (administrador do Espaço do MSIM)
2. sn_msi.workspace_manager (Gerente do espaço do MSIM)
3. sn_msi.workspace_responder (respondente do espaço do MSIM)

Nota: Para qualquer tabela de origem, você deve garantir que as funções necessárias sejam adicionadas à função sn_msi.linkedsivi_read.

Procedimento

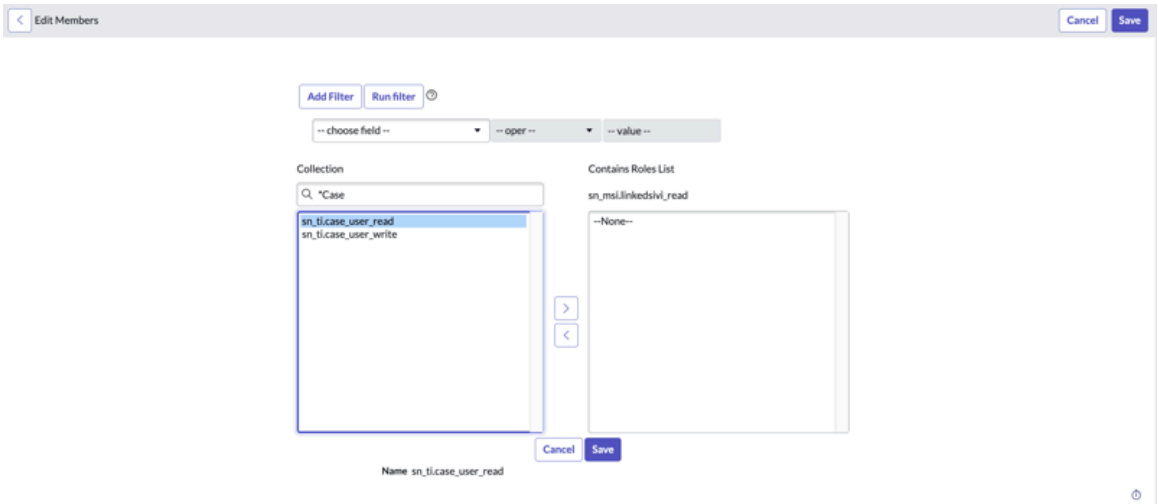
1. Navegar até **Administração de usuários** > **Funções** e pesquise a função **sn_msi.linkedsivi_read**.
2. Clique em **Editar** na seção da lista relacionada Contém funções.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Certifique-se de que as funções da tabela de origem sejam adicionadas na seção Contém funções.
   A página Editar Membros é exibida para configurar as funções necessárias para um caso de segurança.



4. Pesquise as funções da tabela de origem na seção Coleções.
   Selecione as funções necessárias que permitem o acesso de leitura e gravação na tabela de origem para um caso de segurança.

   Nota:

   - Para um caso de segurança, são necessárias duas funções separadas para leitura e gravação.
   - Acesso de gravação em tabelas para a capacidade de selecionar o registro de origem no espaço Gestão de incidentes graves de segurança vinculado ao modal de registro.

5. Clique em **Salvar** para adicionar funções.
6. Verifique se as funções foram adicionadas com sucesso à seção da lista relacionada **Contém funções**.

Etapa 6. Criar regras de negócio para um caso de segurança

Crie regras de negócio necessárias para um caso de segurança.

Antes de Iniciar

Função necessária: administrador

Crie as três regras de negócio a seguir para o novo caso de segurança da tabela de origem (sn_ti_case). Essas regras de negócio são necessárias para manter a consistência no comportamento com a tabela de origem fornecida pronta para uso, como Incidente de segurança (sn_si_incident).

Regras de negócio para a nova tabela de origem:

1. **Desativar link quando inativo**: depois que o caso de segurança for encerrado, as informações relacionadas não serão mais mostradas na página do espaço Gestão de incidentes graves de segurança.
2. **Sincronizar informações da equipe na atualização**: a guia Detalhes do incidente de segurança grave mostra as informações sobre todas as equipes e usuários ativos que trabalham em tarefas diferentes. Depois que atualizarmos o atribuído ao usuário ou

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

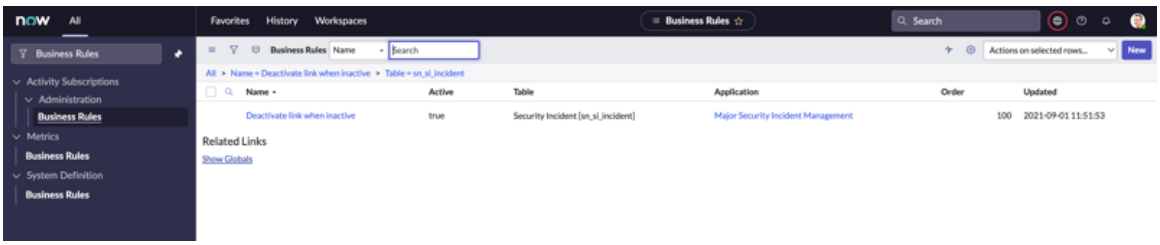
o grupo de atribuição for alterado no caso de segurança, precisamos atualizar as informações da equipe do caso de segurança na seção da equipe ativa do Incidente de segurança grave. Essas regras de negócio atualizarão o novo usuário atribuído e o grupo de atribuição na seção de equipe ativa.

3. **Sincronizar informações da equipe ao excluir**: a guia Detalhes do incidente de segurança grave mostra as informações sobre todas as equipes e usuários ativos que trabalham em tarefas diferentes. Depois de fecharmos o caso de segurança, não precisamos mais mostrar as informações da equipe do caso de segurança na seção da equipe ativa do Incidente de segurança grave. Essas regras de negócio removerão o usuário atribuído e o grupo de atribuição da equipe ativa.

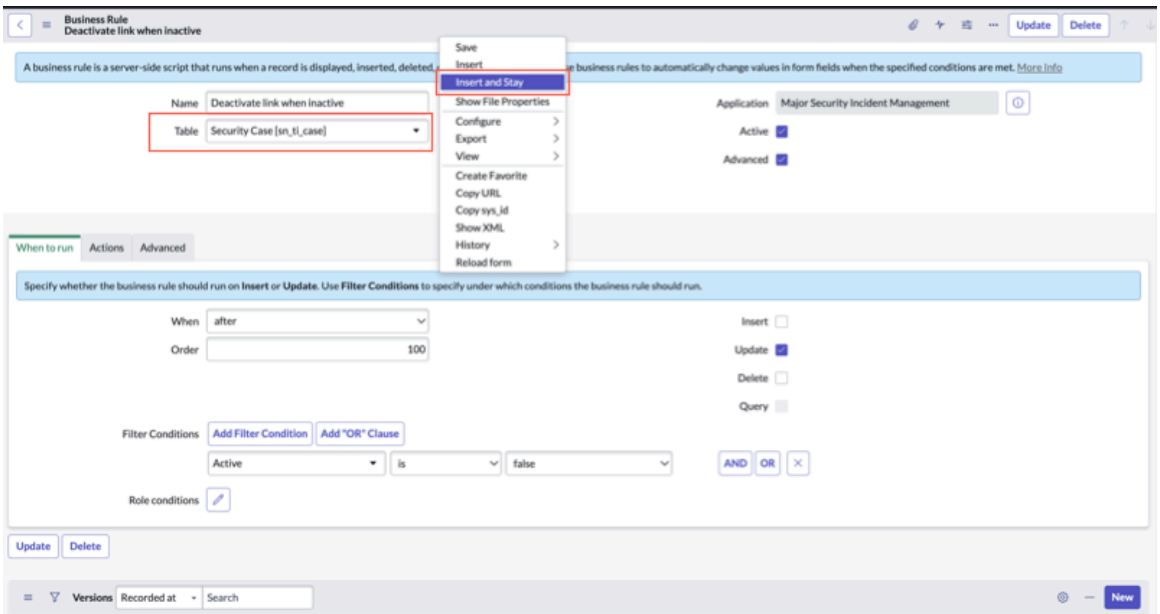
Crie regras de negócio para a nova tabela de origem:

Procedimento

1. Navegar até **Definição do sistema** > **Regras de negócio**.
2. Execute a opção de filtro para filtrar critérios de regras de negócio com as informações abaixo:
   - **Nome**: desativar link quando inativo
   - **Tabela**: sn_si_incident



3. Abra o registro e altere o nome da tabela para uma nova tabela de origem: sn_ti_case.
4. Clique com o botão direito do mouse no menu da página e clique em **Inserir e permanecer** para criar o registro.



5. Repita o procedimento para outras duas regras de negócio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Sincronizar informações da equipe ao excluir
- Sincronizar informações da equipe na atualização

Etapa 7. Criar configurações de registro de acúmulo

Crie uma configuração de registro de acúmulo para vincular e desvincular registros adicionais do MSI.

Antes de Iniciar

Função necessária: administrador e sn_msi.workspace_admin

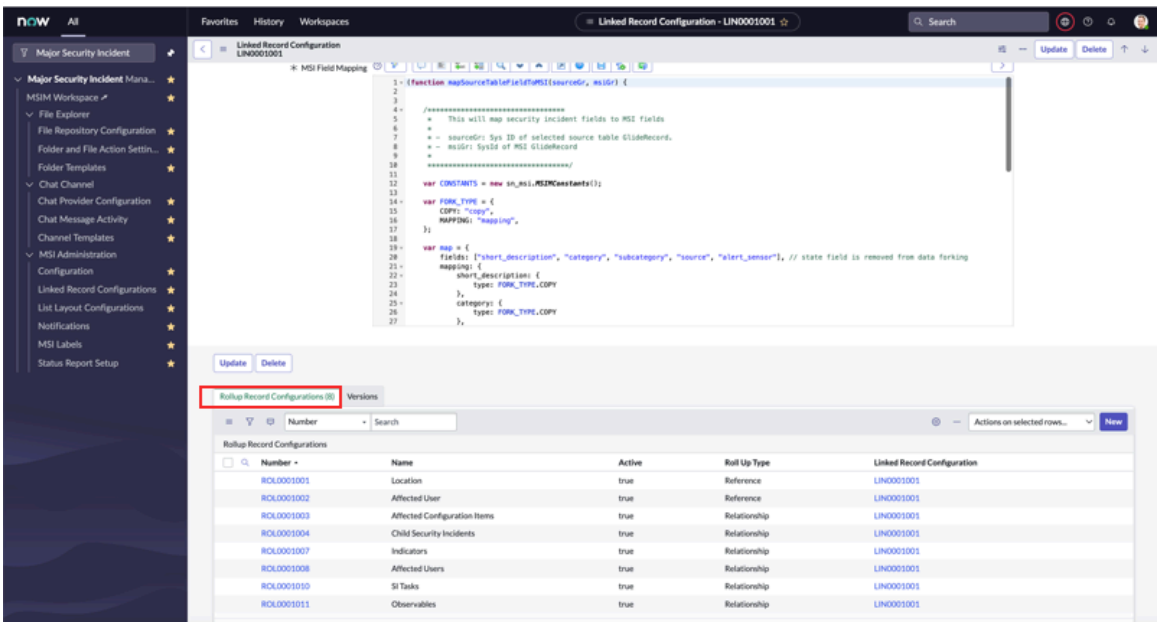
Nota: O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Para acumular informações, como itens de configuração, observáveis e indicadores de comprometimento relacionados a um caso de segurança, crie uma configuração de registro de acúmulo.

Procedimento

1. Navegar até **Resposta a incidentes graves de segurança** > **Configuração de registros vinculados**.
   A página Configurações de registro vinculado é exibida.
2. Selecione ou crie um novo registro vinculado e navegue até a seção **Configuração de registro** de acúmulo na mesma página.

Seção Configuração de registro de acúmulo



O que Fazer Depois

- Para obter informações mais detalhadas, consulte Configurar registros de acúmulo no Gestão de incidentes graves de segurança
- Para obter informações de exemplo de caso de segurança, consulteEscrevendo script para um caso de segurança

Escrevendo script para um caso de segurança

Escrever um script para um caso de segurança para acumular configuração de registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

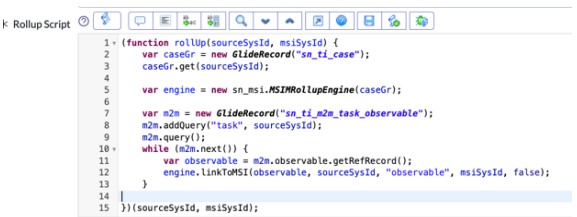
Função necessária: administrador e sn_msi.workspace_admin

Nota: O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Procedimento

1. Pesquise as configurações de registro vinculado usando a navegação à esquerda.
2. Navegar até **Administração do MSI** > **Configuração de registro vinculada**.
3. Abra o registro de configuração que foi criado para um caso de segurança.
4. A configuração do registro de acúmulo será exibida na seção Lista relacionada.
5. Clique em **Novo** para criar uma nova configuração de registro de acúmulo.

   Abaixo está um registro de exemplo criado para acumular dados de observáveis relacionados ao caso de segurança que estamos tentando acumular com os valores de campo como:

Nome	Descrição
Tipo de acúmulo	Relacionamento **Nota:** As informações do observável estão disponíveis em um formato de lista relacionada.
Script de acúmulo	A entrada sourceSysId contém o SYS ID do caso de segurança e msiSysId contém o SYS ID do incidente de segurança grave.  ◦ `Line 2: As a first step, query for Glide Record for sourceSysId from` **Security Case(sn_ti_case)** `table.` ◦ `Line 7: Next, query` **sn_ti_m2m_task_observable** `table using security case sys ID to figure out all the linked observables to a security case.` ◦ `Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method:`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	`MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkedRecordTable", "msiSysId", "isPrimaryRecord")`

Executar rollup atômico sob demanda

A estrutura de acúmulo não pode lidar com atualizações nos registros vinculados existentes. Nesses casos, o acúmulo atômico sob demanda deve acontecer para registros vinculados, o que pode ser obtido por meio de regras de negócio.

Para capturar atualizações para os registros vinculados, as regras de negócio devem ser criadas na tabela de origem.

Essas regras de negócio funcionam em operações de inserção, atualização e exclusão. Ao executar uma inserção ou atualização, você precisa adicionar ou atualizar as informações acumuladas para MSI. Se você excluir, as informações acumuladas serão removidas de MSI.

Por exemplo, quando um incidente de segurança estiver vinculado a MSI, as informações relacionadas serão acumuladas automaticamente MSI. Mais tarde, porém, se você adicionar um novo observável a um MSI, o observável recém-adicionado também será acumulado para MSI. Aqui, a regra de negócio **Sincronizar observável acumulado** captura a atualização e acumula o registro atualizado para MSI. Da mesma forma, a mesma regra de negócio também lida com a remoção dos observáveis acumulados existentes, se eles forem removidos do incidente de segurança.

Regras de negócio predefinidas

A seguir estão algumas regras de negócio predefinidas que ajudam você a entender como lidar com acúmulos atômicos

Regra	Descrição
Sincronizar indicador acumulado (sn_ti_m2m_task_indicator)	Use esta regra de negócio para lidar com o acúmulo e a remoção do indicador de comprometimento do incidente de segurança, caso de segurança e tarefa de correção.
Sincronizar observável acumulado (sn_ti_m2m_task_observable)	Usar esta regra de negócio lida com o acúmulo e a remoção de observáveis vinculados do Incidente de segurança, Caso de segurança e Tarefa de correção.
Sincronizar usuário afetado acumulado (sn_si_m2m_task_affected_user)	Usar esta regra de negócio lida com o acúmulo e a remoção de usuários afetados vinculados do incidente de segurança, caso de segurança e tarefa de correção.
Sincronizar IC afetado acumulado (task_ci)	Usar esta regra de negócio lida com o acúmulo e a remoção de itens de configuração associados do incidente de segurança, caso de segurança e tarefa de correção.

Tradução automática

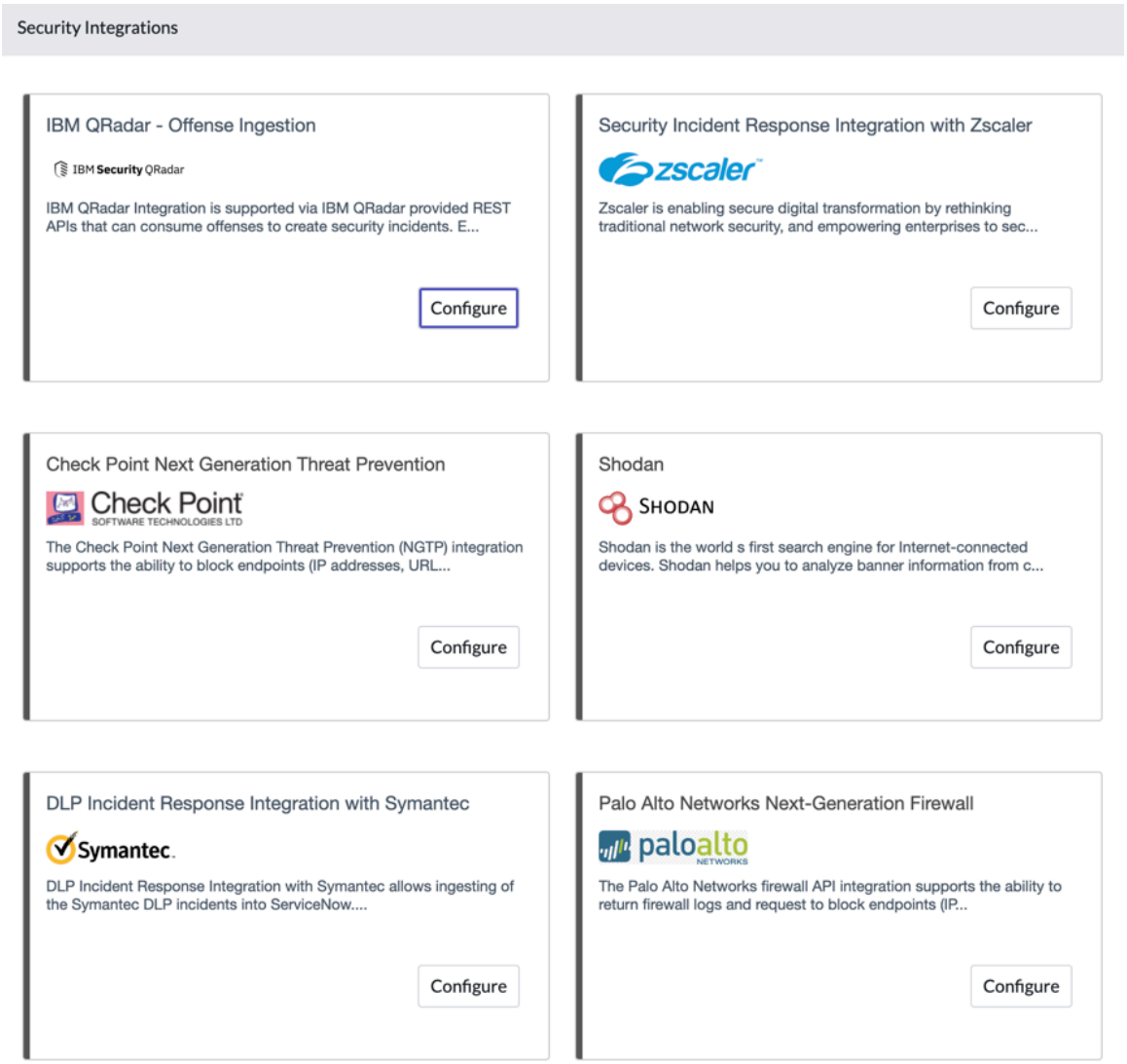
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Security Incident Response

Todas as Operações de segurança aplicações principais e integrações de terceiros não essenciais estão disponíveis na ServiceNow Store. Esta seção fornece instruções para ativar as integrações e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.

Configurações de Integração

O sistema base inclui uma série de "cartões" para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que tenham dependências de Operações de segurança plug-ins. Os cartões de integração podem ser exibidos selecionando **Operações de segurança** > **Configurações de Integração**.



Você pode filtrar as integrações visíveis usando o menu suspenso **Categoria**. O menu suspenso **Mostrar configurações** permite que você veja várias instâncias de implementações que permitem sua criação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Botões em cartões de integração

Os cartões de integração exibem botões diferentes, dependendo do estado atual da integração e da origem do cartão.

Botão	Descrição
Instalar Plug-in	Clique neste botão para instalar o plug-in aplicável para ativar a integração. Depois que o plug-in é instalado, o botão muda para **Configurar**.
Configurar	Clique neste botão para inserir informações para configurar a integração. Para algumas integrações, pode ser necessário inserir chaves de API ou URLs adquiridos do site da integração de terceiros.
Novo	Certas integrações, como Carbon Black e IBM QRadar, permitem que você defina várias implementações da mesma integração. Para essas integrações, clique em **Novo** depois que o plug-in for ativado. Os cartões permitem instalar plug-ins (quando aplicável) e configurar as implementações para uso.
Abrir página	No sistema base, sua instância executa uma consulta na ServiceNow Store para todas as aplicações que tenham dependências de Operações de segurança plug-ins. Quando esses aplicativos são encontrados e os plug-ins do aplicativo associados são ativados, os cartões de integração deles são exibidos com os outros cartões de integração de segurança. Clique em **Abrir página** para acessar o site da aplicação de terceiros para configurar a integração. Depois de concluir a configuração, o botão **Abrir página** mudará para **Configurar**.

ArcSight ESM Ingestão de eventos para integração Operações de segurança

A integração de ingestão de eventos ArcSight ESM com o produto Security Incident Response permite que os analistas de incidentes de segurança coletem eventos correlacionados e automatizem a criação de incidentes de segurança com a plataforma ServiceNow. Os dados são ingeridos continuamente com base em uma programação de pesquisa configurada e são usados por analistas para identificar e responder a possíveis ameaças à segurança cibernética.

Com essa integração, os eventos correlacionados que são candidatos a incidentes de segurança podem ser ingeridos periodicamente. Você pode mapear campos em eventos correlacionados para campos de incidente de segurança, visualizar a configuração de um evento como um incidente de segurança e configurar a ingestão programada de eventos para criar automaticamente incidentes de segurança de forma contínua.

Visão geral

Esta integração fornece a um analista do centro de operações de segurança (SOC) visibilidade para eventos de correlação em ArcSight ESM. Esses dados podem ser integrados a Now Platform incidentes de segurança do Security Incident Response (SIR) para investigação e correção adicionais. Os perfis são criados em sua instância Now Platform para lidar com diferentes tipos de eventos de correlação que são criados e disponibilizados por meio de visualizadores de consulta de correlação em ArcSight ESM. Esses perfis personalizam como diferentes ArcSight ESM campos de eventos correlacionados são exibidos em incidentes de segurança SIR.

Principais recursos

Esta integração inclui os seguintes recursos principais:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Crie vários perfis de ingestão de eventos para criar SIR incidentes de segurança para tipos específicos de ameaças, como malware e tentativas de acesso não autorizado.
- Mapeamento de arrastar e soltar de valores de campo de evento de correlação ArcSight ESM] para campos de incidente de segurança SIR associados.
- Uma visualização do layout de incidente de segurança SIR com base em eventos de correlação de amostra para validar os detalhes do mapeamento de eventos.
- Ingerir eventos de correlação histórica, bem como novos eventos notáveis em intervalos configuráveis.
- Filtrar eventos de correlação que não atendam a SIR critérios de geração de incidentes, por exemplo, eventos de baixa prioridade
- Agregue eventos a incidentes de segurança SIR existentes com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.
- Atualize eventos de correlação com base em SIR condicionais de criação e/ou fechamento de incidentes por meio de uma interface bidirecional.

Versões da Now Platform compatíveis

Esta integração é compatível com as versões New York Patch 6 e Orlando Now Platform.

As seguintes aplicações de Operações de segurança devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Estrutura de integração de segurança
2. Security Support Common
3. Resposta a incidentes de segurança
4. Ingestão de eventos e alertas para Operações de segurança
5. Plug-ins do Integration Hub
   a. Tempo de execução do hub de integração da ServiceNow
   b. Etapa de ação do hub de integração da ServiceNow - REST

Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

ArcSight ESM versões compatíveis

Esta integração foi testada com a versão 7.0.0.2436 do gerenciador ArcSight ESM. A integração é compatível com ambientes de serviço ArcSight ESM no local e em nuvem/ hospedado.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao serviço ArcSight ESM quando o servidor ArcSight ESM estiver implantado em sua rede corporativa. Se você estiver usando o serviço em nuvem ArcSight ESM, um MID Server não será necessário. Consulte o site de documentação de produtos da ServiceNow para obter mais informações sobre MID Servers.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referências

Referência	Identificador de documento	Título do Documento
1	ArcSight ESM documentação do produto	Documentação do produto ArcSight .
2	ServiceNow Site da documentação do produto	Site de documentação do produto da ServiceNow

Configure sua instância Now Platform® para a integração de ingestão de eventos ArcSight ESM

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação a partir do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As funções a seguir são necessárias para a instalação, configuração e uso da integração em sua instância Now Platform®. • Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®: ◦ Nomeia, cria e edita perfis de evento. ◦ Seleciona e mapeia valores de ArcSight ESM eventos de correlação para incidentes de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão contínua de eventos correlacionados. ◦ Habilita atualizações de eventos correlacionados quando um incidente SIR é criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre funções e como atribuir funções a usuários, consulte Funções no site de documentação de produtos da Servicenow .
Verifique se você está usando a versão 7.0.0.2436 ou posterior do gerenciador ArcSight ESM. Versões anteriores não são compatíveis.	Se você tiver acesso ao ArcSight ESM Query Viewer, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.
Configure o Visualizador de consulta em ArcSight ESM.	Antes de ingerir eventos de correlação, você deve configurar o Visualizador de consulta no console do ArcSight ESM. Consulte Configurar o ArcSight ESM Query Viewer para obter detalhes.
Opcional Crie fases personalizadas em ArcSight ESM para atualizações de eventos de correlação.	Um evento de correlação passa por várias fases em seu ciclo de vida antes de ser encerrado. ArcSight ESM fornece fases padrão como Inicial, Monitoramento, Em fila e Encerrado. Algumas dessas fases exigem entradas do usuário, mas outras fases são aplicadas automaticamente ao evento sem qualquer intervenção do usuário (o campo **Usuário obrigatório** está desmarcado no console ArcSight ESM. Você pode criar fases personalizadas que não exigem nenhuma intervenção do usuário e usá-las em sua instância Now Platform®. Consulte Opções adicionais: automatizar atualizações e fechamento de eventos correlacionados com base no status do incidente SIR para obter detalhes.
Verifique se você instalou e configurou uma aplicação do MID Server.	Aplicação de MID Server configurada Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço ArcSight ESM se o servidor ArcSight ESM estiver implantado em sua rede corporativa. Consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos ArcSight ESM para obter instruções sobre como configurar uma aplicação do MID Server. Consulte o MID Server para obter informações sobre MID Servers. Se você estiver usando um serviço hospedado ou em nuvem, que seja acessível pela Internet, um MID Server não será necessário.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	1. Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Ingestão de eventos e alertas para Operações de segurança: esta aplicação requer: ◦ com.glide.hub.integration.runtime => Tempo de execução do IntegrationHub da ServiceNow ◦ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **5.** Núcleo da ameaça Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação ArcSight ESM Ingestão de eventos de segurança para Operações de segurança a partir do ServiceNow Store para a integração.

Configurar o ArcSight ESM Query Viewer

Crie um visualizador de consulta e defina filtros que incluirão eventos de correlação criados recentemente que serão ingeridos ServiceNow.

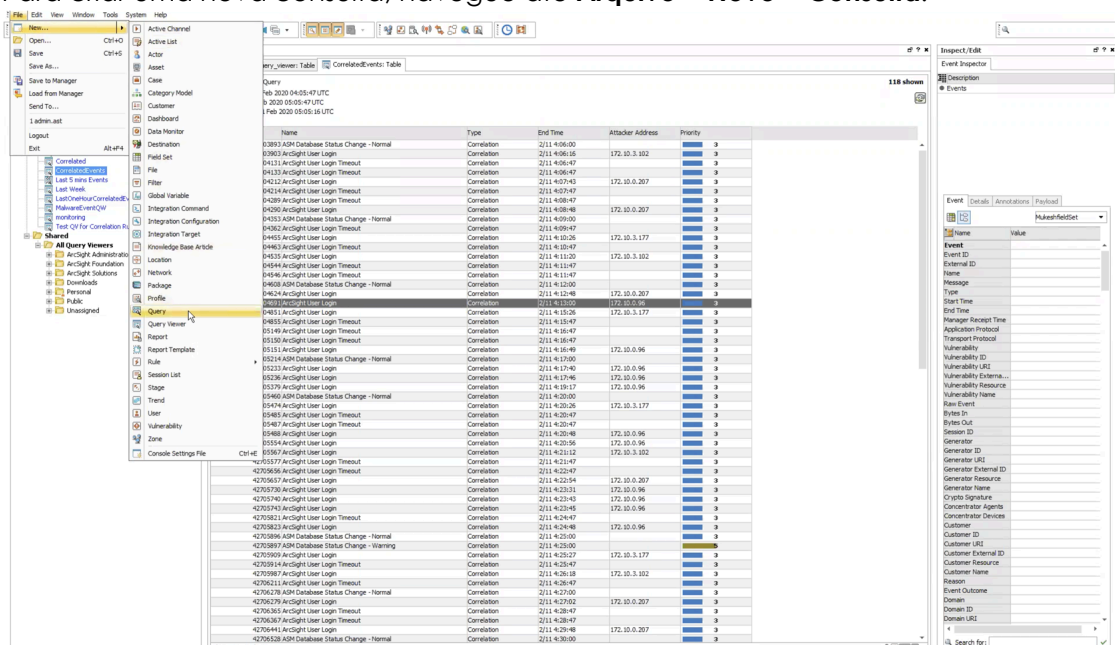
Antes de Iniciar

Função necessária: administrador do ArcSight

Procedimento

1. Faça login no console ArcSight ESM para criar um visualizador de consulta.

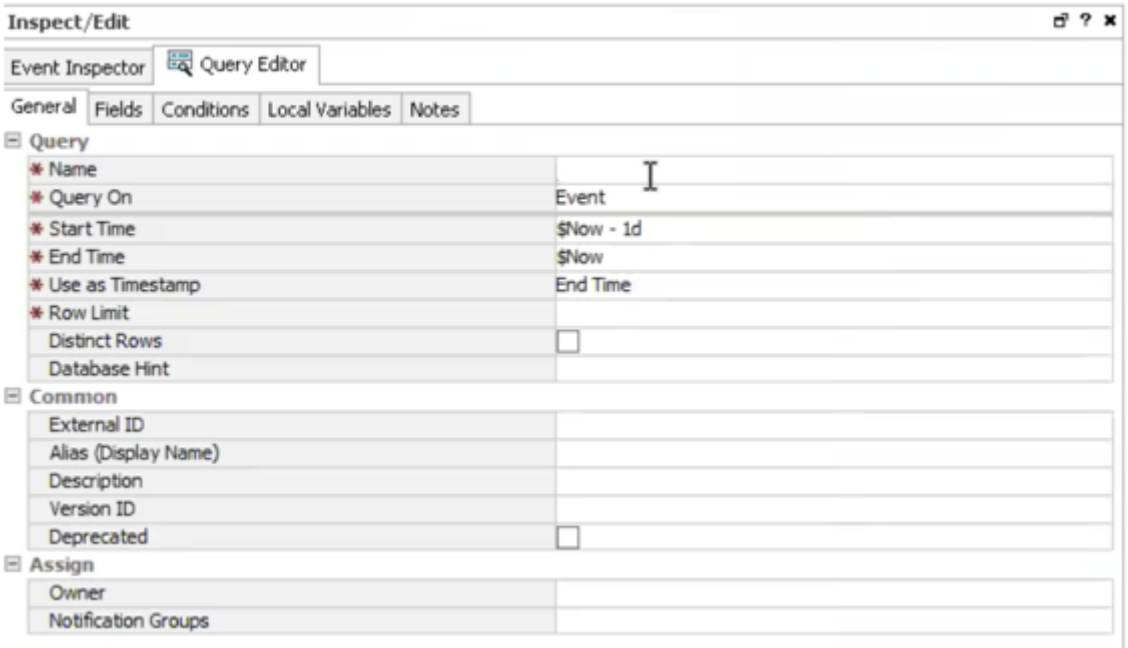
2. Para criar uma nova consulta, navegue até **Arquivo** > **Novo** > **Consulta**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Defina condições para o Visualizador de consultas no painel **Inspecionar/Editar**.

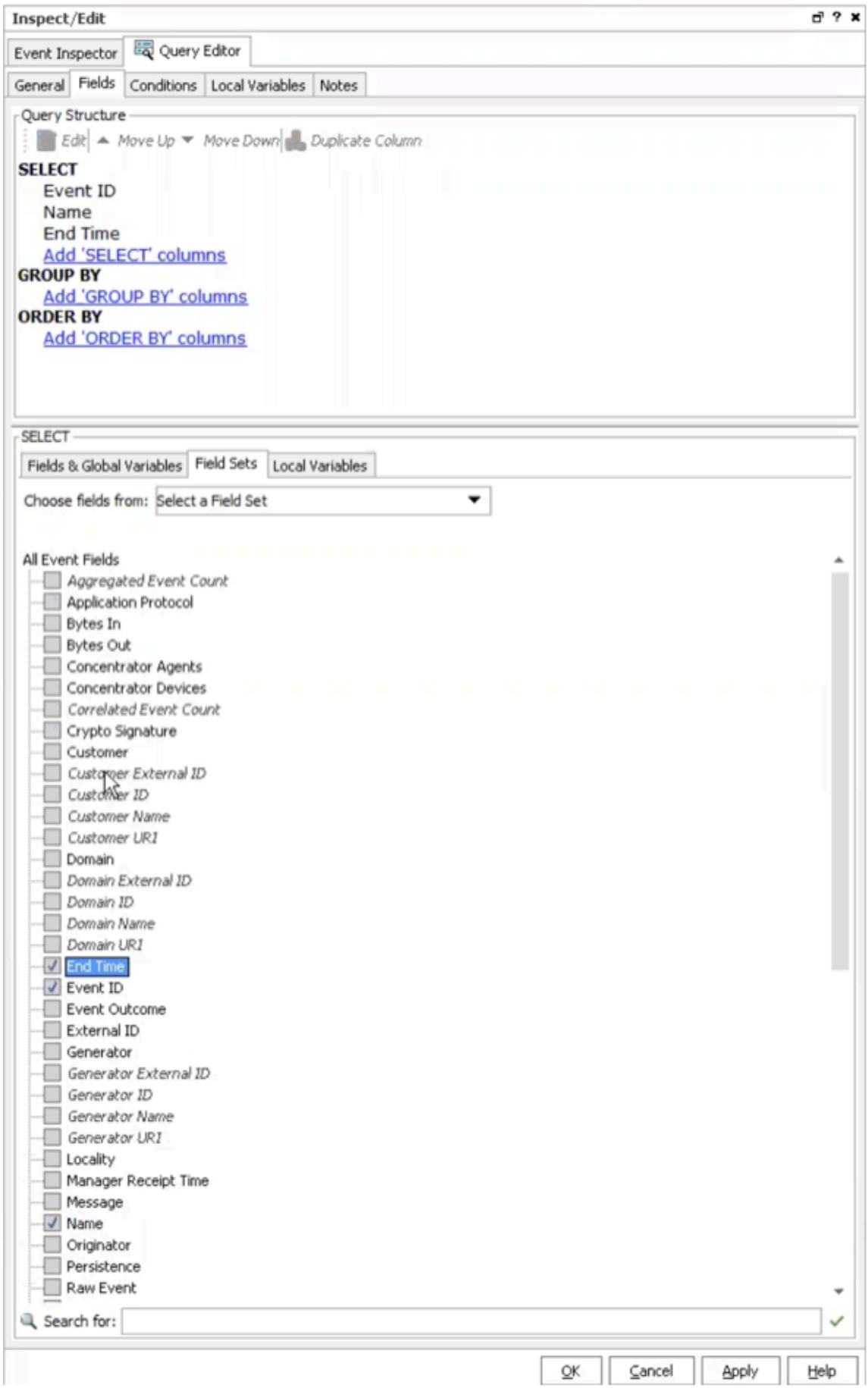


Nome do Campo	Descrição
Nome	Insira um nome para a consulta.
Consulta em	Selecione **Evento** na lista suspensa.
Hora de início	Para ingerir os dados mais recentes, selecione a data em que os eventos serão ingeridos. Especifique uma data que seja um dia ou alguns dias anterior à data atual. **Nota:** Você não pode especificar uma data que seja mais de 7 dias mais antiga que a data atual. Se você estiver ingerindo um grande número de eventos, deverá especificar uma data que seja 1 ou 2 dias mais antiga que a data atual.
Hora de término	Esta é a data atual.
Limite de linha	O número máximo de eventos que podem ser ingeridos por vez. Especifique um valor inferior a 5000 aqui.

4. Clique na guia **Campos**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

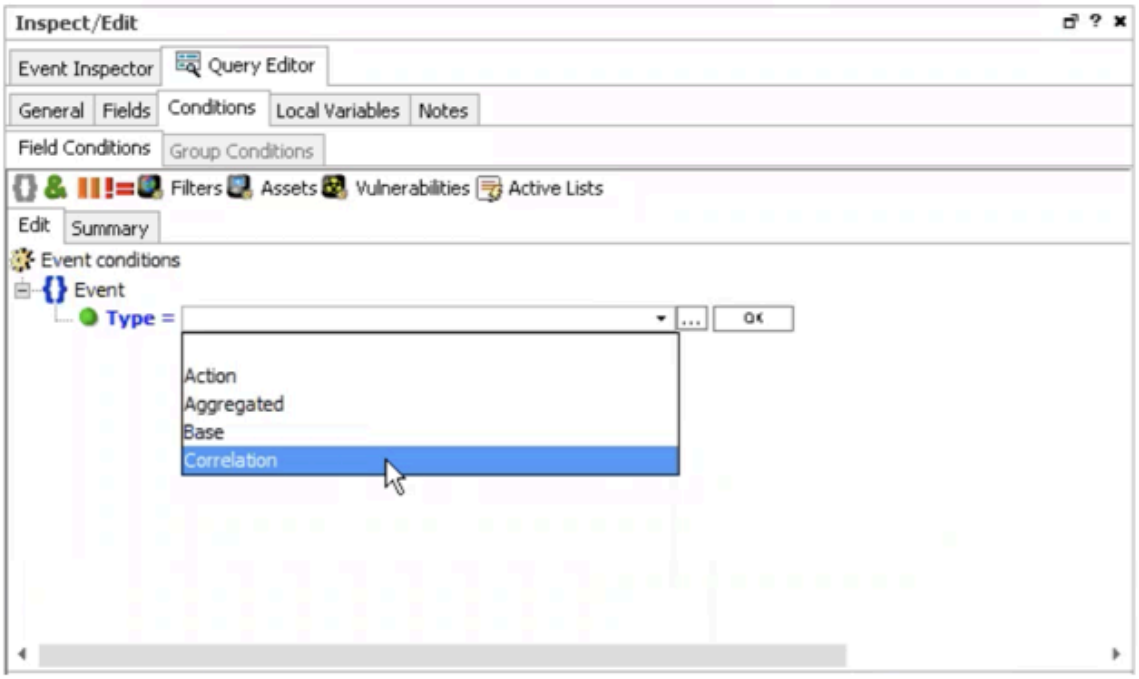


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os campos que devem ser incluídos durante a ingestão.
   Você deve selecionar os campos *ID do evento*, *Nome* e *Hora de término* para que a ingestão seja bem-sucedida.
6. Clique no link **Adicionar colunas "ORDER BY"**, selecione o campo **ID do evento** e especifique a ordem de classificação como **Decrescente** para garantir que os eventos mais recentes sejam ingeridos.
7. Clique na guia **Condições**.
8. Clique com o botão direito do mouse em **Evento** em **Condições de evento** na seção **Resumo**.
9. Clicar **Nova condição** > **Raiz** > **Tipo** e selecione o Tipo de evento como **Correlação**.

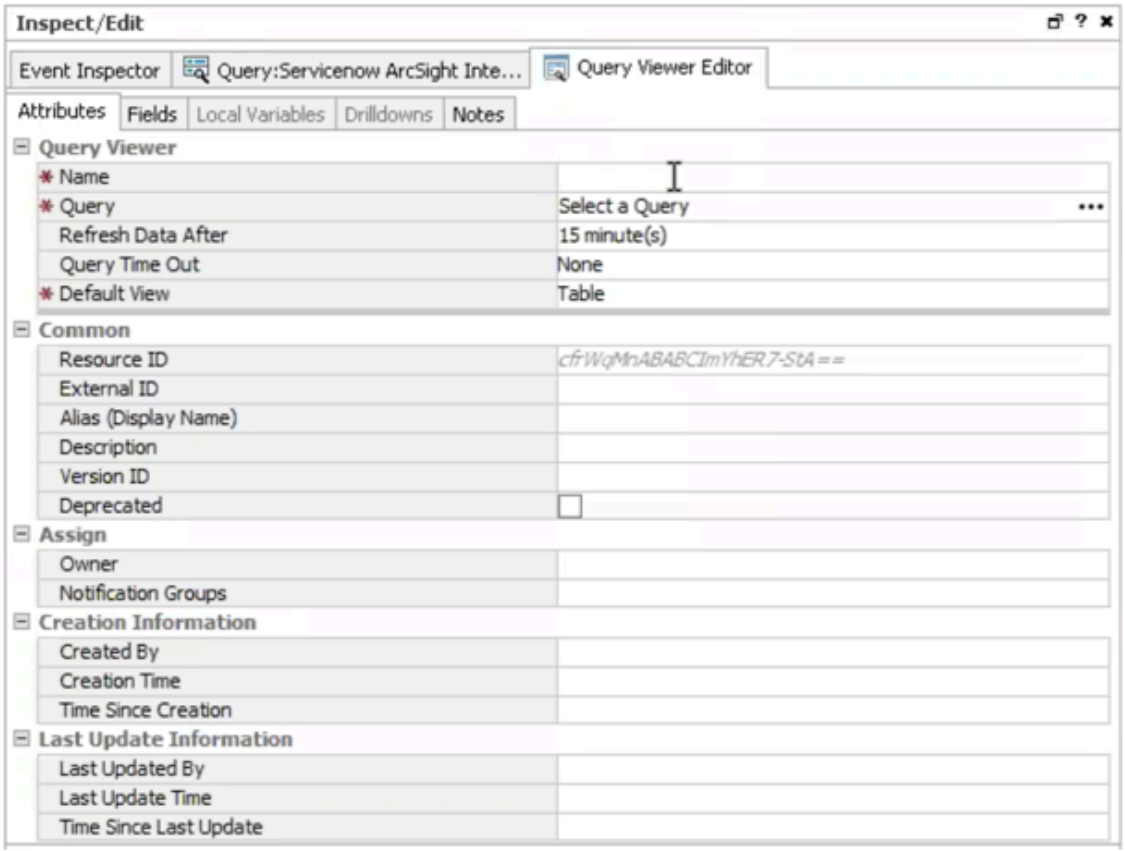
> **Importante:** Somente eventos de correlação serão recuperados; eventos de base para correlações não serão recuperados.



10. Clique em **OK** para salvar a consulta.
    A próxima etapa é criar um Visualizador de consulta para esta consulta.
11. Navegar até **Arquivo** > **Novo** > **Visualizador de consulta**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



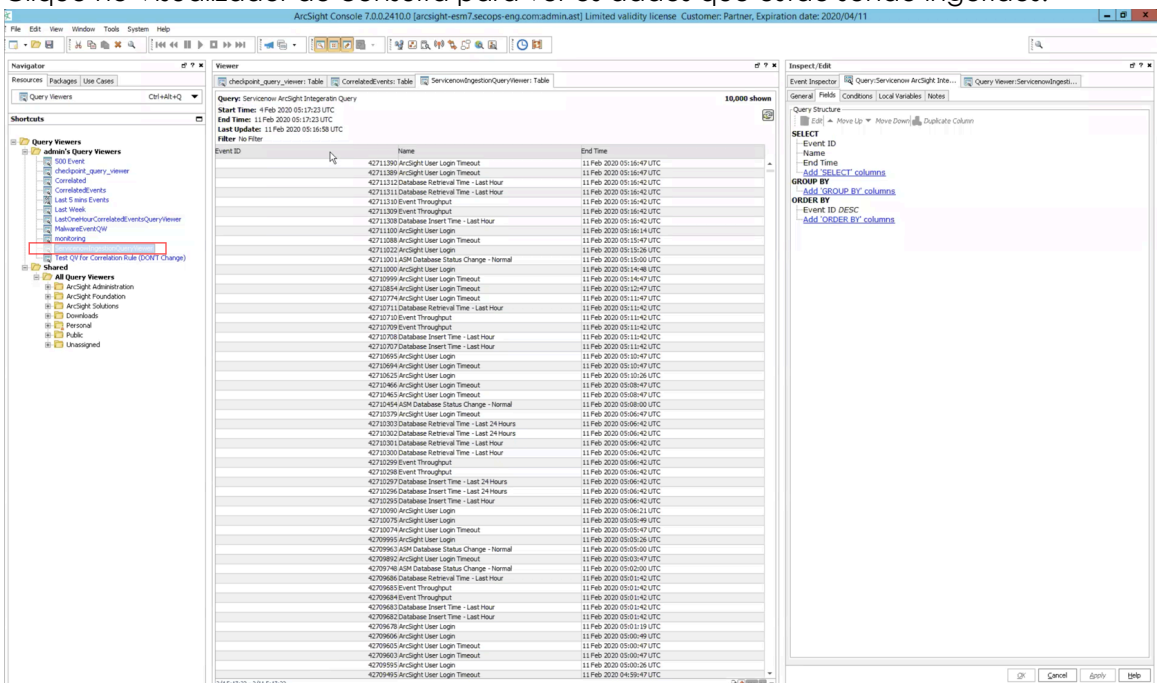
Nome do Campo	Descrição
Nome	Insira um nome para o Visualizador de consulta.
Consulta	Selecione a consulta que você acabou de criar.
Atualizar dados após	Especifique a frequência com que os dados devem ser atualizados.

12. Clique na guia **Campos** e certifique-se de que os campos obrigatórios (*ID do evento, Nome, Hora de término*) especificados na consulta estejam selecionados.
13. Clique em **Aplicar** para salvar o Visualizador de consulta.
    O novo Visualizador de consulta que você criou é listado na seção Visualizadores de consulta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

14. Clique no Visualizador de consulta para ver os dados que estão sendo ingeridos.



Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos ArcSight ESM

Antes de executar a integração em sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Operações de segurança em sua instância Now Platform.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se você não instalou a aplicação [ArcSight ESM de ServiceNow Store para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize o bloco ArcSight ESM.
3. Para configurar a aplicação, clique em **Novo**.
4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome exclusivo para o gerenciador ArcSight ESM que será usado na configuração do perfil de integração para distinguir entre várias origens do gerenciador ArcSight ESM, se necessário. Espaços são compatíveis com nomes, mas parênteses não são compatíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

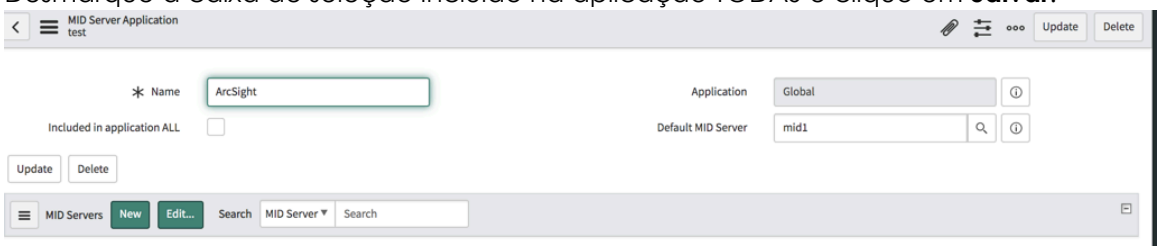
Campo	Descrição
URL do endpoint da API do ArcSight	URL do seu servidor ArcSight ESM Manager. Observe que a URL deve incluir a porta da API, por exemplo: `https://arcsight-esm.com:8443`
Nome de usuário da conta da API	Nome de usuário que você criou para sua conta de usuário de API no ArcSight ESM Console do gerenciador.
Senha da API	Senha que você criou para sua conta de usuário de API no ArcSight ESM Console do gerenciador.
Implantação no Local	O padrão é desmarcado. Se você estiver usando a versão baseada em nuvem do ArcSight ESM, que tem acesso direto à Internet, verifique se a caixa de seleção está desmarcada. Para uma implantação no local, marque esta caixa de seleção e especifique a aplicação do MID Server.
Aplicação do MID Server	Especifique um nome de aplicação do MID Server aqui. Esta aplicação de MID Server pode apontar para qualquer um dos MID Servers que foram configurados e qualquer MID Server disponível será usado. Se você não tiver uma aplicação de MID Server configurada, deverá criar uma nova aplicação de MID Server para esta integração. **Nota:** A aplicação do MID Server pode ser configurada somente por usuários com a função de administrador do sistema.

Para criar uma nova aplicação do MID Server, siga estas etapas:

a. Navegar até **MID Server** > **Aplicações** e clique em **Novo**.

b. Insira um nome para a aplicação do MID Server e selecione um MID Server a ser usado como padrão.

c. Desmarque a caixa de seleção Incluído na aplicação TODAS e clique em **Salvar**.

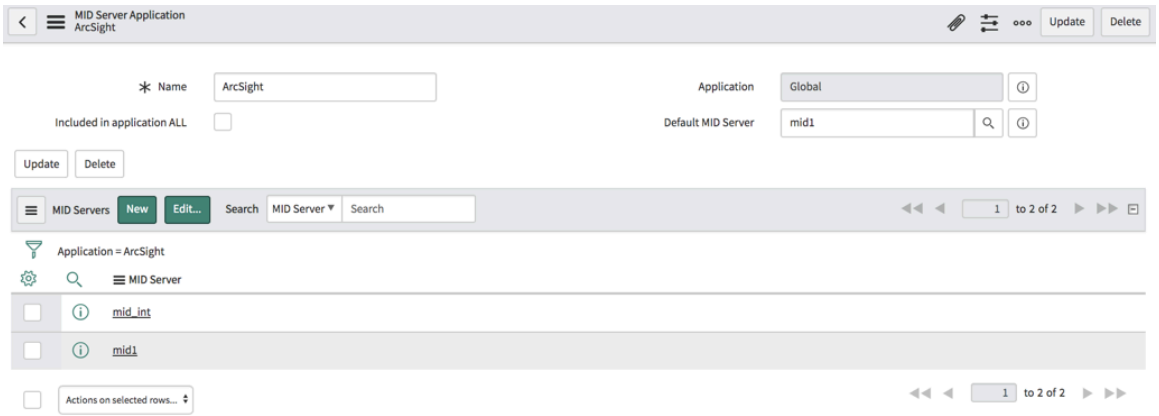


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

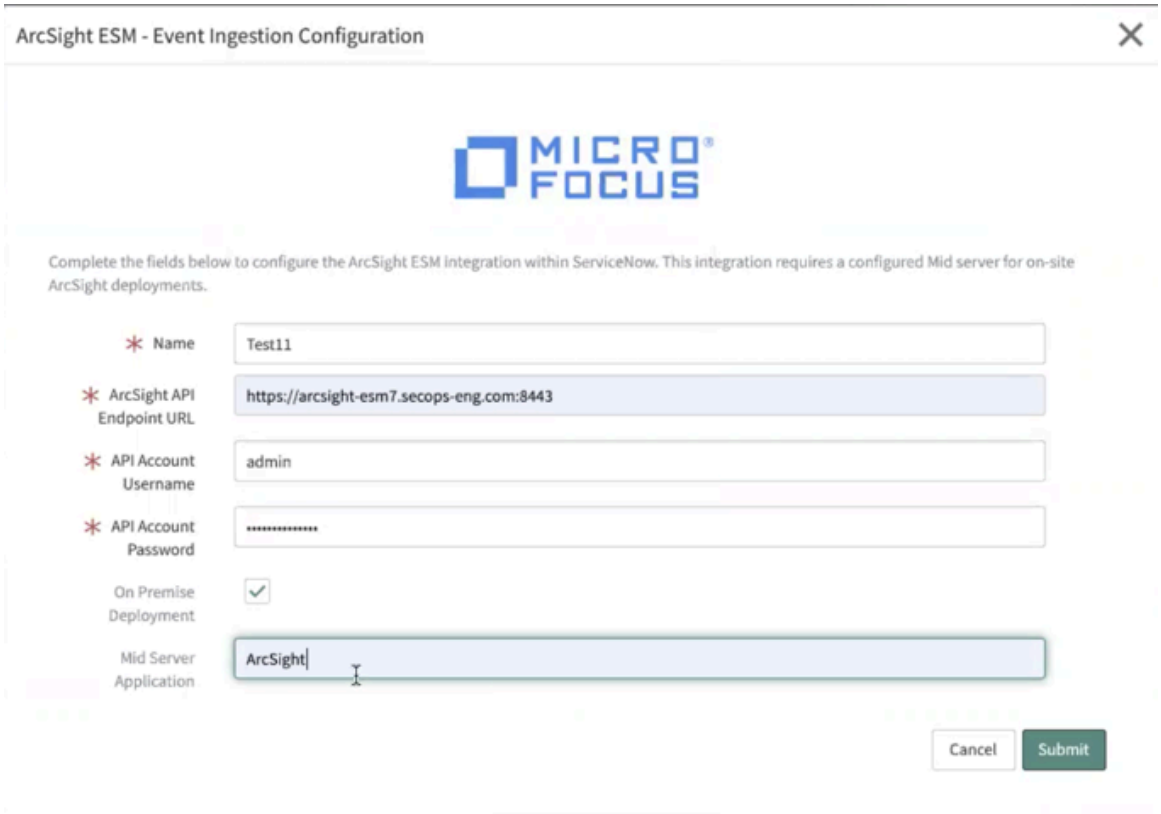
d. Clique em **Editar**. Na página **Editar Membros**, selecione todos os MID Servers disponíveis, mova-os para a Lista de MID Servers e clique em **Salvar**.

e. Os MID Servers selecionados serão listados conforme mostrado abaixo.



Dependendo da disponibilidade, um dos MID Servers configurados com a aplicação MID Server será usado.

6. Insira os detalhes da configuração e especifique a aplicação do MID Server que você criou.



Cada evento de correlação que você ingere do console do gerenciador ArcSight ESM requer um perfil de evento exclusivo em sua instância. No entanto, a origem ArcSight ESM que você configura no formulário Configuração de ingestão de eventos pode ser reutilizada para vários perfis, desde que cada perfil ingere tipos de evento de correlação exclusivos.

7. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de ser validada e enviada com sucesso, cada configuração de servidor ArcSight ESM é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Criar um perfil para ArcSight ESM integração de ingestão de eventos de correlação

Como um usuário com a função sn_si.admin, você cria um perfil em sua instância Now Platform e determina quais eventos de correlação criam incidentes de segurança. Antes que os incidentes de segurança Now Platform Security Incident Response (SIR) sejam criados a partir de eventos de correlação, os valores de campo dos eventos são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será criado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Os eventos de correlação são ingeridos automaticamente no ambiente Operações de segurança da sua instância Now Platform, dependendo do tipo de perfil definido. Um perfil é um encapsulamento de um tipo de evento de correlação, como tentativas de acesso não autorizado ou malware.

Depois que um evento de correlação tiver sido ingerido, você poderá mapear campos de evento de correlação individuais para campos correspondentes no incidente de segurança. Você pode filtrar eventos de correlação para especificar quais eventos criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para eventos de correlação identificados como de alto risco. Você também pode definir critérios de agregação de eventos adicionais para que os eventos de correlação duplicados de entrada sejam agregados a um incidente de segurança aberto. Por fim, você pode definir uma programação de ingestão e ativar o perfil.

Os nomes dos perfis de evento em sua instância Now Platform devem ser exclusivos e só podem ser mapeados para um perfil de evento ativo por vez.

Criar e nomear o perfil para ArcSight ESM integração de ingestão de eventos

Você pode configurar um perfil para ingerir eventos de correlação.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil de evento para um evento de correlação em sua instância Now Platform, navegue até **Integração do ArcSight ESM** > **Perfil de evento do ArcSight ESM**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

Tradução automática

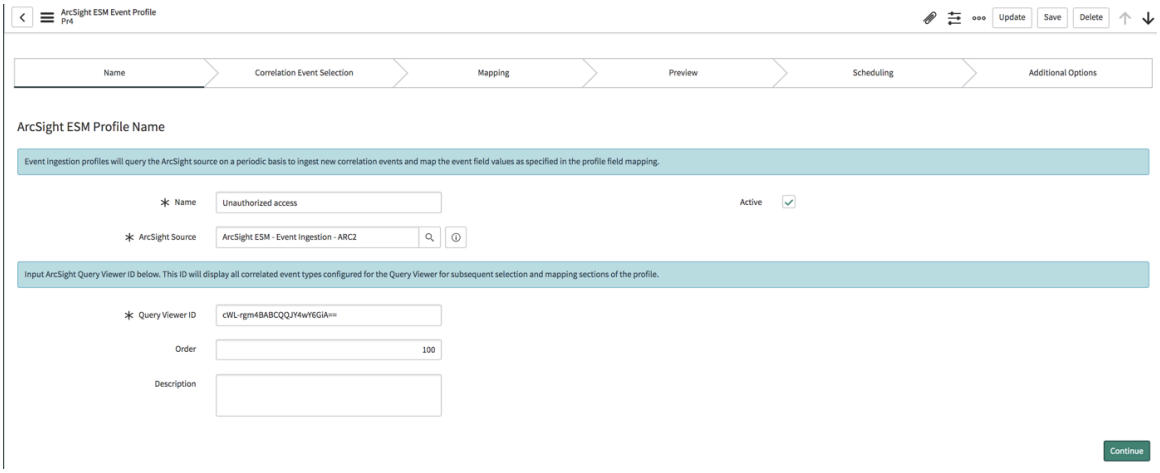
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e nomes de perfil duplicados não serão salvos. Os nomes de perfil em sua instância Now Platform devem ser exclusivos.
Ativo	A caixa de seleção está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo e a ingestão não ocorrerá. **Nota:** Você deve concluir todas as seções no perfil antes de torná-lo ativo.
Origem do ArcSight	O servidor ArcSight ESM configurado durante a etapa de autenticação inicial. Se você tiver vários servidores ArcSight ESM configurados, selecione o servidor apropriado para os tipos de evento de correlação que serão ingeridos para o perfil. É necessário selecionar um valor.
ID do visualizador de consulta	Insira o ID do recurso do Visualizador de consulta configurado no ArcSight ESM Console. O ID do recurso é um identificador exclusivo para qualquer Visualizador de consulta configurado no servidor ArcSight ESM. Depois que o ID do recurso for enviado, o nome da Exibição de consulta será retornado para garantir que o Visualizador de consulta correto tenha sido selecionado. Consulte a seção abaixo para obter uma exibição de captura de tela de como determinar o ID do recurso do Visualizador de consulta selecionado em ArcSight ESM.
Ordem	O padrão é 100. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem as mesmas condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

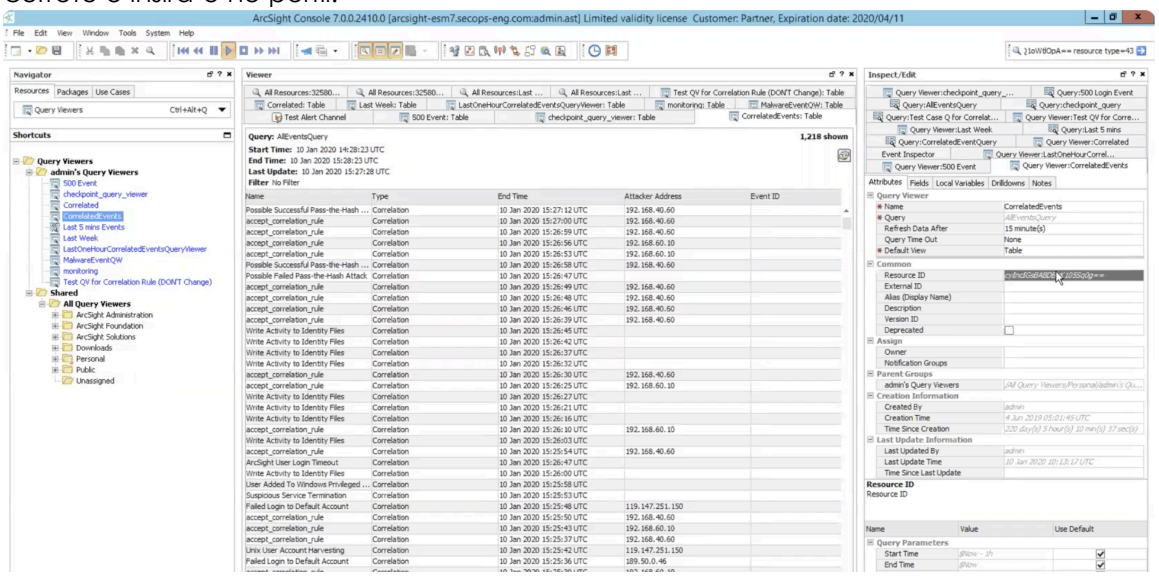
A figura a seguir é um exemplo de um formulário preenchido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois de inserir os detalhes do perfil, clique em **Continuar**. O ID do Visualizador de consulta é validado e se um ID de recurso correspondente estiver presente no ArcSight ESM Visualizador de consulta, o nome do Visualizador de consulta será retornado conforme mostrado abaixo. Se a validação falhar, verifique se o ID do recurso existe no console ArcSight ESM. Se o ID do recurso não for encontrado, encontre o ID do recurso correto e insira-o no perfil.



Tradução automática

O que Fazer Depois

A próxima etapa é selecionar os tipos de evento de correlação para ingestão no Visualizador de consulta selecionado na etapa anterior.

Selecione eventos de correlação para ArcSight ESM integração de ingestão de eventos

Com base na origem ArcSight ESM e no Visualizador de consulta configurado, selecione uma regra de evento de correlação para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba os eventos de correlação disponíveis listados na Seleção de eventos de correlação na sua instância da Now Platform para que você possa determinar quais eventos de correlação deseja ingerir e criar incidentes de segurança. Você só pode selecionar um tipo de regra de correlação na lista para cada perfil.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ID do visualizador de consulta e o nome do visualizador de consulta conforme especificado no formulário do visualizador de consulta são exibidos. Selecione um evento de correlação na lista que você pode usar para criar um mapeamento de configuração para o evento correlacionado ingerido.

Clique na lista suspensa no campo Lista de eventos de correlação. Uma lista de eventos de correlação que estão presentes no ArcSight ESM Query Viewer Console é exibida.

Clique em **Continuar** para prosseguir para a próxima etapa no assistente.

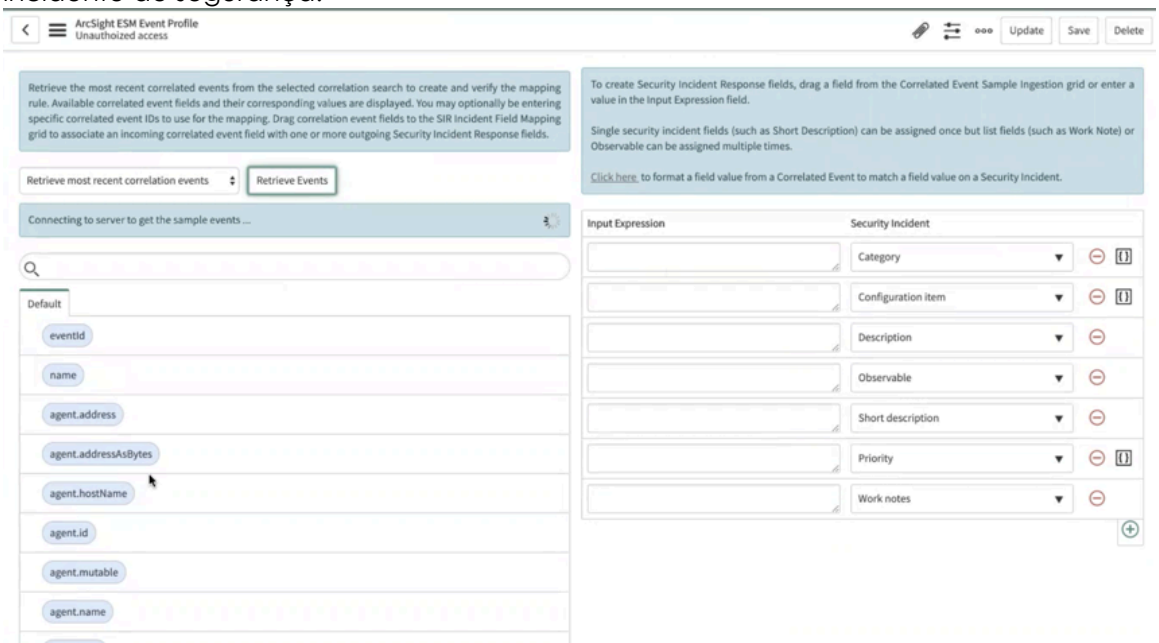
Mapeamento de campos de evento de correlação para a integração de ingestão de eventos ArcSight ESM

Depois de identificar a regra de evento de correlação específica na lista, a próxima etapa é mapear campos de evento de correlação para os campos no formulário de incidente de segurança.

Visão geral

Para a etapa de mapeamento, você pode ingerir eventos de correlação de amostra para a regra de correlação selecionada. Durante esta fase de mapeamento, você pode garantir que todos os dados de campo de evento de correlação relevantes estejam mapeados para o local apropriado no formulário de incidente SIR e, em seguida, visualizar o incidente SIR na seção de visualização.

A figura a seguir mostra a configuração de mapeamento padrão fornecida para criar o perfil de evento de correlação. Você pode personalizar os campos que preenchem o incidente de segurança.



Quando você clica em **Recuperar eventos**, os nomes do campo de evento de correlação e os valores correspondentes são preenchidos no lado esquerdo do formulário. Estes são os campos de evento de correlação ArcSight ESM que estão disponíveis para mapeamento para os campos de incidente de segurança.

Você pode preferir revisar alguns eventos de correlação de amostra no console para ingerir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada como Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento. Você pode ingerir até cinco eventos de correlação de amostra do gerenciador ArcSight ESM para a regra de correlação selecionada para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ajudar no processo de mapeamento de campo. Há opções para ingerir os cinco eventos de correlação mais recentes para o evento de correlação selecionado ou ingerir até cinco eventos de correlação específicos com base nos IDs de evento.

Abaixo está um resumo das etapas necessárias para mapear eventos de correlação:

- Mapeamento de campo: edite a configuração de mapeamento arrastando os campos de evento de correlação do lado esquerdo e soltando-os na seção de mapeamento de incidente SIR à direita. O mapeamento à direita associa o campo de evento de correlação de entrada a um campo de incidente de segurança de saída.
- Experiência de mapeamento: personalize a grade de mapeamento adicionando ou removendo campos usando o ícone + na parte inferior da seção de mapeamento de campo de incidente SIR. Rastreie campos ignorados ou mapeados anteriormente com a codificação de cores fornecida (os campos mapeados estão esmaecidos e os campos azuis não estão mapeados).
- Condições de geração de incidentes: quando a seção de mapeamento estiver concluída, você poderá definir condições de filtro para filtrar quais eventos de correlação devem criar incidentes de segurança versus eventos de correlação que devem ser filtrados, por exemplo, eventos de correlação de baixa prioridade. Isso é feito na seção Condições de geração de incidentes localizada abaixo da seção Ingestão de amostra de evento de correlação.
- Critérios de agregação de eventos: defina critérios de agregação de eventos adicionais que agregam um evento de correlação de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de eventos notáveis de segurança relacionados em um único incidente de segurança.
- Conversão de campo de formato: em determinados casos, os valores de campo de evento no evento de correlação ArcSight ESM podem não ser convertidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos.

  Por exemplo, com o editor de script, um valor de categoria de Alerta de Malware e Infecção de Vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos para uma Atividade de Código Mal-intencionado comum no campo Categoria no incidente de segurança SIR usando o Funcionalidade Formatar tradução de campo.

A próxima etapa é ingerir eventos de correlação de amostra e mapear valores para os campos de incidente de segurança SIR.

Criar mapeamentos para ArcSight ESM integração de ingestão de eventos

Nesta etapa, você ingere eventos de correlação de amostra e mapeia valores para os campos de incidente de segurança SIR.

Antes de Iniciar

Função necessária: administrador, sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, você pode revisar até cinco eventos de correlação de amostra da coluna Ingestão de amostra de evento de correlação à esquerda do formulário para ajudar no mapeamento e na conversão de valores de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

campo de evento para os campos de incidente de segurança no Incidente de SIR Coluna Mapeamento de campo à direita.
Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos exibidos por padrão são normalmente campos importantes a serem preenchidos no formulário de resposta a incidentes de segurança. No entanto, esses campos podem ser removidos e quaisquer campos adicionais podem ser exibidos usando os botões + e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. A personalização dos campos permite mapear ArcSight ESM campos que não são exibidos na grade de mapeamento padrão no incidente de segurança.

Procedimento

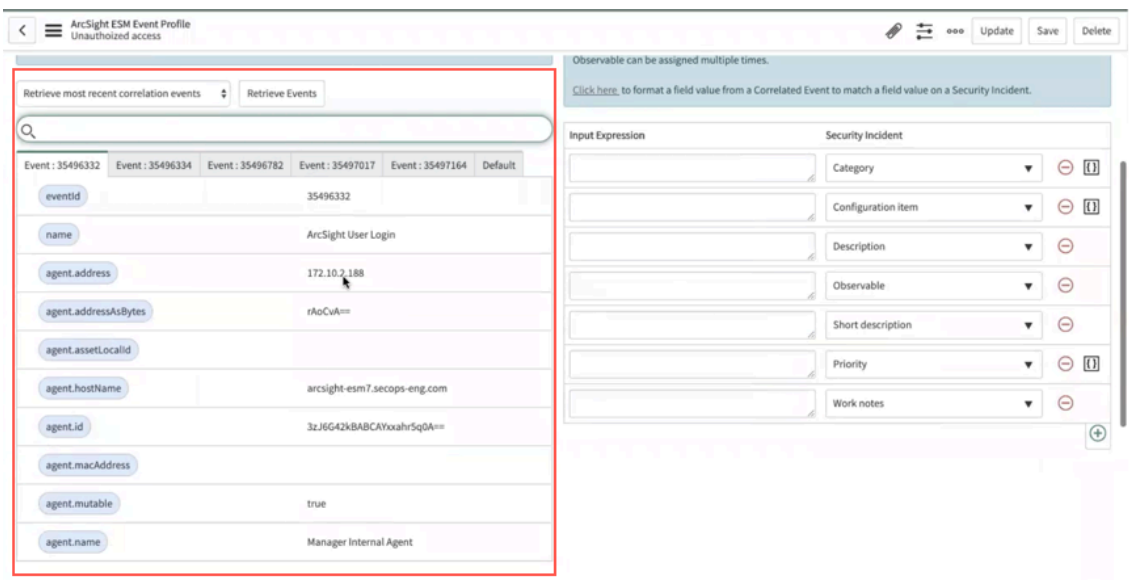
1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair os eventos de correlação de amostra mais recentes para a regra de correlação selecionada ou fornecer os IDs de evento de correlação exclusivos para os eventos de correlação específicos que você deseja usar para sua experiência de mapeamento de eventos de correlação.
3. Na lista suspensa, selecione uma das seguintes opções:
   - Recuperar eventos de correlação mais recentes
   - Selecionar eventos de correlação com base no ID do evento

   Clique **em Recuperar eventos** para extrair os eventos de correlação de amostra mais recentes do console ArcSight ESM para a regra de pesquisa de correlação selecionada.

   Os campos de evento de correlação e os resultados dos valores são exibidos como guias individuais.

   A extração de eventos de correlação de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

   Na figura a seguir, os pares de valores de nome de campo para o evento de correlação ingerido ou os eventos de amostra importados são exibidos no lado esquerdo deste formulário após a conclusão da extração de ingestão. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.



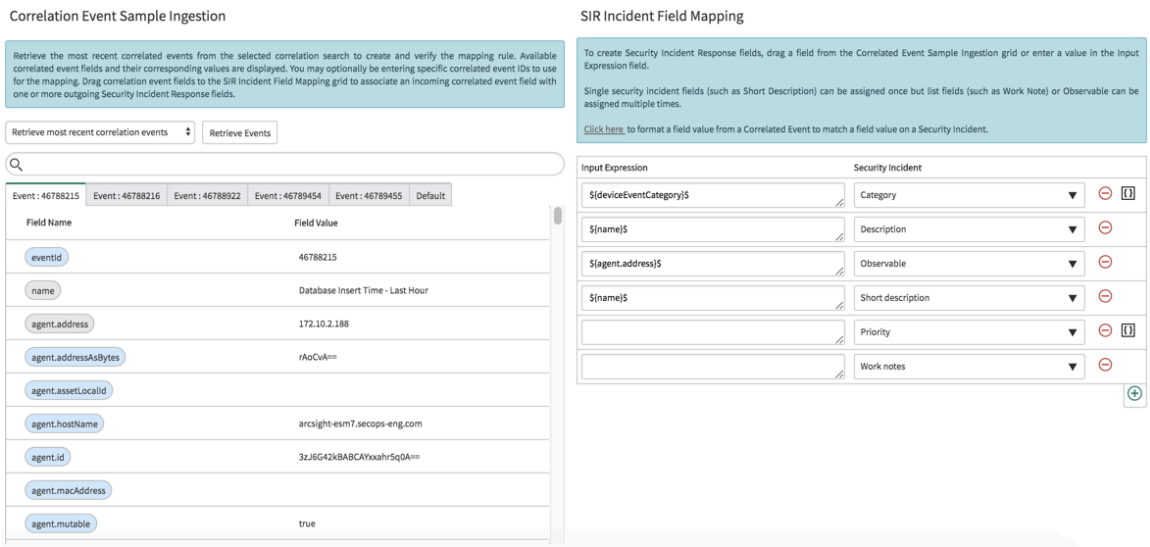
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
5. Arraste o nome do campo, por exemplo, `agent.hostname`e solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

   Para ajudá-lo a garantir que nenhum campo de evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Os campos em azul claro à esquerda indicam que um campo de evento de correlação ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de correlação de entrada a mais de um campo em um incidente de segurança.

   Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear quais campos de evento já foram utilizados para mapeamentos de campo de incidentes de segurança futuros.



6. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

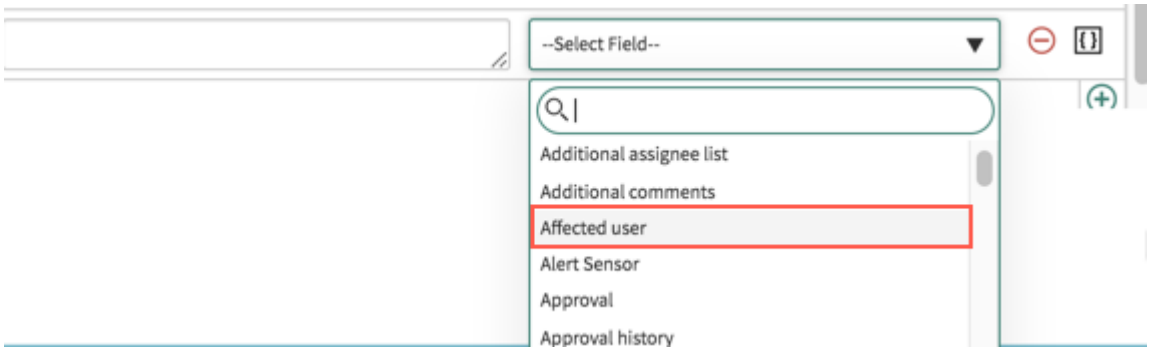
   a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de mais.
   Um novo campo é exibido.

   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

   Na lista de seleção expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, o `usuário afetado` tem um plano de fundo cinza porque foi mapeado no incidente de segurança. Semelhante à codificação de cores para os campos de eventos de correlação no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente SIR já mapeados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o **ID do evento** desejado no campo **Expressão de entrada**.
Com o recurso de arrastar e soltar, mapeie-o ao lado do novo campo.

7. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de scripts, consulte Use o editor de script para formatar valores de evento de correlação para integração ArcSight ESM.**Condições de filtragem de geração de incidente**

8. Opcional: Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um evento de correlação de entrada deve satisfazer para criar um incidente de segurança SIR.
Para definir condições de geração de incidentes, siga estas etapas.

a. Role até a seção Condições de geração de incidente no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

(Optional) O Construtor de condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

As opções nas listas de seleção do primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de evento de correlação para os eventos que você ingeriu. Esses campos são dinâmicos e mudam dependendo dos eventos de correlação que você ingere. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores do evento de correlação ArcSight ESM.

Tradução automática

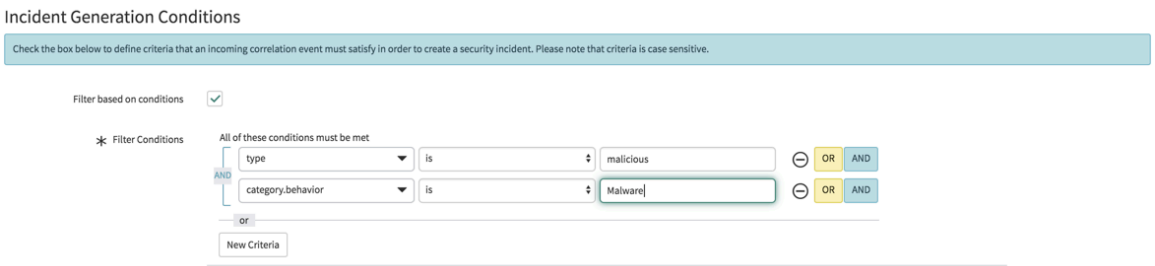
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando as listas de seleção e os campos do Construtor de condições, defina filtros para a primeira linha.

b. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
Se **E** for selecionado, todas as condições deverão ser atendidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

c. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser atendidas antes que os incidentes de segurança sejam criados.



(Optional) Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Esse tipo de filtragem de condição de geração de incidente ajuda a restringir os eventos de segurança e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a pesquisa de correlação subjacente ou filtrar eventos em ArcSight ESM. Se critérios de filtragem adicionais forem definidos, somente os eventos de correlação que corresponderem a todos os critérios serão mapeados para os incidentes.

Nota: Se algum dos nomes de campo de evento tiver caracteres especiais, como aspas (“), hifens ('), sublinhados (-) ou e comercial (@), talvez esses caracteres precisem ser substituídos para fins de tradução de mapeamento e possivelmente criar um evento duplicado nome. O mapeamento pode ser feito corretamente, mas um sufixo numérico é anexado para diferenciar campos com nomes de evento duplicados. Por exemplo, se o primeiro campo de evento for `Events.event` e o segundo campo de evento for `Events.event`, esses campos não poderão ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de evento e o campo é renomeado para `eventos@event(1)`.

Critérios de agregação de eventos para lidar com eventos de correlação semelhantes e evitar incidentes duplicados

9. Opcional: Para evitar a criação de incidentes de segurança duplicados, defina critérios de agregação de eventos adicionais para que os eventos de correlação de entrada sejam agregados a um incidente de segurança aberto.
Para definir os critérios, siga estas etapas abaixo:

Tradução automática

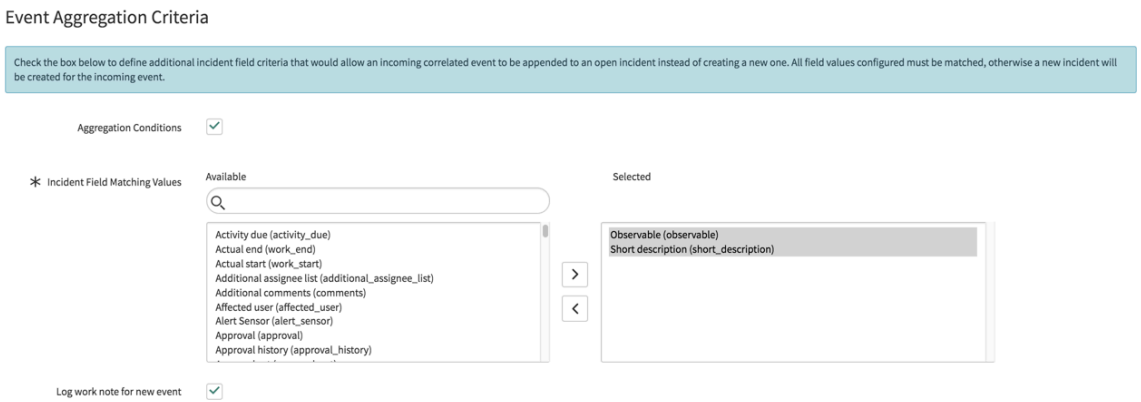
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Role até a seção **Critérios de agregação de eventos** no formulário e marque a caixa de seleção Condições de agregação para habilitar essa opção.

(Optional) As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

b. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes em seu Now Platform e mova-os para a lista Selecionado.

(Optional) Todos os valores de campo selecionados devem ser correspondidos para anexar este evento de correlação de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de evento de correlação mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de eventos não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para mapeamento de campos de vários valores.

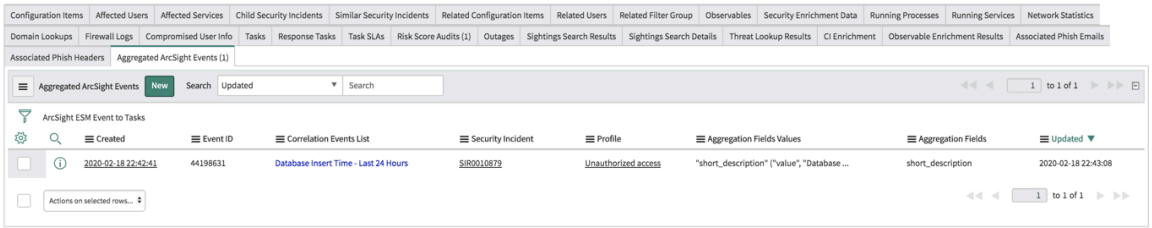


Se um novo evento de correlação corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o novo evento de correlação será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como analista do SOC que trabalha com incidentes de segurança, você pode exibir todos os eventos de correlação agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os eventos de correlação agregados em um incidente de segurança são exibidos na lista relacionada de **Eventos agregados do ArcSight**. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que esses eventos de correlação estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em **Links relacionados** e clique no link **Mostrar todas as listas** relacionadas.

Nota: Se você não vir esta lista relacionada, siga estas etapas:

- Clique com o botão direito do mouse no cabeçalho do formulário Incidente de segurança e clique em **Configurar** > **Listas relacionadas**.
- Selecione **Eventos agregados do ArcSight** na lista Disponível, mova-o para a lista Selecionado e clique em **Salvar**.
- Clique **em Mostrar listas relacionadas**. Agora você verá a guia **Eventos agregados do ArcSight** na seção Lista relacionada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Opcional: Para registrar uma anotação de trabalho para cada vez que um evento for agregado no incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra que um novo evento correlacionado foi adicionado junto com um link para os detalhes do evento correlacionado.

Você mapeou com sucesso valores de um evento de correlação para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidente. Você também agregou eventos de correlação a incidentes de segurança SIR existentes quando os valores do campo de evento correspondem aos critérios de agregação configurados.

10. Escolha um para continuar com a configuração do perfil.

Opção	Descrição
Continuar	O formulário Mapeamento é exibido. A**visualização** está selecionada na barra de andamento. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR.
Atualizar	Seus dados são salvos e a lista ArcSight ESM de Perfis de eventos é exibida.
Anterior	O formulário Seleção de evento de correlação é exibido.
Excluir	Exclua este perfil de evento e a lista Perfis de eventos será exibida.

Visualizar o incidente de segurança para a integração de ingestão de eventos ArcSight ESM

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um incidente de segurança Now Platform Security Incident Response (SIR). Esta etapa de visualização permite que você verifique se mapeou todos os campos de correlação que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin.

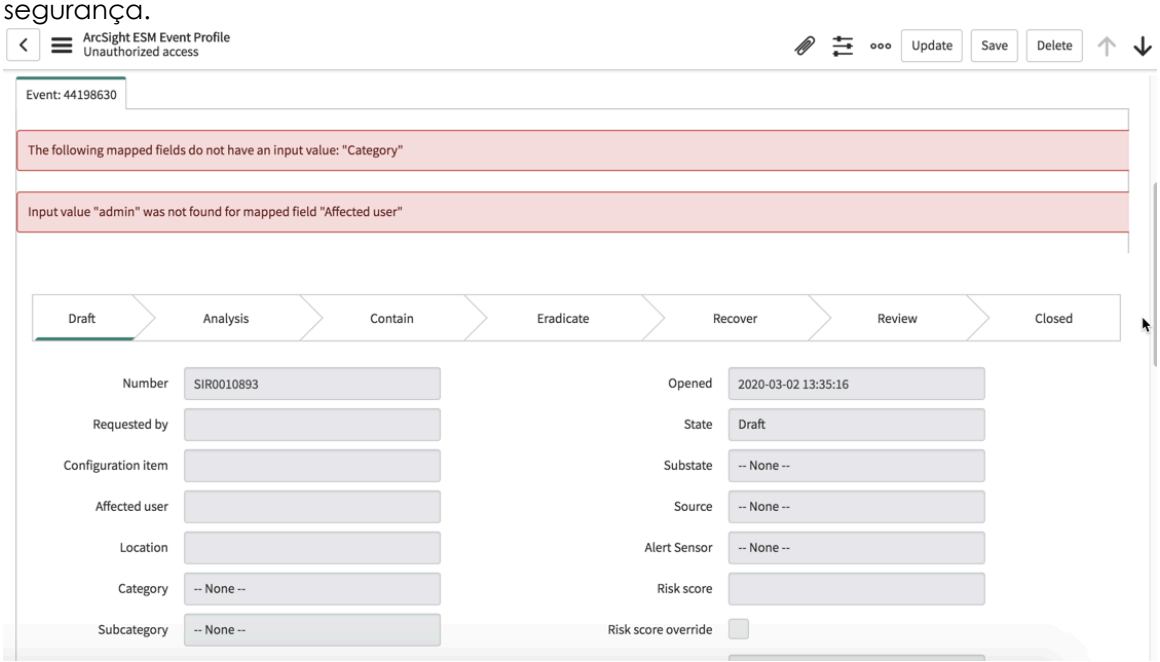
Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Na lista de seleção IDs de evento de amostra, selecione um item.
   O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de evento de correlação no incidente de segurança.



   A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um valor de campo do evento de correlação não tem um valor aceitável para o campo de referência no formulário de incidente SIR. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para o campo `Categoria`, que é um campo de referência com um conjunto específico de valores. Como resultado, este valor de campo mapeado não aparecerá no formulário de incidente de segurança SIR sem modificações adicionais.

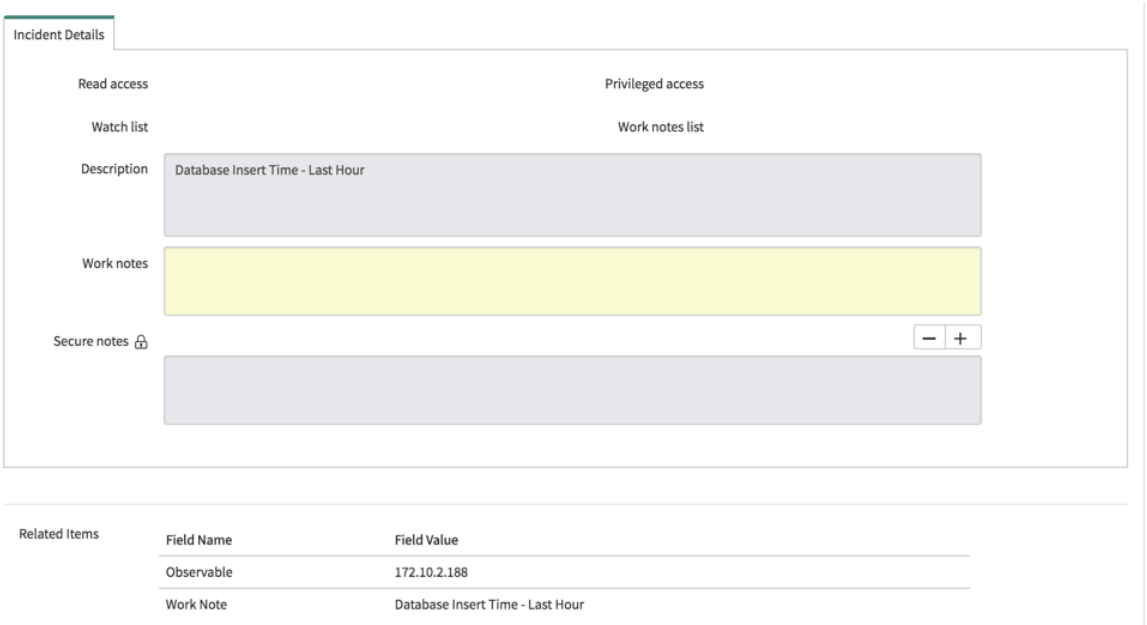
4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

   A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

campos são preenchidos com os valores dos pares de valores extraídos das amostras de evento de correlação ArcSight ESM.



O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campos no incidente de segurança, a próxima etapa será definir a programação.

Criar uma programação para ingestão de eventos ArcSight ESM ingestão

Você pode definir a programação de pesquisa ou extração para novos eventos correlacionados. Durante esta etapa, você pode verificar as configurações existentes para recuperação de eventos de correlação ou modificar a programação conforme necessário. Esta etapa também permite recuperar eventos de correlação histórica usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.admin.

Por Que e Quando Desempenhar Esta Tarefa

Você pode escolher se deseja ingerir eventos de correlação histórica durante a etapa de Programação. Você também escolhe com que frequência pesquisará novos eventos de correlação futuros que correspondam à configuração do perfil.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de eventos de correlação ArcSight ESM pode ser afetado pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a redução da sobrecarga de pesquisa no servidor ArcSight ESM com o desejo de ser notificado assim que possível quando um evento for criado ou atualizado. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo eventos de correlação novos e atualizados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

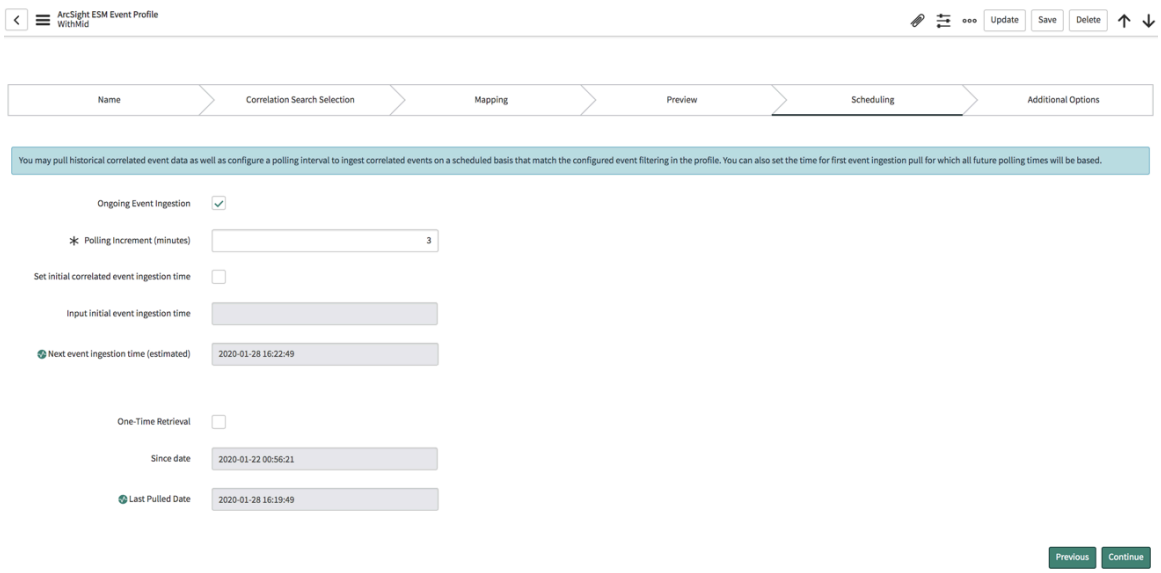
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os eventos de correlação são extraídos do<ArcSight> console.

Opção	Descrição
◦ Campo de ingestão de eventos contínuos selecionado ◦ Campo de recuperação única limpo	Evento contínuo Com base na configuração padrão, a instância Now Platform extrai do servidor ArcSight ESM novos eventos de correlação a cada cinco minutos. Os incidentes de segurança serão criados se eventos de correlação forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar a sobrecarga de pesquisa de ingestão para obter os dados mais atuais, cinco minutos é a configuração padrão. No entanto, este valor pode ser modificado para até um minuto, se necessário.
◦ Campo de ingestão de eventos contínuos limpo ◦ Campo de recuperação única selecionado	Recuperação Única Use esta configuração se quiser que uma extração única inclua eventos de correlação histórica. Quando esta configuração é definida, um perfil é usado uma vez para recuperar eventos de correlação de eventos históricos que são baseados em um intervalo de datas. À direita do campo Data desde, clique no ícone de calendário. No calendário exibido, selecione a data em que deseja começar a extrair alertas. Começando com o valor de data Desde, os eventos de correlação são recuperados até a data atual. Observe que você pode recuperar eventos até sete dias a partir da data atual. Esta funcionalidade não se destina a recuperar quantidades significativas de eventos históricos por motivos de arquivamento, mas sim uma quantidade mínima de eventos em andamento que estão sendo trabalhados ativamente no momento da ativação do perfil. Depois que os eventos de correlação forem extraídos, esta configuração não recuperará mais eventos de correlação para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	com todos os eventos de correlação encontrados para o intervalo inserido.



Como um exemplo para programar um tempo de ingestão de evento de correlação inicial, se você tiver uma verificação de segurança diária ArcSight ESM que é executada uma vez por dia às 4h, horário local, você pode configurar o perfil de evento de correlação correspondente em sua instância Now Platform para ser executado em 4 :05 AM, horário local, para capturar o evento de falha de segurança imediatamente e criar um incidente de segurança. Insira `04 05 00` no campo Ingestão de evento inicial. No campo Incrementar (minutos), insira `1440` (24 horas) para programar a próxima ingestão de eventos por 24 horas a partir da ingestão de eventos inicial. O tempo de ingestão do evento inicial e o tempo de ingestão do próximo evento são exibidos nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

   a. Com a página Programação exibida, marque a caixa de seleção **Ingestão de eventos contínuos** para habilitar essa opção.

   b. No campo Incrementar (minutos), insira `1440` (24 horas).

   c. Clique na caixa de seleção **Definir tempo de ingestão do evento correlacionado inicial** para habilitar a edição dos campos Ingestão de evento inicial e Ingestão de próximo evento.

   d. No campo Tempo de ingestão do evento inicial, insira `04 05 00`.
   No campo Tempo de ingestão do próximo evento (estimado), a hora da ingestão do próximo evento é exibida.

4. Clique em **Continuar** para navegar até a página Opções adicionais.

   Nota: O número padrão de incidentes de segurança que podem ser criados e agregados em um dia e o período de fluxo são definidos nas ArcSight ESM Configurações de integração. Você pode modificar essas configurações, se necessário. Consulte ArcSight ESM Configurações de integração para integração de ingestão de eventos para obter detalhes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opções adicionais: automatizar atualizações e fechamento de eventos correlacionados com base no status do incidente SIR

A integração ArcSight ESM tem uma interface bidirecional que permite que ambos os eventos de correlação criem incidentes de segurança, bem como a capacidade de atualizar os eventos de correlação depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como o número do incidente de segurança , grupo de atribuição, SIR URL de incidente e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração para atualizar eventos correlacionados quando o incidente de segurança for criado.

Opção ou campo	Descrição
Atualizar eventos correlacionados após a criação do incidente SIR	Selecione esta opção se quiser atualizar a fase do evento de correlação em ArcSight ESM e atualizar o evento com comentários adicionais quando um incidente de segurança for criado a partir do evento de correlação. Isso pode ocorrer para eventos de correlação que podem criar um novo incidente de segurança, bem como agregar incidentes de segurança existentes. **Nota:** Se esta opção não estiver selecionada, a fase do evento não será atualizada quando o incidente de segurança for criado.
Atualização da fase do evento correlacionado	Selecione uma opção de fase na lista de seleção Atualização de fases de eventos correlacionados que exibe todas as fases disponíveis recuperadas do servidor ArcSight ESM.

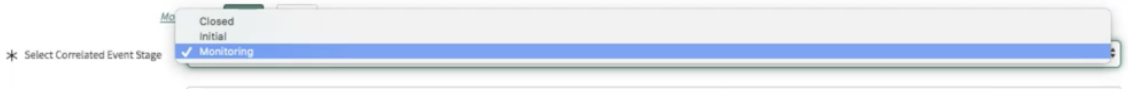
Fase de eventos correlacionados não configurada: se você não configurou nenhuma fase de eventos correlacionados em sua instância Now Platform, você verá somente **Atribuir fase - Configuração inicial** na lista de seleção Atualização de fase de eventos correlacionados. Para configurar a fase, siga estas etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Insira um ID de recurso no campo Inserir ID de recurso da fase e clique em **Enviar**. O ID do recurso é validado no console ArcSight ESM e a tela a seguir é exibida.

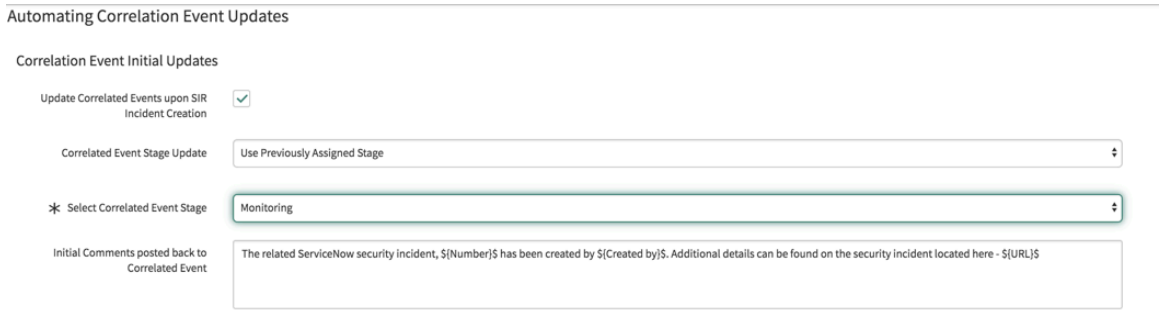
- Clique em **Salvar** para salvar a nova fase (**Monitoramento**).
- Clique na lista suspensa Selecionar fase de evento correlacionado.



- Você pode selecionar a fase recém-criada na lista.

Fase de eventos correlacionados já configurada: se você já configurou a fase de eventos correlacionados, siga estas etapas:

- Selecione **Usar fase atribuída anteriormente** na lista de seleção Atualização de fase de eventos correlacionados.
- Selecione uma fase existente na lista de seleção Selecionar fase de evento correlacionada, conforme mostrado abaixo.



- Comentários iniciais retornados para o evento correlacionado: além de atualizar o valor da fase do evento de correlação, você também pode publicar comentários nas anotações da fase de correlação. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente do Security Incident Response.

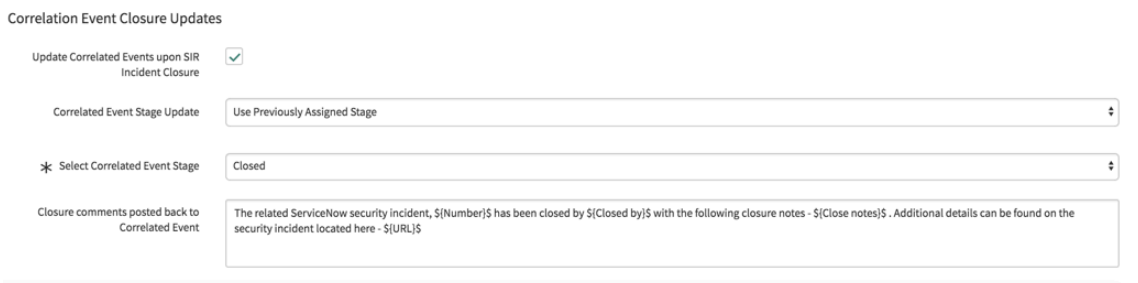
Nota: Você pode usar as fases padrão definidas no console ArcSight ESM ou criar suas próprias fases personalizadas. Para criar uma nova fase, siga estas etapas:

- No console ArcSight ESM, selecione **Arquivo** > **Novo** > **Fase**. A guia Inspecionar/editar é exibida.
- Defina a nova fase e não marque a caixa de seleção **Usuário obrigatório**. Certifique-se de que a fase esteja definida corretamente e na posição correta no ciclo de vida do evento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na seção Automatização do fechamento de eventos correlacionados, você pode definir como atualizar o incidente de segurança quando ele for fechado.
4. No formulário, preencha os campos.

Opção ou campo	Descrição
Atualizar eventos correlacionados após o fechamento do incidente SIR	Selecione esta opção se quiser atualizar o status do evento de correlação e adicionar comentários adicionais quando um incidente de segurança for encerrado a partir do evento correlacionado. Isso ocorrerá para os eventos notáveis de acionamento inicial que criam o incidente de segurança, bem como para os eventos agregados. **Nota:** Se esta opção não estiver selecionada, a fase do evento não será atualizada quando o incidente de segurança for encerrado.
Atualização da fase do evento correlacionado	Selecione uma opção de fase no menu que exibe todas as fases disponíveis recuperadas do servidor ArcSight ESM. Selecione o valor de fase a ser definido para todos os eventos de correlação quando um incidente de segurança for encerrado. **Nota:** As fases exibidas aqui são baseadas nas fases configuradas na seção Atualizações iniciais do evento de correlação.
Selecionar fase de evento correlacionado	Selecione um status apropriado aqui.
Comentários de fechamento retornados para o evento correlacionado	Além de atualizar o valor do status do evento de correlação, você também pode publicar comentários de fechamento nas anotações do evento de correlação. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente do Security Incident Response.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

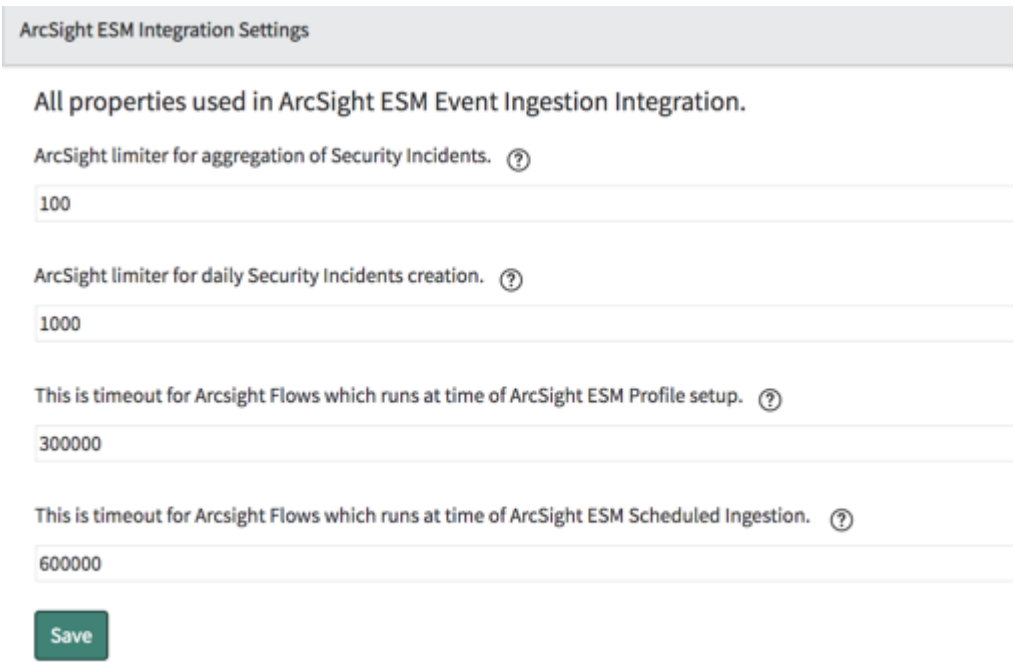
5. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair eventos de correlação do console ArcSight ESM com base em sua programação.

ArcSight ESM Configurações de integração para integração de ingestão de eventos

Use esta opção para modificar as ArcSight ESM configurações de ingestão padrão.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Integração do ArcSight ESM** > **Configurações de integração do ArcSight ESM**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.



Solução de problemas de integração de ingestão de eventos ArcSight ESM

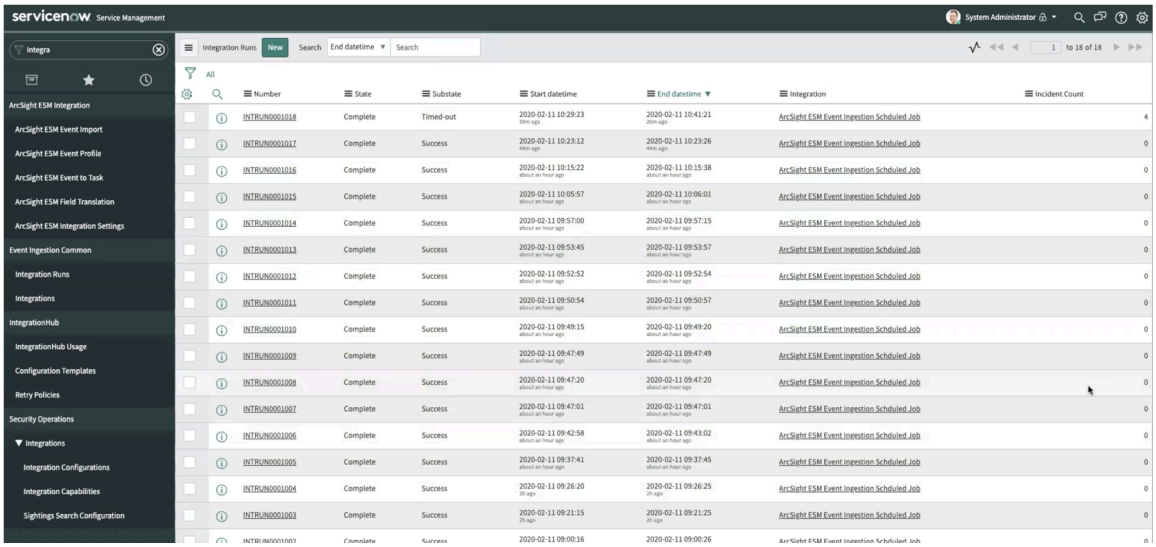
Esta seção fornece informações sobre como solucionar problemas de erros que podem ocorrer durante a ingestão de eventos.

Execuções de integração

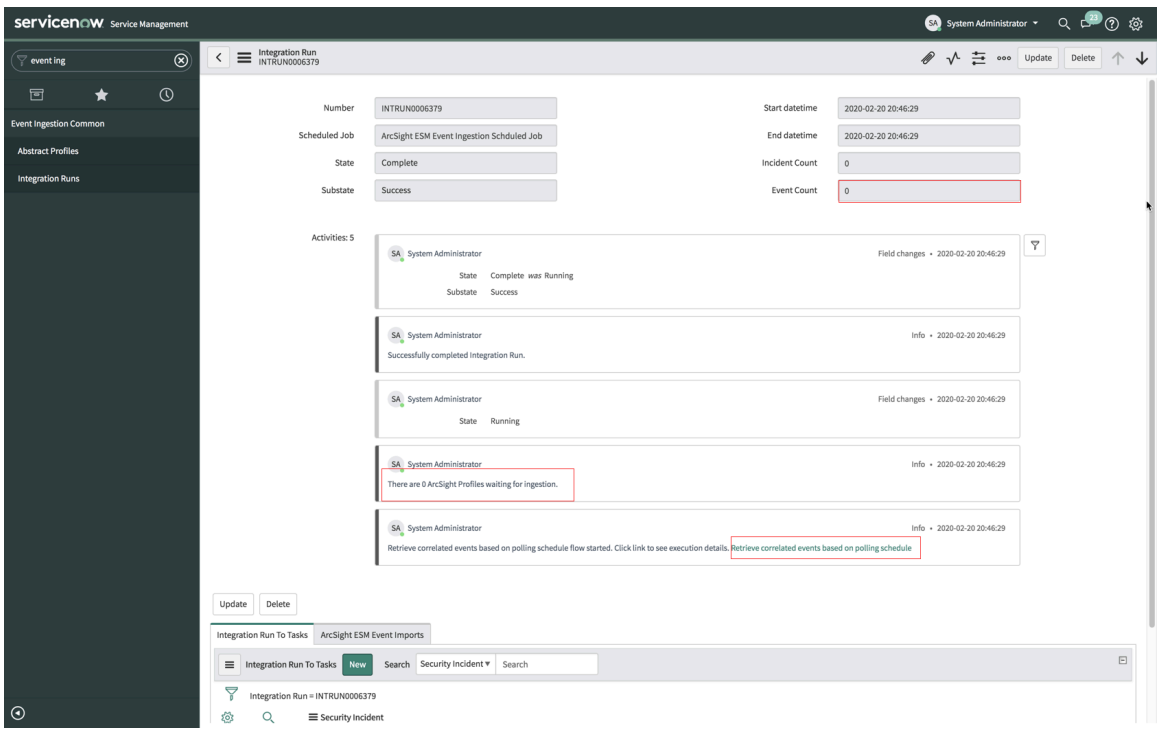
Navegar até **Ingestão de eventos comuns** > **Execuções de Integração**. Uma execução de integração ocorre a cada minuto e captura detalhes sobre os eventos ingeridos durante o trabalho agendado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode ver a lista de execuções de integração e o status de cada execução (Êxito, Tempo esgotado, Aguardando) e o número de incidentes de segurança que foram criados. Clique no link Número para ver a página detalhada Execução de integração.



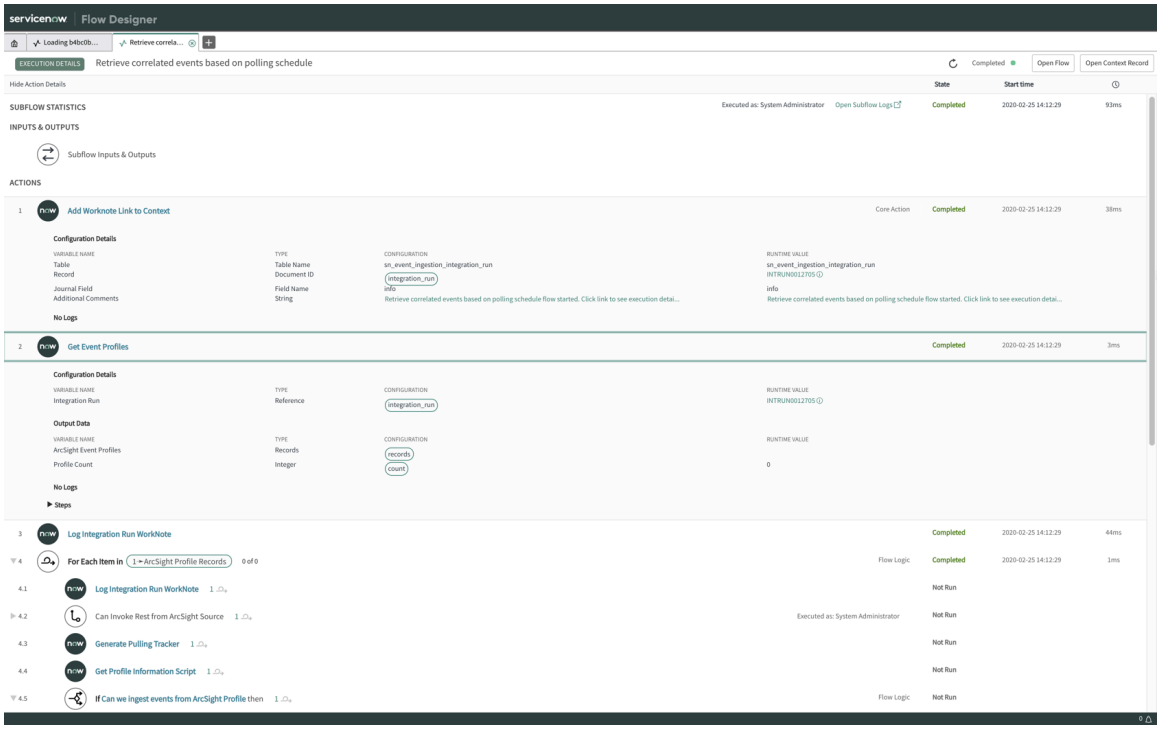
Você pode exibir detalhes como o número de eventos que foram ingeridos, o status, qual evento foi transformado em um incidente de segurança e as diferentes tarefas realizadas durante a ingestão. Além disso, você pode clicar no link para exibir os detalhes da execução do fluxo.

Detalhes do fluxo de execução

Clique no link de detalhes da execução para ver o fluxo associado à ingestão de eventos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode exibir uma execução passo a passo do fluxo detalhando as várias ações e subfluxos que foram executados como parte do fluxo.

Copiar ArcSight ESM perfil para integração de ingestão de eventos

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar os perfis para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

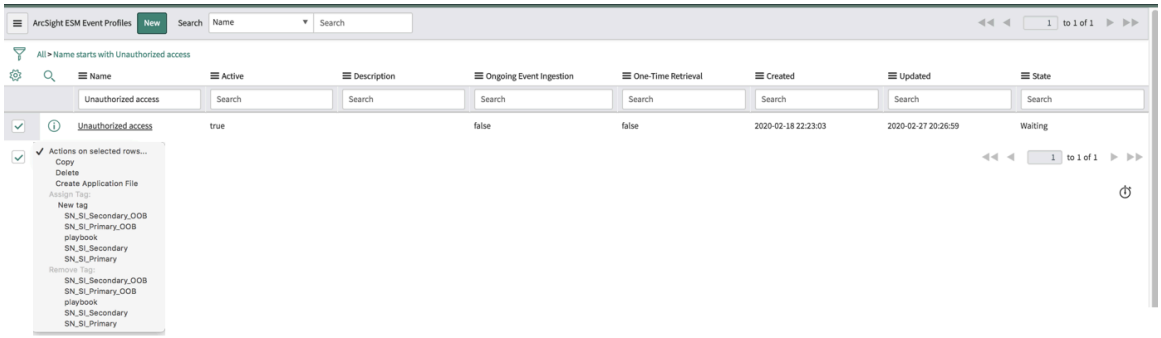
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

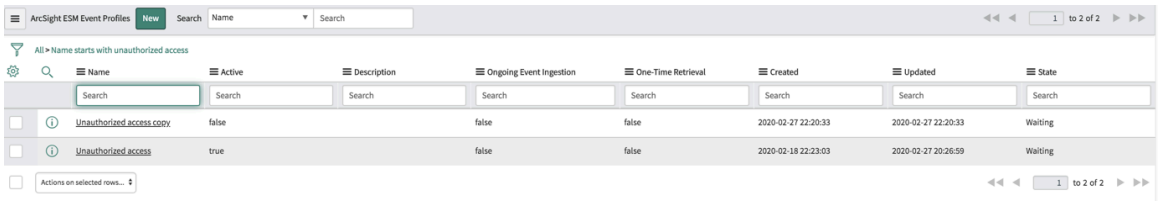
1. Navegar até **Todos** > **Integração do ArcSight ESM** > **Perfil de evento do ArcSight ESM**.
2. Na lista Perfis do ArcSight exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (`verdadeiro`), a cópia está desabilitada neste ponto (`falso`). Você pode preferir editar valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativo** está definido como falso, pois o perfil precisa ser ativado.

Use o editor de script para formatar valores de evento de correlação para integração ArcSight ESM

Além dos campos mapeados diretamente dos valores de evento de correlação ingeridos, use o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
O editor de script muda os valores de um campo de evento de correlação ArcSight ESM para que os valores compatíveis com o incidente de segurança Now Platform SIR sejam mapeados para os campos Categoria, Item de configuração (IC), Observável e outros incidentes de segurança.

Em determinados casos, os valores de evento de correlação ArcSight ESM são mapeados para campos de referência, como Categoria, Item de configuração (IC) e campos Observável no incidente de segurança. Como um usuário com a função sn_si.admin, você pode preferir editar os valores do campo de evento mapeado para converter o formato ou os valores de dados para que estejam em conformidade com os formatos e valores esperados do campo de incidente. Se você quiser converter o valor de um evento de correlação ArcSight ESM para um valor compatível com esses campos no incidente de segurança SIR, use o editor de script.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de script.
2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete `[{}]` ao lado de um campo para abrir o editor de script desse campo.

   Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um evento de correlação, por exemplo, um valor do item de configuração pode não ser correspondido.

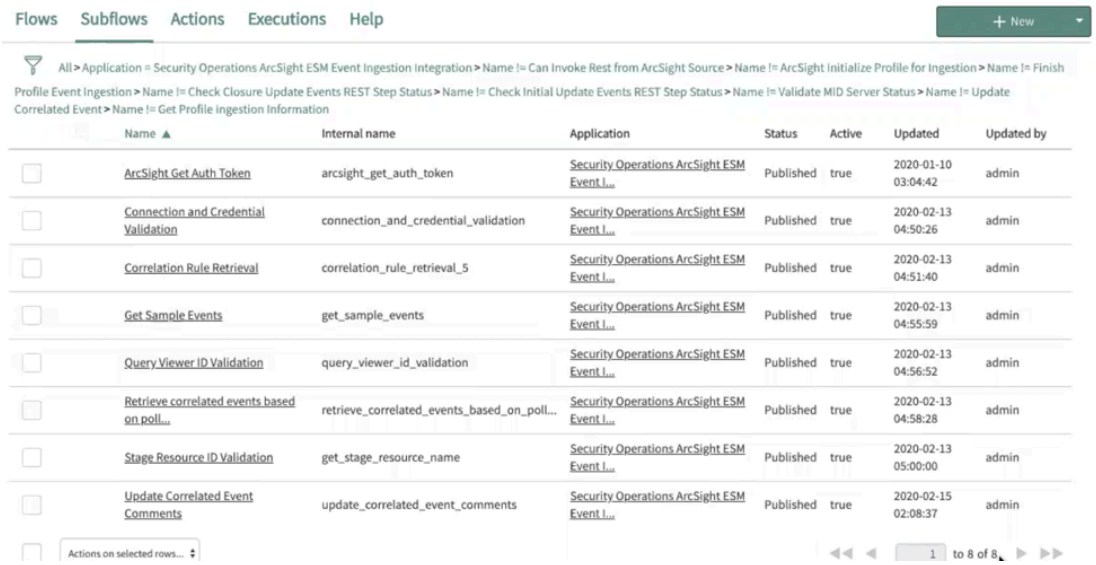
   Conforme mostrado na figura a seguir, se uma correspondência para um nome de host não puder ser encontrada no Now Platform CMDB para o campo Item de configuração, você poderá editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração.

   O editor é aberto com o campo exibido em Campo de destino.
4. Insira todas as mudanças no script e clique em **Atualizar** para salvar suas mudanças. A tabela ArcSight ESM Traduções de Campo é exibida.
5. Feche a tabela para retornar ao formulário Mapeamento.

Uso do Flow Designer com integração de ingestão de eventos ArcSight ESM

Usando o Integration Hub e o Flow Designer, vários fluxos, subfluxos e ações estão disponíveis com a integração ArcSight ESM.

Para exibir esses subfluxos, navegue até **Flow Designer** > **Designer** e clique na guia **Subfluxos**. A figura abaixo mostra os subfluxos importantes usados durante a criação do perfil e o trabalho de ingestão programada.



Esses subfluxos são listados na sequência em que são executados abaixo:

- **Validação de conexão e credencial**: este subfluxo valida a conectividade ServiceNow com o servidor ArcSight ESM e as credenciais especificadas. Este subfluxo é usado quando você clica no botão **Configurar** no bloco **ArcSight ESM - Ingestão de eventos**no **Operações de segurança** > **Integrações** > **Configuração de integrações** página.
- **Obter token de autenticação do ArcSight**: este subfluxo gera o token de autenticação ArcSight ESM a partir do nome de usuário e senha usando o serviço de login ArcSight ESM. O serviço de login fornece o token de autenticação que pode ser usado para chamar qualquer outro ArcSight ESM endpoint. Este subfluxo é usado em todos os outros subfluxos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Validação do ID do visualizador de consulta**: este subfluxo verifica se o ID do visualizador de consulta especificado durante a criação do perfil está presente no servidor ArcSight ESM.
- **Recuperação de regra de correlação**: este subfluxo recupera as regras de correlação com base na ID do visualizador de consulta.
- **Obter evento de amostra**: este subfluxo busca os eventos de correlação de amostra do servidor ArcSight ESM. Esses eventos de amostra são mapeados para os campos de incidente de segurança na seção Mapeamento do perfil.
- **Validação do ID do recurso da fase**: este subfluxo valida o ID do recurso da fase especificado no console ArcSight ESM e busca o nome do recurso.
- **Atualizar comentários de eventos correlacionados**: este subfluxo atualiza os comentários de eventos correlacionados nas seções Inicial e Fechamento do incidente na página Opções adicionais do perfil.
- **Recuperar eventos correlacionados com base na programação de pesquisa**: este subfluxo executa o trabalho agendado que busca os eventos correlacionados com base no intervalo de pesquisa.

Durante a execução, os subfluxos acima também acionam vários outros subfluxos e ações direta ou indiretamente, conforme mostrado abaixo.

Flows | Subflows | Actions | Executions | Help

+ New

Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Carbon Black - Integração de enriquecimento de incidentes

Use a integração Carbon Black para investigar e responder a incidentes de segurança usando APIs para consultar e interagir com endpoints associados a incidentes de segurança.

Localizar recursos de integração com Carbon Black- Incident Enrichment

- Introdução ao Carbon Black - Integração de enriquecimento de incidentes
- Integração do Carbon Black das Operações de segurança - Obter fluxo de trabalho dos processos em execução

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração do Carbon Black das Operações de segurança - Fluxo de trabalho Isolar host
- Integração do Carbon Black das Operações de segurança - Remover fluxo de trabalho de isolamento de host

Entenda os conceitos de integração

- Tipos de ServiceNow integrações fornecidas
- Operações de segurança gatilhos de fluxo de trabalho

Obtenha ajuda de recursos ServiceNow

- Fazer ou responder a perguntas na comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente
- Upgrade para Madri

Introdução ao Carbon Black - Integração de enriquecimento de incidentes

O enriquecimento de incidentes do Carbon Black facilita a investigação de um incidente de segurança, consultando logs em busca de indicadores potencialmente maliciosos. Antes de poder usar a integração Carbon Black - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar o URL base do endpoint e o MID Server apropriados.

Antes de Iniciar

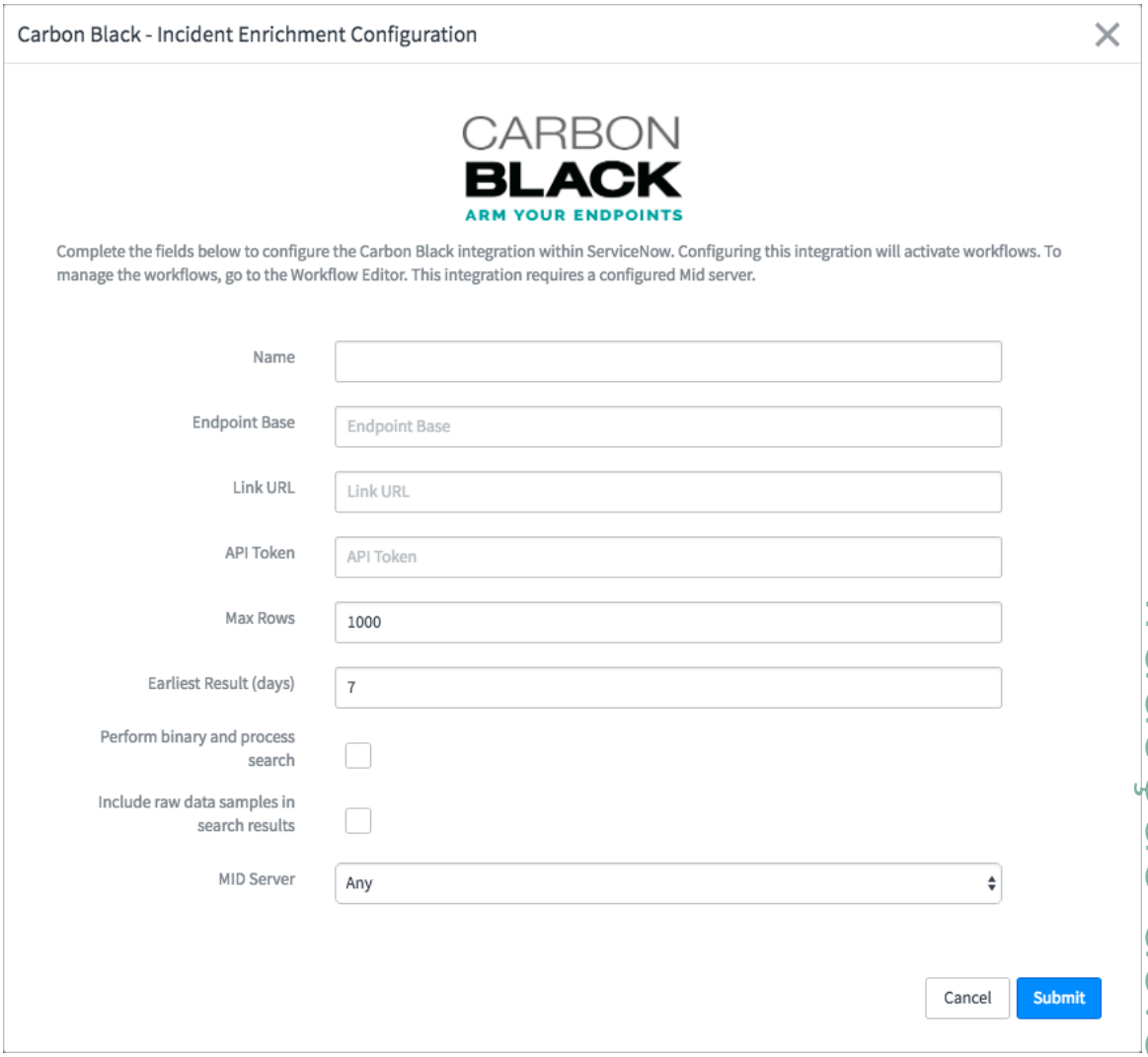
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando o download estiver concluído, acesse o site Carbon Black e obtenha a URL base do endpoint e o token de API no seu perfil.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
4. No cartão Carbon Black - Aprimoramento de incidente, clique em **Configurar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Base do endpoint	A URL do endpoint que você adquiriu no site do Carbon Black.
URL do Link	A URL do link que vincula a uma instância do Carbon Black, quando disponível.
Token de API	O token de API que você adquiriu no site do Carbon Black.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar. O padrão é 1000 linhas.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Executar pesquisa binária e de processo	Selecione esta opção para executar pesquisas binárias para encontrar arquivos binários, como hashes de arquivo, e processar pesquisas para processos .exe que podem ter sido executados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração do Carbon Black

A integração do Carbon Black permite que você investigue e responda a incidentes de segurança usando APIs para consultar e interagir com endpoints associados a incidentes de segurança.

Explorar

- Integrações do Security Incident Response
- Carbon Black - Integração de enriquecimento de incidentes

Configurar

Introdução à integração do Carbon Black

Usar

- Operações de segurança gatilhos de fluxo de trabalho
- Exibir itens afetados por um incidente de segurança
- Operações de segurança - Obter fluxo de trabalho de processos em execução
- Integração do Carbon Black das Operações de segurança - Obter fluxo de trabalho dos processos em execução
- Exibir itens afetados por um incidente de segurança
- Executar bloqueio de solicitação
- Integração de Operações de segurança - Fluxo de trabalho de solicitação de bloqueio
- Executar host isolado

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

• Integração do Carbon Black das Operações de segurança - Fluxo de trabalho Isolar host • Integração do Carbon Black das Operações de segurança - Remover fluxo de trabalho de isolamento de host	
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução à integração do Carbon Black

Carbon Black é um sistema de segurança avançado que se integra facilmente com Operações de segurança. Antes de poder usar a integração do Carbon Black, você deve baixar a integração do ServiceNow Store e adicionar a base de endpoint e o token de API apropriados.

Antes de Iniciar

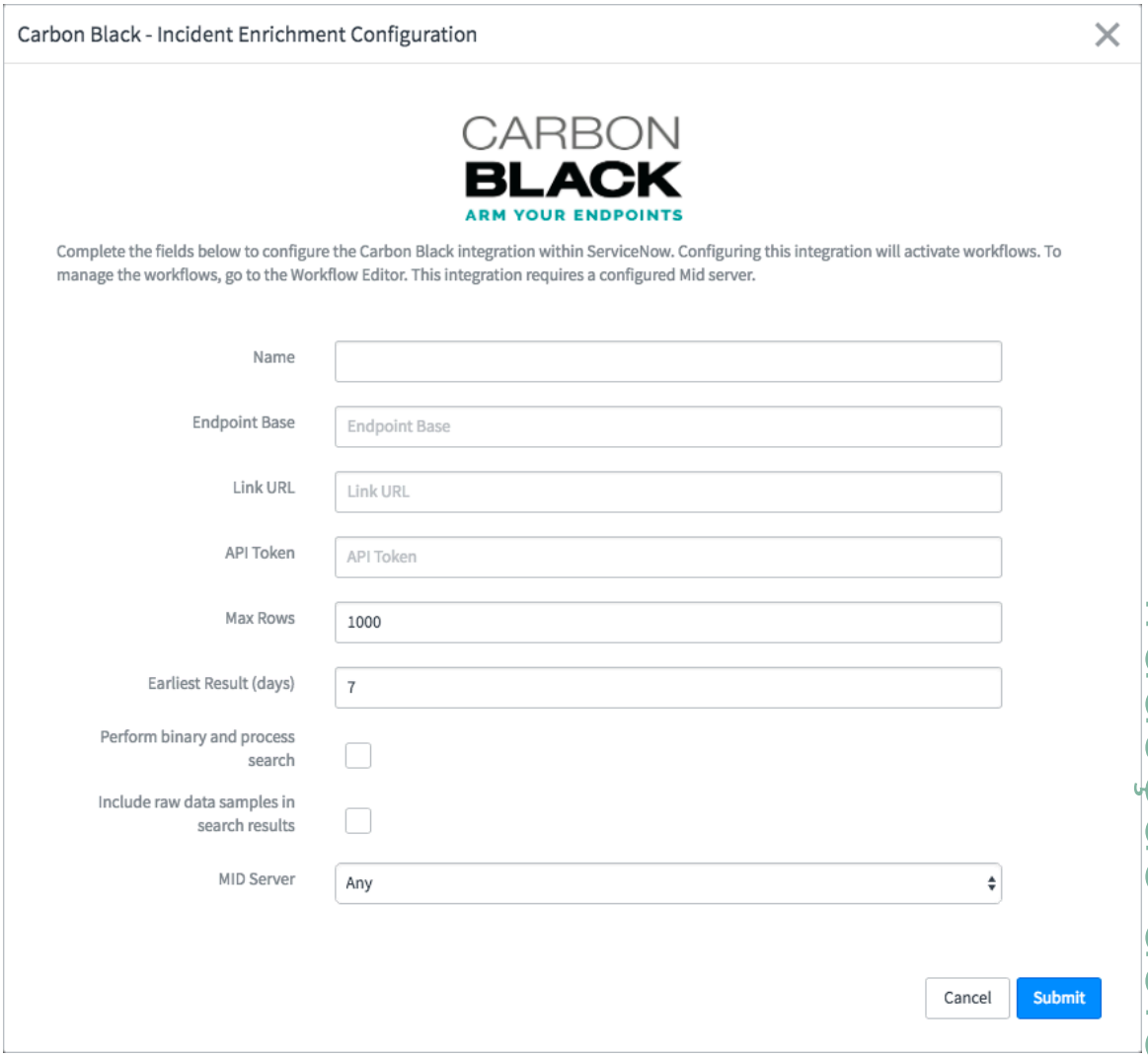
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse o site Carbon Black e obtenha a URL base do endpoint e o token de API no seu perfil.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Carbon Black, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Base do endpoint	A base do endpoint que você adquiriu no site do Carbon Black.
Token de API	O token de API que você adquiriu no site do Carbon Black.
Usar MID Server	Marque esta caixa de seleção se ela ainda não estiver marcada.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.
Ativar Isolar Host	Marque esta caixa de seleção para permitir que os itens de configuração selecionados sejam isolados da guia da lista relacionada **Itens de configuração** em um incidente de segurança.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Antibot Check Point - Integração do analisador de e-mails

A integração do Check Point Anti-bot - Analisador de e-mail é compatível usando um analisador de e-mail que consome notificações por e-mail do Check Point Anti-bot para criar incidentes de segurança e gerar fluxos de trabalho de enriquecimento e de resposta.

Configurar a integração do Check Point Anti-bot - Analisador de e-mail

A integração Check Point Anti-bot - Analisador de e-mail usa notificações por e-mail para gerar fluxos de trabalho de enriquecimento e de resposta.

Antes de Iniciar

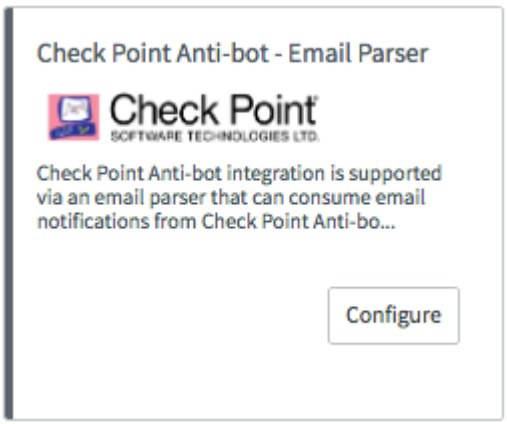
Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa

Um modelo de analisador de e-mail do Check Point Anti-bot é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. A atualização do analisador o ativa.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão Antibot do Check Point - Analisador de e-mail, clique em **Configurar**.
3. Na caixa de diálogo **Antibot do Check Point - Configuração do analisador de e-mail**, clique no link **Configurar analisador de e-mail**.
4. Clique no link **Antibot do Check Point** para editar as configurações no analisador de e-mail de modelo fornecido.
   No mínimo, preencha o campo O `e-mail é de`. Para criar um analisador de e-mail, consulte Criar analisadores de e-mail em Operações de segurança.
5. Marque a caixa **Ativo**.
6. Clique em **Atualizar** no formulário **Analisador de e-mail**.
   O analisador de e-mail está ativo. Você não precisa retornar às **Configurações de integração**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de Check Point Next Generation Threat Prevention

Este documento descreve as etapas necessárias para integrar os recursos de prevenção de ameaças de última geração (NGTP) do Check Point com ServiceNow® Security Incident Response (SIR) para que as aplicações funcionem corretamente juntas.

Depois de instalado e configurado, o analista de incidentes de segurança usa essa integração para bloquear endereços IP, URLs e domínios mal-intencionados usando recursos da Lista de solicitações de bloqueio com os produtos ServiceNow Security Incident Response (SIR). Esta Lista de Solicitação de Bloqueio está configurada nos Gateways do Check Point como um Feed de Inteligência Personalizado. O recurso Feeds de inteligência personalizados permite adicionar feeds de inteligência cibernética personalizados ao mecanismo de prevenção de ameaças de última geração. Ele permite a busca de feeds de um servidor de terceiros, neste caso, a aplicação ServiceNow Security Incident Response, diretamente para o Gateway de Próxima Geração do Check Point a ser aplicado por blades Antivírus e Antibot. O analista de resposta a incidentes de segurança cria entradas para a Lista de bloqueios do Check Point a partir de observáveis determinados como mal-intencionados em ServiceNow incidentes de segurança SIR.

Para a maioria das implementações, uma Lista de Solicitação de Bloqueio é um arquivo CSV hospedado em um servidor Web externo. Para esta integração, este servidor web é sua instância da Now Platform, o que permite que o Mecanismo de prevenção de ameaças de última geração do Check Point busque a lista de endereços IP, URLs e domínios a serem bloqueados.

Para impor os observáveis de bloqueio no Gateway do Check Point, certifique-se de que a Política de prevenção de ameaças esteja configurada com os Blades Anti-Bot e Anti-Virus ativados. Conforme as entradas da Lista de bloqueios são modificadas, o Mecanismo de prevenção contra ameaças importa dinamicamente a lista no intervalo configurado e impõe a política sem uma mudança de configuração ou uma confirmação no firewall. Para esta integração, a Now Platform criou uma tabela que contém entradas da Lista de bloqueios que são recuperadas pelo Gateway de próxima geração do Check Point autorizado nos intervalos de recuperação configurados.

A integração inclui os seguintes recursos:

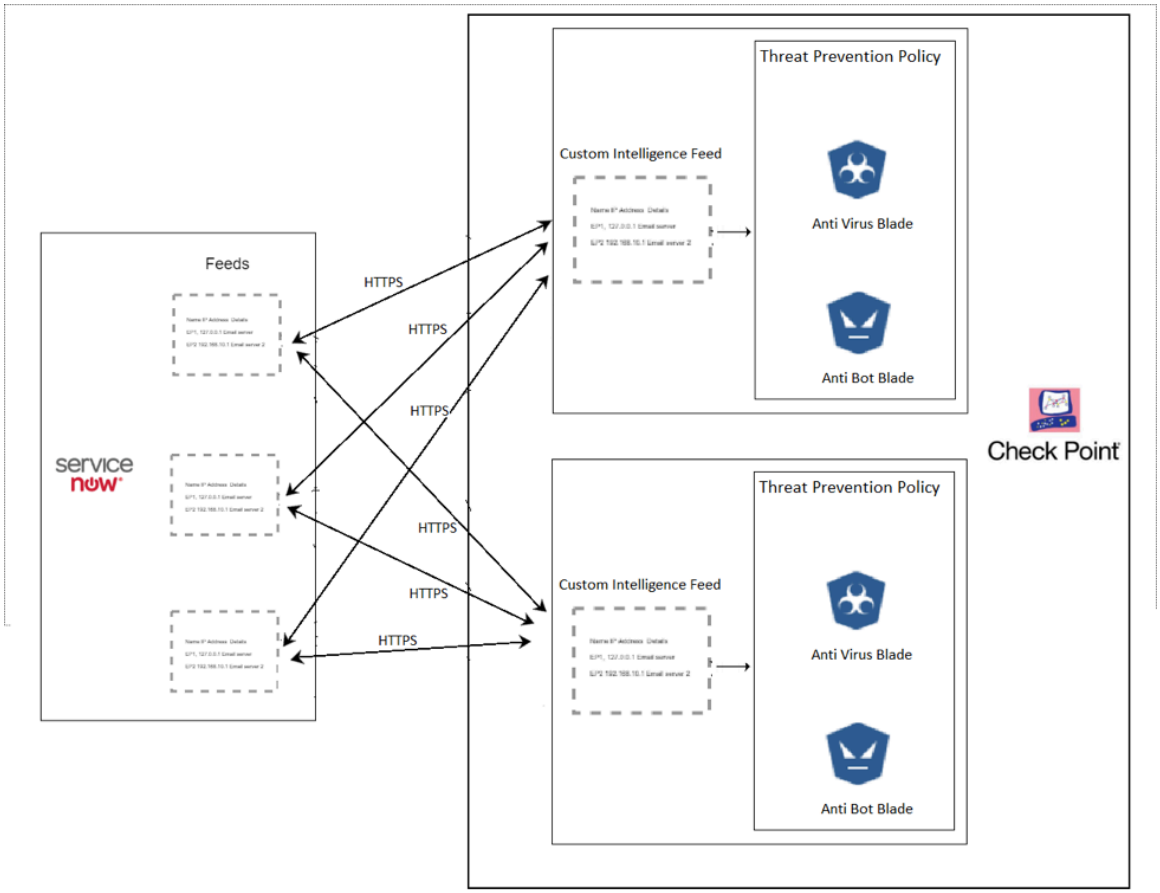
- Flexibilidade para criar várias listas de bloqueios que se aplicam a vários gateways do Check Point.
- Relatórios detalhados sobre os tipos de sites que estão sendo bloqueados (phishing, malware e sites permitidos).
- Marcação de incidentes de segurança da Now Platform com entradas da Lista de bloqueios pelo tipo de observável (URL, domínio, endereço IP).
- Configurar períodos de expiração da Lista de bloqueios para manter o tamanho da Lista de bloqueios expirando automaticamente ou removendo entradas mais antigas.
- Pesquisando entradas da Lista de bloqueios entre diferentes Listas de bloqueios.
- Vinculando entradas da Lista de bloqueios a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Diagrama de arquitetura de integração

Abaixo está o diagrama de arquitetura de alto nível que descreve os componentes envolvidos e os pontos de integração entre a NOW Platform e a Check Point Systems.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: O logotipo da Check Point Systems, a imagem do blade antivírus e a imagem do blade antibot são da Check Point Systems ©. Eles são propriedade da Check Point Systems.

Plug-ins

A integração requer que o plug-in Security Incident Response (com.snc.security_incident) esteja ativado.

Para instalar Security Incident Response plug-ins:

1. Faça login na sua instância com suas credenciais HI.
2. Verifique se você tem a função de administrador (admin).
3. Navegue até Definição do sistema>plug-ins em sua instância.
4. Selecione e clique em Security Incident Response.

Depois que esses plug-ins forem instalados, você poderá carregar o novo plug-in de integração do Check Point na ServiceNow Store e seguir as instruções de configuração a seguir.

Versões compatíveis do SO do Check Point

Esta integração requer o Feed de inteligência personalizado do Check Point e as blades Anti-Bot e Anti-Virus. Eles são compatíveis com R80.20 e superior. Instale o hotfix do Recurso de Inteligência Personalizada conhecido como Check Point R80.10 Jumbo HF, versão 121 e superior. Consulte a seção Instalação da documentação do feed de inteligência personalizada do Check Point para obter mais informações sobre a matriz de compatibilidade do produto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Depois de instalar o hotfix, certifique-se de que os comandos abaixo estejam acessíveis no Check Point Gateway. SSH para o gateway e login no modo especialista.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Versões compatíveis da ServiceNow

A versão de lançamento San Diego ou posterior é compatível.

Referências

Abaixo estão algumas das referências do Check Point que são úteis na configuração dos pré-requisitos.

1. Recurso de feeds de inteligência personalizados - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Para configurar os blades Anti-Bot e Anti-Virus, consulte o Guia do usuário do Check Point. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Para configurar a Inspeção de HTTPS no Check Point, siga o link abaixo. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Permissões e funções

As seguintes funções da ServiceNow são necessárias.

- Administrador (admin) para instalação do plug-in da aplicação de integração
- Administrador de incidentes de segurança (sn_si.admin) para criar listas de bloqueios na ServiceNow e aprovar solicitações para adicionar e desativar entradas da lista de bloqueios.
- Analista de segurança (também conhecido aqui como Analista de SOC, sn_si.analyst) para criar e manter registros de Entrada da Lista de Bloqueios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como atribuir a função de analista de segurança, no site de documentação da ServiceNow , navegue até Operações de segurança>Security Incident Response> Atribuição de analistas de segurança.

Configuração do Check Point NGTP

Antes de poder usar a integração Check Point NGTP, você deve criar uma conta de API, configurar políticas e ativar a integração.

Criar uma conta de API para a integração Check Point NGTP

Uma função de conta de API é necessária em sua instância da Now Platform para esta integração. O nome de usuário e a senha associados a esta conta são criados na Now Platform e inseridos no Check Point, para que o Check Point seja autenticado com a Now Platform ao recuperar entradas da Lista de bloqueios.

Antes de Iniciar

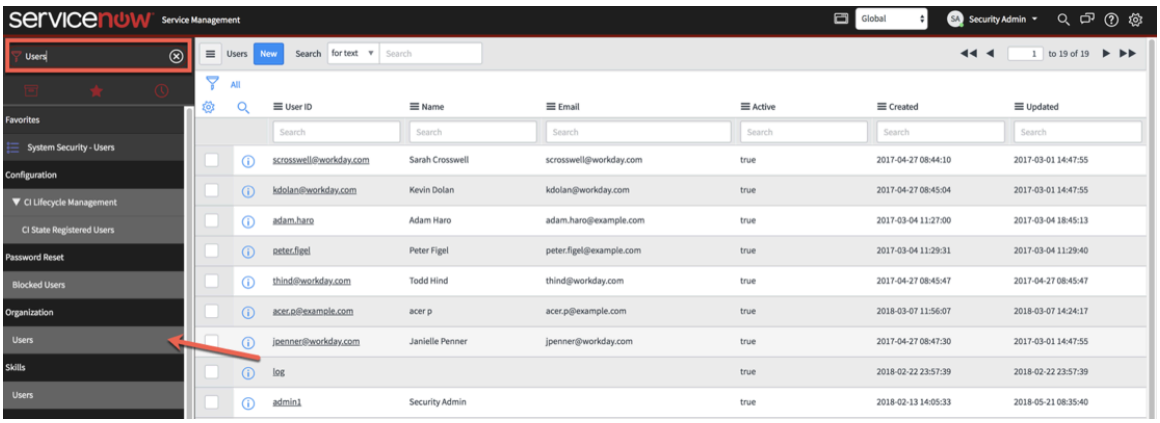
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O administrador da Now Platform cria uma função de conta de API (sn_sec_checkpoint.api_account_access). Esta conta é usada exclusivamente para inserir as credenciais necessárias para autenticação no Check Point, para que o gateway possa recuperar listas de bloqueios da Now Platform. Esta conta é uma conta de usuário de API separada e exclusiva na instância da Now Platform e atribuída ao administrador do Check Point.

Procedimento

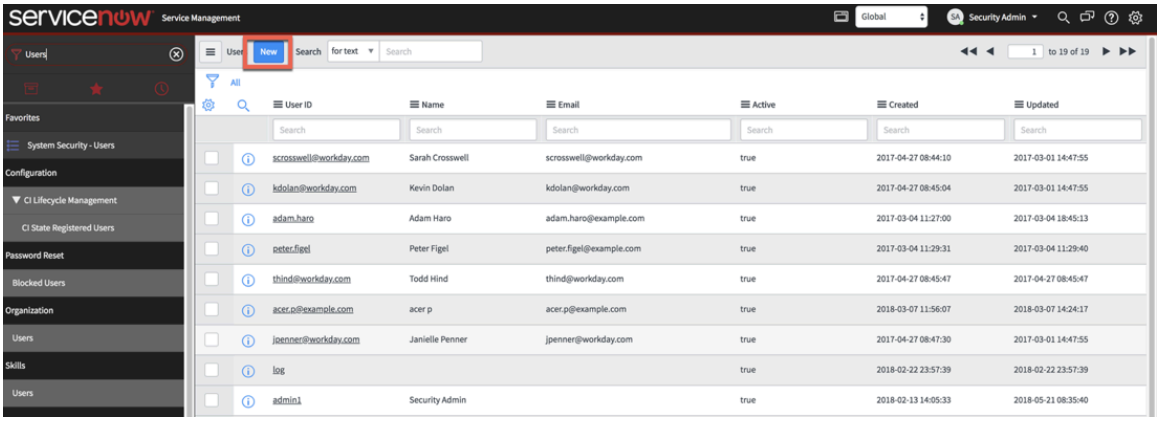
1. Navegar até **Todos** > **Organização** > **Usuários**.
2. Clique no módulo **Usuários**.



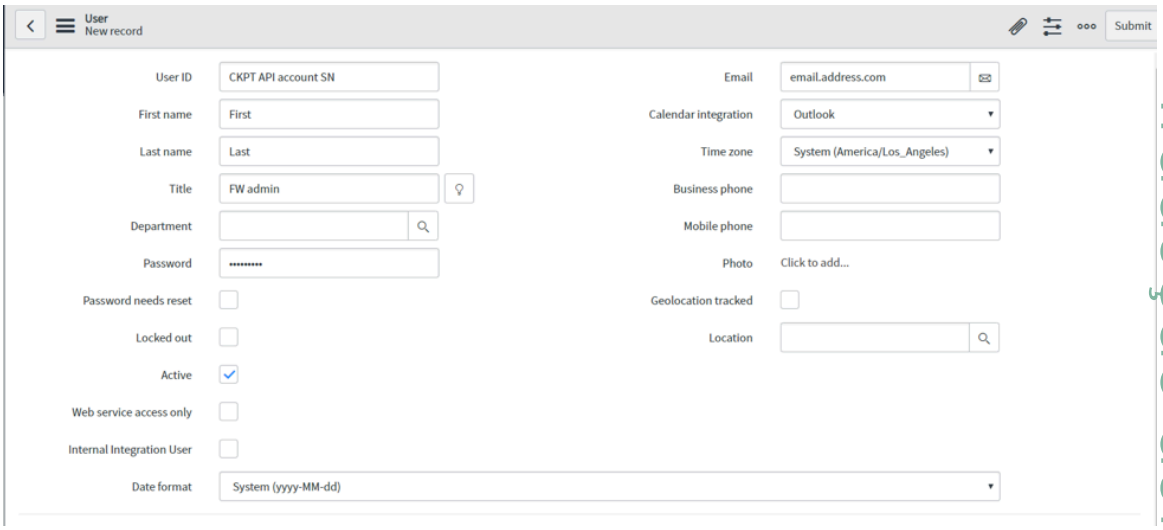
3. Na lista Usuários exibida, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Um novo formulário é exibido.



4. Preencha o formulário, conforme necessário.

Nota: Os valores de título do ID do usuário e endereço de e-mail mostrados na tabela e na figura a seguir são valores de exemplo.

Campo	Descrição
ID do Usuário	ID de usuário exclusivo para a função na sua instância da Now Platform. Este ID de usuário é inserido no campo **Nome** de usuário na seção **Autenticação de cliente** do gateway do Check Point de configuração da lista de bloqueios. Um exemplo é o SN da conta da API CKPT.
Nome	Pessoa que você está atribuindo
Sobrenome	Pessoa que você está atribuindo
Título	Cargo, por exemplo, administrador de FW.
Senha	Senha exclusiva criada para esta função. Essa senha é inserida no campo **Senha** na seção **Autenticação de cliente** da Configuração da lista de bloqueios no gateway do Check Point.
E-mail	Endereço de e-mail exclusivo

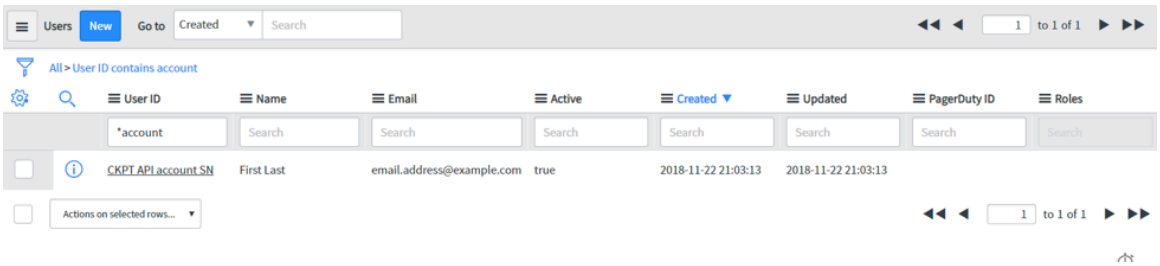
5. Clique em **Enviar**.

Tradução automática

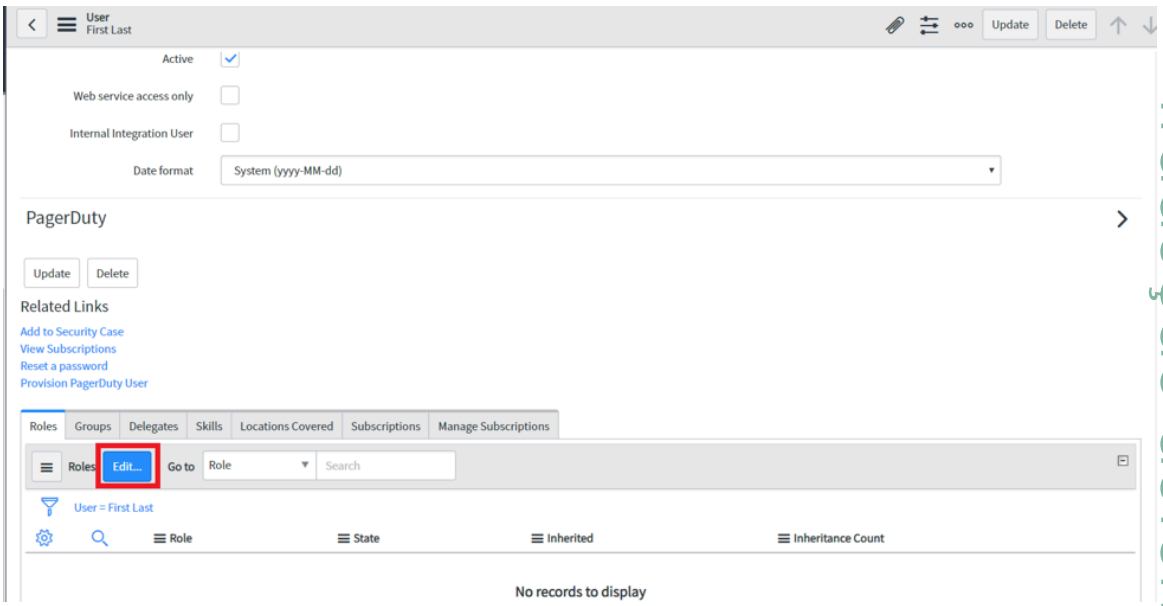
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de enviado, você pode atribuir a função.

6. Na lista Usuários na coluna ID do usuário, clique no nome do ID do usuário que você inseriu, SN da conta CKPTAPI, por exemplo.



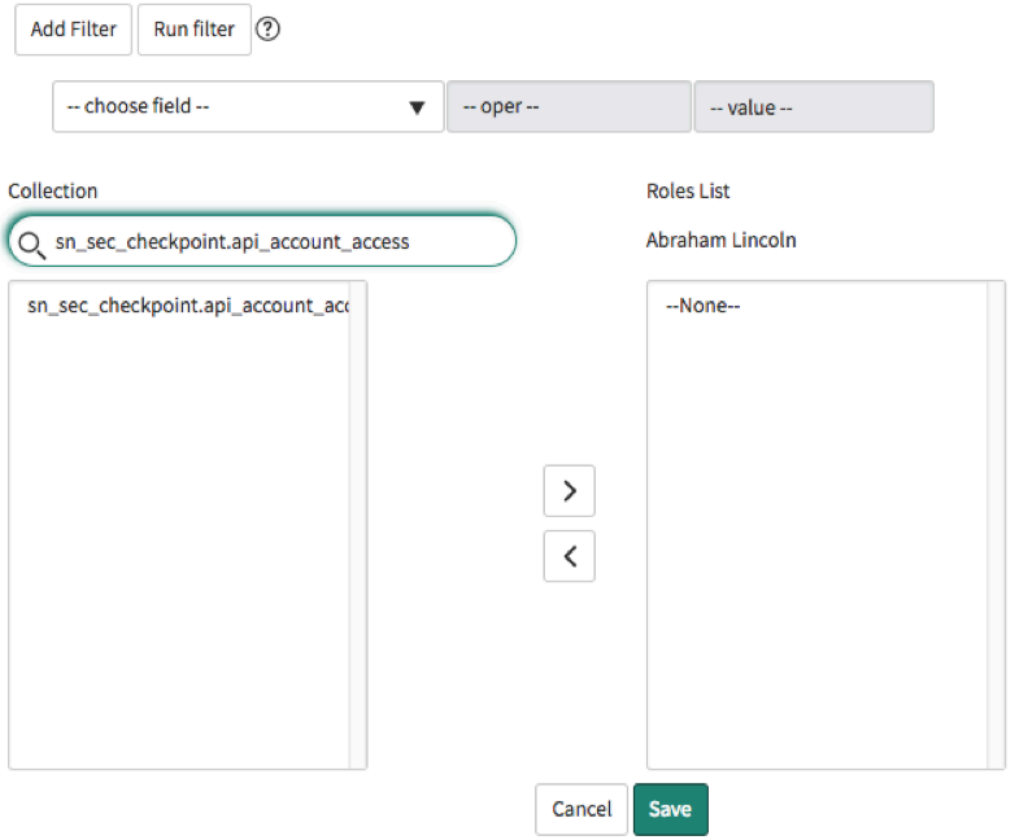
7. No registro aberto na seção Funções, clique em **Editar**.



8. No formulário **Editar membros** exibido, insira sn_sec_checkpoint.api_account_access no campo **Coleção**.

Tradução automática

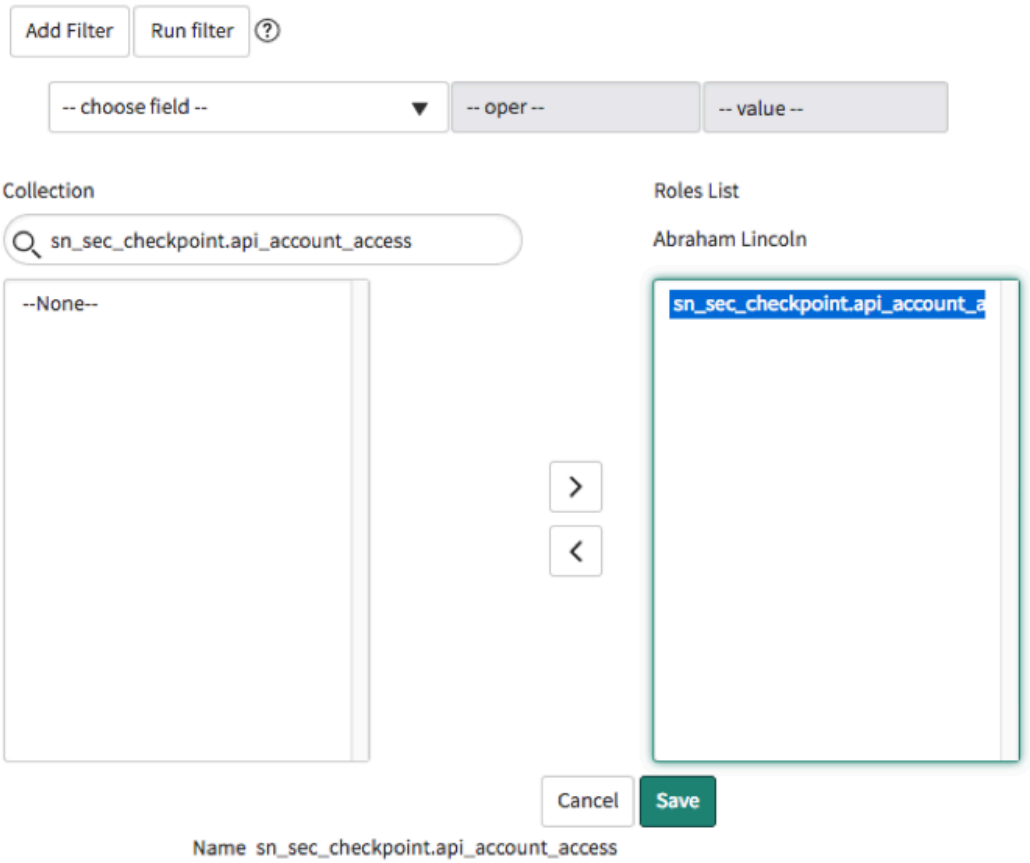
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Na coluna **Coleção**, selecione e mova sn_sec_checkpoint.api_account_access para a **Lista de funções**.
10. Clique em **Salvar**.
11. Navegue até **Usuários**e, na coluna **Usuário** da lista, clique no nome do ID que você criou para a função (SN da conta da API do CKPT).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. O registro do usuário é exibido. Este registro verifica se a conta do usuário foi atribuída.

Configurar a integração Check Point NGTP

Conclua as etapas a seguir para configurar a integração Check Point Next Generation Threat Prevention. Isso garantiria que os pré-requisitos para que a integração funcionasse.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Verifique se a Política de prevenção de ameaças está configurada com os Blades Anti-Bot e Anti-Virus ativados.
   Consulte o Guia do usuário do Check Point mencionado na seção Referência para obter informações detalhadas sobre como configurar os blades anti-bot e antivírus.

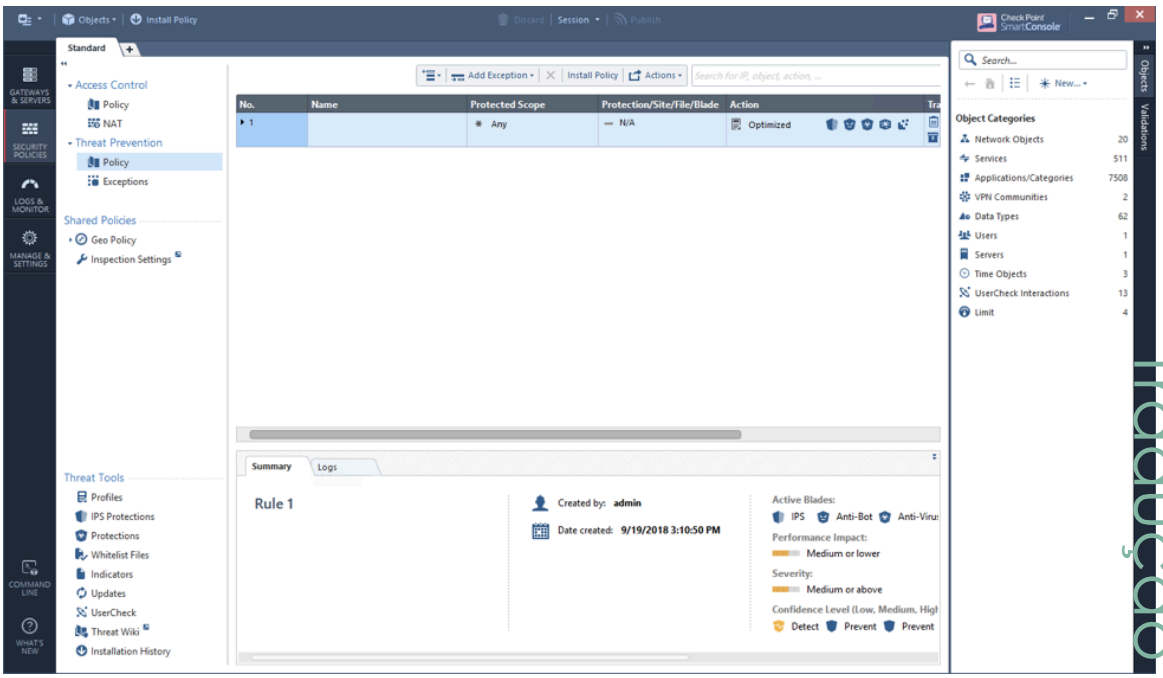
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

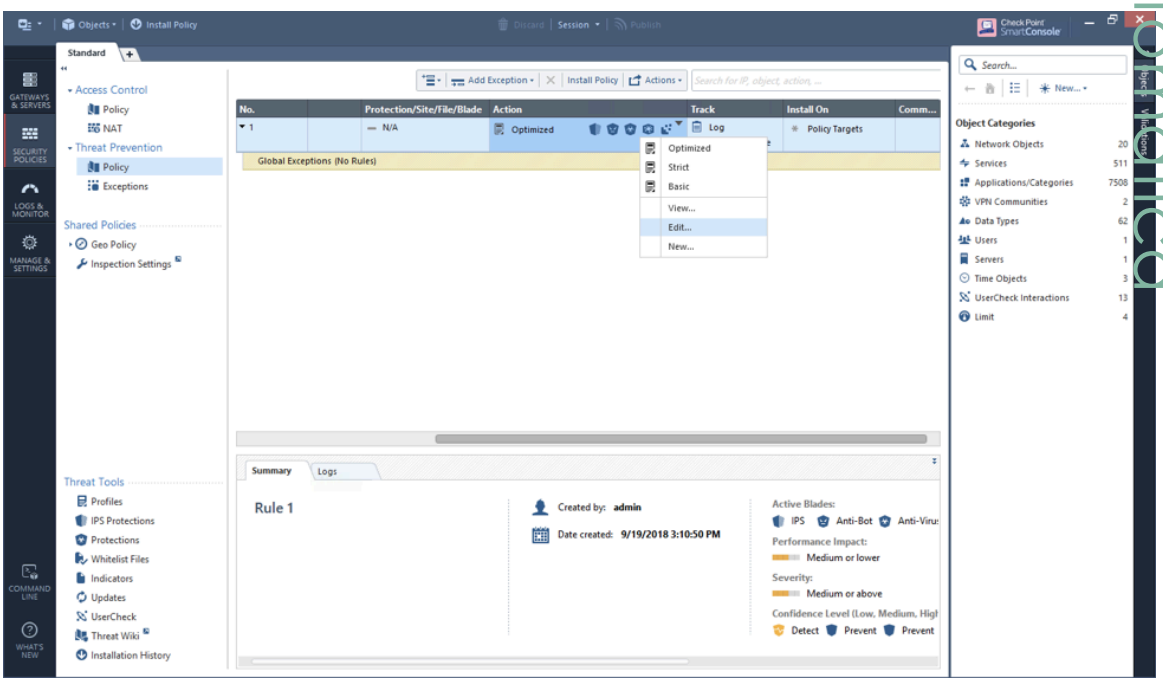
Nota: As imagens neste tópico são privilegiadas e proprietárias e são usadas com permissão da Check Point Software Tecnologias, Ltd.

a. Faça login no **Console inteligente**.

b. Navegar até **Políticas de Segurança** > **Prevenção de ameaças** > **Política**.



c. Abra a Política de prevenção de ameaças no modo de edição.



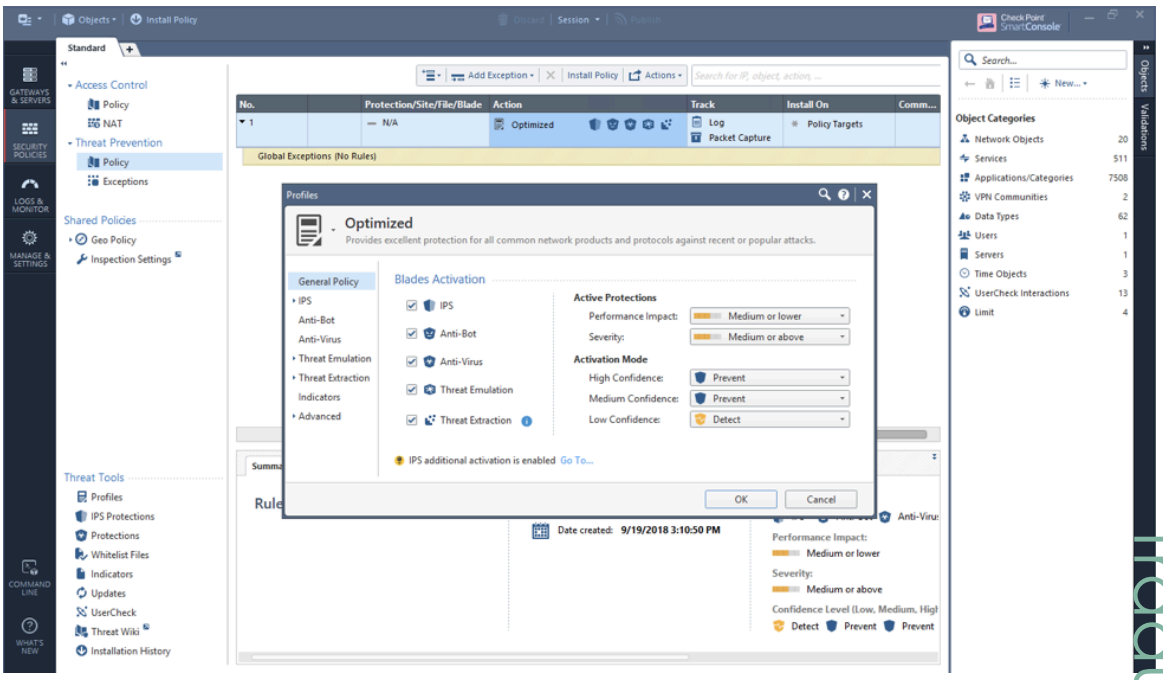
d. Proteções ativas → A gravidade deve ser "Média ou superior"

e. Modo de ativação → Confiança alta deve ser "Impedir"

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Ativação de blades a Antivírus e Antibot deve ser selecionada.



g. Publique as mudanças (se houver) e instale a política.

2. Se ainda não estiverem configurados, os feeds de inteligência personalizados deverão ser adicionados após a ativação dos blades antibot e antivírus.
Consulte a seção Instalação da documentação do Recurso de feed de inteligência personalizada do Check Point.https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Se ainda não estiver configurado, configure o Check Point Gateway para rotear todo o tráfego da Internet via Proxy HTTP (se estiver configurando a Inspeção HTTPS).

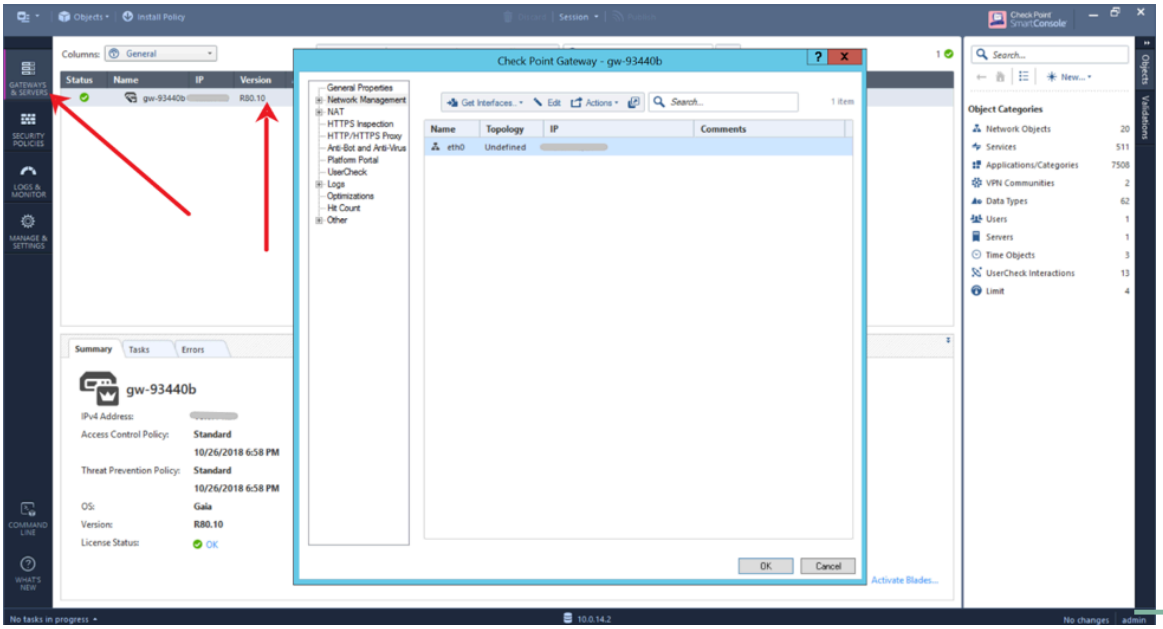
Nota: Para o bloqueio de URL no Check Point NGTP, há determinadas configurações que precisam ser garantidas. O tráfego de internet HTTPS usa o protocolo SSL (Secure Sockets Layer) e é criptografado para fornecer privacidade de dados. No entanto, o HTTPS pode ocultar tráfego mal-intencionado que deveria ter sido bloqueado. Para que o Gateway do Check Point obtenha a visibilidade do tráfego HTTPS, roteie o tráfego por meio do proxy HTTP ou configure a inspeção de HTTPS (recomendado). Esta seção detalha as etapas a serem seguidas para configurar o proxy HTTP no gateway do Check Point.

a. Faça login no **Console inteligente**.

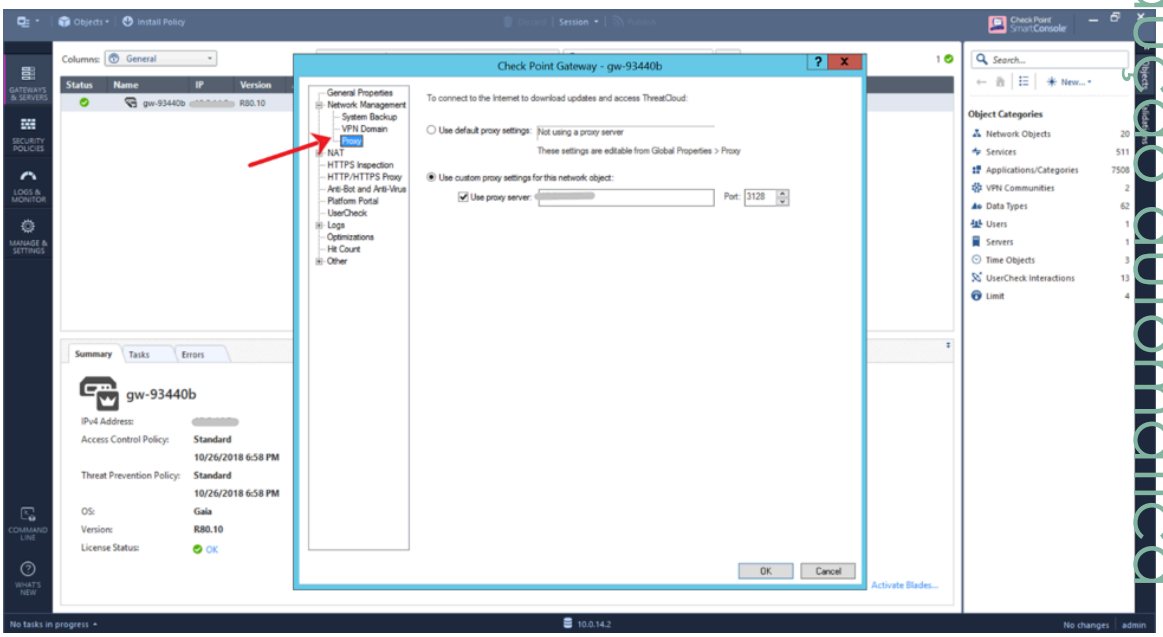
b. Navegue até **Servidores e gatewayse**clique duas vezes no servidor aplicável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Navegar até **Gestão de redes** > **Proxy**.



d. Forneça os detalhes do proxy a serem usados para roteamento do tráfego HTTP.

e. Certifique-se de que as solicitações HTTP do endpoint do cliente sejam feitas por meio do proxy HTTP.

4. Se ainda não estiver configurado, habilite a inspeção HTTPS (se o Proxy HTTP estiver configurado).
Quando a maior parte do tráfego é sobre SSL, é recomendável usar o HTTPS Inspection Blade. Isso torna o tráfego transparente para o GW. Habilite a Inspeção HTTPS no Check Point Gateway, da seguinte forma.

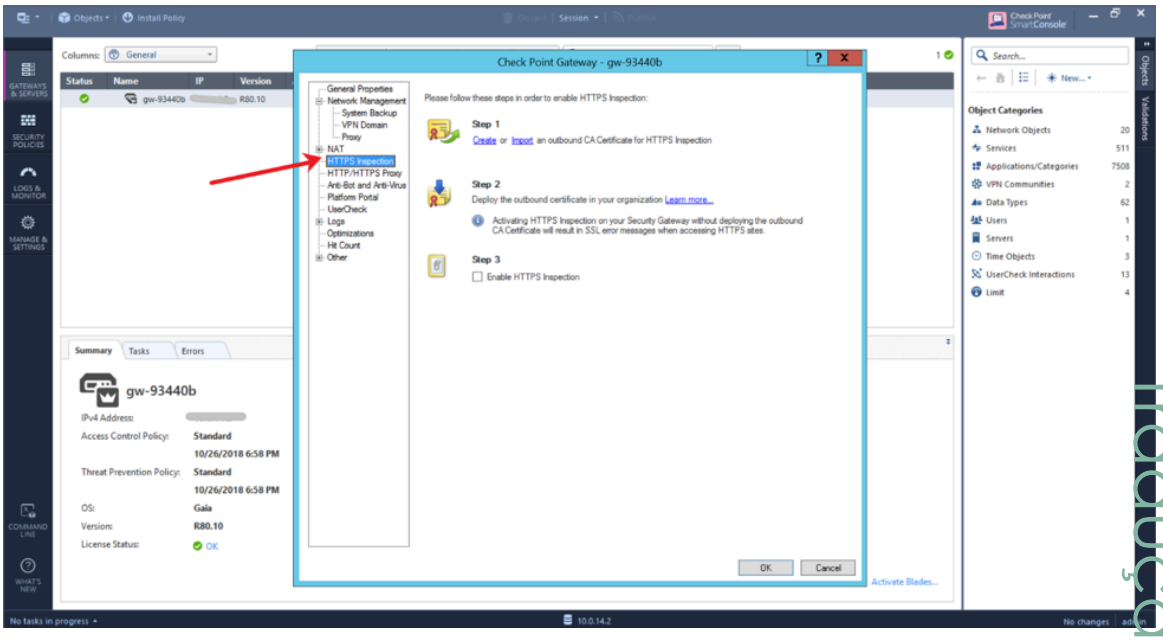
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Faça login no **Console inteligente**.

b. Navegue até **Servidores e gatewayse**clique duas vezes no servidor aplicável.

c. Navegue até **HTTPS Inspeção**.



d. Siga as etapas para configurar a Inspeção de HTTPS no Guia do usuário do Check Point.

Ativar a integração Check Point NGTP

Se você não instalou a aplicação, siga as instruções para instalá-la.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar a aplicação.
2. Navegar até **Aplicações do sistema** > **Aplicações**.
3. Clique na guia **Downloads**.
   Uma lista de aplicações disponíveis para instalação é exibida.
4. Localize a aplicação Check Point Next Generation Threat Prevention, selecione-a e clique em **Instalar**.
   Sua aplicação é instalada automaticamente em sua instância.

Trabalho com listas de bloqueios

A integração ServiceNow Check Point Next Generation Threat Prevention é compatível com listas de bloqueios que aceitam observáveis de IP, URL e domínio.

ServiceNow A lista de bloqueios configurada é um arquivo CSV hospedado em um servidor Web externo, que para esta integração é a instância da Now Platform. O Feed de inteligência personalizado é configurado no Check Point Gateway, que extrai os endereços IP, URLs e domínios da Now Platform em intervalos pré-configurados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta integração oferece suporte a três tipos de listas de bloqueios:

- Endereço IP (inclui um endereço IP individual (somente IPv4) para a lista de bloqueios e blocos CIDR (intervalos) de endereços para a lista de permissões).
- URL
- Domínio

Observáveis compatíveis com a integração Check Point NGTP

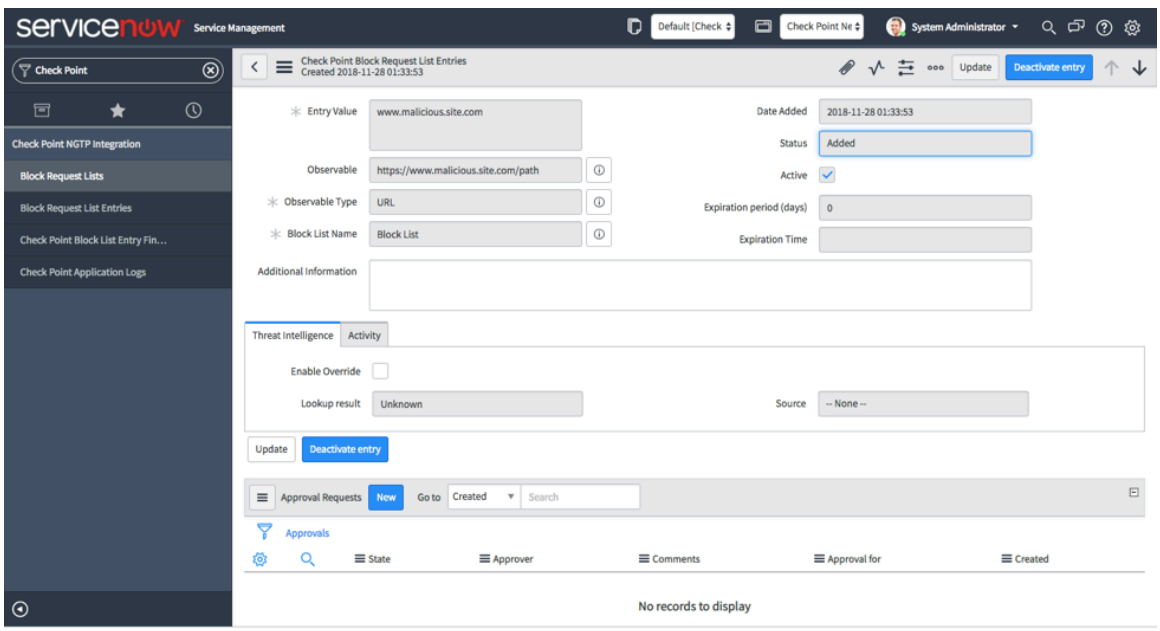
A seção lista as descrições dos observáveis compatíveis com esta integração e formatos de exemplo para cada tipo.

Tipo de Observável	Exemplos	Descrição
Domínio	• example.com • mail.example.com	Caracteres curinga não são compatíveis.
Endereço IP	95.153.103.54 (IPv4)	Representa um endereço de interface único e distinto. A integração é compatível somente com os formatos IPv4 e CIDR (o formato CIDR só é compatível para fins de listagem de permissão). Para fins de lista de permissões, a integração tem suporte para observáveis de endereço IP, incluindo intervalos CIDR (Roteamento entre domínios sem classe), por exemplo, 95.153.100.0/22. **Nota:** Uma mensagem de erro é exibida quando você tenta anexar um único endereço IP a uma Lista de Bloqueios que você já permitiu listar como parte de um intervalo CIDR. Por exemplo, o endereço único 95.153.103.54 faz parte do intervalo CIDR representado por 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.example.com • http://www.example.com	Descrição — A URL HTTPS é formatada pela aplicação para cortar o caminho da

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

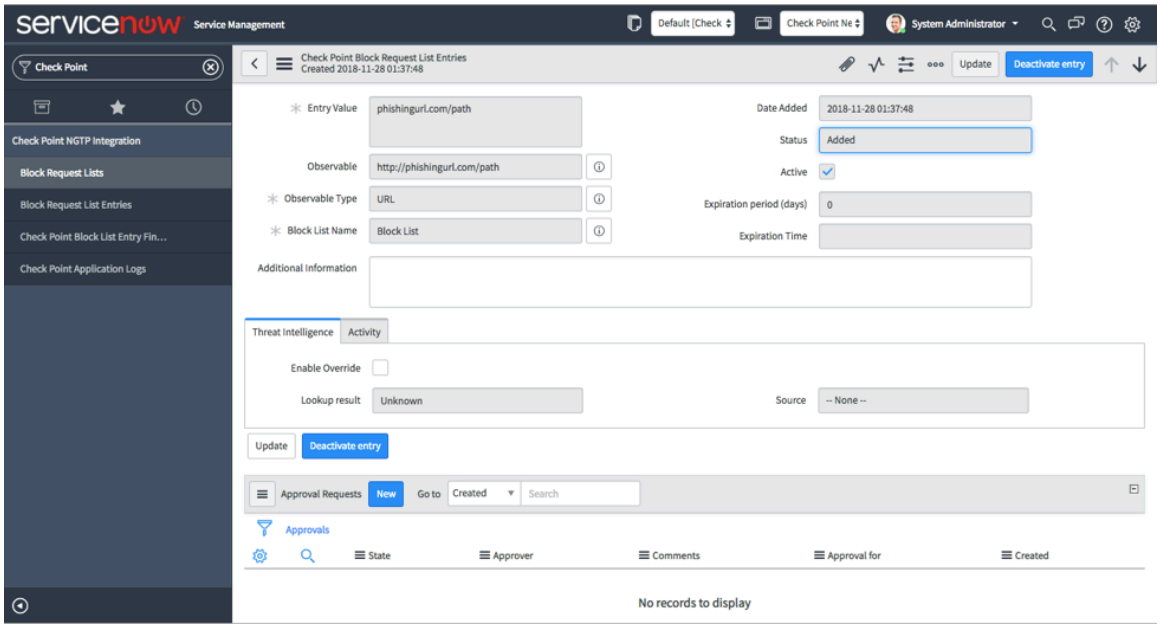
Tipo de Observável	Exemplos	Descrição
		URL e reter somente o nome do domínio. O NGTP do Check Point depende da solicitação HTTP CONNECT para avaliar o tráfego da web e impor o bloqueio. Para a solicitação HTTPS CONNECT, o URL inteiro não está visível na solicitação e somente o nome do domínio está visível. Quando um usuário bloqueia qualquer URL HTTPS com caminho específico (por exemplo: https://www.exemplo.com/caminho), a aplicação ajusta o caminho automaticamente (www.exemplo.com). A aplicação mantém o relacionamento entre o observável original e a URL formatada. Abaixo está a captura de tela da entrada da lista de bloqueios que mostra a URL formatada e o observável original.



Para URLs HTTP com um caminho específico (por exemplo, http://www.example.com/path), o Check Point bloquearia a URL especificada, pois a URL inteira está visível na solicitação CONNECT.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar uma lista de bloqueios para a integração Check Point NGTP

Crie uma lista de bloqueios em sua instância da Now Platform. Depois de aprovado e ativado, você pode criar entradas para essas listas de bloqueios a partir de observáveis determinados como mal-intencionados em incidentes do Now Platform Security Incident Response (SIR) e solicitar aprovação para bloqueá-los.

Antes de Iniciar

Função necessária: administrador de incidentes de segurança (sn_si.admin)

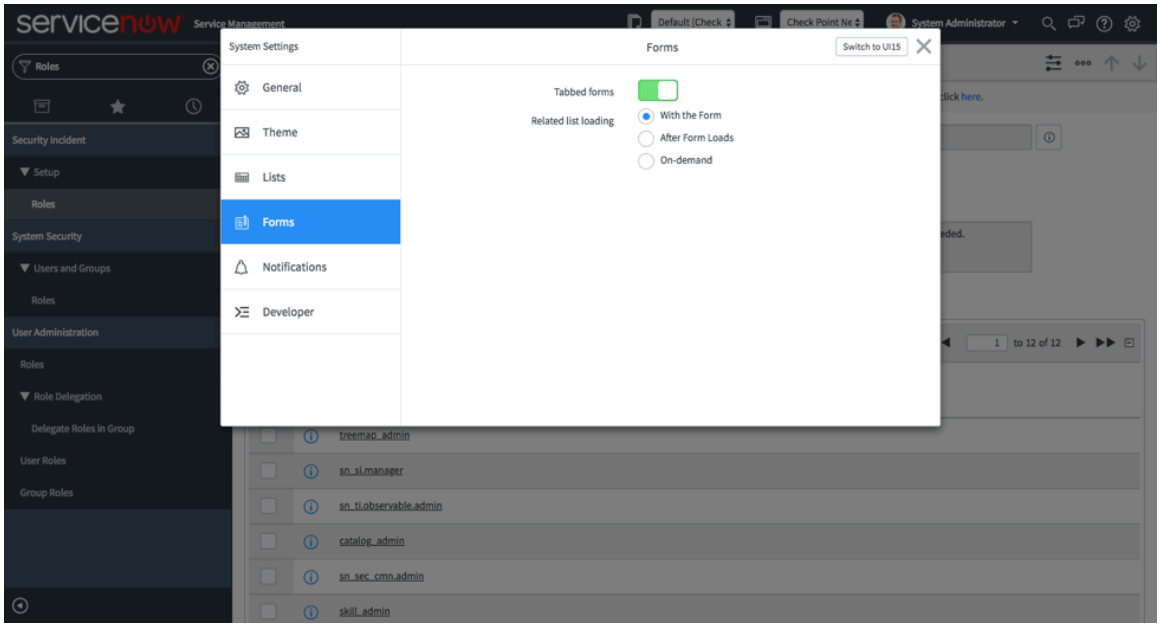
Por Que e Quando Desempenhar Esta Tarefa

Crie a lista de bloqueios em sua instância da Now Platform para que o Check Point possa importar objetos (endereços IP, URLs, domínios) incluídos na lista. O feed de inteligência personalizado é configurado no Check Point Gateway, que extrai os endereços IP, URLs e domínios da plataforma Now em intervalos pré-configurados. Para garantir o bloqueio dos observáveis, a Política de prevenção de ameaças deve ser configurada com os Blades Anti-Bot e Anti-Virus ativados.

Nota: As imagens neste tópico são mostradas com os **Formulários** com guia limpos em Configurações do sistema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Procedimento

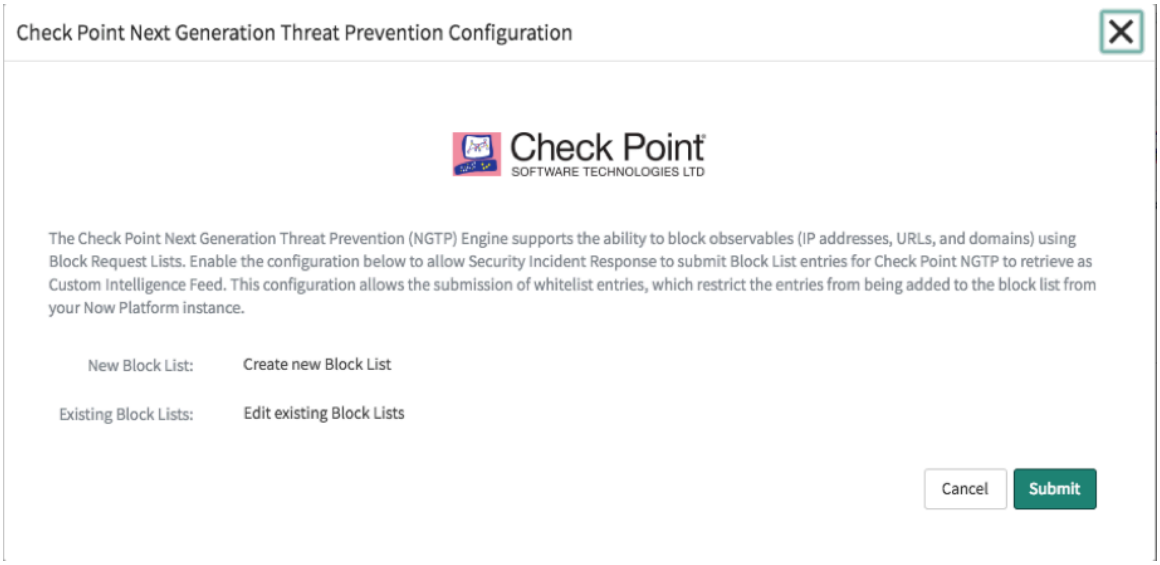
1. Depois que a instalação da aplicação estiver concluída, navegue até **Integrações** > **Configurações de Integração**.
2. Localize o cartão **de prevenção de ameaças de última geração do Check Point** e clique em **Configurar**.

Nota: Conteúdo privilegiado e proprietário usado com permissão da Check Point Software Tecnologias, Ltd.

3. Clique **em Criar nova lista de bloqueios**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da lista de solicitações de bloqueio do Check Point. Inclua o tipo de observável (URL, IP, domínio) neste campo para que o analista de segurança possa reconhecer facilmente a intenção da Lista de Bloqueios pelo nome. O nome também deve indicar claramente para qual política de firewall esses objetos da Lista de bloqueios estão mapeados. Alguns exemplos de nomes de lista de bloqueios são IP de malware de saída ou URL de phishing de saída.
Ativo	Esta caixa de seleção está desmarcada por padrão para indicar que a Lista de bloqueios está inativa. Quando inativa, a Lista de Bloqueios não pode receber entradas adicionais. Quando a caixa de seleção está marcada (quando a solicitação de mudança é fechada ou a solicitação de mudança não é gerada), a lista de bloqueios é ativada e fica disponível para entradas da lista de bloqueios.
Marcador de exibição	A caixa de seleção é marcada por padrão para marcar automaticamente o observável e o registro de incidente de segurança associado se o observável estiver bloqueado na Lista de bloqueios. Quando selecionado, o campo "Marcador para observáveis" fica disponível no formulário. **Nota:** Um nome de marcador é criado por padrão a partir do valor inserido no campo Nome com um prefixo de Check Point, por exemplo, Check Point-Malware OutBound IP. Você pode mudar o nome e a cor do marcador. O nome do marcador é exibido no campo "Marcador para observáveis" quando a lista de bloqueios é salva.

Tradução automática

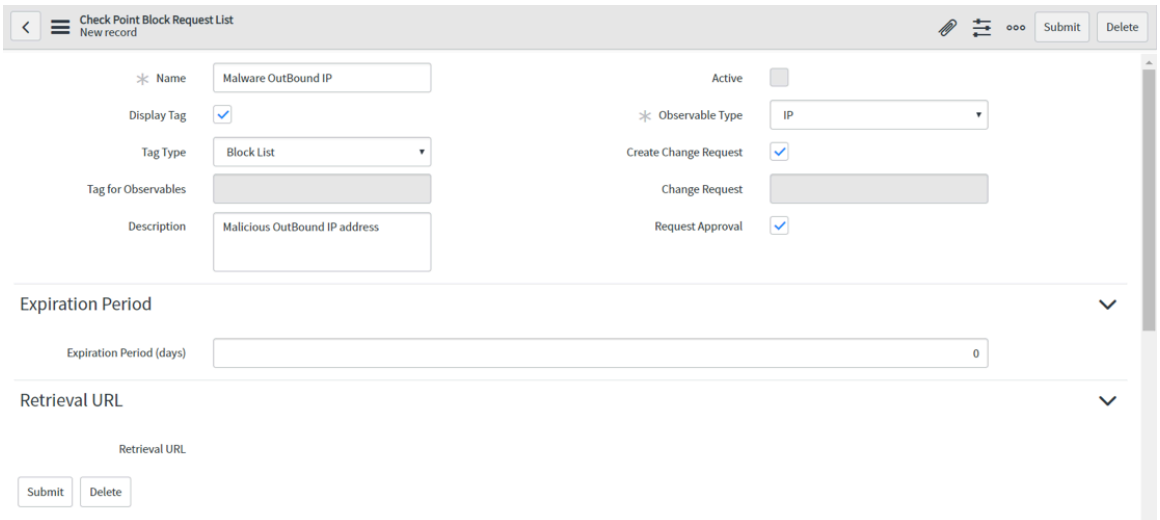
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Quando a caixa de seleção está desmarcada, nenhum marcador é criado e o campo "Marcador para observáveis" não está disponível no formulário.
Tipo de Observável	Selecione um tipo de observável que esta Lista de Bloqueios aceita na lista: Endereço IP (incluindo CIDR para lista de permissões), URL ou domínio.
Tipo de marcador	Marcadores que estão disponíveis na lista. Uma Lista de bloqueios é uma lista de observáveis que você deseja que a Prevenção contra ameaças de última geração do Check Point bloqueie. Uma lista de permissões é uma lista de observáveis que você não deseja bloquear na Prevenção contra ameaças de última geração do Check Point. Por padrão, a cor do marcador da Lista de bloqueios é preta e a cor do marcador da lista de permissões é Cinza. Você pode mudar a cor.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em sua instância da Now Platform, que estão anexadas ao registro da Lista de bloqueios. A solicitação de mudança é usada para configurar a URL de recuperação da Lista de Bloqueios no gateway de firewall do Check Point Next Geração. Esta opção é recomendada se o administrador do firewall também estiver usando a Now Platform para mudanças de política ou regra de firewall. Se você criar uma solicitação, depois que ela for fechada, a Lista de bloqueios será ativada automaticamente. Desmarque a caixa de seleção para ativar manualmente a Lista de bloqueios após receber um aviso por e-mail do administrador do firewall de que o Feed de inteligência personalizado foi configurado em todos os gateways do Check Point. Quando a caixa de seleção de Criar solicitação de mudança está desmarcada, o campo Solicitação de mudança fica indisponível.
Solicitar Aprovação	Esta caixa de seleção é marcada por padrão para solicitar aprovações para ativar/remover entradas da Lista de bloqueios das Listas de bloqueios. A aprovação é solicitada aos usuários com a função de Administrador de incidentes de segurança (sn_si.admin). A solicitação de aprovação será enviada por e-mail para os aprovadores. Depois que a aprovação for aceita, a entrada será ativada nessa Lista de Bloqueios. Quando a caixa de seleção não estiver marcada, as entradas dessa lista de bloqueios não seguirão o fluxo de trabalho de aprovação e serão ativadas diretamente na lista de bloqueios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

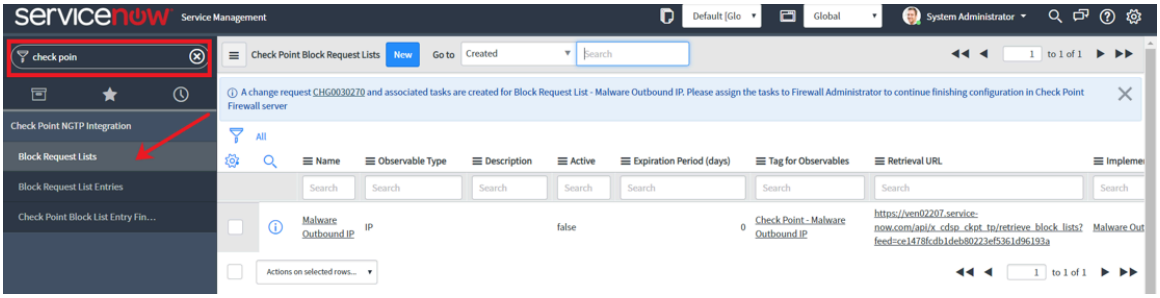
Campo	Descrição
Marcador para observável	Este campo será exibido somente se a caixa de seleção Exibir marcador estiver marcada. O campo é preenchido automaticamente depois que a Lista de bloqueios é salva com um valor padrão do campo Nome. Se a Lista de bloqueios for criada com o nome "URL do malware", o nome do marcador derivado será "Lista de bloqueios - URL do malware"
Solicitação de mudança	Quando a caixa de seleção Criar solicitação de mudança está marcada, o número da solicitação de mudança é exibido na instância da Now Platform depois que a Lista de bloqueios é salva. Quando a caixa de seleção de Criar solicitação de mudança está desmarcada, este campo não é exibido.
Descrição	Descrição da lista de blocos do Check Point. O nome geralmente contém os tipos de sites e observáveis que você espera que estejam nesta Lista de Bloqueios e você pode usar este campo para obter mais detalhes.
Período de Expiração (dias)	Período de expiração da lista de bloqueios. 0 (o padrão) indica que a entrada da Lista de bloqueios nunca expira. Se você alterar este valor, esta entrada ficará ativa pelo número de dias inserido. Você pode inserir um valor mínimo de 1, que corresponde a 24 horas, e não há valor máximo.
URL de recuperação	A URL de Recuperação será gerada automaticamente, depois que a Lista de Bloqueios for salva. Para configurar esta Lista de Bloqueios em Gateways do Check Point, você deve usar este URL. Depois que este URL é configurado, o Check Point busca os observáveis a serem bloqueados no formato csv.



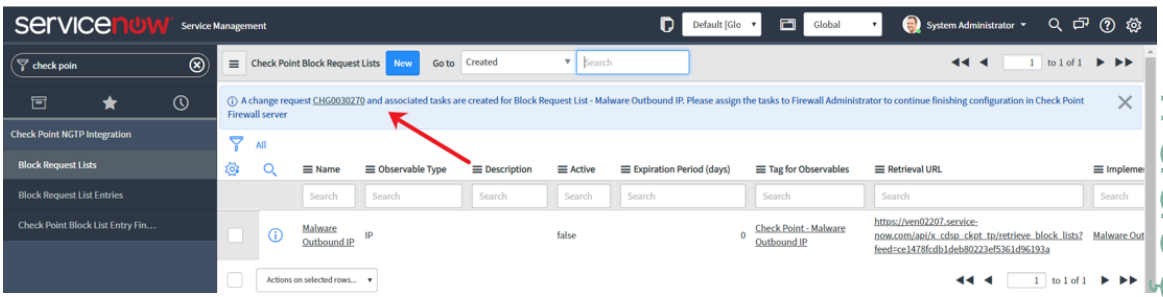
5. Clique em **Enviar**.
6. Se a Lista de Solicitação de Bloqueio do Check Point não for exibida, navegue até **Integração de NGTP do Ponto de Verificação** > **Listas de solicitações de bloqueio**.

Tradução automática

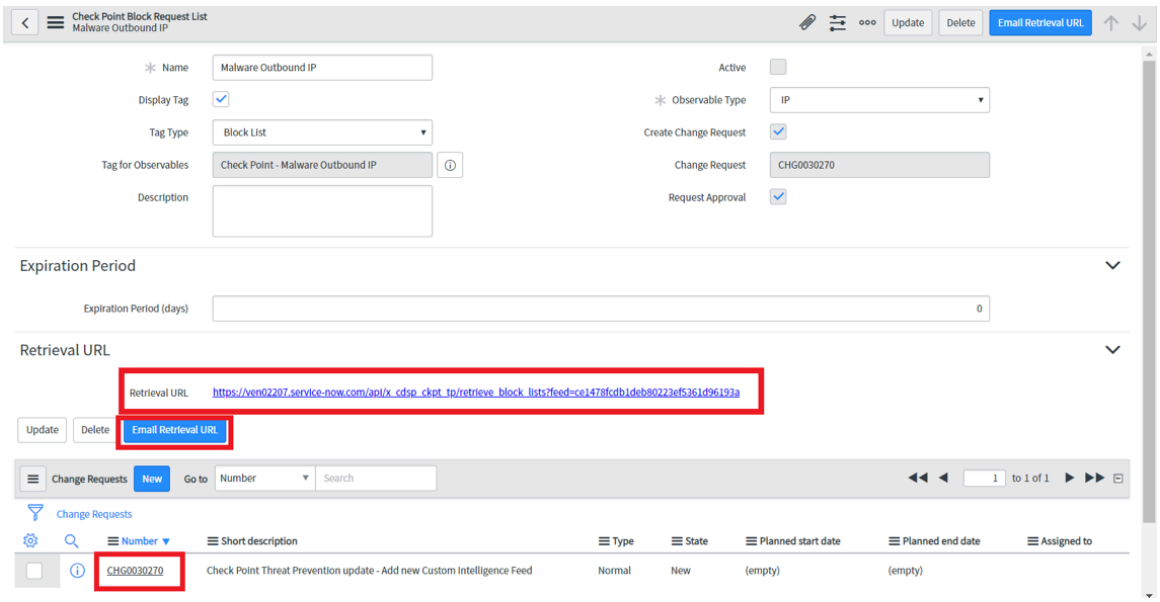
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A nova lista de bloqueios é exibida. O status da Lista de bloqueios ainda está inativo (falso), o que significa que a Lista de bloqueios não está disponível para aceitar entradas. Se Criar solicitação de mudança tiver sido configurado, uma mensagem será exibida indicando que uma solicitação de mudança e tarefas foram criadas em sua instância da Now Platform.



7. Na coluna **Nome**, clique em um item para abrir o registro.
O registro da Lista de bloqueios é exibido. Este exemplo mostra uma Lista de Bloqueios de IP de Saída de Malware. Os campos, opções e links a seguir são exibidos no novo registro após o envio e descritos na tabela a seguir.



Campo	Descrição
URL de Recuperação de E-mail	Envia por e-mail um aviso de que o link do bloco está disponível para configuração para o administrador do firewall do Check Point.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL de recuperação	Este URL é usado para configurar o feed de inteligência personalizado em gateways do Check Point. **Nota:** Se você tiver as Configurações do sistema definidas como Formulários com guias, este link será exibido na guia Informações de recuperação da lista de bloqueios na parte inferior do registro.
Solicitação de mudança da Now Platform	Um link para o registro de solicitação de mudança é exibido na seção Solicitações de mudança quando configurado, e o número da solicitação é exibido no campo Solicitação de mudança.
Atualizar	Modifique os dados e atualize os campos editáveis.
Excluir	Exclua o registro.

8. Crie e adicione mais listas de bloqueios conforme necessário.
   As Listas de Bloqueio são exibidas na Página de Listas de Solicitação de Bloqueio do Check Point.

O que Fazer Depois
Ative a lista de solicitação de bloqueio manualmente ou com uma solicitação de mudança da Now Platform.

Ativar uma lista de bloqueios para a integração Check Point NGTP

Depois que a Lista de bloqueios tiver sido criada na Now Platform e o URL estiver disponível, o administrador do Check Point configurará a Lista de bloqueios como Feed de inteligência personalizado em todos os Gateways de última geração do Check Point. Antes que ele possa aceitar entradas da Lista de bloqueios, a Lista de bloqueios deve ser configurada no Check Point e ativada na Now Platform.

Antes de Iniciar
Função necessária: administrador de incidentes de segurança (sn_si.admin)

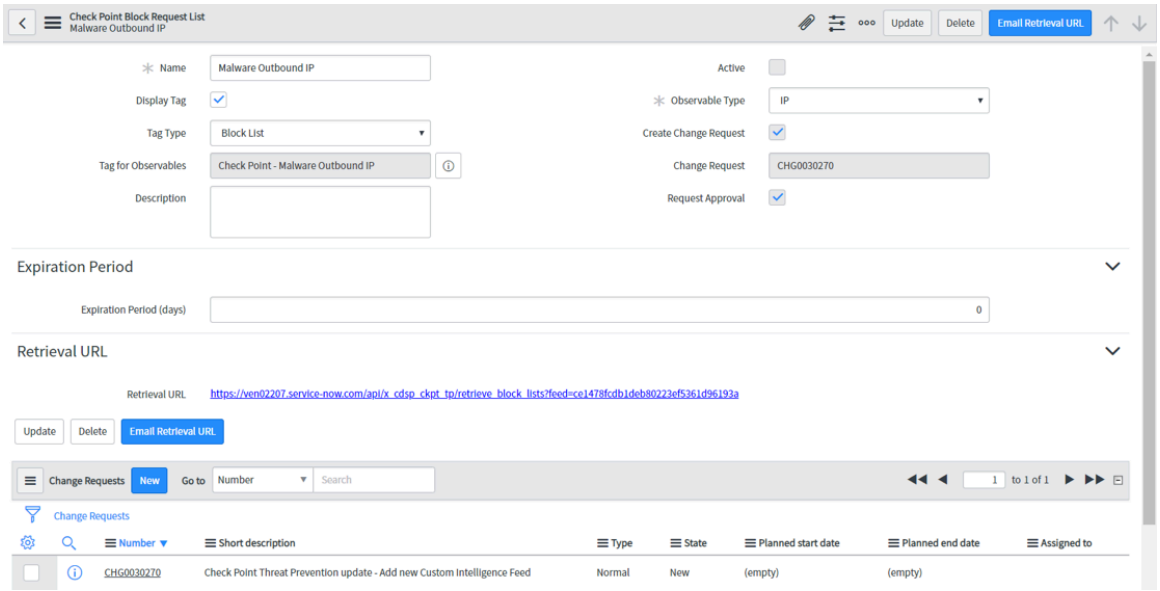
Por Que e Quando Desempenhar Esta Tarefa
Depois que a Lista de bloqueios for configurada, como administrador do incidente de segurança, você poderá ativar a Lista de bloqueios manualmente ou a Lista de bloqueios será ativada automaticamente após a conclusão de uma solicitação de mudança da Now Platform. A Solicitação de Mudança deve ser aprovada e movida do estado inativo para o estado ativo antes que possa aceitar entradas da Lista de Bloqueio.

Procedimento

1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Listas de solicitações de bloqueio**e selecione o módulo **Listas de solicitação de bloqueio**.
2. Na lista **Listas de solicitação de bloqueio do Check Point** exibida, selecione sua nova Lista de bloqueios na coluna **Nome**.
3. No registro exibido, observe o botão **URL de recuperação de e-mail**, o link ativo da URL de recuperação da lista de bloqueios e, se configurado, a solicitação de mudança da Now Platform na seção Solicitações de mudança.
   Observe também que a caixa de seleção Ativo está desmarcada.

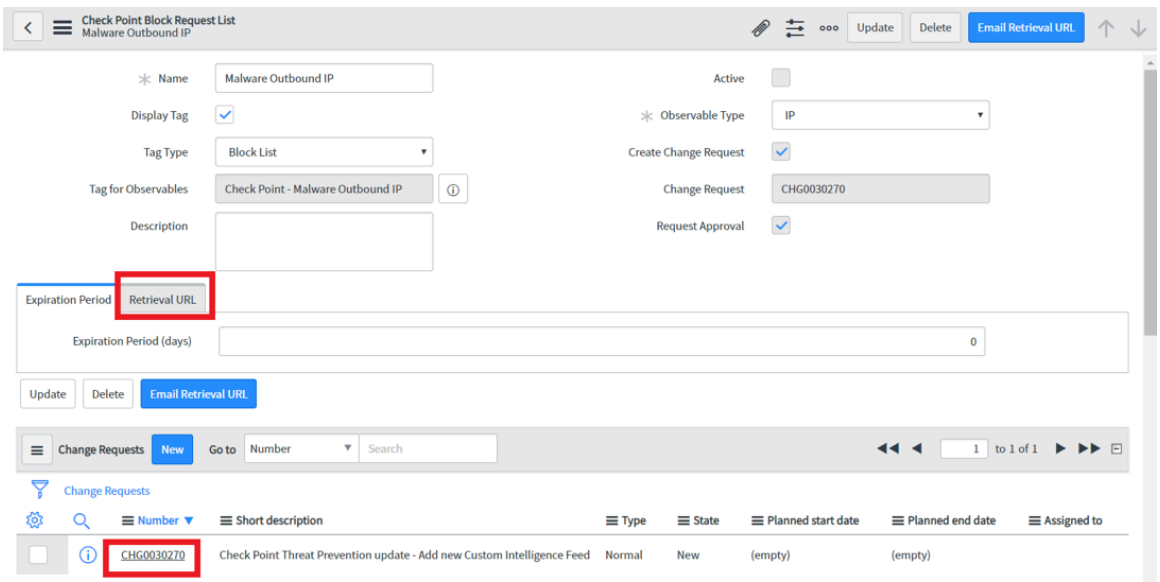
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Com os Formulários com guias limpos nas configurações do sistema, a URL de Recuperação da Lista de Bloqueios aparece na seção URL de Recuperação.

4. Clique na guia **URL de recuperação da lista de bloqueios** para exibir a URL de recuperação.
   A figura a seguir mostra a URL de Recuperação da Lista de Bloqueios exibida como uma guia com os Formulários com guia selecionados nas configurações do sistema. O link para a solicitação de mudança (CH0030270) também é exibido.



5. Para concluir a configuração e mover a Lista de bloqueios de inativa para ativa, você deve escolher uma das seguintes opções para notificar o administrador do firewall de que o URL de recuperação está disponível.

Opção	Descrição
Clique em URL de recuperação de e-mail.	URL de Recuperação da Lista de Bloqueios de E-mail diretamente para o administrador do firewall. Esta opção permite que o administrador do firewall conclua a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	configuração na plataforma Check Point. Escolha esta opção se o administrador do firewall não estiver usando a Now Platform.
Conclua a solicitação de mudança da Now Platform e atribua as tarefas de configuração ao administrador do firewall.	Esta opção estará disponível somente se o administrador de firewall do Check Point também estiver usando a Now Platform e os processos de aprovação e gestão de mudanças da Now Platform estiverem configurados. **Nota:** Usuários com a função de Administrador de incidentes de segurança (sn_si.admin) podem aprovar a solicitação de mudança da Now Platform. Depois que as tarefas de configuração são concluídas e a solicitação de mudança é encerrada, a Lista de bloqueios é ativada automaticamente.

O que Fazer Depois

Depois de notificar o administrador do firewall de que o URL de recuperação está disponível e você confirmar que a Lista de bloqueios foi configurada no Check Point, como administrador de incidentes de segurança, a próxima etapa é ativar a Lista de bloqueios. Você ativa a Lista de bloqueios manualmente ou, se configurada, usa o formulário de solicitação de mudança da Now Platform para ativar a Lista de bloqueios. A Lista de Bloqueios é ativada automaticamente quando a solicitação de mudança é fechada.

Configurar uma lista de bloqueios como um Feed de inteligência personalizado na integração Check Point NGTP

O administrador do firewall deve configurar o feed de inteligência personalizado correspondente à lista de bloqueios criada na plataforma NOW.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Esta tarefa precisa ser realizada em cada um dos Gateways NGTP do Check Point. O administrador do firewall precisaria do acesso SSH dos servidores de gateway. Se sua organização tiver processos de aprovação e gestão de mudanças na Now Platform, verifique se a capacidade de envio/recebimento de e-mail está habilitada.
O administrador do firewall precisaria da URL de recuperação da Lista de bloqueios e das credenciais do usuário da ServiceNow com a função Função de acesso à conta da API do Check Point (sn_sec_checkpoint.api_account_access).

Se o administrador do firewall não estiver usando a plataforma NOW, o administrador de incidentes de segurança NOW poderá fornecer as informações necessárias por e-mail. Como alternativa, se o administrador do firewall estiver usando a plataforma NOW, a solicitação de mudança associada à lista de bloqueios poderá ser atribuída ao administrador do firewall. Esta solicitação de mudança tem as informações necessárias para configurar o Feed de inteligência personalizado.

Para obter mais informações sobre como configurar o feed de inteligência personalizado em gateways do Check Point, consulte: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Verifique se a capacidade de envio/recebimento de e-mail está habilitada em sua instância da Now Platform navegando até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**.
2. Em Configuração de e-mail de saída, verifique se **Envio** de e- **mail** e Recebimento de e-mail estão selecionados.
3. Modifique o SSH para o gateway do Check Point com o modo especialista.
4. Execute o comando para adicionar o feed de inteligência personalizado.
   A execução do comando é interativa e solicita o formato e a senha do feed.
   - Quando solicitado a informar o formato do feed, insira "cp_csv"
   - Quando a senha do usuário da plataforma NOW for solicitada com acesso de API.

   A execução do comando avisaria sobre o certificado do servidor (plataforma NOW) que não é confiável para a máquina e solicitaria a adição do certificado de segurança do servidor ao armazenamento confiável da máquina. Insira **Y**.

   A mensagem "Status:Êxito" será exibida, confirmando que o feed foi adicionado com sucesso.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Enviar entradas da lista de bloqueios de um incidente de segurança para a integração Check Point NGTP

Os observáveis anexados a um registro de incidente de segurança são enviados para aprovação como entradas da Lista de bloqueios para diferentes Listas de bloqueios. Um processo de aprovação opcional para entradas da Lista de bloqueios faz parte do fluxo de trabalho pré-configurado. O Gateway importa entradas da Lista de bloqueios - endereços IP, URLs, domínios - que estão incluídas nas Listas de bloqueios.

Antes de Iniciar

Função necessária:

- Analista de incidentes de segurança (sn_si.analyst) para enviar entradas da lista de bloqueios.
- Administrador de incidentes de segurança (sn_si.admin) para aprovar entradas da lista de bloqueios. Esta autoridade pode ser atribuída conforme exigido pela sua organização.

Por Que e Quando Desempenhar Esta Tarefa

Usuários com a função sn_si.analyst enviam entradas de bloqueio solicitando um bloqueio em observáveis anexados a um registro de incidente de segurança. Depois de enviada, uma entrada da Lista de bloqueios com um status Pendente é gerada e enviada para

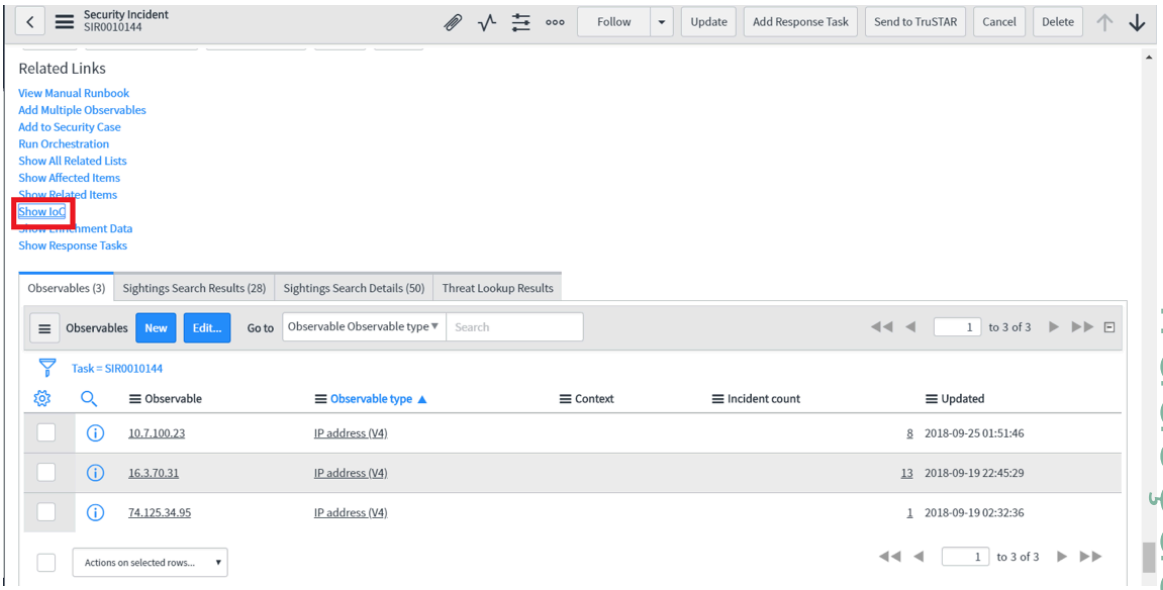
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

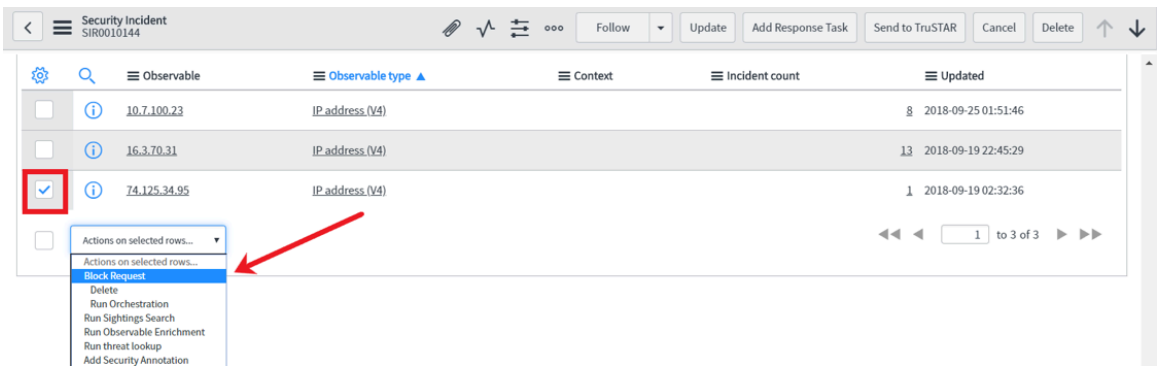
aprovação. O exemplo a seguir mostra uma solicitação de bloqueio para um observável de URL.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**e clique em um registro de incidente de segurança para abri-lo.
2. Clique no link relacionado **Mostrar IoC**.



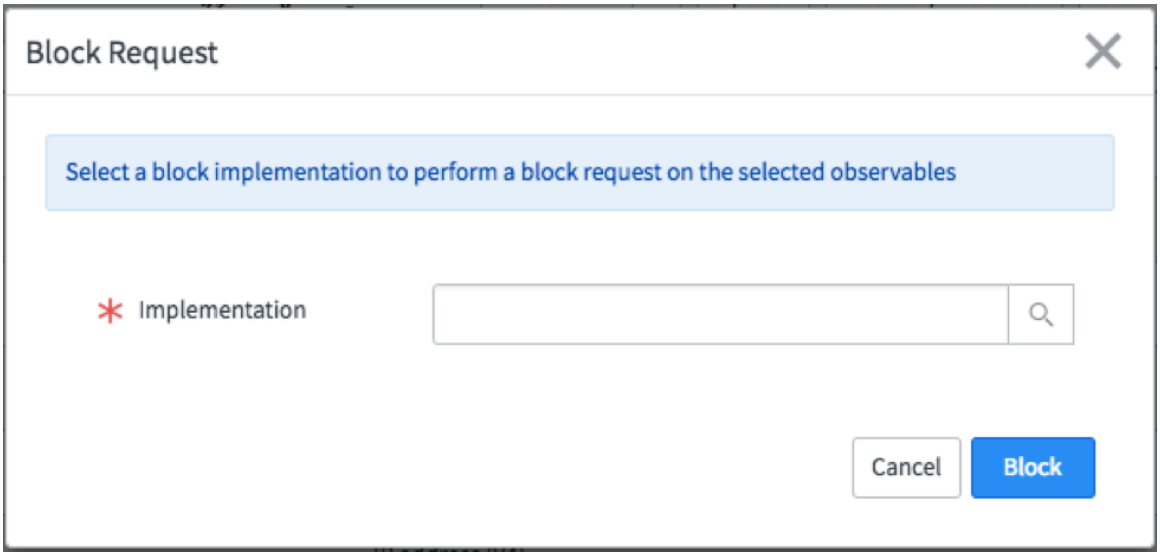
3. Na lista relacionada Observáveis, selecione os observáveis que você deseja bloquear e, na lista **Ações nas linhas selecionadas**, selecione **Bloquear solicitação**.



4. Na caixa de diálogo exibida, clique no ícone de pesquisa (ícone)

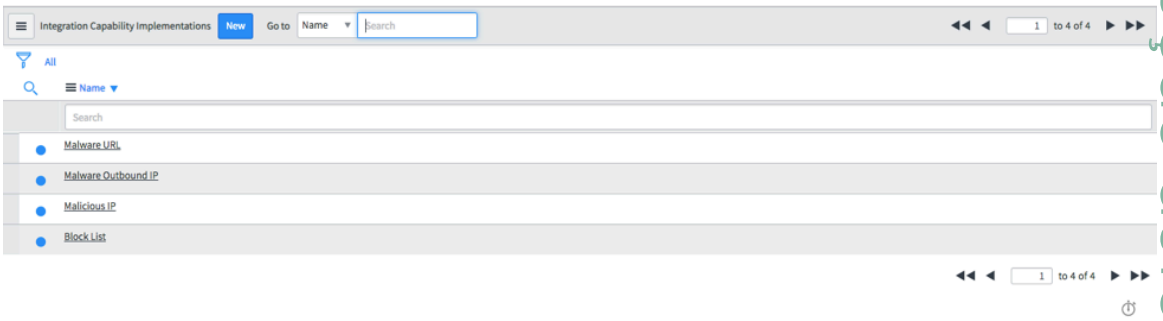
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

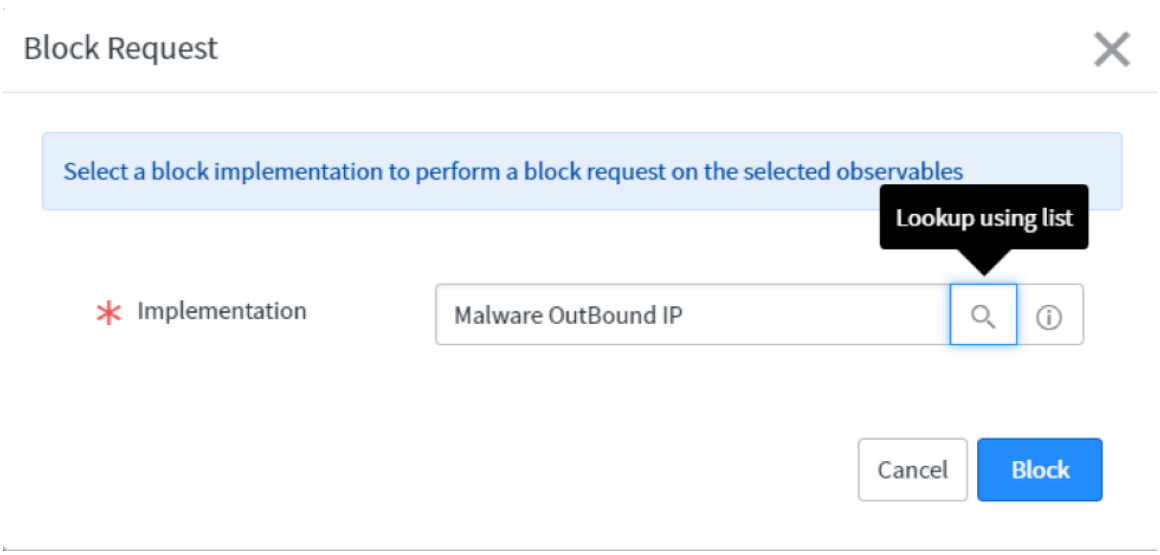


5. Na lista, selecione a Lista de bloqueios à qual deseja anexar esta entrada.

Nota: Para este exemplo, o tipo de observável entrada (IP) deve corresponder ao tipo de observável lista de bloqueios (IP).



6. Na caixa de diálogo Solicitação de bloqueio com o nome da Lista de bloqueios exibido no campo Implementação, clique em **Bloquear**.

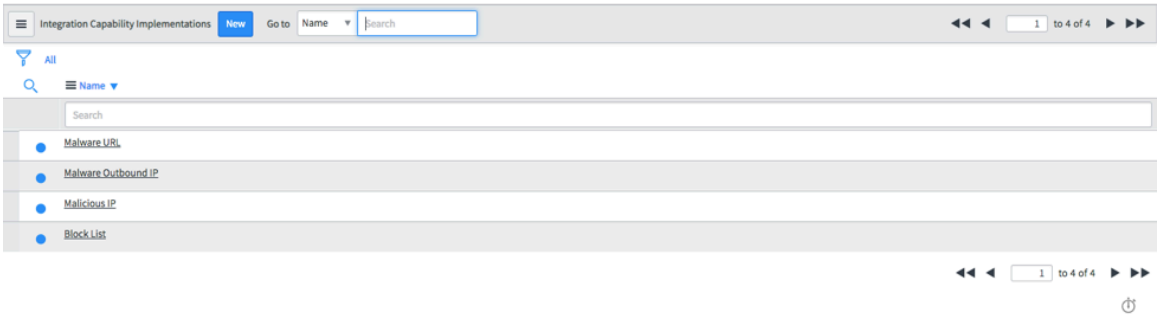


7. Na lista exibida, selecione a Lista de bloqueios à qual deseja anexar esta entrada.

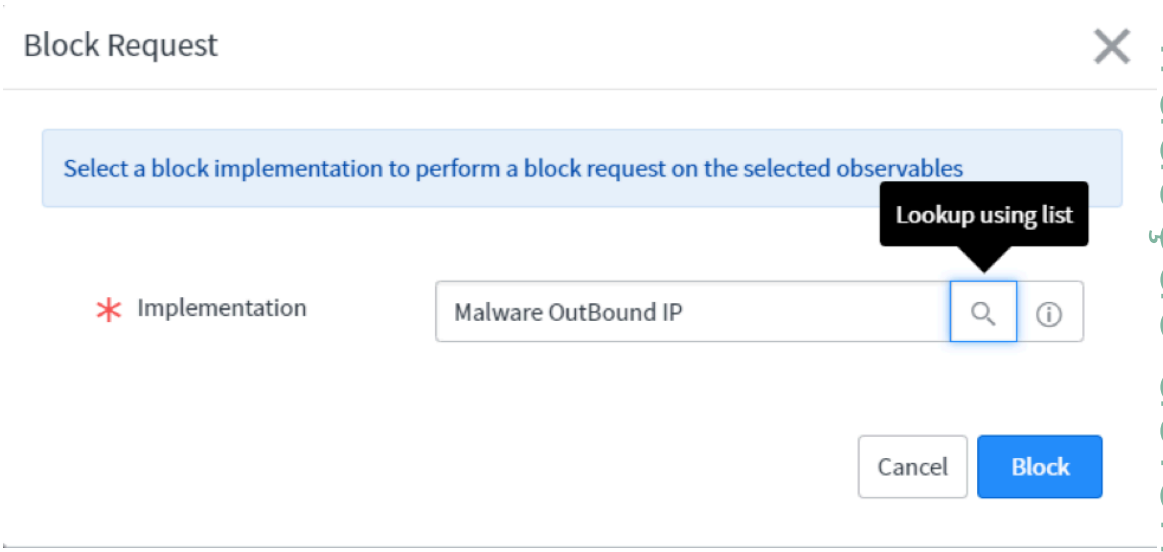
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

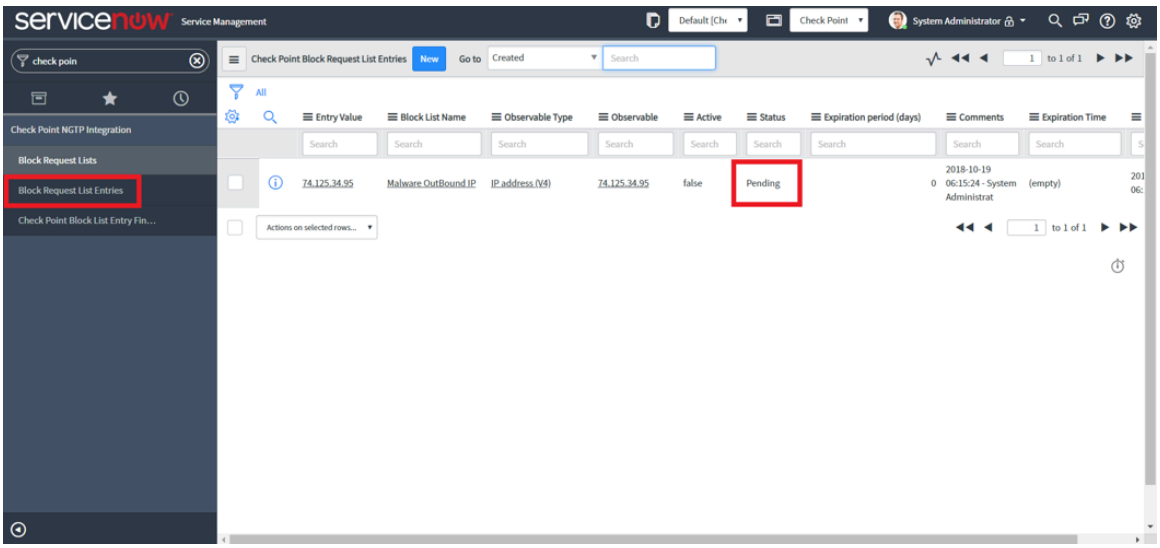
Nota: Para este exemplo, o tipo de observável entrada (IP) deve corresponder ao tipo de observável lista de bloqueios (IP).



8. Na caixa de diálogo Solicitação de bloqueio com o nome da Lista de bloqueios exibido no campo **Implementação**, clique em **Bloquear**.



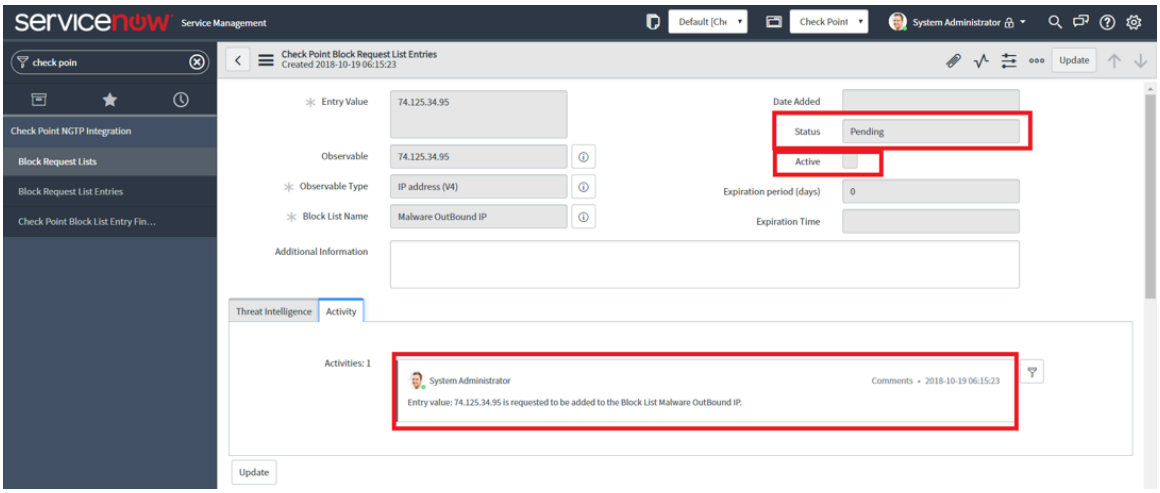
9. Navegar até **Integração de NGTP do Ponto de Verificação** > **Bloquear Entradas da Lista de Solicitaçõe**s e clique em **Entradas da lista de solicitação de bloqueio**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Na lista Entradas da lista de solicitações de bloqueio do Check Point, clique no observável na coluna **Valor de entrada** para abrir o registro.
Para este exemplo, o registro para **74.125.34.95** é exibido.



O status é Pendente, a caixa de seleção Ativo está desmarcada e as anotações de trabalho mostram que há uma solicitação para adicionar o observável. Esta solicitação de entrada da lista de bloqueios está pronta para aprovação.

O ícone ao lado do campo Observável é um link para a tabela Observável da Now Platform.

O valor no campo Observável (74.125.34.95) está vinculado à tabela Observável e corresponde ao formato que foi trazido do evento de acionamento de incidente do Security Incident Response.

Enviar entradas da lista de bloqueios diretamente da Tabela de entrada da lista de bloqueios

Para observáveis determinados como mal-intencionados e não associados a um incidente de segurança específico da Now Platform, você envia entradas da Lista de bloqueios da lista de bloqueios.

Antes de Iniciar
Função necessária: administrador de incidentes de segurança (sn_si.analyst)

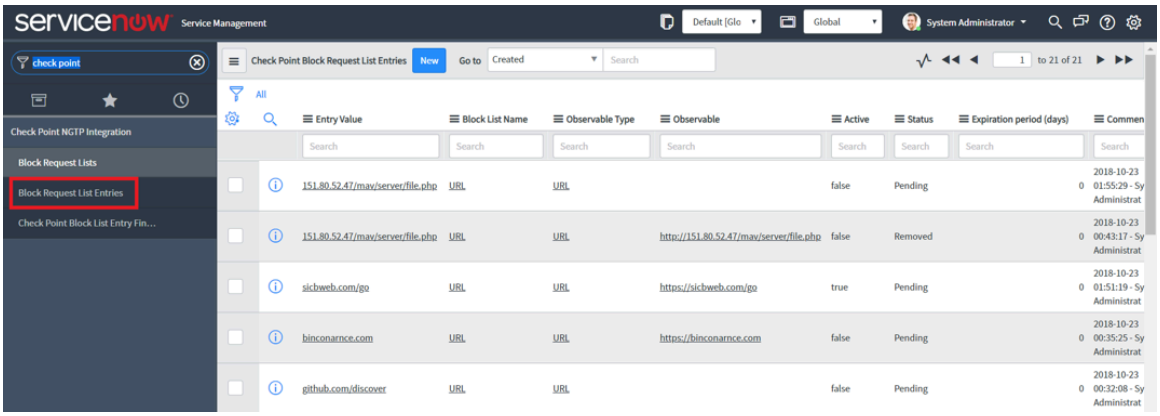
Por Que e Quando Desempenhar Esta Tarefa
Quando você quiser bloquear um observável que você determinou ser mal-intencionado ou permitir que um observável que você determinou não seja mal-intencionado e o observável não estiver associado a um registro de incidente de segurança específico da Now Platform, envie entradas da Lista de bloqueios diretamente da lista de bloqueios. Exemplos desses tipos de entradas da Lista de bloqueios podem ser URLs ou domínios para sites específicos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

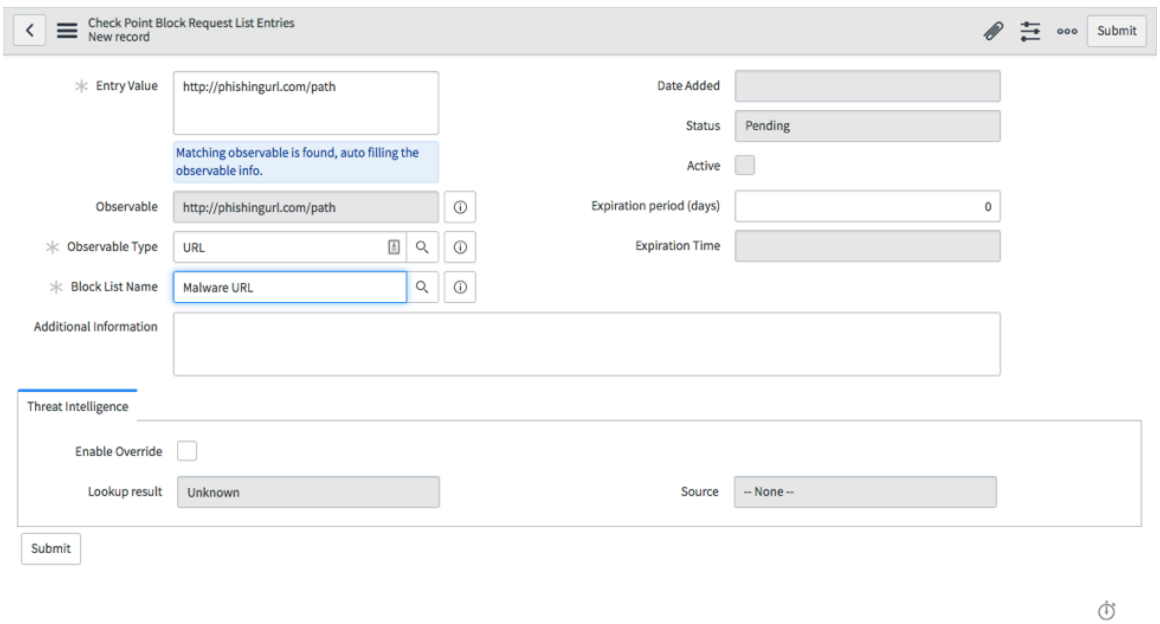
Procedimento

1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Bloquear entradas de solicitação**.



2. Clique no módulo **Listas de solicitação de bloqueio**.
3. Na lista Entradas da lista de solicitações de bloqueio do Check Point, clique em **Novo**.
4. No campo **Valor de entrada**, insira um valor para o observável.
   Os dois resultados possíveis desta entrada:
   - Os campos restantes no formulário são preenchidos automaticamente.
   - Um observável correspondente é encontrado e uma mensagem é exibida informando que existe um observável correspondente. Selecione a Lista de Bloqueios à qual deseja anexar esta entrada e clique em Enviar. Selecione a lista de bloqueios à qual você deseja anexar esta entrada antes de definir o período de expiração.

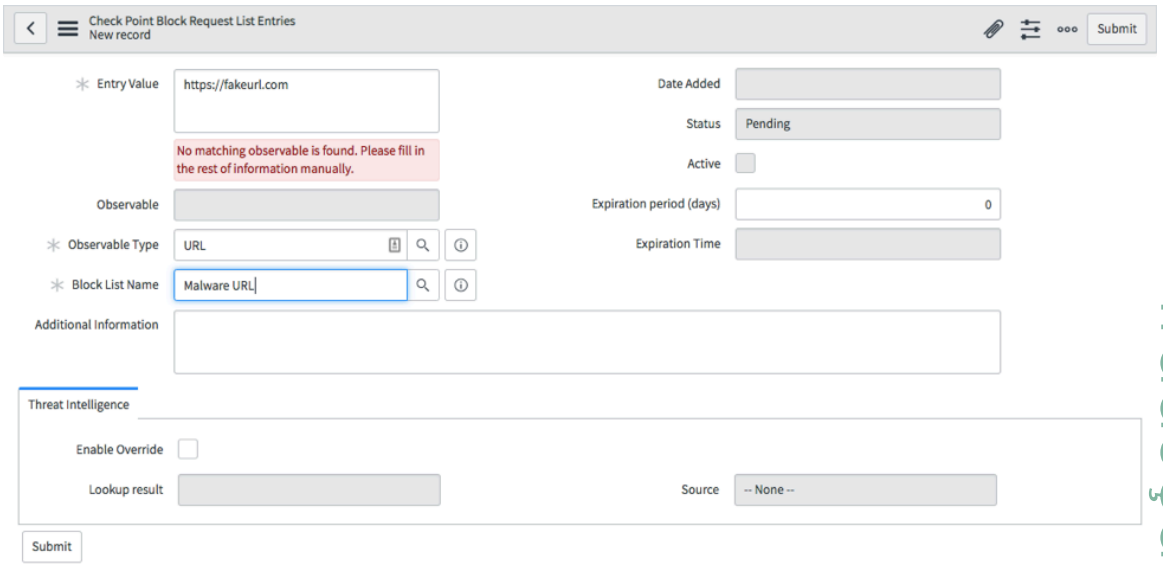
   Uma mensagem será exibida instruindo você a preencher o formulário. Um observável correspondente não foi encontrado e você deve preencher o formulário. Depois de concluir, selecione a Lista de bloqueios à qual deseja anexar o observável e clique em Enviar. Um registro observável é criado. A figura a seguir mostra um exemplo de um observável de domínio existente e como os campos são preenchidos automaticamente.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique no ícone de pesquisa para selecionar a Lista de Bloqueios à qual você deseja anexar a entrada.
6. Clique em **Enviar**.
7. Se você tiver a aprovação por e-mail configurada no fluxo de trabalho, uma solicitação de aprovação por e-mail será enviada.
   Se for exibida uma mensagem solicitando que você preencha o restante das informações manualmente, preencha os campos.



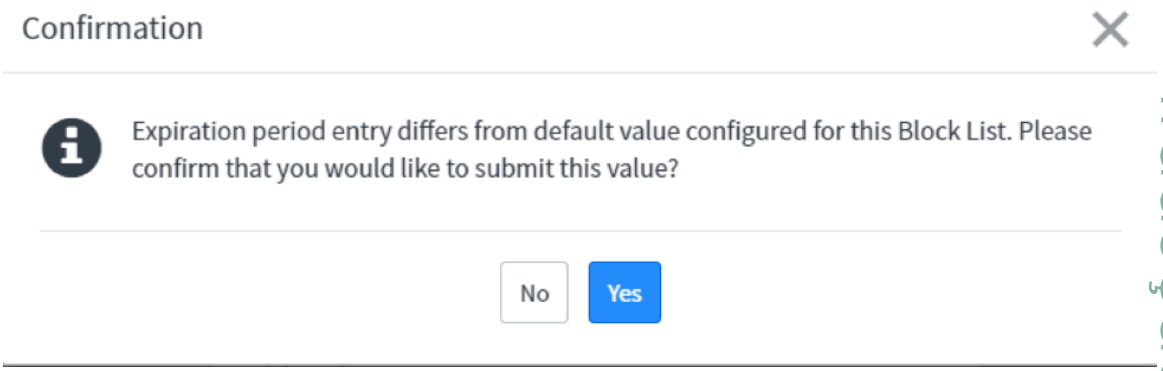
Campo	Descrição
Tipo de observável	Tipo de observável compatível com a caixa de diálogo.
Nome da lista de bloqueios	Lista de bloqueios para a qual você deseja a entrada. **Nota:** Selecione a lista de bloqueios à qual você deseja anexar a entrada antes de definir o período de expiração.
Habilitar substituição (o padrão é selecionado)	Resultado ou origem da pesquisa. Quando configurado, permite que você insira um resultado de pesquisa e a origem usada para encontrar os resultados. Esses campos são normalmente preenchidos quando um registro de incidente de segurança é criado. Nesse caso, não há resultado de pesquisa ou origem e você preenche esses campos manualmente.
Resultado da pesquisa	Selecione **Desconhecido** ou **Mal**-intencionado .
Origem	Origem que executa uma pesquisa de ameaças na entrada da Lista de bloqueios, por exemplo, ThreatCrowd etc.
Período de expiração	O período de expiração herdado da Lista de Bloqueios por padrão. Você pode substituir este valor, mas somente durante a criação da entrada. 0 indica que a entrada da Lista de bloqueios nunca expira.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se você alterar este valor, esta entrada ficará ativa pelo número de dias inserido. Você pode inserir um valor mínimo de 1 e não há valor máximo. Por exemplo, se você inserir 30 dias às 14h01 do dia 1º de maio, a entrada da Lista de bloqueios expirará às 14h do dia 31 de maio. No entanto, o programador verifica se há entradas expiradas às 00:00 todos os dias e muda o estado da entrada para "expirado" às 00:00 de 1º de junho.

8. Clique em **Enviar**.
   Se você alterou o período de expiração padrão da entrada da Lista de bloqueios, uma caixa de diálogo de confirmação de aviso será exibida indicando que o período é diferente da Lista de bloqueios selecionada.

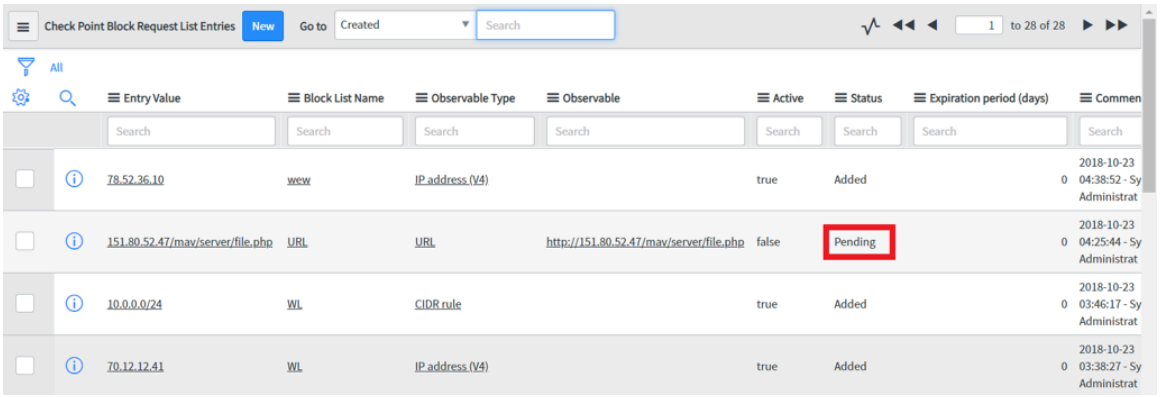


Opção	Descrição
Sim	Confirma a substituição da expiração, salva o registro e retorna você para as Entradas da Lista de Bloqueios do Check Point. Se você tiver a aprovação por e-mail configurada no fluxo de trabalho, uma solicitação de aprovação por e-mail será enviada.
Não	Cancela a substituição. Neste ponto, você pode alterar o valor do **Período de expiração**. Depois de alterar o valor, clique em Enviar para retornar à lista Entradas de bloco do Check Point.

9. Se não for exibido, navegue até **Check Point Solicitação de bloqueio Entradas da lista** e observe que o status da entrada é **Pendente**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A entrada agora está pronta para aprovação.

Aprovar entradas da lista de bloqueios para a integração Check Point NGTP

Um processo de aprovação para entradas da Lista de bloqueios faz parte do fluxo de trabalho pré-configurado. Você aprova as entradas da Lista de bloqueios antes que as entradas sejam ativadas nas Listas de bloqueios. Depois de aprovar a entrada da Lista de bloqueios, o Gateway recupera a entrada e seu observável é bloqueado desse ponto em diante.

Antes de Iniciar

- A aprovação para entradas da Lista de bloqueios é atribuída ao Administrador de incidentes de segurança (sn_si.admin) por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização. No exemplo a seguir, o administrador da Now Platform tem autoridade de aprovação.

Função necessária: sn.si.admin

Por Que e Quando Desempenhar Esta Tarefa

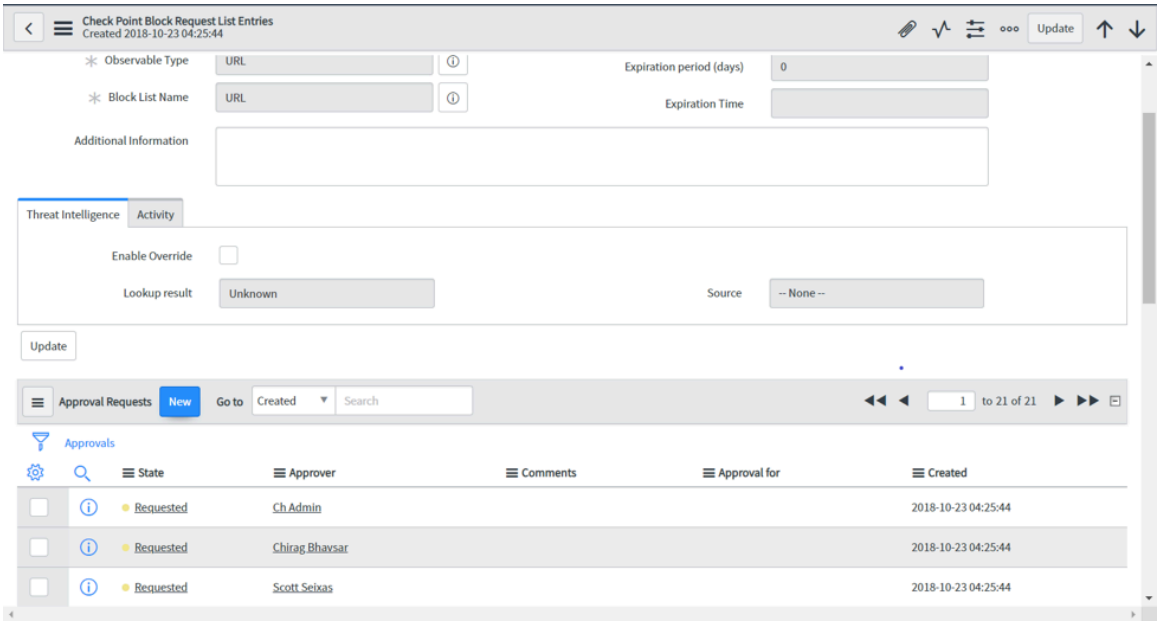
Quando o processo de aprovação está habilitado, uma entrada da Lista de bloqueios não é ativada ou desativada na Lista de bloqueios até que seja aprovada.

Procedimento

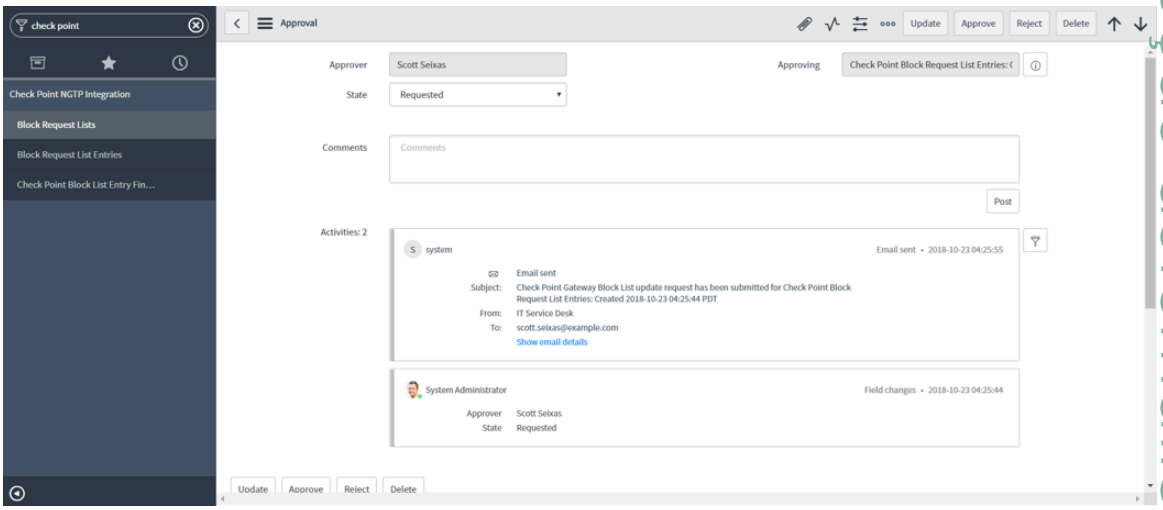
1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Bloquear Entradas da Lista de Solicitaçõe**s e abra o registro de entrada da lista de bloqueios.
2. No registro Entrada da lista de bloqueios, role até a seção **Solicitações de aprovação**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Em Solicitações de aprovação, clique em um item na coluna **Estado** para abri-lo.
   O registro de aprovação é exibido.



4. Escolha uma opção para aprovar a entrada da Lista de bloqueios.

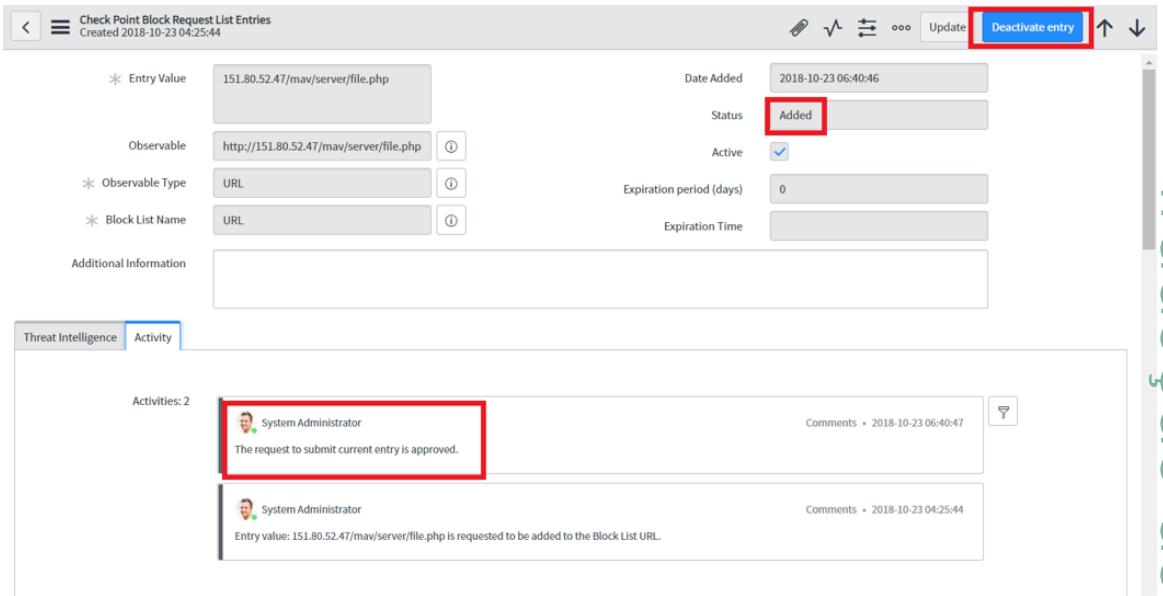
Opção	Descrição
Aprovar	No registro de entrada, o campo Status muda para Adicionado e a caixa de seleção Ativo é marcada. O botão Desativar é exibido e ativo. As anotações de trabalho mostram que a solicitação da entrada da Lista de bloqueios foi aprovada.
Rejeitar	No registro de entrada, o campo Status muda para Rejeitado e a caixa de seleção Ativo é desmarcada, indicando que a entrada não está bloqueada no Gateway.

Tradução automática

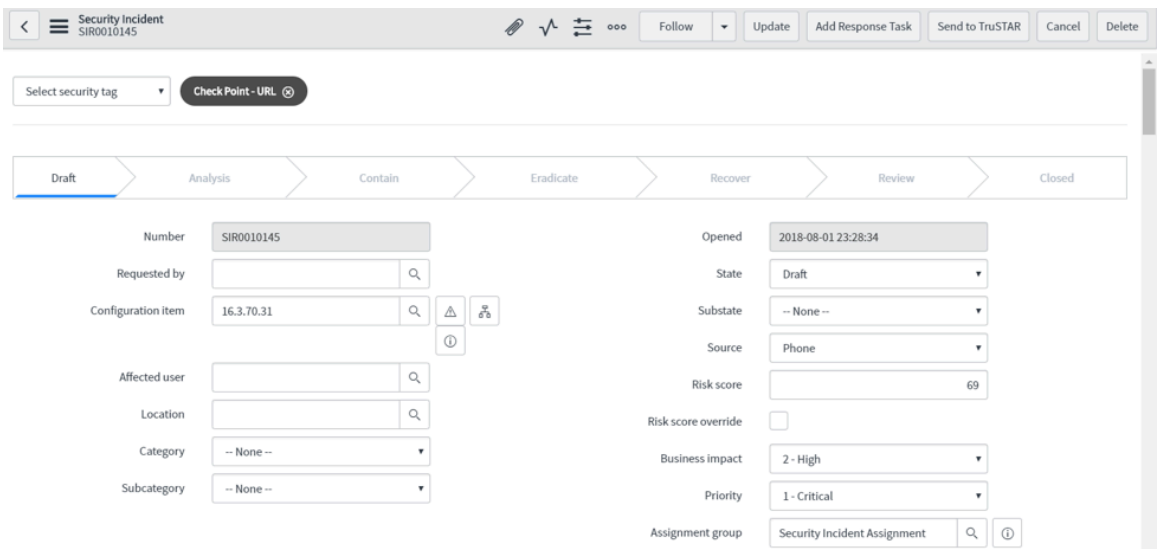
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	As anotações de trabalho mostram que a solicitação da entrada da Lista de bloqueios foi rejeitada.

Depois que você aprovar a entrada da Lista de bloqueios e ela for ativada, o firewall de última geração do Check Point recuperará a entrada da Lista de bloqueios após o próximo intervalo de recuperação. Depois que a entrada é recuperada, o observável é bloqueado desse ponto em diante. Na figura a seguir, observe que a caixa de seleção Ativo está marcada, o status é Adicionado e as anotações de trabalho indicam que a solicitação foi aprovada.



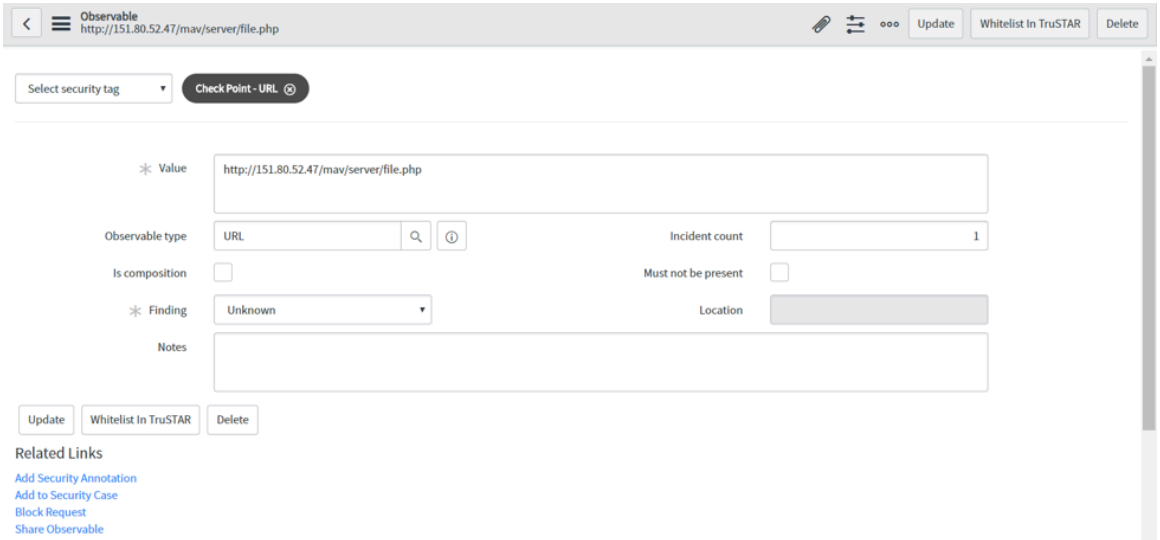
Depois que a entrada da Lista de bloqueios é aprovada e ativada, o registro do incidente de segurança é marcado com um marcador de segurança. O marcador é exibido na parte superior do registro.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O marcador de segurança também é exibido no registro do observável.



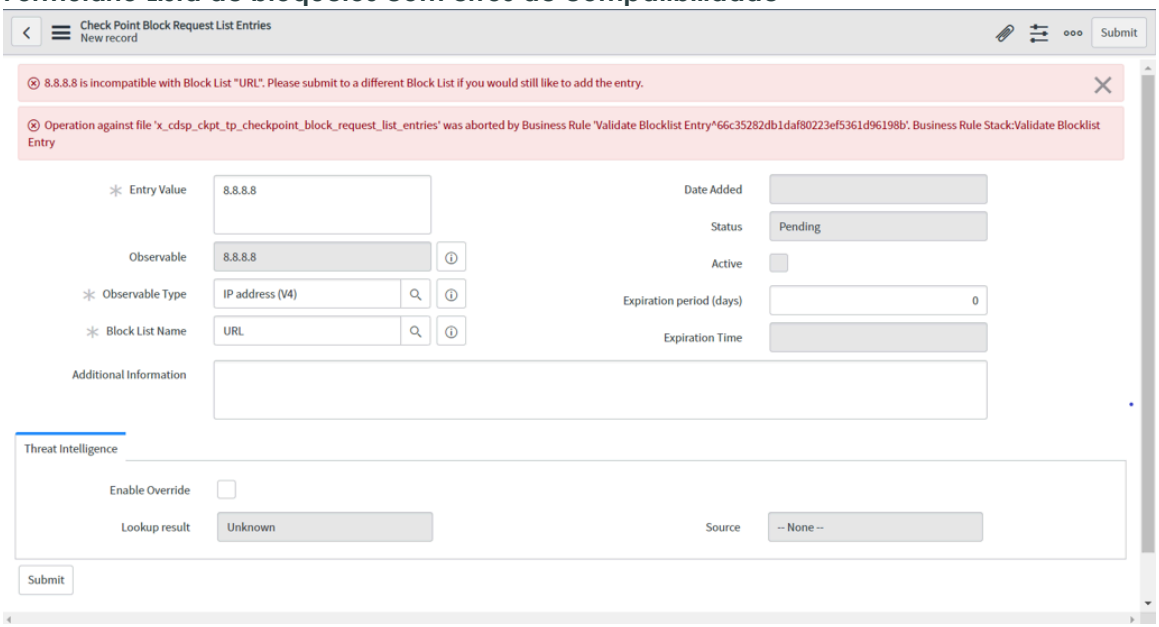
Exceções de entrada da lista de bloqueios para a integração Check Point NGTP

Há restrições para adicionar entradas da Lista de bloqueios a Listas de bloqueios. Se houver conflitos duplicados, de compatibilidade ou de CIDR (Roteamento entre domínios sem classe) quando você tentar adicionar entradas da Lista de bloqueios a Listas de bloqueios, serão exibidas mensagens de erro que ajudarão a resolver esses erros.

Exceção de compatibilidade

Cada lista de bloqueios aceita somente entradas compatíveis com seu tipo de observável. Se você criar uma lista de bloqueios de domínio e tentar anexar um observável de endereço IP a ela, uma mensagem de erro incompatível será exibida. Por exemplo, uma lista de bloqueios de domínio só pode aceitar observáveis de domínio, conforme ilustrado na figura a seguir.

Formulário Lista de bloqueios com erros de compatibilidade

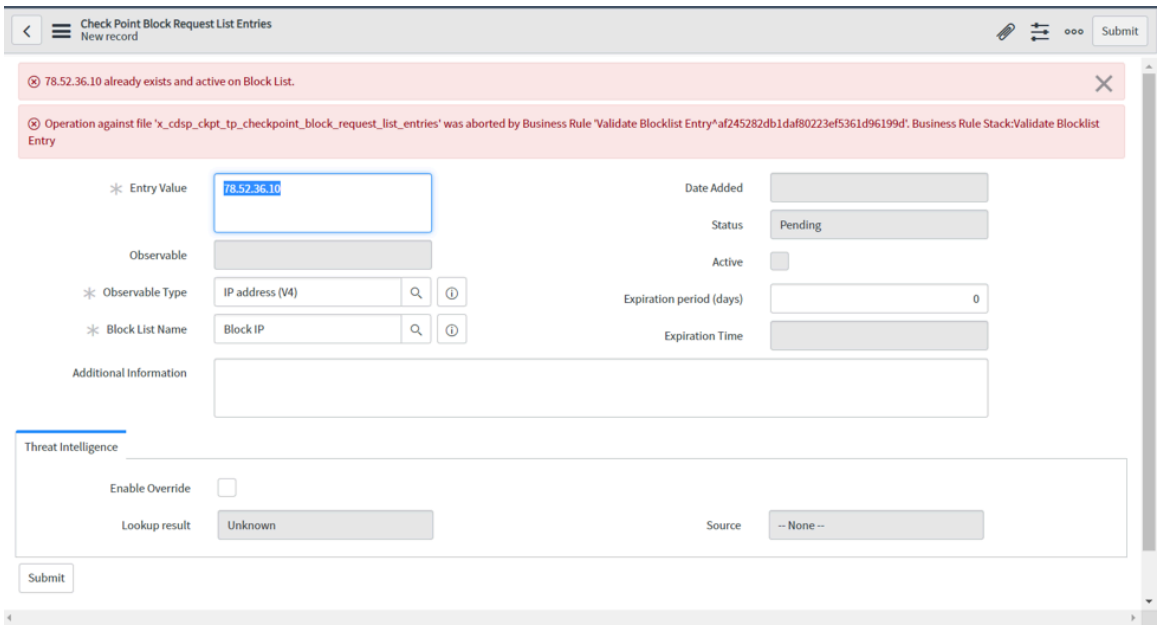


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

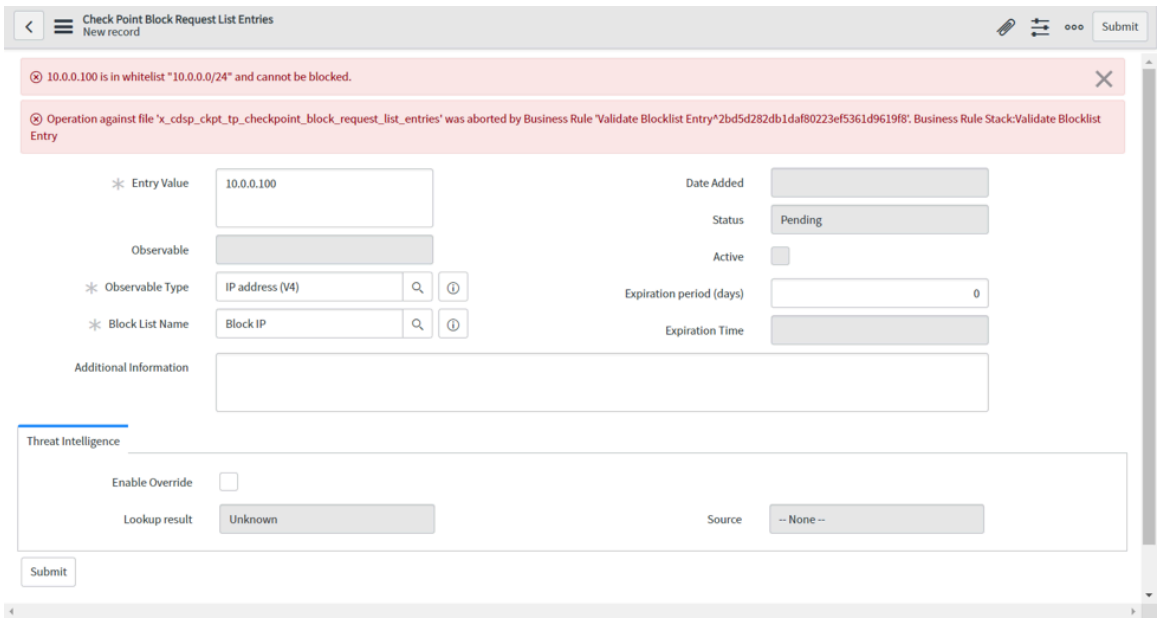
Exceção de duplicação

Um observável não pode ser ativado em várias listas de bloqueios do mesmo tipo de observável. Se um observável de URL já estiver ativado em uma lista de bloqueios de URL e você tentar ativar o mesmo observável em uma lista de bloqueios de URL de phishing, será exibida uma mensagem de erro de duplicação.



Exceção de CIDR (Roteamento entre domínios sem classe)

Se você tentar anexar um único endereço IP a uma lista de permissões e esse endereço IP fizer parte de um observável CIDR já em uma lista de bloqueios/lista de permissões, será exibido um erro de conflito de CIDR. Este erro indica que o único endereço IP já está incluído na lista de bloqueios ou na lista de permissões como parte do observável CIDR. Por exemplo, 192.168.24.25 faz parte do bloco CIDR 192.168.0.0/22.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Editar o nome do marcador de segurança para a integração Check Point NGTP

Se a caixa de seleção Exibir marcador estiver marcada ao criar o registro da Lista de bloqueios, você poderá editar os nomes dos marcadores e as cores dos marcadores de segurança. Os marcadores de segurança ajudam a rastrear observáveis que já estão bloqueados.

Antes de Iniciar

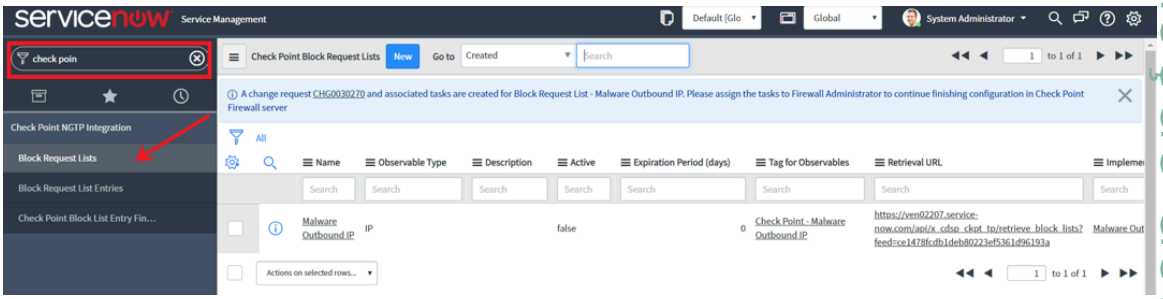
Função necessária: sn.si.admin

Por Que e Quando Desempenhar Esta Tarefa

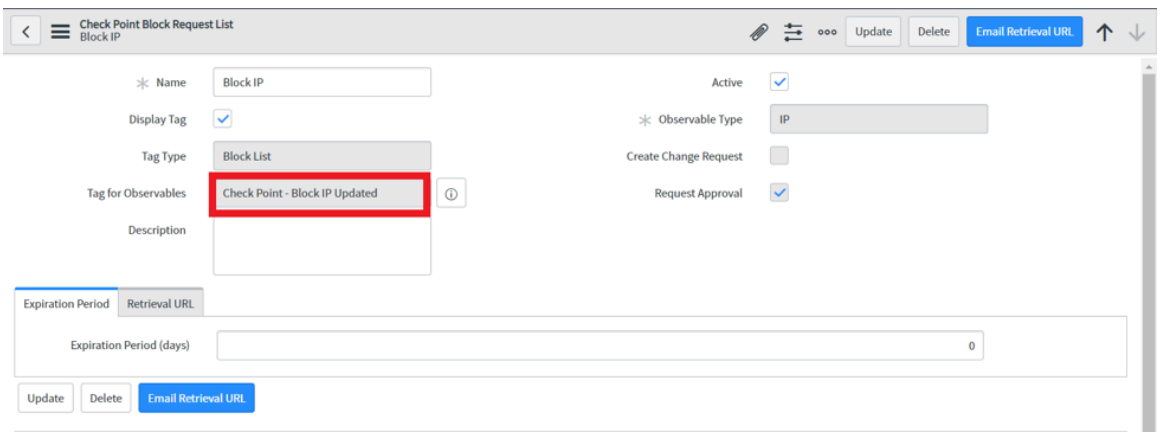
Os marcadores de segurança ajudam a identificar rapidamente quais incidentes de segurança têm observáveis em uma lista de bloqueios. Os marcadores também ajudam a identificar se um observável já está bloqueado ou se foi removido de uma lista de bloqueios. Por padrão, a cor do marcador de segurança é preta para entradas da lista de bloqueios e cinza para entradas da lista de permissões. Você pode mudar os nomes e as cores dos marcadores para ajudá-lo a reconhecer determinados marcadores com mais facilidade.

Procedimento

1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Configuração da lista de solicitação de bloqueio**.



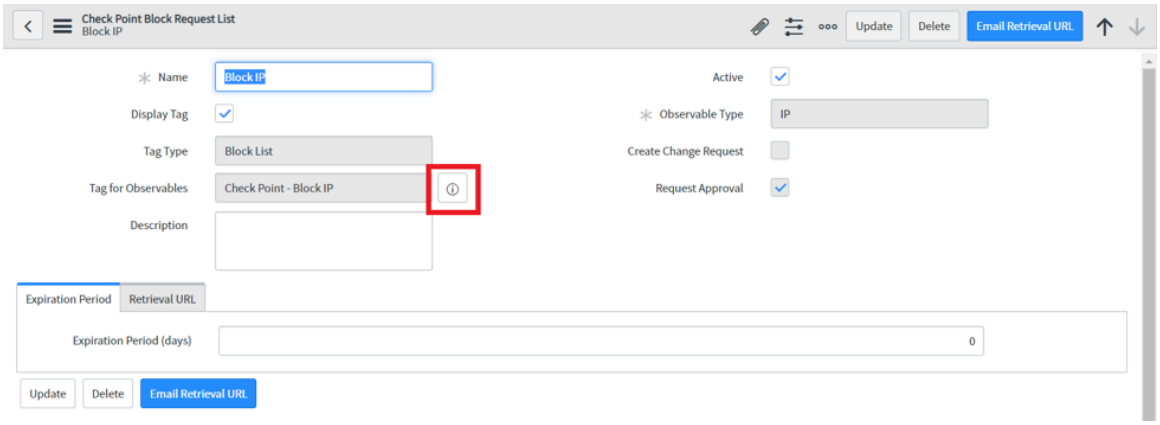
2. Clique em um item na coluna **Nome** para abri-lo.
   O registro da Lista de bloqueios é exibido. Por padrão, o nome do marcador de segurança é o mesmo valor que você inseriu no campo Nome da Lista de Bloqueios ao criá-la. Por padrão, o nome também inclui um prefixo de Lista de bloqueios, por exemplo, Lista de bloqueios – URLs de malware malicioso.



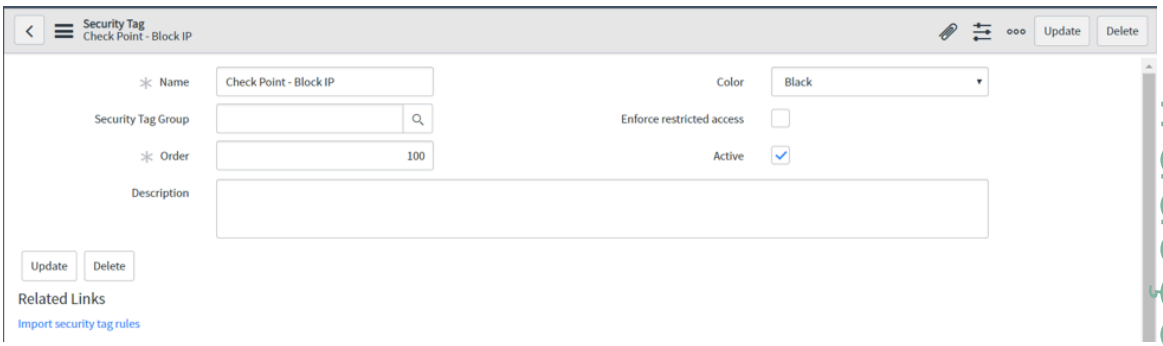
3. Clique no ícone de informações ao lado do marcador para observáveis e, em seguida, em Abrir registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

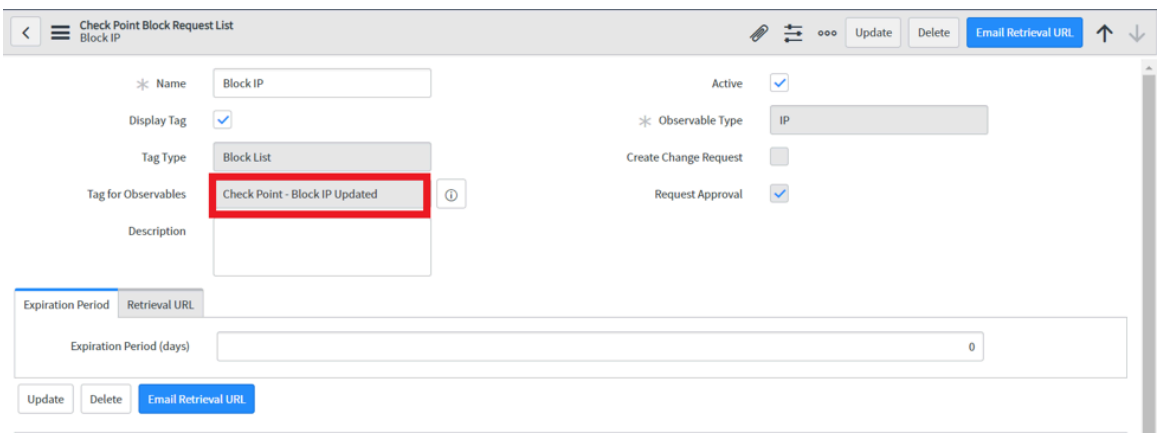


O formulário de marcador de segurança é exibido.



4. No campo **Nome**, modifique o nome do marcador de segurança.
5. Clique em **Atualizar**.
   O registro da lista de bloqueios atualizado é exibido com o nome do marcador modificado.

Nota: No exemplo a seguir, Saída foi adicionado ao nome do marcador. Mantenha o prefixo do Check Point no novo nome do marcador para ajudá-lo a identificar que o marcador está associado à integração de firewall de última geração do Check Point.

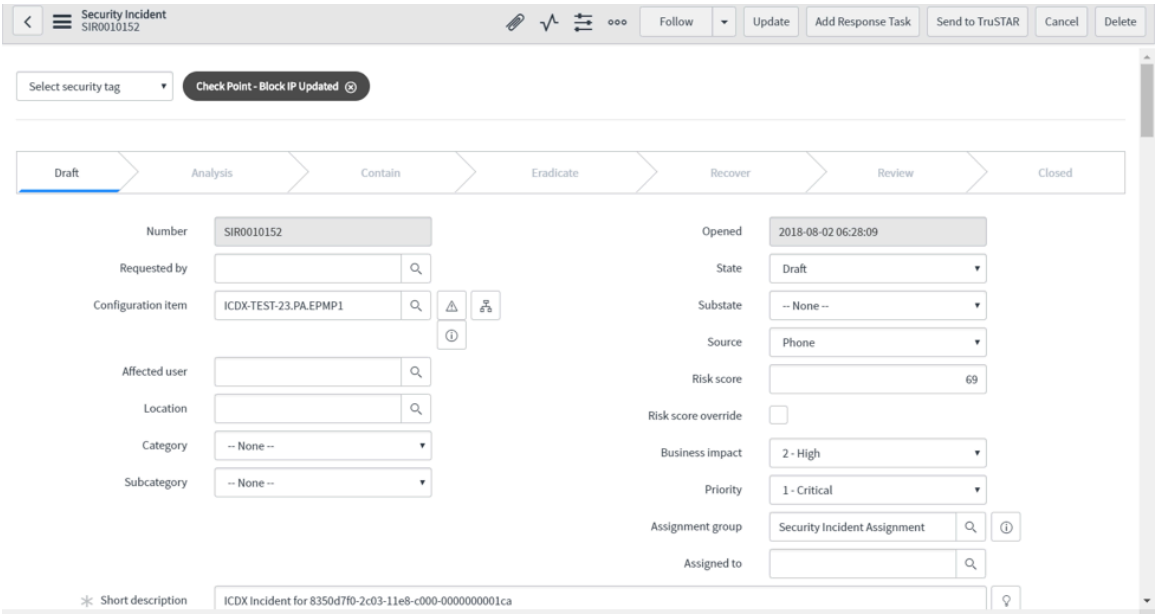


Os marcadores de segurança são exibidos para cada tipo de observável (IP, URL, domínio) no registro do Incidente de segurança e no registro do Observável sempre que esse observável é adicionado à Lista de bloqueios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados



Se um observável já tiver sido adicionado a uma lista de bloqueios e um marcador de segurança for exibido em um incidente de segurança para esse observável, o marcador de segurança da lista de bloqueios também será exibido automaticamente em todos os registros de incidentes de segurança subsequentes que forem criados. Essa duplicação informa que o observável já está em uma lista de bloqueios. Você não precisa adicionar este observável e bloqueá-lo novamente.

Quando um observável não está mais bloqueado, um marcador de segurança não é exibido no registro de incidente de segurança ou no registro do observável. Nesta instância, nenhum marcador de segurança indica que a data de expiração do observável pode ter passado ou que o observável foi desativado de uma lista de bloqueios.

Desinstalar a integração Check Point NGTP

Se você quiser desinstalar a integração Check Point NGTP da sua instância da Now Platform e remover todos os remanescentes da integração, consulte o site de documentação da ServiceNow para obter instruções sobre como desinstalar aplicações.

Função necessária: administrador

Integração do CrowdStrike Falcon Host

A integração CrowdStrike Falcon Host permite que você envie observáveis em um incidente de segurança para uma lista de observação, tornando-os capazes de gerar alertas adicionais. Esta integração é uma implementação do fluxo de trabalho CrowdStrike Falcon Host - Publicar na lista de observação.

Explorar Integrações do Security Incident Response	Configurar Comece com a integração CrowdStrike Falcon Host
Usar	Desenvolver

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

• Executar pesquisas em observáveis • Atividade Publicar na lista de observação	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Comece com a integração CrowdStrike Falcon Host

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo a integração CrowdStrike Falcon Host. Antes de poder usar a integração CrowdStrike Falcon Host, você deve baixá-la do ServiceNow Store e adicionar um nome de usuário e senha.

Antes de Iniciar

- Se você estiver atualizando a integração CrowdStrike Falcon Host de uma versão anterior, deverá excluir a configuração existente e definir uma nova configuração. A nova integração oferece suporte à autenticação OAUTH2. Esta atualização requer que você insira o **ID do cliente de API** e o **segredo do cliente** de API para autenticar e concluir a configuração.
- Nos CrowdStrike Falcon Host**Escopos de API**do portal, habilite a configuração de **Leitura** e **Gravação** para **IOCs (Indicadores de Compromisso)**.

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão CrowdStrike Falcon Host, clique em **Configurar**.
4. No formulário, preencha os campos para concluir a configuração:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de host do CrowdStrike Falcon

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
ID do cliente da API	O ID de cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Host.
Segredo do cliente de API	A chave secreta do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Host.

5. Clique em **Enviar**.

Resultados

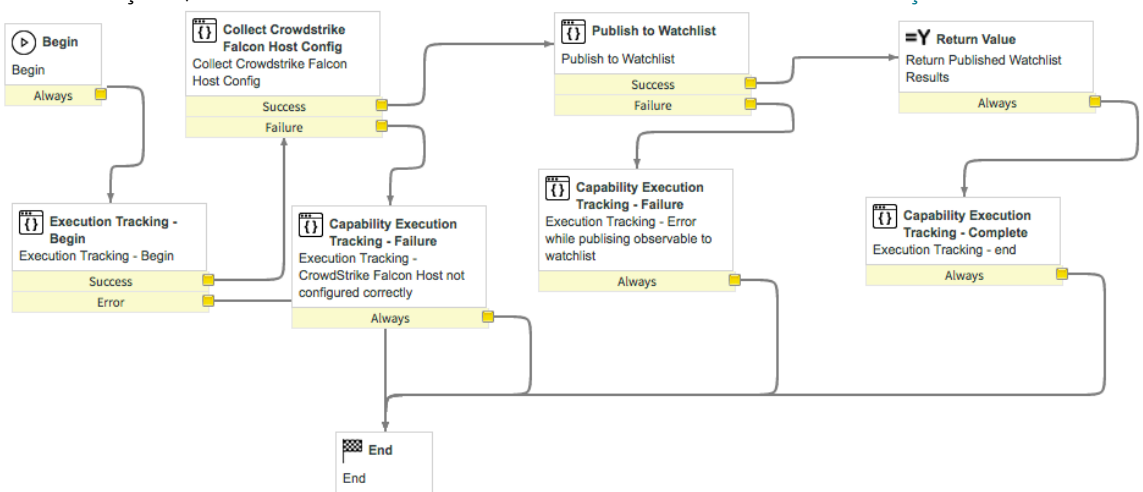
Depois de configurada, a integração CrowdStrike Falcon Host pode ser selecionada para publicar observáveis em listas de observação em Security Incident Response.

Host do CrowdStrike Falcon das Operações de segurança - Fluxo de trabalho Publicar na lista de observação

O fluxo de trabalho **CrowdStrike Falcon Host - Publicar na lista de observação das Operações de segurança** é usado para especificar a lista de observação para gerar alertas ou eventos. Os alertas e eventos são exibidos no sistema CrowdStrike Falcon Host com base em como ele está configurado.

Publicar no fluxo de trabalho da lista de observação

Este fluxo de trabalho é acionado pelo Integração de Operações de segurança - Capacidade de publicar na lista de observação quando você seleciona um ou mais observáveis associados a um incidente de segurança e usa a ação de IU Publicar na lista de observação para enviar os observáveis para uma lista de observação. Os observáveis podem ser usados para gerar alertas adicionais. Para obter mais informações, consulte Publicar observáveis em uma lista de observação de terceiros.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Coletar configurações de host do CrowdStrike Falcon

A atividade de fluxo de trabalho **Coletar configurações de host do CrowdStrike Falcon** reúne informações de configuração a serem usadas no fluxo de trabalho.

A **atividade Coletar configuração de host do CrowdStrike Falcon** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do host do CrowdStrike Falcon.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
user_name	Nome de usuário do CrowdStrike Falcon Host
senha	Senha do CrowdStrike Falcon Host

Atividade Publicar na lista de observação

A atividade de fluxo de trabalho **Publicar na lista de** observação envia observáveis em um incidente de segurança para uma lista de observação para gerar alertas ou eventos. Os alertas e eventos são exibidos no sistema CrowdStrike Falcon Host com base em como ele está configurado.

A atividade **Publicar na lista** de observação pode ser usada com qualquer fluxo de trabalho para publicar observáveis em uma lista de observação.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	A lista de observáveis de Security Incident Response.
user_name	O nome de usuário do indivíduo responsável pela integração do CrowdStrike Falcon Host.
senha	A senha do indivíduo responsável pela integração do CrowdStrike Falcon Host.
task_sys_id	O identificador do sistema para este trabalho de publicação na lista de observação.
capabilityExecutionId	O nome da capacidade associada.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status	O status da atividade de publicação.

CrowdStrike Falcon Insight para integração Operações de segurança

Com a integração CrowdStrike Falcon Insight para Operações de segurança, você pode fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o produto Now Platform Security Incident Response.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

A integração CrowdStrike Falcon Insight para Operações de segurança funciona com o Now Platform para que você possa obter informações adicionais sobre o escopo de um incidente. O CrowdStrike Falcon Insight captura todas as atividades de evento de endpoint relevantes. Você pode usar o Now Platform para se concentrar em investigações e ações de correção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça esta integração

Identificador do documento	Título do documento
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow
CrowdStrike Falcon Insight para Operações de segurança	Introdução à integração CrowdStrike Falcon Insight

Introdução à integração CrowdStrike Falcon Insight

Você pode ativar e configurar o CrowdStrike Falcon Insight para interagir com sua instância [Now Platform e o produto Security Incident Response.

Antes de Iniciar

Função necessária: administrador

Antes de poder usar CrowdStrike Falcon Insight para a integração Operações de segurança, você deve baixá-lo do ServiceNow Store.

Por Que e Quando Desempenhar Esta Tarefa

Check-list

Configuração de tarefa	Descrição
Atribua e verifique as funções Now Platform e Security Incident Response.	Essas funções são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin configura a integração, cria e ativa perfis e atribui a função sn_si.analyst. • A função sn_si.analyst responde a incidentes de segurança, inicia perfis manualmente e pode enviar solicitações para ações como isolar o host e remover o isolamento do host para um grupo aprovado.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.	O plug-in ServiceNow Integration Hub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] é necessário. Este plug-in permite a execução de ações e fluxos do IntegrationHub: O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Operações de segurança que são necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação, uma de cada vez, na seguinte ordem para garantir uma instalação sem problemas: **1.** Security Incident Response Dependência (com.snc.si_dep) **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança **5.** Inteligência contra ameaças Suporte comum **6.** Trusted Security Circles **7.** Operações de segurança Assistente de configuração **8.** Security Incident Response
Configure um grupo de aprovação.	Uma capacidade de aprovação opcional está disponível para isolar máquinas host, restaurá-las na rede e iniciar pesquisas de detecções. Para habilitar esta opção, você precisa de aprovação prévia da função sn_si.admin antes que as máquinas host sejam isoladas e restauradas na rede ou quando as pesquisas de detecções forem realizadas. Se você precisar de um nível extra de controle sobre essas ações, habilite a opção **Requer aprovação** ao configurar o perfil. A autoridade de aprovação é atribuída ao usuário com a função sn_si.admin. Você também pode reatribuir esta autoridade de aprovação a um grupo de aprovação.
Atribua e verifique as funções da plataforma CrowdStrike Falcon.	As funções a seguir são necessárias na plataforma CrowdStrike Falcon para a configuração da integração:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• A função de administrador do Falcon é necessária para exibir, criar ou modificar clientes ou chaves de API. • A função de Respondente em tempo real – Administrador é necessária para criar e executar scripts personalizados. • A função Respondente em tempo real – Respondente ativo é necessária para criar e executar scripts personalizados.
Verifique se as funções e permissões de scripts personalizados estão habilitadas na plataforma CrowdStrike Falcon.	Esta integração usa scripts personalizados do CrowdStrike para alguns dos recursos de enriquecimento. • Verifique se as funções de Respondente em tempo real – Administrador e Respondente em tempo real – Respondente ativo estão disponíveis. • Verifique se a opção **de política Padrão (Windows)** está habilitada em Configuração > Políticas de resposta na IU do CrowdStrike Falcon. • Verifique se a **resposta em tempo real** e **os scripts personalizados** na funcionalidade em tempo real estão habilitados na IU do CrowdStrike Falcon.
Gere clientes de API e chaves na plataforma CrowdStrike Falcon.	Crie clientes ou chaves de API do CrowdStrike na plataforma CrowdStrike Falcon para usar na configuração de integração Now Platform.

Criar cliente da API do CrowdStrike e gerar chaves

Crie o cliente da API do CrowdStrike e gere o ID e a chave do cliente, que você usa para configurar a integração CrowdStrike Falcon Insight.

Antes de Iniciar

Função necessária: administrador do CrowdStrike Falcon

Procedimento

1. Na plataforma CrowdStrike Falcon, navegue até **Clientes e chaves de API**.
2. Na tabela Clientes de API do OAuth2, clique em **Adicionar novo cliente de API**.
3. Insira os seguintes detalhes para definir seu cliente de API:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome do cliente	Insira o nome do cliente. Este campo é obrigatório.
Descrição	Insira a descrição do nome do cliente.
Escopos de API	É necessário definir os escopos. **Importante:** Certifique-se de habilitar a conta de API e de que os seguintes escopos estejam habilitados para a conta de API: ◦ Habilitar escopos de leitura e gravação para API de hosts ◦ Habilitar escopo de leitura para API de indicadores

4. Clique em **Adicionar** para salvar o cliente de API e gerar o ID do cliente e a chave secreta.

Instalar e configurar CrowdStrike Falcon Insight

Instale e configure a aplicação CrowdStrike Falcon Insight para Operações de segurança a partir de ServiceNow Store em sua instância Now Platform.

Antes de Iniciar

Função necessária: administrador

Nota: Você pode associar uma capacidade a apenas um perfil. Você não pode associar uma capacidade a vários perfis. Ao configurar os servidores do CrowdStrike, você não pode reutilizar uma capacidade do CrowdStrike com vários perfis que compartilham o servidor do CrowdStrike. Seus perfis podem ter a mesma capacidade do CrowdStrike. Cada perfil deve usar seu próprio servidor CrowdStrike.

Procedimento

1. Baixe o CrowdStrike Falcon Insight para integração de Operações de segurança do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco de integração CrowdStrike Falcon Insight para Operações de segurança e clique em **Configurar**.
4. No formulário, preencha os campos para concluir a configuração:

Configuração do CrowdStrike Falcon Insight

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
URL da API do CrowdStrike Falcon Insight	URL base que hospeda a API do CrowdStrike. Insira o URL com o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	protocolo HTTPS. Por exemplo, https://api.crowdstrike.com.
ID de cliente	O ID de cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Insight.
Segredo do cliente	A chave secreta do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Insight.

5. Clique em **Enviar**.

Resultados
Depois que a integração é validada e enviada com sucesso, ela é salva na página Integrações de segurança como um bloco. Você pode exibir o módulo CrowdStrike Falcon Insight no navegador de aplicações.

Criar um grupo de aprovação

Crie um grupo de aprovação para a integração CrowdStrike Falcon Insight para Operações de segurança que pode aprovar solicitações para isolar máquinas host, restaurá-las na rede e iniciar pesquisas de detecções.

Antes de Iniciar
Você não pode reatribuir a autoridade de aprovação a um grupo, a menos que um grupo de aprovação esteja disponível em sua instância.

Nota: A opção de aprovações na configuração do perfil aparece somente para as capacidades Isolar host e Remover isolamento de host.

Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na lista de grupos, clique em **Novo**.
3. No formulário, preencha os campos.

Formulário de grupo de aprovação

Campo	Descrição
Nome	Nome do grupo que você vê ao enviar uma solicitação de aprovação.
E-mail do grupo	Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo.
Gerente	Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	Nome do grupo primário, se associado a um primário.
Tipo	Categorias de grupos.
Fornecedores	função vendor_manager que você atribui a usuários no processo de gestão de fornecedores da sua organização.
Descrição	Informações adicionais sobre o grupo.

4. Clique em **Enviar**.
   O novo grupo é exibido na lista Grupos.

   Este grupo está disponível para processar solicitações quando você habilita a opção **Requer aprovação** durante a configuração deste perfil.

   Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação navega até a guia **Minhas aprovações** no Now Platform.

O que Fazer Depois

A próxima etapa é instalar e configurar a aplicação CrowdStrike Falcon Insight da ServiceNow Store.

Criar um perfil de capacidade para a integração CrowdStrike Falcon Insight

Crie um perfil e selecione os CrowdStrike Falcon Insight recursos que você deseja que o perfil execute.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Considere por que você deseja criar um perfil antes de adicionar capacidades CrowdStrike Falcon Insight a ele. A tabela a seguir lista os recursos que você deve adicionar a um perfil quando quiser que o perfil execute determinadas consultas ou ações.

Você pode criar um único perfil que executa consultas de detalhes do sistema, lista usuários conectados, busca serviços em execução, busca processos em execução, busca

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

estatísticas de rede, isola o host e remove o host isolado. Como alternativa, você pode criar vários perfis, cada um com sua própria capacidade.

Nota: As capacidades Isolar host, remover isolamento e obter arquivo não podem ser mescladas com nenhuma outra capacidade ao criar um perfil.

Tipos de perfil e capacidades necessárias do CrowdStrike Falcon Insight

Finalidade do perfil	Recursos do CrowdStrike
Reúna detalhes do host e usuários conectados	• **Obter detalhes do host** • **Obter usuários conectados**
Buscar as estatísticas, processos e serviços de rede em execução para um host	• **Obter estatísticas de rede** • **Obter processos em execução** • **Obter serviços em execução**
Isolar um host	**Isolar host**
Remover isolamento de um host	**Remover isolamento**
Obter um arquivo de um endpoint de host	**Obter arquivo**

Procedimento

1. Navegar até **Todos** > **Integração com CrowdStrike Falcon Insight** > **Perfis de capacidade do CrowdStrike**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

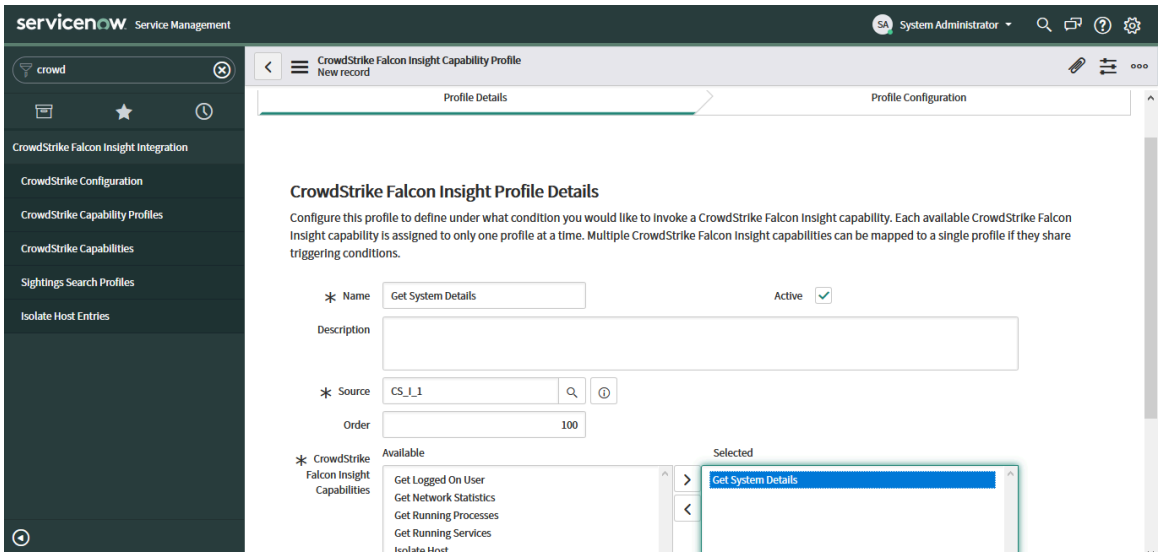
Campo	Descrição
Nome	Nome do novo perfil de capacidade. Este nome ajuda a identificar o tipo de perfil e também é o nome padrão para o marcador de segurança associado a este perfil.
Ativo	Indica se o perfil está ativo ou não. Quando o perfil está ativo, ele é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem que você especificou na configuração.
Descrição	Descrição exclusiva do perfil de capacidade.
Origem	Nome do servidor. Você só pode exibir servidores configurados anteriormente na lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400. Padrão: 100
Capacidades do CrowdStrike Falcon Insight	Capacidades do perfil do CrowdStrike Falcon Insight. Selecione os recursos desejados para este perfil na coluna **Disponível** para o **selecionado**.

O exemplo a seguir mostra um formulário completo para um perfil com a capacidade Obter detalhes do sistema.



4. Clique em **Avançar**.

O que Fazer Depois

Agora você podeconfigurar seu perfil. Certifique-se de ter revisado os conceitos de configuração de perfis e condições de gatilho antes de configurar o perfil.

Configurar perfis e incidentes de segurança para a integração CrowdStrike Falcon Insight

Defina as configurações de perfil para que o perfil seja acionado somente nas condições definidas por você.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Defina as condições que acionam automaticamente as capacidades CrowdStrike Falcon Insight que você selecionou para o perfil. Você também pode selecionar um campo de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

entrada alternativo para o campo Item de configuração (IC). Neste campo alternativo, você pode definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento acionem automaticamente o perfil.

Nota: Navegue até a página Configuração de perfil somente depois de inserir os detalhes do perfil. Para obter mais informações, consulte Criar um perfil de capacidade para a integração do CrowdStrike Falcon Insight.

Procedimento

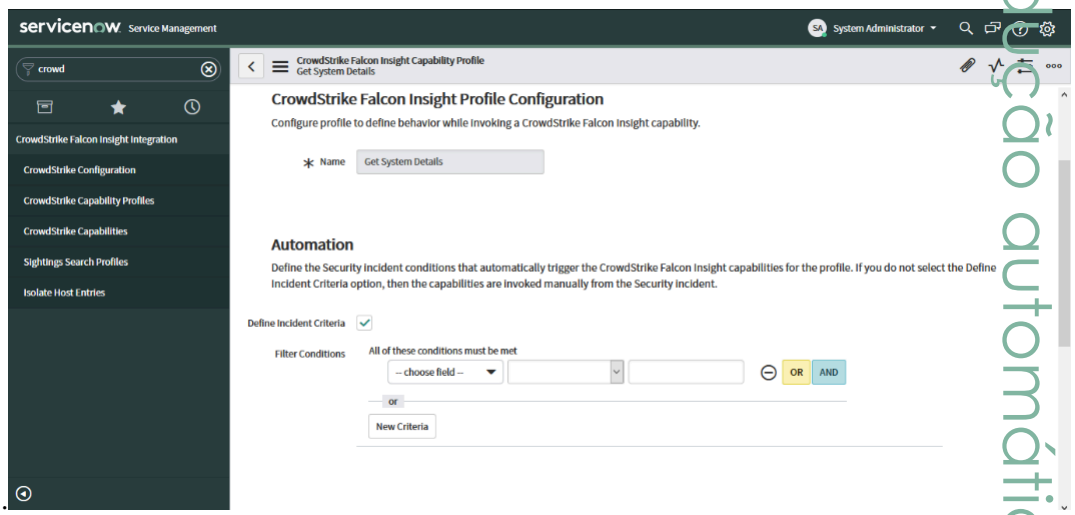
1. Na página Configuração de perfil, revise e configure as seguintes seções:

Definir critérios de incidente (automação)

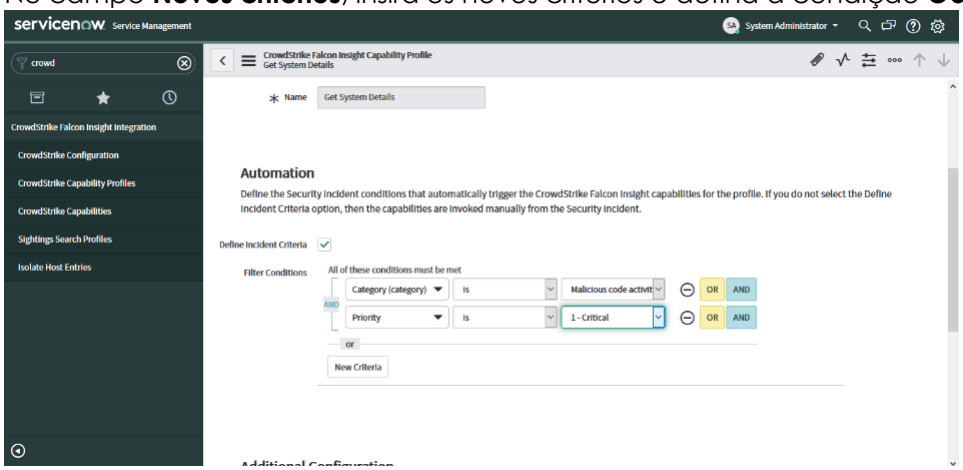
Defina as condições de incidente de segurança que acionam automaticamente as capacidades CrowdStrike Falcon Insight do perfil. Se você não selecionar a opção **Definir critérios de incidente**, as capacidades serão invocadas manualmente a partir do incidente de segurança.

a. Selecione a opção **Definir critérios de incidente**.

b. Para definir as condições, na seção Condições do filtro, selecione um campo e o requisito correspondente.



c. No campo **Novos critérios**, insira os novos critérios e defina a condição **OU** ou **E.**



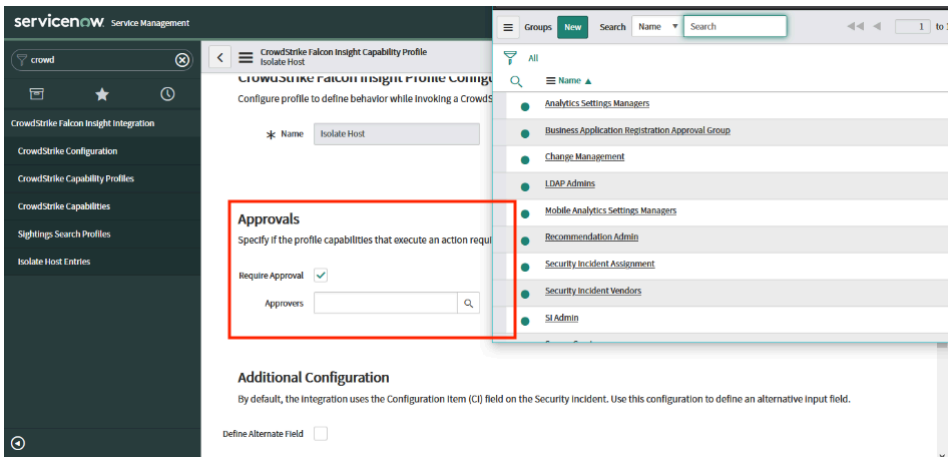
Approvals

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para fornecer um nível extra de controle ao usar os recursos do CrowdStrike Falcon Insight, selecione a opção **Requer aprovação**. A opção de aprovações na configuração do perfil aparece somente para as capacidades Isolar host e Remover isolamento de host.

Nota: A autoridade de aprovação é atribuída ao usuário com a função sn_si.admin. Você também pode reatribuir esta autoridade de aprovação a um grupo de aprovação. Para obter mais informações, consulte configuração de um grupo de aprovação.



Configuração adicional

Selecione um campo alternativo no incidente de segurança para exibir todos os dados de IC correspondentes que você encontrar durante a verificação de seus ativos. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança.

a. Selecione a opção **Definir campo** alternativo.

b. No **Campo de gatilho de IC alternativo**, selecione um campo de entrada.

Nota: Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração para um perfil.

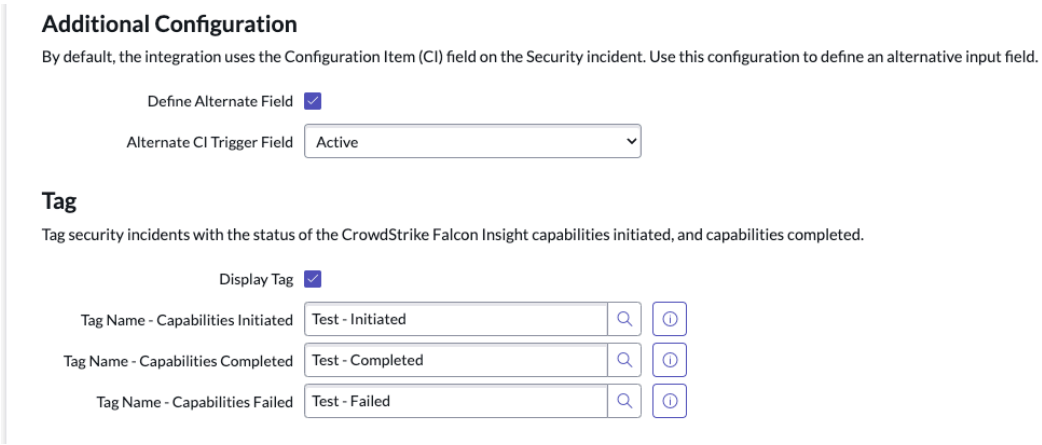
Marcadores

Para marcar incidentes de segurança com os marcadores CrowdStrike Falcon Insight Capacidades-Iniciadas, Capacidades-Concluídas e Capacidades-Falha, selecione a opção **Exibir** marcadores. Por padrão, esta opção está desabilitada para todos os perfis.

Nota: Esses marcadores são fornecidos com o sistema de base. Você pode criar seus próprios marcadores, se necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique em **Concluído**.

Como as condições do gatilho funcionam com um item de configuração para um perfil

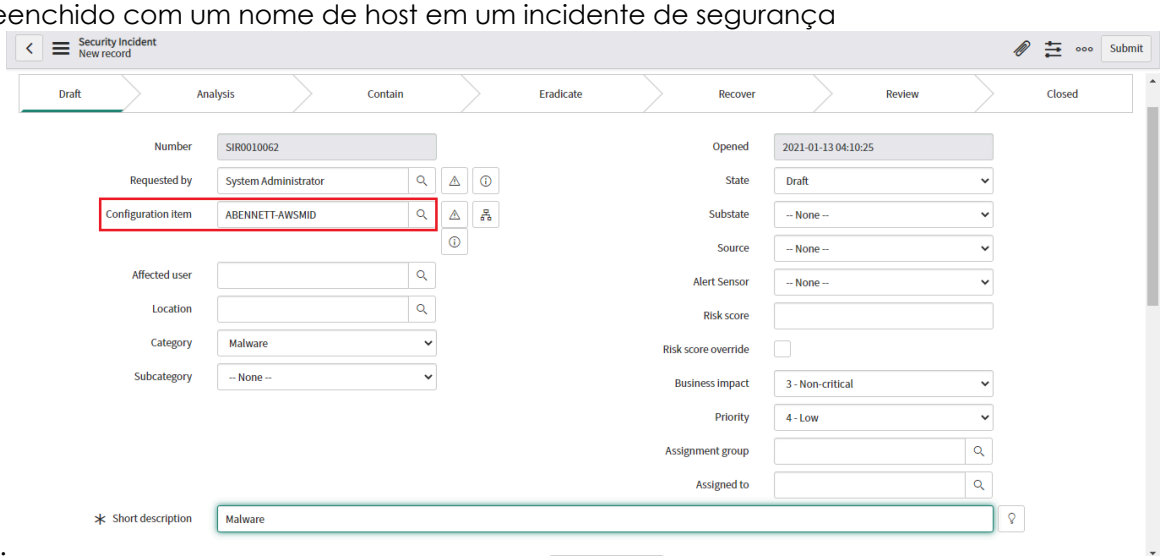
Você pode definir as configurações de perfil para que um perfil seja executado somente quando um conjunto de condições específicas for atendido ou pode configurar um perfil para pesquisar valores de campos específicos em um incidente de segurança.

Depois de criar um perfil e selecionar os recursos CrowdStrike Falcon Insight nos quais deseja que o perfil seja executado, você pode definir condições de gatilho para que seu perfil seja executado automaticamente quando os valores de campo padrão corresponderem ao incidente de segurança Now Platform.

Por padrão, a integração usa o campo **Item de configuração** (IC) em um incidente de segurança. Este campo é usado para corresponder seus IDs de ativo com as informações armazenadas no banco de dados Now Platform. Quando um incidente de segurança SIR é criado por um evento de segurança e um perfil é ativado, seus ativos são verificados quanto a um valor correspondente no nome do host ou em um endereço IP.

Quando um valor correspondente é encontrado no banco de dados, esses dados são coletados do console CrowdStrike Falcon Insight e extraídos para a instância Now Platform, onde são exibidos nas listas relacionadas de um incidente de segurança.

O exemplo a seguir mostra um campo Item de configuração que é preenchido com um nome de host em um incidente de segurança SIR.



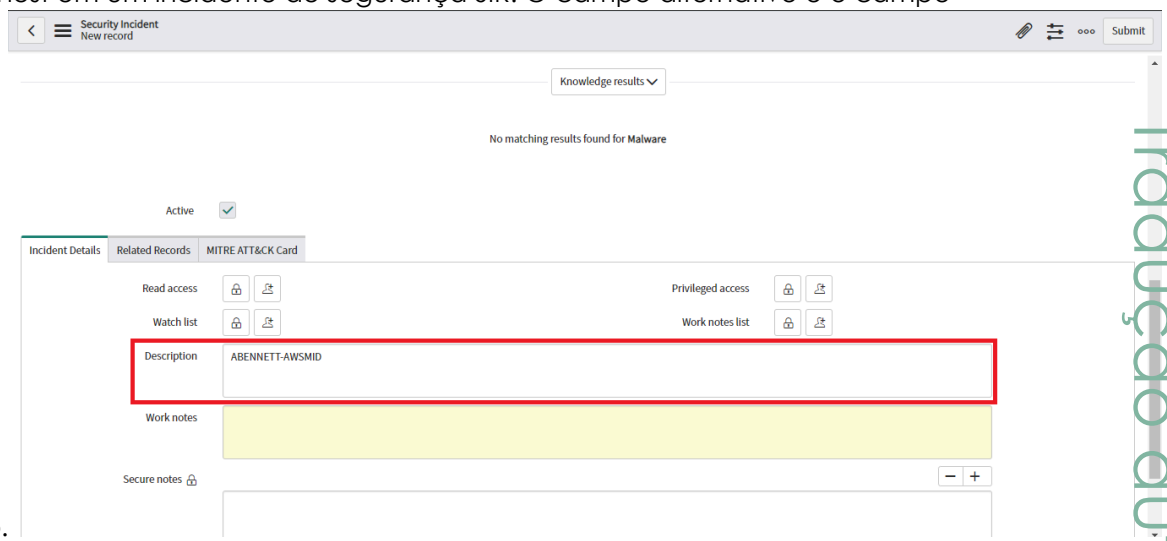
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o campo **Item de configuração** (IC) não estiver preenchido com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar outro campo no incidente de segurança para exibir todos os dados de IC correspondentes encontrados durante a verificação de seus ativos.

Ao definir a configuração do perfil, você pode selecionar um campo de **gatilho de IC** alternativo para identificação de endpoint para garantir que os dados de IC da pesquisa CrowdStrike Falcon Insight sejam preenchidos no incidente de segurança associado. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Se o campo de IC não estiver preenchido no incidente de segurança associado quando o incidente for criado, selecione o campo de IC alternativo para garantir que seus perfis sejam acionados.

O exemplo a seguir mostra um campo alternativo que é preenchido com um nome de host em um incidente de segurança SIR. O campo alternativo é o campo **Descrição**.



Verificar CrowdStrike Falcon Insight condições do gatilho de perfil

Teste o perfil e verifique se os filtros de condição do gatilho que você configurou funcionam conforme o esperado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Ative o perfil que se baseia nas condições de gatilho configuradas que você especificou para que você possa exibir os resultados da consulta nos Now Platform incidentes de segurança.

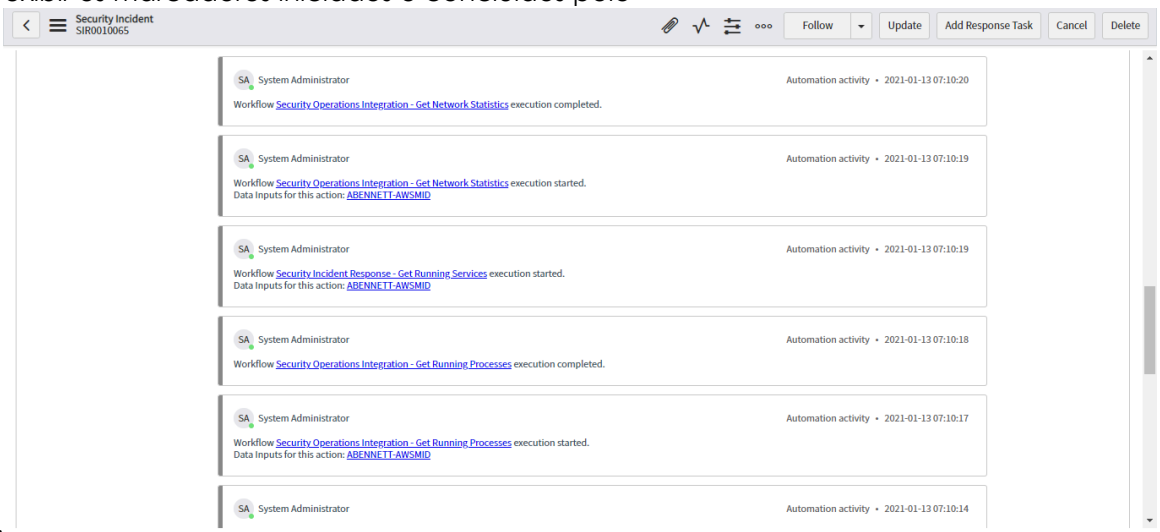
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione **Novo** para criar um incidente de segurança.
3. Para criar um incidente de segurança, preencha as informações necessárias e clique em **Salvar**.

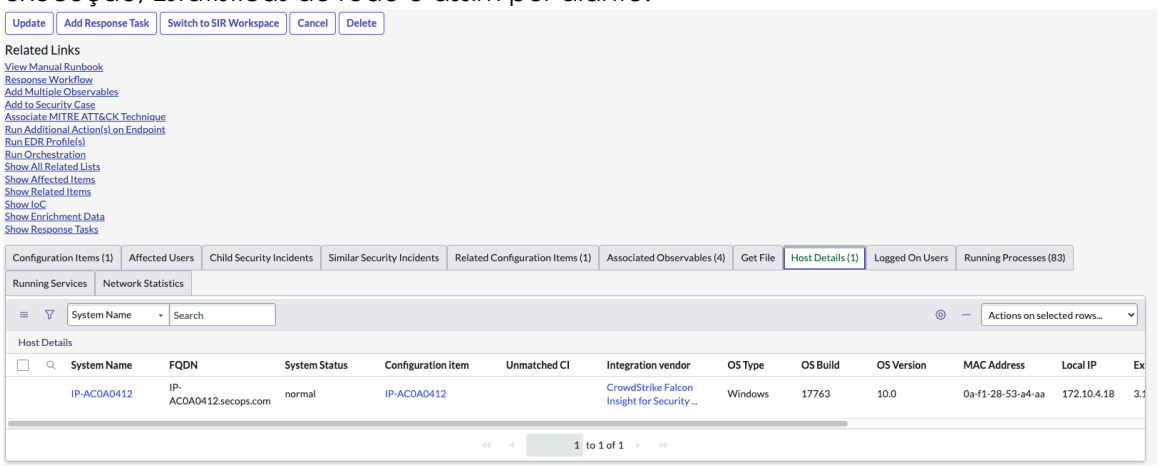
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Revise as anotações de trabalho e a seção de atividades para exibir os marcadores iniciados e concluídos pelo perfil.



5. Revise os detalhes nas listas relacionadas CrowdStrike Falcon Insight Detalhes, como Obter arquivo, Detalhes do host, Usuários conectados, Processos em execução, Serviços em execução, Estatísticas de rede e assim por diante.



Acionar um perfil CrowdStrike Falcon Insight manualmente a partir de um incidente de segurança

Acione um perfil manualmente depois de revisar um incidente de segurança.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos Now Platform incidentes de segurança. CrowdStrike Falcon Insight também permite que você execute capacidades individuais em itens de configuração (ICs) sem usar um perfil.

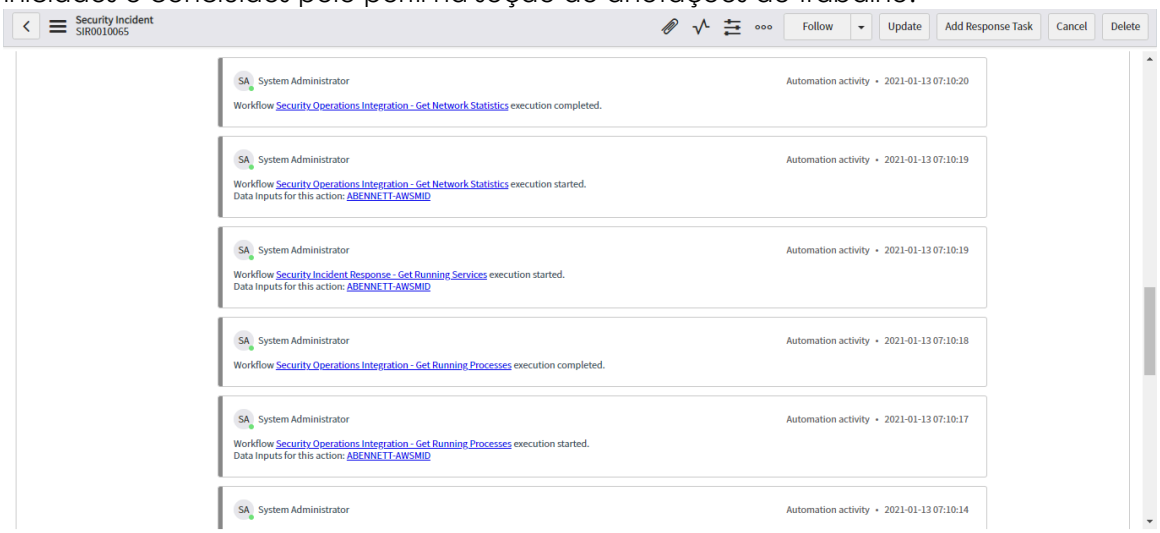
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações CrowdStrike Falcon Insight.
3. Na seção de listas relacionadas, selecione **Executar perfil(is) de EDR**.

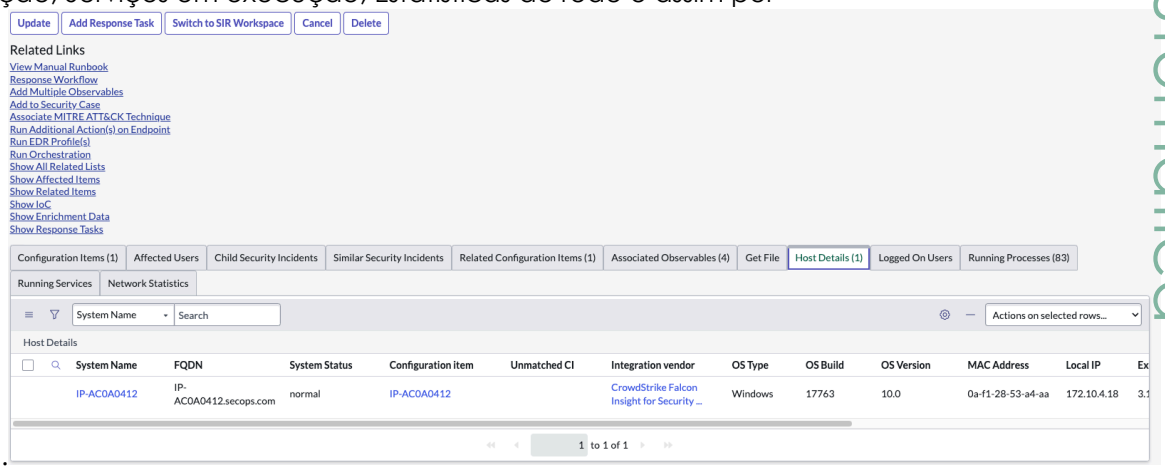
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Navegue e selecione um perfil na lista de perfis disponíveis.
5. Selecione **Incluir IC relacionado** para executar este perfil em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique em **Enviar**.
   O perfil selecionado é acionado manualmente. Você pode revisar a seção de anotações de trabalho e atividades e os marcadores iniciados e concluídos pelo perfil na seção de anotações de trabalho.



7. Os resultados aparecem na forma de listas relacionadas, como Obter arquivo, Detalhes do host, Usuários conectados, Processos em execução, Serviços em execução, Estatísticas de rede e assim por diante.



8. Para executar capacidades individuais em um IC, execute as seguintes etapas:

   a. Na lista relacionada Itens de configuração, selecione o IC necessário.

   b. Clique na lista suspensa **Ações em linhas selecionadas...** e selecione a capacidade necessária que você deseja executar para o IC selecionado.
   Por exemplo, Isolar host.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Pesquise a implementação da capacidade necessária para o IC usando a opção de pesquisa e selecione **Isolar host do CrowdStrike Falcon Insight**.

d. Clique em **Isolar host** para executá-lo no IC selecionado.

Criar e configurar um perfil para a pesquisa de detecções

Use pesquisas de detecções para CrowdStrike Falcon Insight para localizar máquinas infectadas na rede da sua organização e para lidar com casos de resposta a incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Selecione observáveis individuais ou múltiplos e execute uma pesquisa de detecções manual em CrowdStrike Falcon Insight para determinar a predominância de uma ameaça ao longo do tempo.

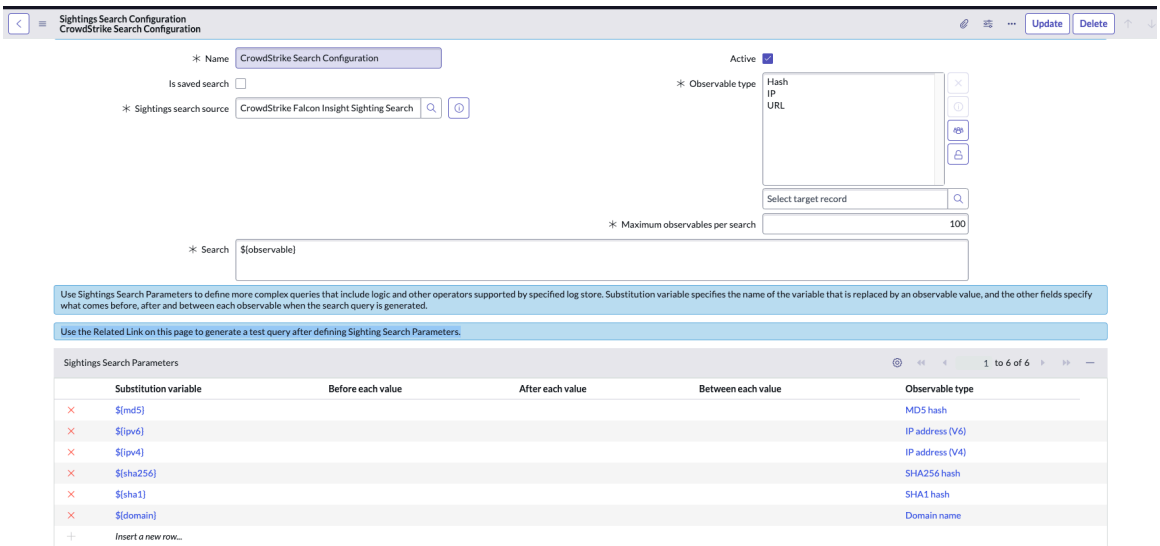
Procedimento
1. Navegar até **Todos** > **Integração com CrowdStrike Falcon Insight** > **Perfis de pesquisa de detecções**.
2. Clique em **Nova**.
3. Configure este perfil para determinar em quais servidores pesquisar uma capacidade de pesquisa específica do CrowdStrike Falcon Insight.
4. No formulário, preencha os campos:

Campo	Descrição
Nome	Nome do perfil da Pesquisa de detecções.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem da pesquisa de detecções	A origem da pesquisa de detecções. Selecione a Pesquisa de detecções do **CrowdStrike Falcon Insight** como a origem.
Ativo	Opção para indicar se o adicional está ativo ou não.
Tipo de observável	A integração do CrowdStrike Falcon Insight é compatível com os seguintes tipos de observável: ◦ Hash ◦ IP ◦ URL A pesquisa de detecções é compatível com os seguintes tipos de observáveis: ◦ Nome do domínio ◦ Endereço IP (V4)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Endereço IP (V6) ◦ Hash MD5 ◦ Hash SHA1 ◦ Hash SHA256
Máximo de observáveis por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa.
Pesquisar	A cadeia de caracteres de pesquisa padrão é `$(observable)`, mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com a integração CrowdStrike Falcon Insight.
Parâmetros da Pesquisa de detecções	Parâmetros para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado Você pode usar os Links relacionados na parte inferior da página para gerar uma consulta de teste depois de definir os Parâmetros de pesquisa de detecções.



5. Clique em **Enviar**.
   A configuração está concluída e você pode invocar a pesquisa de detecções a partir do incidente de segurança Now Platform.
6. Para verificar a configuração e executar uma pesquisa de detecções, execute as seguintes etapas:

   a. Abra um incidente de segurança, role até a parte inferior do incidente de segurança e clique em **Mostrar todas as listas relacionadas**.

   b. Se você selecionar um ou mais itens de configuração (IC) nas listas relacionadas a **Processos em execução**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você executar uma pesquisa de detecções para um IC da lista relacionada Processos em execução, será somente uma pesquisa de detecções de hash de processo.

c. Clique na lista suspensa **Ações nas linhas selecionadas...** e selecione **Executar Pesquisa de detecções do CrowdStrike**.

d. Pesquise o perfil de pesquisa de detecções necessário usando a opção de pesquisa.

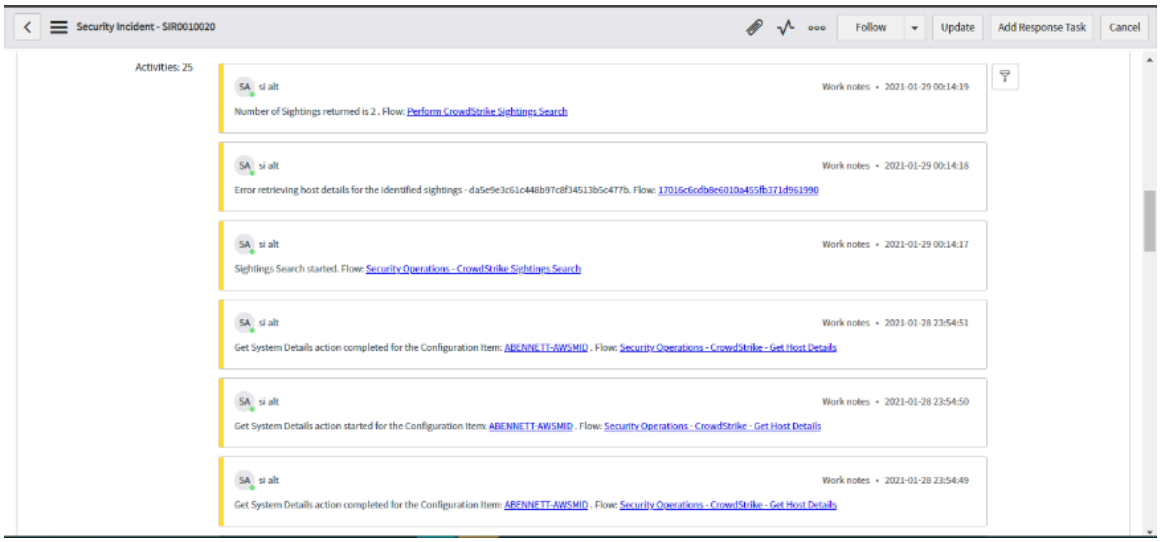
e. Selecione o perfil de pesquisa de detecções necessário e clique em **Enviar**.

f. Se você selecionar um ou mais observáveis nas listas relacionadas a **observáveis associados**.

g. Clique na lista suspensa **Ações nas linhas selecionadas...** e selecione **Executar pesquisa de detecções**.

h. No pop-up do intervalo de tempo, selecione qualquer valor aleatório e clique em **Pesquisar**.

i. Ao concluir a pesquisa, valide os resultados e detalhes nas anotações de trabalho e nas listas relacionadas.



j. Selecione a guia **Detecções** para exibir os detalhes da detecção.

k. Clique no ícone **Visualizar** ao lado do IC para exibir mais informações sobre os detalhes de detecções do CrowdStrike.

l. Clique em **Detalhes da pesquisa** de detecções para exibir os detalhes da pesquisa de detecções e clique na guia **Resultados**da pesquisa de detecções para obter os resultados da pesquisa.

Configurar e acionar ações adicionais no CrowdStrike Falcon Insight

A integração CrowdStrike Falcon Insight oferece suporte à execução de ações adicionais, como expressão regular (regex). A integração CrowdStrike Falcon Insight fornece 40 ações adicionais com o sistema de base.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Integração com CrowdStrike Falcon Insight** > **Ações adicionais do CrowdStrike**.
2. Clique em **Novo** para criar sua própria ação adicional ou selecione uma ação existente que vem com o sistema de base.
   Por exemplo, vamos criar uma nova ação adicional.
3. No formulário, preencha os campos.

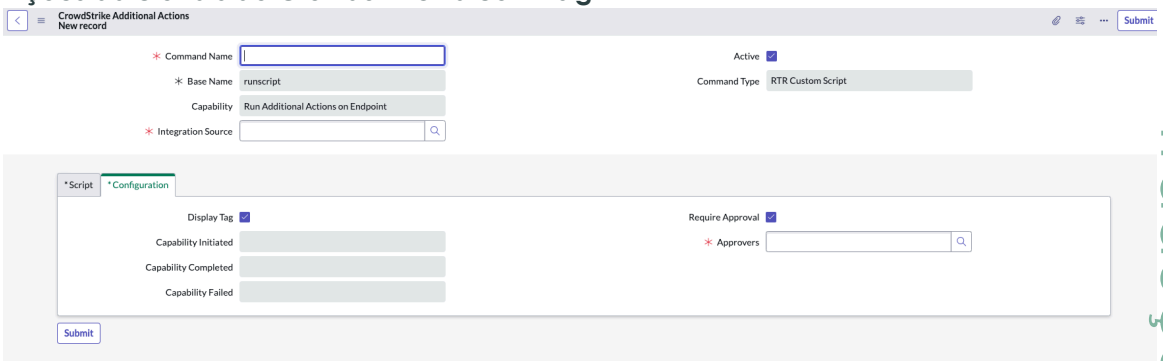
Campo	Descrição
Nome do Comando	Nome do comando para a ação adicional. Por exemplo, reg set.
Nome base	Nome base da ação adicional. Este campo é definido por padrão. Por exemplo, reg.
Capacidade	Nome da capacidade da ação adicional. Este campo é definido por padrão. Por exemplo, Executar ações adicionais no endpoint.
Origem da integração	A origem da ação adicional. Por exemplo, Integração do CrowdStrike Falcon Insight.
Ativo	Opção para indicar se o adicional está ativo ou não.
Tipo de Comando	Tipo de comando para a ação adicional. Este campo é definido por padrão. Por exemplo, Script personalizado de RTR.
Script	◦ **Tipo de SO**: opção para selecionar o tipo de SO para o script. Selecione uma das seguintes propriedades: ▪ **Windows** ▪ **MAC OS X** ▪ **Linux** ▪ **Nenhum(a)** ◦ **Script**: opção para inserir seu script se você selecionou um dos seguintes sistemas operacionais, exceto para a opção Nenhum.
Configuração	◦ **Exibir**marcador: opção para exibir o marcador da configuração. Você pode selecionar o marcador para os seguintes campos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	▪ Capacidade - Iniciada. Por exemplo, reg set - Iniciado. ▪ Capacidade - Concluída. Por exemplo, reg set - Completed. ▪ Capacidade - Falha. Por exemplo, reg set - Failed. ◦ **Exigir aprovação**: opção para selecionar um aprovador ou grupo que precisa aprovar a configuração.

Ações adicionais do CrowdStrike Falcon Insight



4. Clique em **Enviar**.
5. Você também pode escolher entre as seguintes ações adicionais existentes.
   Existem 40 ações adicionais que vêm com o sistema de base, que você pode usar para executar configurações adicionais.

> **Nota:** Certifique-se de abrir a lista Ações adicionais do CrowdStrike e definir a ação adicional necessária como **verdadeira**, caso contrário, a ação adicional não estará disponível no espaço.

Lista de ações adicionais que vem com o sistema de base

Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione o incidente de segurança que você deseja revisar com a execução de ações adicionais no endpoint.

   a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.

   b. Navegue e selecione a capacidade necessária.
   Por exemplo, clique na capacidade de **definir reg**.

   c. Selecione **Incluir IC relacionado** para executar as ações adicionais em todos os ICs relacionados do endpoint.

   d. Você pode definir a **subchave** para executar as ações adicionais no endpoint.
   Esta subchave pode ser uma chave HKLM/Software/nova.

8. Para iniciar a execução de ações adicionais no endpoint, clique em **Executar ação adicional**.
9. Exibir as atividades de automação da execução e validá-las.
10. Valide o status da ação nas listas relacionadas Ações adicionais nas listas relacionadas ao endpoint.

Usando a integração CrowdStrike Falcon Insight no Espaço do analista

Use a integração CrowdStrike Falcon Insight para aproveitar os recursos CrowdStrike Falcon Insight no espaço do analista SIR.

Antes de Iniciar

Função necessária: sn_si.admin

Antes de usar a integração CrowdStrike Falcon Insight no espaço do Security Incident Response, você deve baixá-la do ServiceNow Store e configurá-la. Para obter mais informações, consulte Introdução à integração CrowdStrike Falcon Insight.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar a integração CrowdStrike Falcon Insight para realizar ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o espaço Security Incident Response.

A integração CrowdStrike Falcon Insight permite que os analistas usem os seguintes recursos [CrowdStrike Falcon Insight no espaço do analista Security Incident Response :

- **Obter detalhes do host**
- **Obter usuários conectados**
- **Obter estatísticas de rede**
- **Obter processos em execução**
- **Obter serviços em execução**
- **Isolar host**
- **Remover isolamento**
- **Obter arquivo**

Tradução automática

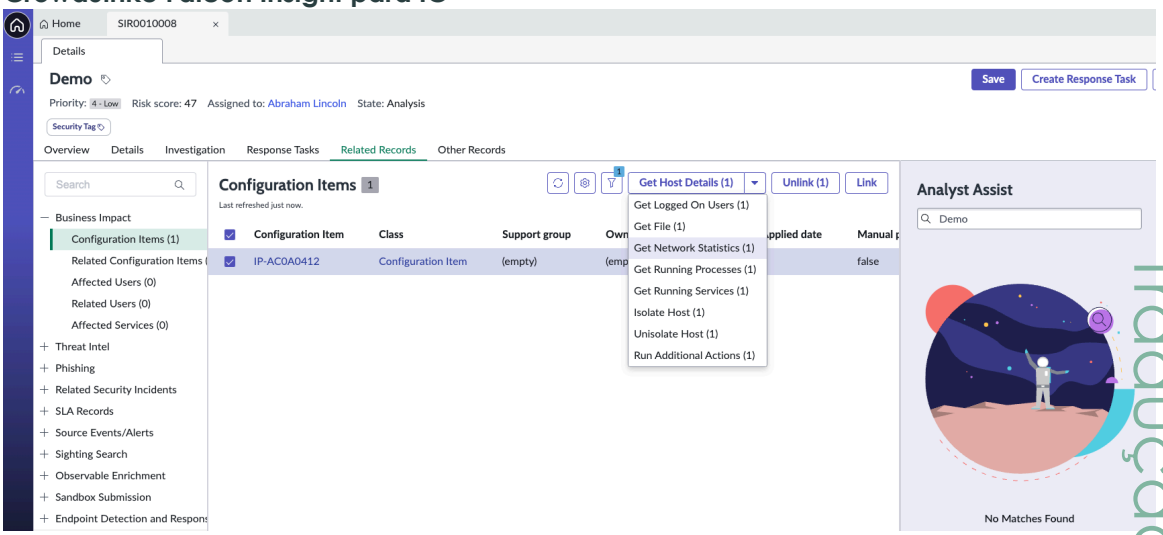
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No espaço SIR, abra o incidente de segurança necessário e selecione a guia **Registros relacionados**.
2. Você pode usar as capacidades do CrowdStrike Falcon Insight na lista relacionada Impacto nos negócios para análise.

   a. Selecione um **Item de configuração**e escolha uma capacidade na lista suspensa.

CrowdStrike Falcon Insight para IC



   b. Selecione a implementação do **CrowdStrike Falcon Insight** e clique em **Enviar**. A capacidade Obter estatísticas de rede é invocada no IC. Você pode exibir as anotações de trabalho dos resultados e descobertas.

3. Você pode usar os recursos do CrowdStrike Falcon Insight na lista relacionada de **Detecção e resposta de endpoint (EDR)** para análise.

   a. Na lista relacionada Detecção e resposta de endpoint (EDR), escolha um EDR na lista.

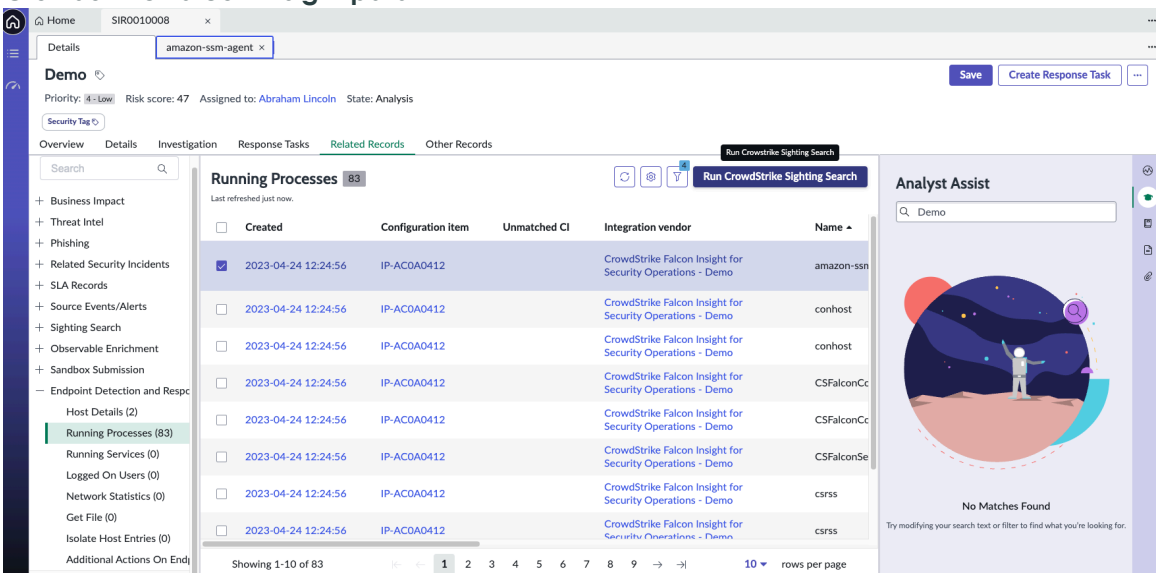
   b. Clique em um processo em execução específico para exibir os detalhes do processo em execução do CrowdStrike Falcon Insight.

   c. Para executar uma Pesquisa de detecções do CrowdStrike Falcon em um processo em execução específico, selecione o processo em execução e clique em **Executar detecção de detecções do CrowdStrike**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

CrowdStrike Falcon Insight para EDR



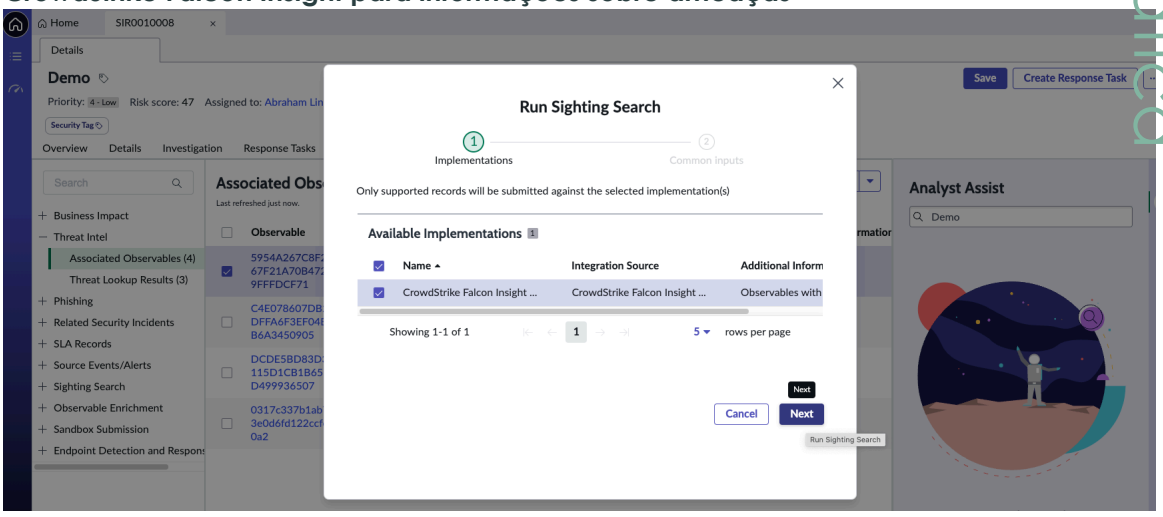
d. Selecione a implementação do **CrowdStrike Falcon Insight** e clique em **Executar pesquisa**.
Em seguida, uma pesquisa de detecção de hash é executada no processo em execução selecionado. Você pode exibir as anotações de trabalho dos resultados e descobertas.

4. Você pode usar as capacidades do CrowdStrike Falcon Insight no **Threat Intel** para análise.

a. No grupo Informações sobre ameaças, selecione um **Observável**e escolha uma capacidade CrowdStrike Falcon Insight na lista suspensa.

b. Selecione a implementação do **CrowdStrike Falcon Insight** e clique em **Avançar**.

CrowdStrike Falcon Insight para informações sobre ameaças



c. No pop-up Selecionar data/hora, selecione um valor aleatório e clique em **Enviar**.
Em seguida, uma pesquisa de detecções é executada no observável selecionado. Você pode exibir as anotações de trabalho dos resultados e descobertas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sandbox do CrowdStrike Falcon X para integração de Operações de segurança

Com a integração CrowdStrike Falcon X Sandbox para Operações de segurança, você pode enviar arquivos e URLs como parte do processo de resposta a incidentes de segurança para CrowdStrike Falcon X Sandbox para executar uma análise detalhada de malware e ameaças.

A integração CrowdStrike Falcon X Sandbox fornece um ambiente virtual isolado sob demanda onde você pode executar a análise de malware e fornecer resultados para o incidente de segurança ServiceNow por meio da integração.

Quando você envia seus incidentes de malware, eles são retidos como parte do registro de incidentes de segurança. Você pode usar esses registros paraou avançar na resolução de incidentes e automatizar o envio de arquivos e URLs.

A integração oferece suporte à automação de playbooks de resposta a phishing e malware , o que permite que a equipe do centro Operações de segurança seja mais produtiva e eficiente na resposta a incidentes de segurança.

Principais benefícios

Com testa integração, você pode fazer o seguinte:

- Automatize o envio de arquivos e URLs do usuário-que relatou phishing (URP), mensagens de e-mail, anexos e outros incidentes de segurança.
- Envie ou reenvie manualmente arquivos e URLs analisados anteriormente para análise atualizada.
- Crie várias configurações de envio que aplicam automaticamente CrowdStrike Falcon X Sandbox parâmetros de envio, como sistema operacional, tipo de verificação e opções de tempo de execução.
- Analise o malware e os resultados da ameaça em um relatório no formato HTML dentro do incidente SIR. Você pode exibir tresultados de pesquisa e o histórico do indicador de arquivos e URLs que foram analisados várias vezes.
- Marque ServiceNow incidentes com o status de processamento de envio, bem como os resultados da descoberta de ameaças.

Consulte também

Identificador do documento	Título do documento
CrowdStrike Falcon X Sandbox	Perguntas frequentes sobre a área restrita do CrowdStrike Falcon
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Comece com a integração CrowdStrike Falcon X Sandbox

Ative e configure o CrowdStrike Falcon X Sandbox para interagir com sua instância [ServiceNow e o produto Security Incident Response.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Antes de poder usar o CrowdStrike Falcon X Sandbox para integração de Operações de segurança, você deve baixá-lo da ServiceNow Store.
- Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração sem problemas CrowdStrike Falcon X Sandbox.

Função necessária: administrador, sn_si.admin

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • O administrador (admin) instala a integração sandbox da loja de aplicativos da ServiceNow e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O sn_si.admin cria e edita a configuração e configurações globais e , então atribui a função de analista de incidentes de segurança (sn_si.analyst). • O analista de incidentes de segurança (sn_si.analyst) responde a incidentes de segurança, como enviando arquivos e URLs para a caixa se analisando os resultados do envio.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.	Esta integração é compatível com as versões Paris e Orlando. Certifique-se de que esses plug-ins dependentes estejam instalados. Esses plug-ins habilitam a execução de Integration Hub ações e fluxos: • ServiceNow Etapa de ação do IntegrationHub - REST (com.glide.hub.action_step.rest) • ServiceNow Tempo de execução do IntegrationHub (com.glide.hub.integration.runtime) **Nota:** Se vocênão encontrar um plug-in, talvez precise solicitá-lo à equipe ServiceNow. Para solicitar um plug-in, siga as etapas em Solicitar um plug-in .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações que são exigidas pela integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Security Incident Response Dependência (com.snc.si_dep) **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança **5.** Inteligência contra ameaças Suporte comum (necessário para uver as capacidades de integração da área restrita) **6.** Trusted Security Circles **7.** Operações de segurança Assistente de configuração **8.** Security Incident Response Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito de um produto ou aplicação das Operações de segurança e Ativar uma aplicação da ServiceNow Store.
Verifique se você está licenciado para a chave de API privada do Falcon Sandbox e oobtenha a CrowdStrike Falcon X Sandbox chave de API completa.	Esta integração é compatível somente com a nuvem privada Falcon Sandbox. **Nota:** Esta versão não é compatível com a integração do Falcon X. CrowdStrike Falcon X Sandbox O oferece uma chave de API restrita autoassinada e uma chave de API completa atualizada. Use a chave de API completa para esta

Tradução automática

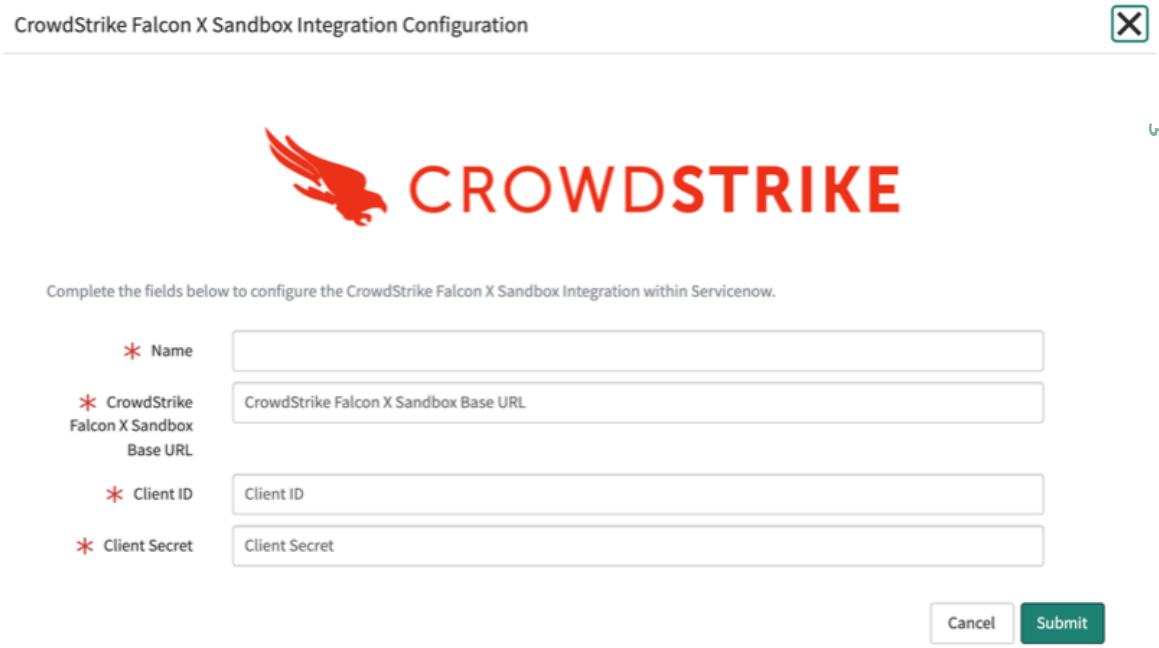
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	integração porque permite acesso irrestrito para envios automatizados. Para obter mais informações, consulte Base de conhecimento do CrowdStrike Falcon Sandbox .

Procedimento

1. Baixe a integração do CrowdStrike Falcon Sandbox para Operações de segurança na ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de integração**.
3. Pesquise o bloco de integração CrowdStrike Falcon X Sandbox e clique em **Configurar**.



4. Insira os seguintes detalhes para concluir a configuração:

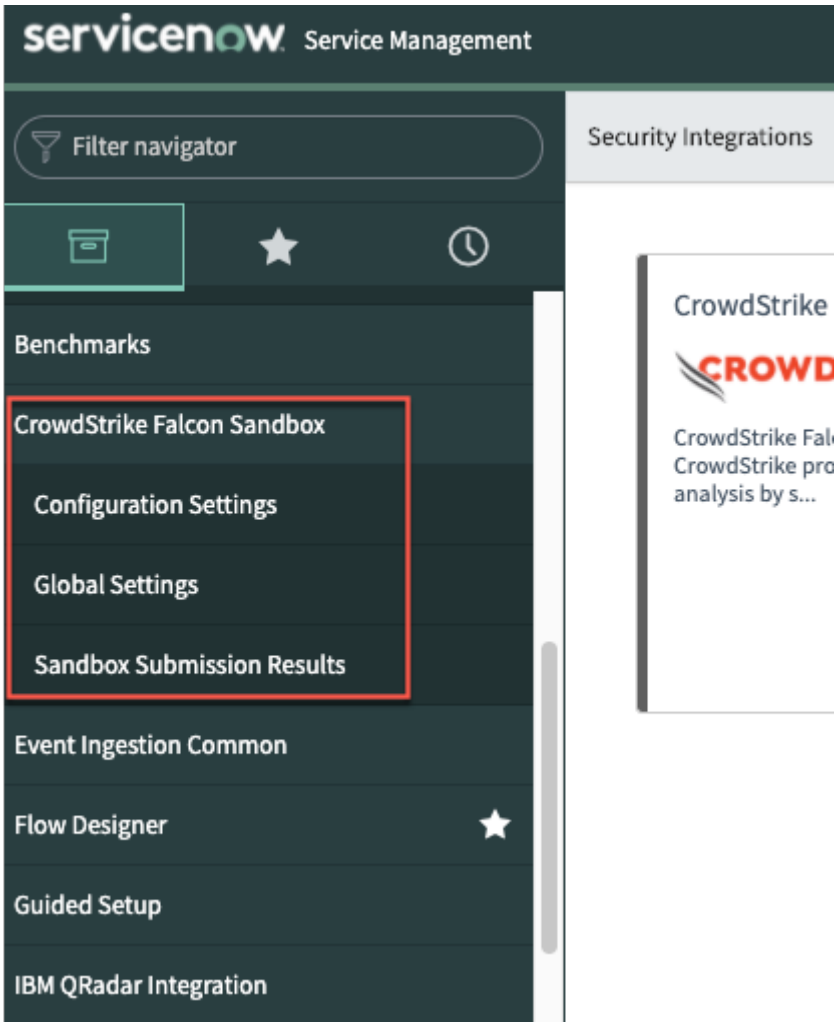
Campo	Descrição
Nome	Nome desta integração, por exemplo, `demo-1`. Embora este seja um nome exclusivo para identificar a configuração sandbox, você só pode configurar uma integração por instância da ServiceNow.
URL base da área restrita do CrowdStrike Falcon	SURL base do andbox. Este URL está disponível depois que você configura a caixa s.Por exemplo, `https://`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	`servicenow.falcon-sandbox.com` é um URL base.
ID de cliente	ID do cliente da API OAuth2. Para obter mais informações, consulte Clientes e chaves de API .
Segredo do cliente	Chave secreta do cliente da API OAuth2. Para obter mais informações, consulte Clientes e chaves de API .

5. Clique em **Enviar**.
   Depois que a área restrita for validada e enviada com sucesso, ela será salva na página Integrações de segurança como um bloco. Agora você pode exibir o módulo Sandbox no navegador de aplicações .



O que Fazer Depois

Depois de concluir com sucesso a integração, a próxima etapa é definir as configurações de envio da Sandbox.

Definir configurações de envio da área restrita

Defina a configuração da Sandbox para definir o ambiente de análise e as opções de tempo de execução para os envios de registros de incidentes de segurança para a análise de malware.

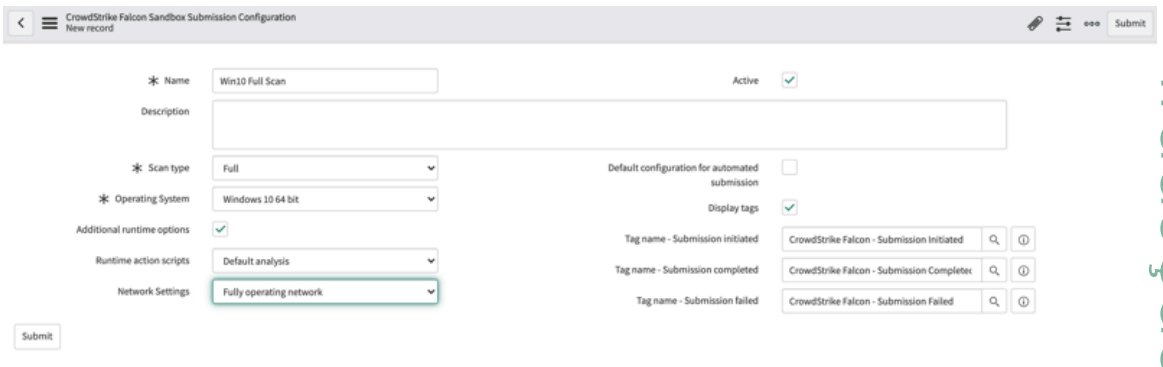
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Antes de enviar arquivos ou URLs para o CrowdStrike Falcon X Sandbox usando a integração, você deve definir pelo menos uma configuração de envio. A configuração de envio define o sistema operacional Sandbox, o tipo de verificação, as opções de tempo de execução e outras características de manipulação de incidentes. Você pode criar várias configurações para usar as diferentes opções que estão disponíveis no ambiente CrowdStrike Falcon X Sandbox.

Procedimento
1. Navegar até **Todos** > **CrowdStrike Falcon X Sandbox** > **Definições de Configuração**.
2. Clique em **Nova**.



3. Preencha os campos a seguir para criar uma configuração para um tipo **de verificação**completa.

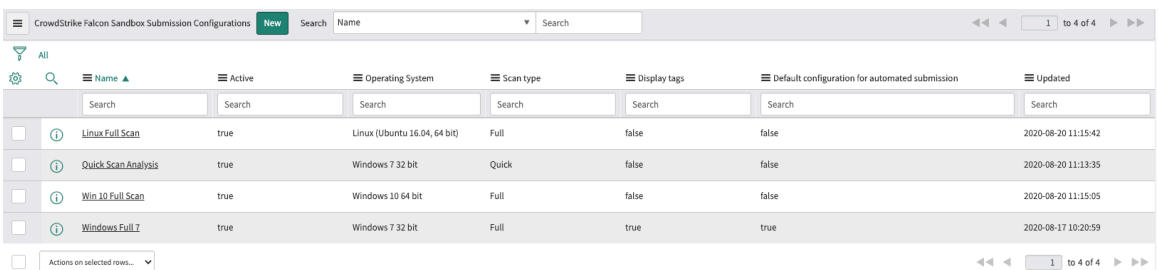
Campo	Descrição
Nome	Nome exclusivo para a configuração de envio. Este nome aparece para os analistas quando eles enviam um arquivo. É importante garantir que o nome seja descritivo e facilmente distinguível de outras configurações (por exemplo, Win 10 Full Scan). Se o nome não for exclusivo, será exibido um erro e os nomes de registro de configuração duplicados não serão salvos.
Tipo de verificação	Spode digitar como **Full**. Um tipo de verificação **rápida** fornece uma análise de ameaça limitada.
Sistema operacional	Um ambiente de VM de análiseem que a caixae verifica o arquivo ou a URL em.
Ativo	Oopção que você seleciona ao enviar arquivos ou URLs manualmente.
Configuração padrão para envio automatizado	Oopção que é limpo por padrão. A seleção desta opção permite que esta configuração esteja disponível para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	automatizar os envios de análise de malware. **Nota:** Você pode ter apenas uma configuração de envio ativa como configuração padrão para envios automatizados.
Marcadores de exibição	Oopção que é limpo por padrão. Quando você seleciona esta opção, os marcadores são exibidos para fornecer o status de um envio de arquivo ou URL. A análise pode levar vários minutos para ser processada. Os marcadores de exibição são envio iniciado, envio concluído, ou envio falhou.
Opções adicionais de tempo de execução	Oopção que é limpo por padrão. Quando você seleciona essa opção, os parâmetros de tempo de execução adicionais compatíveis com a Sandbox ficam disponíveis.
Scripts de ação de tempo de execução	Opção que permite usar um umscript de ação que simulas comportamento humano e interages com o arquivo ou URL durante a análise. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Consulte a documentação CrowdStrike Falcon X Sandbox para obter mais detalhes.
Configurações de rede	Opção que permite selecionar o tipo de configurações de rede usadas ao enviar uma URL ou arquivo para a Sandbox.

4. Clique em **Enviar**.
   Depois de enviar a configuração, ela é salva na página Definições de configuração como um registro. A configuração deve estar **Ativa** para ser usada em senvios de andbox.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de configurar envios de sandbox, a próxima etapa é enviar manualmente arquivos ou ULRs para a área restrita

.

Enviar arquivos ou URLs manualmente para a área restrita

Você pode enviar manualmente um arquivo ou URL para uma área restrita quando determinados critérios de incidente, como categoria é phishing, são atendidos.

Antes de Iniciar

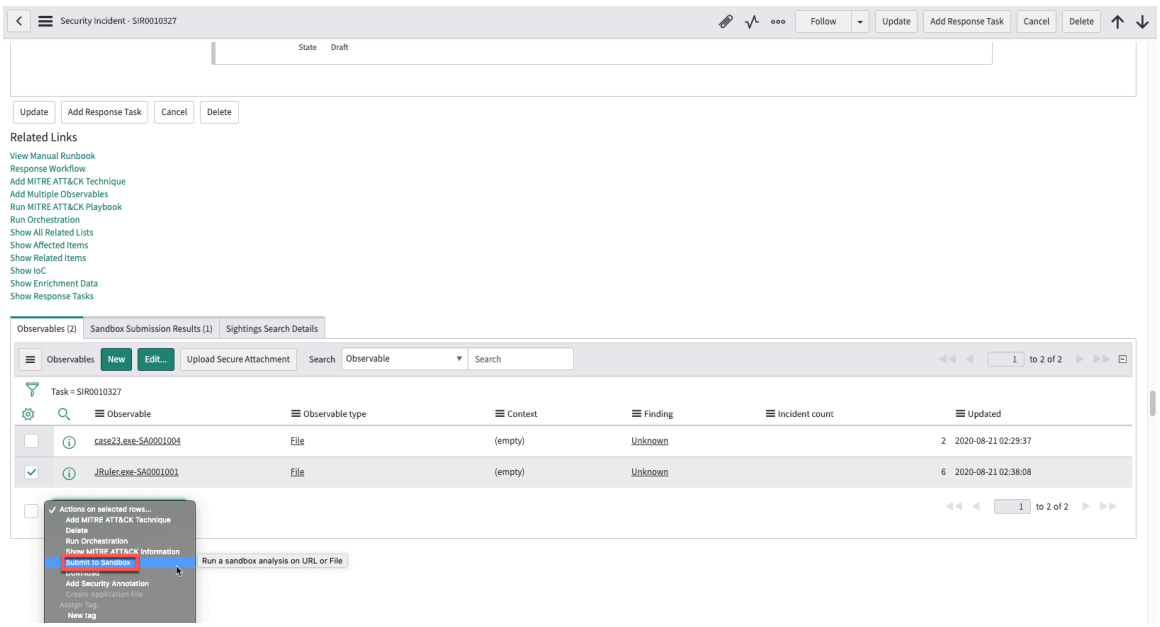
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Depois de revisar o incidente de segurança e o arquivo ou URL, você pode selecionar a opção **Enviar para área restrita** para executar uma análise de malware.

Procedimento

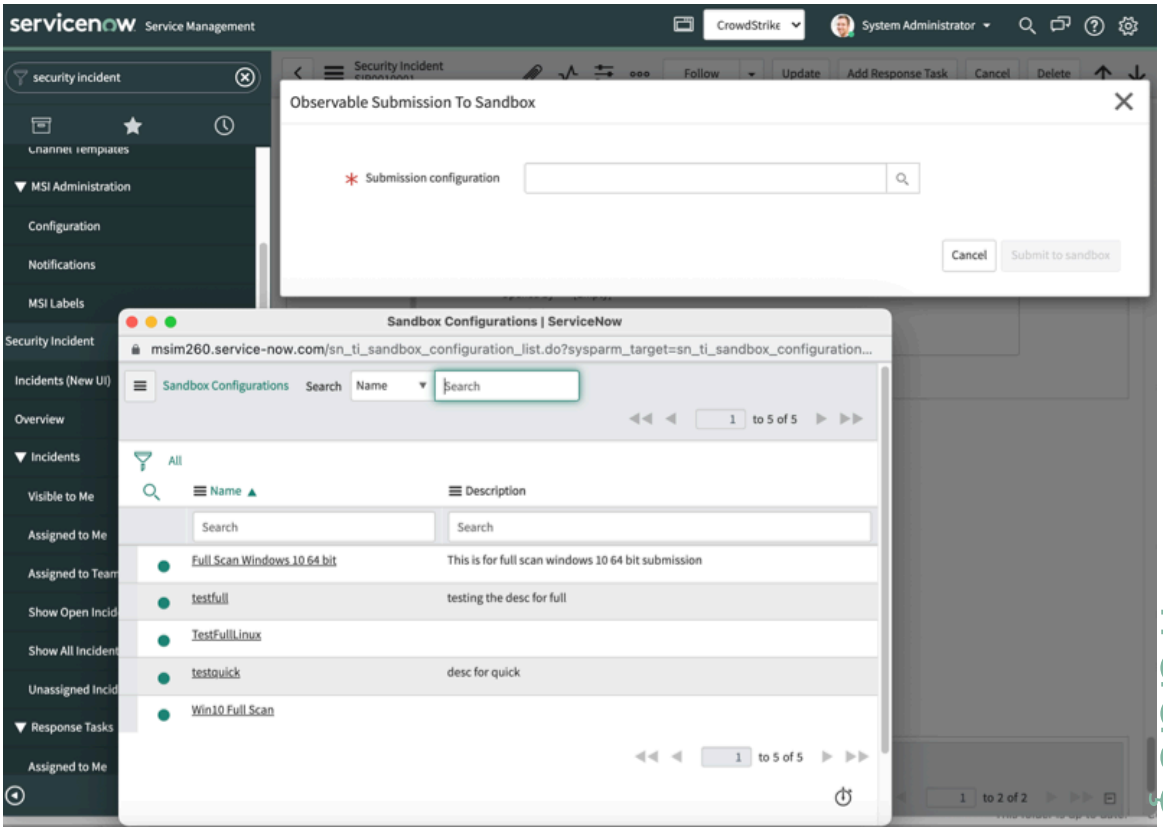
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes** e abra um incidente de segurança para o qual você deseja enviar um arquivo ou registro de tipo de observável URL.
2. Clique no link relacionado **Mostrar IoC**.
3. Na guia **Observáveis**, selecione um ou vários registros para os quais você deseja executar a análise de malware ou ameaças e clique em **Enviar para área restrita**.



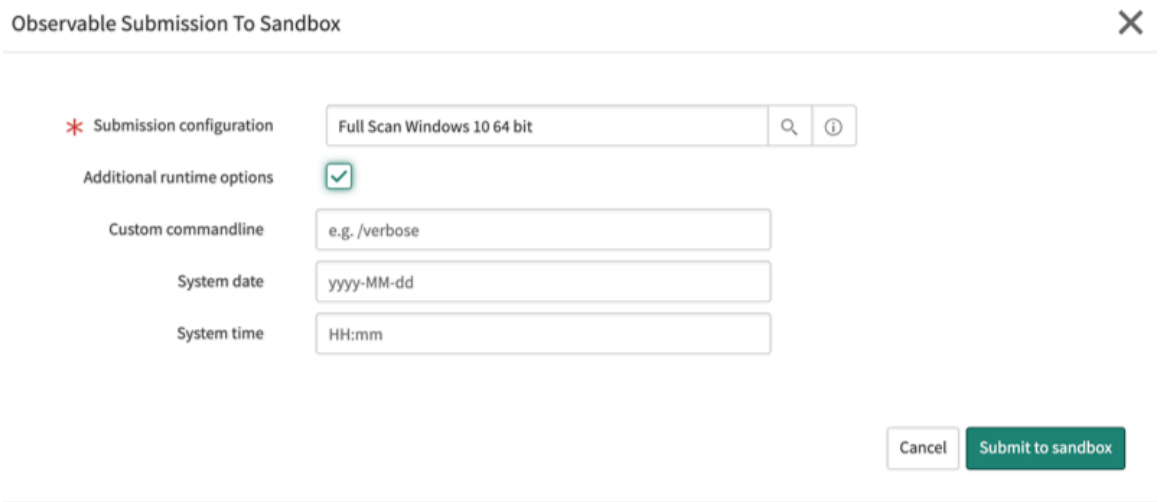
4. Quando o filtro Envio de arquivo for exibido, selecione a configuração de área restrita preferencial em Configuração de **envio**e clique em **Enviar para área restrita**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Opcional: Selecione **Opções adicionais de tempo de execução** se quiser fornecer mais opções personalizadas.



Campo	Descrição
Linha de comando personalizada	Linha de comando de aplicação comum ou uma operação especial.
Data do sistema	Data do sistema no formato aaaa-MM-dd.
Horário do sistema	Hora do sistema no formato HH:mm.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de iniciar o envio, você pode exibir as Anotações de trabalho para ver o status do envio. Para obter mais informações sobre o status do envio ou para analisar os resultados, exiba os **Resultados de envio**da área restrita.

Nota: No CrowdStrike Falcon X Sandbox, a verificação rápida não é compatível com URLs. Se as anotações de trabalho tiverem muitas informações, você poderá usar a opção Filtro para fazer uma busca detalhada nas anotações de trabalho necessárias que são relevantes para você.

O que Fazer Depois

Ao enviar os observáveis para a área restrita para análise de malware, exiba os resultados do envio da área restrita para executar as próximas etapas em relação a possíveis ameaças.

Automatizar CrowdStrike envios do Falcon Sandbox usando o Flow Designer

A integração CrowdStrike Falcon X Sandbox inclui modelos de fluxo criados usando Flow Designer que funcionam com registros de incidentes de segurança.

Antes de Iniciar

- Verifique se você criou uma configuração de envio da área restrita e habilitou uma configuração como a **configuração padrão para envio automatizado**. Quando o fluxo é acionado, o envio da área restrita ocorre em sua configuração padrão.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Esses fluxos foram projetados principalmente para você começar quando quiser automatizar envios de arquivo ou URL como parte do fluxo de trabalho de resposta do incidente.
Quando você ativa um fluxo de amostra, seus anexos de arquivo de phishing são enviados automaticamente se você definir os incidentes de segurança como phishing em seu fluxo de amostra. Como alternativa, você pode enviar todos os arquivos .exe quando esse tipo de arquivo estiver anexado a um registro de observável.

Você pode modificar esses fluxos de amostra para acionar um envio automatizado sob diferentes condições, categorias, condições compostas e assim por diante.

A integração da área restrita consiste em dois fluxos do sistema de base que são desativados por padrão.

- **Enviar arquivo quando a categoria for phishing**: este fluxo envia um arquivo para a área restrita para análise de malware quando a categoria de incidente de segurança é definida como phishing. Você deve anexar um arquivo ao registro do observável no incidente de segurança. Se você estiver usando a funcionalidade URP (User Reported Phishing), qualquer anexo de e-mail será analisado automaticamente e adicionado ao registro de incidente SIR como um registro observável. Nenhuma ação adicional é necessária para automatizar o envio.
- **Enviar quando o tipo de arquivo do observável for exe**: este fluxo envia um arquivo para a área restrita para análise de malware quando o observável do incidente de segurança é um exe. Semelhante ao fluxo de categoria de phishing, você deve anexar um arquivo a um registro observável no incidente de segurança. Você pode fazer isso manualmente, carregando o arquivo, ou automaticamente se um anexo de e-mail de phishing ou outro mecanismo que esteja criando o incidente estiver associado aos registros observáveis.

Quando os fluxos são configurados e as condições do incidente atendem aos parâmetros, os envios da área restrita são acionados automaticamente quando você revisa o incidente

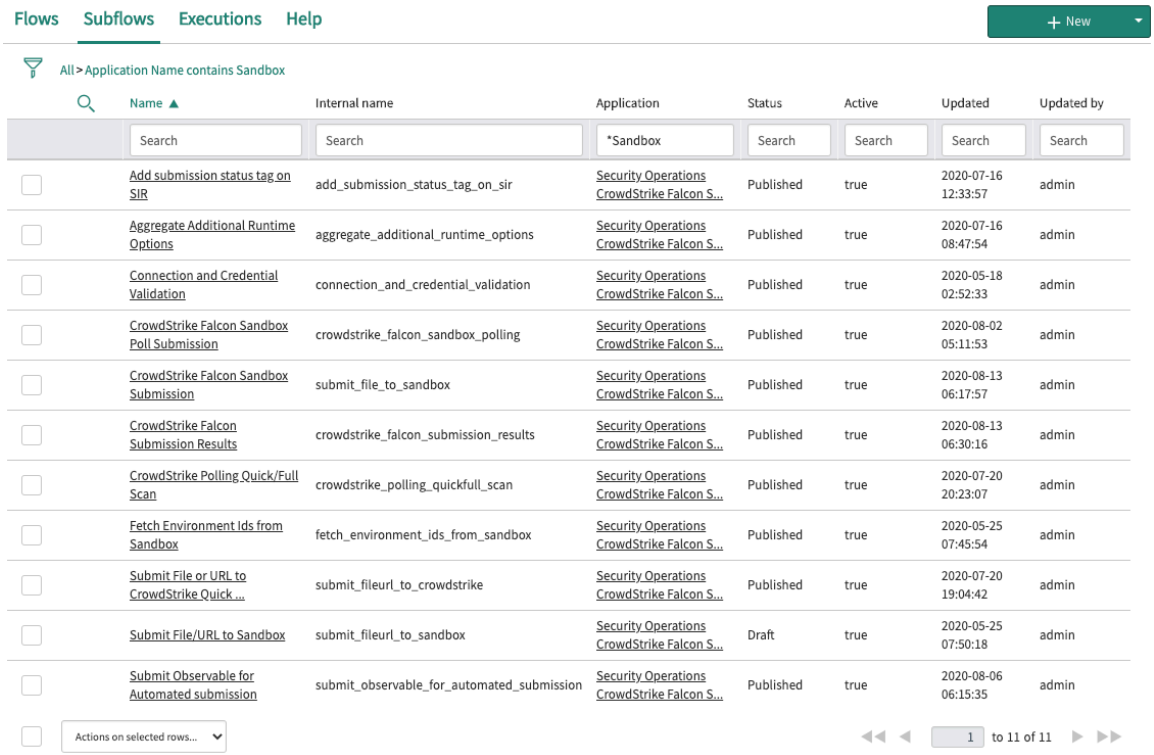
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de segurança. Revise a anotação de trabalho que indica que um envio foi iniciado, um marcador aparecerá se habilitado na configuração e um registro de resultados de envio pendentes.

A integração da área restrita também contém vários subfluxos. Os subfluxos são componentes internos das capacidades gerais de envio de integração. Você pode personalizar e editar os subfluxos para atender aos seus critérios de segurança.

Você pode consultar os subfluxos para solucionar problemas com envios da área restrita. Um registro de execução é criado sempre que você invoca um subfluxo. Este registro indica onde ocorreu um erro específico no fluxo e permite que você corrija o problema.

Sandbox Integration - Vários fluxos de trabalho



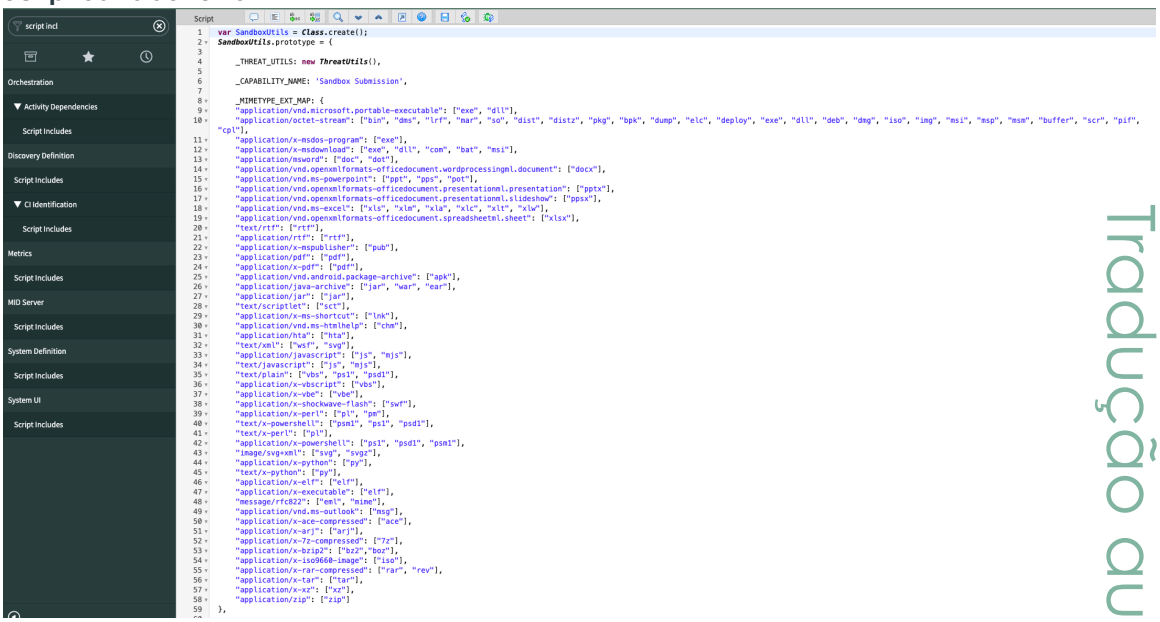
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

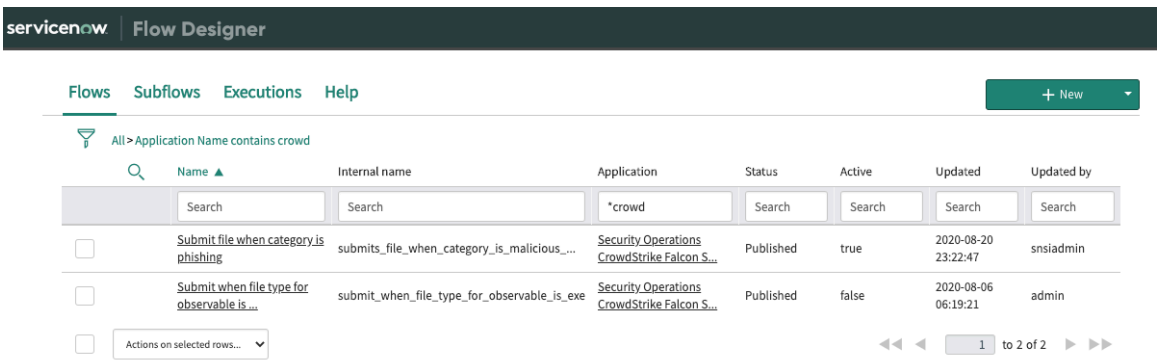
- Se você optar por personalizar os fluxos padrão, verifique se o subfluxo Enviar observável para envio automatizado está incluído no fluxo para acionar envios automáticos.
- Você pode personalizar e definir suas extensões de arquivo para um exe. Crie uma cópia do fluxo **Enviar quando o tipo de arquivo do observável for exe**e faça mudanças na cópia. O tipo de conteúdo e as extensões de arquivo são mapeados no script SandboxUtils. Para acessar as inclusões de script, navegue até **Definições do sistema > Inclusões de script** e pesquise SandboxUtils.

Script SandboxUtils



Procedimento

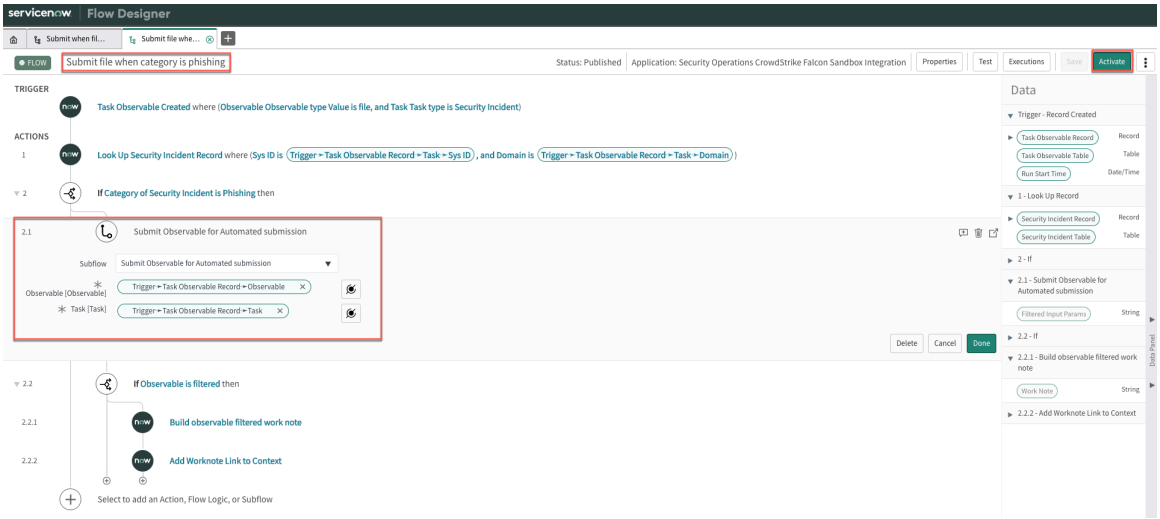
1. Navegar até **Todos** > **Flow Designer** > **Designer** > **Fluxos**.
2. Filtrar os fluxos pelo tipo de **aplicação**.
   Por exemplo, *crowd filtra os dois fluxos CrowdStrike Falcon X Sandbox.



3. Selecione um fluxo para exibir os detalhes.
   O exemplo abaixo mostra o fluxo Enviar arquivo quando a categoria for phishing.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Ativar** e em **OK** quando a mensagem de confirmação for exibida.

O que Fazer Depois

Depois de configurar fluxos de envio automatizados, você pode Exibir os resultados de envio da área restrita para analisar quaisquer ameaças.

Monitorar os resultados de envio na área restrita

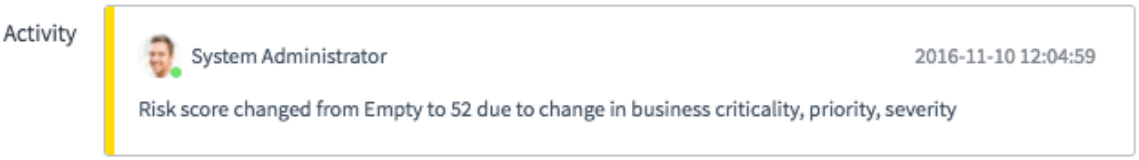
Os resultados de todos os envios do Sandbox são mostrados na guia **Resultados de envio do Sandbox** para cada incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

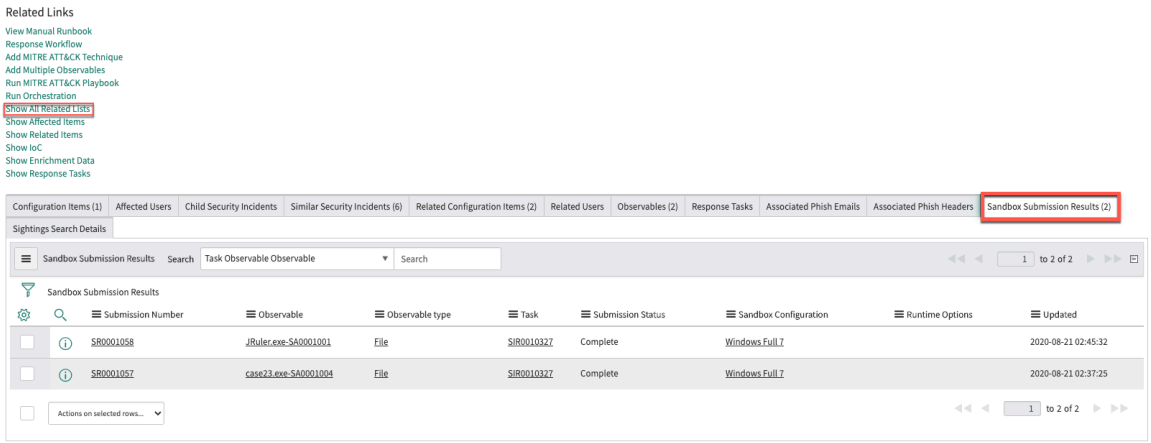
1. Abra o incidente de segurança no qual você está trabalhando e verifique se o envio da caixa se foi bem-sucedido.



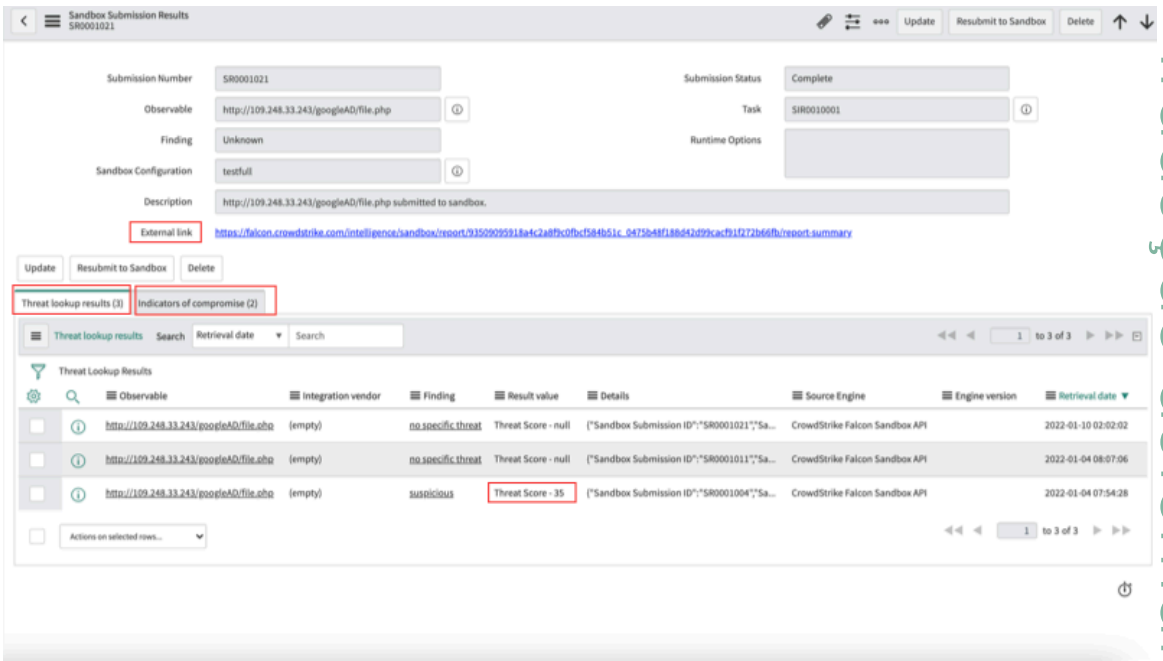
2. Revise as Wanotações de trabalho para obter mais informações e saiba como prosseguir se você não puder verificar se a verificação foi bem-sucedida.
3. Clique no link de resultados completos em Wnota de orks ou em na parte inferior do incidente de segurança, navegue até **Mostrar todas as listas relacionadas**> **Resultados de envio**da área restrita.
   Os resultados são exibidos na guia Resultados de envio da área restrita.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em abrir qualquer registro para exibir a análise completa secaixa.



5. Opcional: Clique **em Reenviar para área restrita** para reprocessar o observável.

Resultados

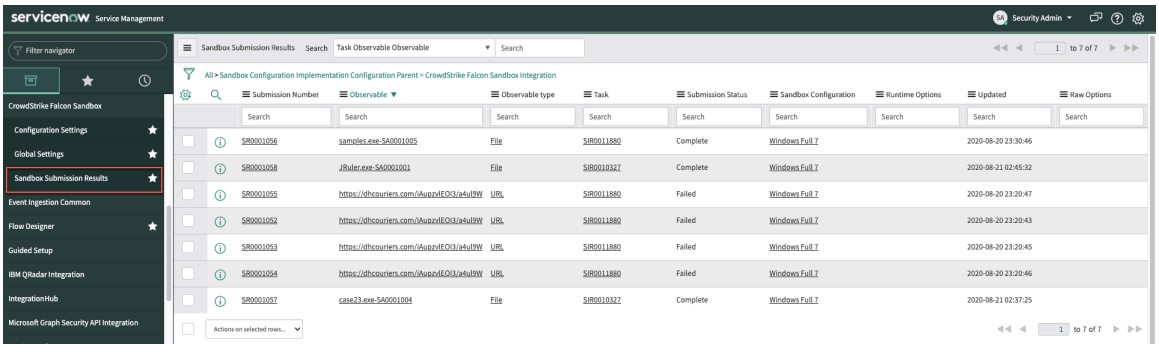
- A guia **Resultados da pesquisa de ameaças** fornece a avaliação da ameaça, incluindo descobertas mal-intencionadas, pontuações de ameaças e detalhes adicionais. Essesdetalhes são fornecidos na estrutura de formato de pesquisa de ameaças padrão para todas as ServiceNow integrações de pesquisa de ameaças.
- A guia **Indicadores de comprometimento** fornece os resultados maliciosos ou suspeitos secaixa com as pontuações de confiança. As pontuações de confiança são semelhantes a outras informações do indicador que são armazenadas na plataforma ServiceNow. Os indicadores classificados como informativos não são incluídos nesta guia.
- Clique em **Link externo** para exibir os resultados da Sandbox no portal CrowdStrike Falcon X Sandbox.

> **Nota:** Esta opção requer que você tenha a função [CrowdStrike Falcon X Sandbox para exibir os resultados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode também monitorar os resultados de envio de sebox para todos os incidentes de segurança navegando até **Área restrita do CrowdStrike Falcon** > **Resultados de envio de sandbox**.



Marcar incidentes de segurança com o status de envio da área restrita

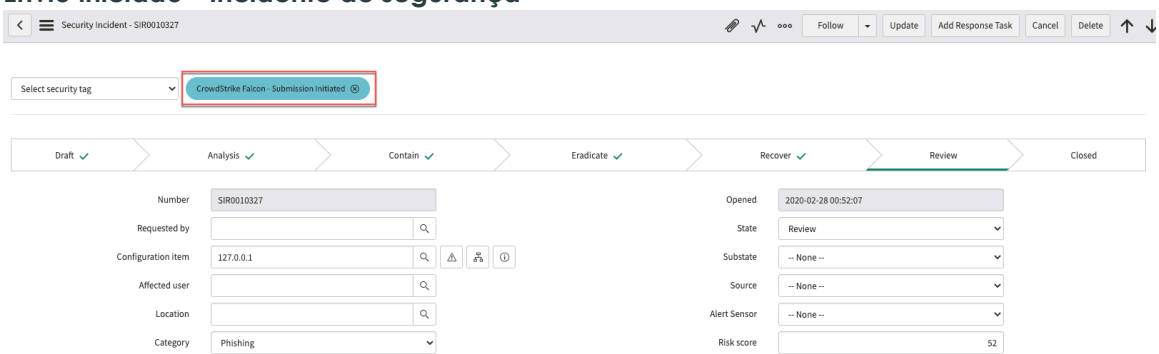
Opcionalmente, você pode marcar incidentes de segurança com os marcadores Envio iniciado e Envio concluído.

Quando você seleciona a opção **Exibir marcadores** na configuração de envio da Sandbox, os marcadores são exibidos para fornecer o status de um envio de arquivo ou URL. Verificar o status dessa forma é útil porque a análise se pode levar vários minutos para ser processada.

Os marcadores de exibição são chamados de envio iniciado, envio concluído e falha no envio.

O exemplo a seguir mostra um incidente de segurança em que o envio foi iniciado.

Envio iniciado - Incidente de segurança

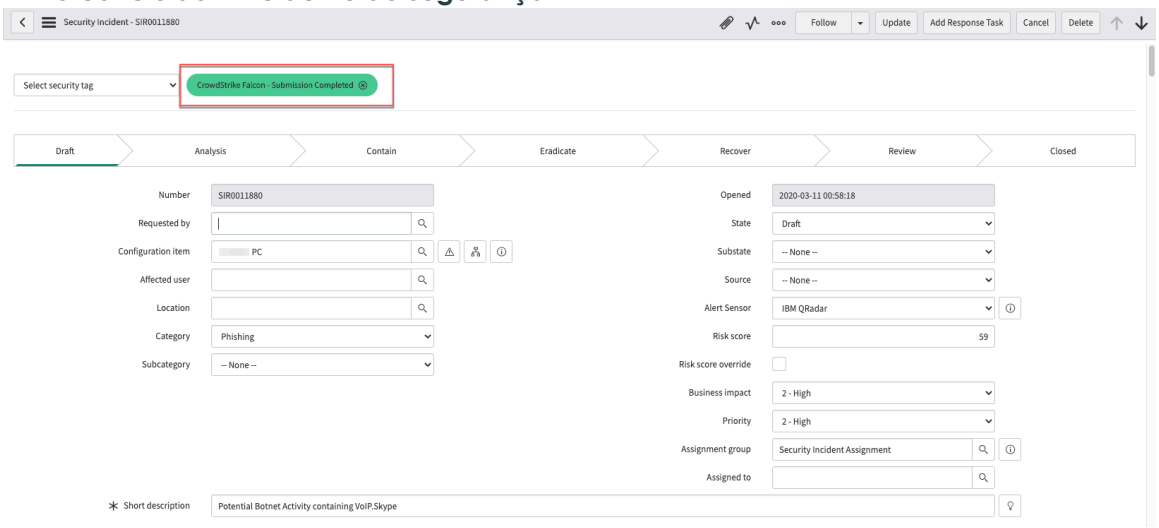


O exemplo a seguir mostra um incidente de segurança em que o envio foi concluído.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Envio concluído - Incidente de segurança



Revisar as configurações globais secaixa

Se você tiver problemas com os resultados de envio de arquivo ou URL, revise e modifique as configurações globais secaixa.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Sandbox do CrowdStrike Falcon** > **Configurações globais**.
2. Revise e modifique as configurações conforme necessário.

Campo	Descrição
Limite de tamanho de arquivo (MB)	Limite de tamanho do arquivo de carregamento da área restrita em megabytes. **Nota:** O limite de tamanho de arquivo de 256 MB é configurado por padrão. Não aumente o valor além de 256 MB. No entanto, você pode reduzir o limite máximo de tamanho de arquivo para evitar o envio de arquivos grandes.
Tempo limite máximo para resultados de envio (minutos)	Tempo limite máximo para resultados de envio de a caixa se.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O tempo limite padrão] é de 30 minutos. Se os resultados demorarem mais de 30 minutos, você poderá aumentar o tempo. Além disso, você pode exibir os resultados no sportal do andbox.

3. Clique **em Salvar** .

Integração de enriquecimento de incidentes do Elasticsearch

A integração Elasticsearch - Incident Enrichment pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	Configurar • Introdução ao Elasticsearch - Incident Enrichment integration • Criar registros de configuração de pesquisa de detecções
Usar • Executar uma pesquisa de detecções • Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções • Operações de segurança - Fluxo de trabalho de pesquisa de detecções do Elasticsearch	Desenvolver • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução ao Elasticsearch - Incident Enrichment integration

Elasticsearch é um mecanismo de pesquisa e análise RESTful distribuído que se integra facilmente com Operações de segurança. Antes de poder usar a integração Elasticsearch - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL base da API e as credenciais de login apropriadas.

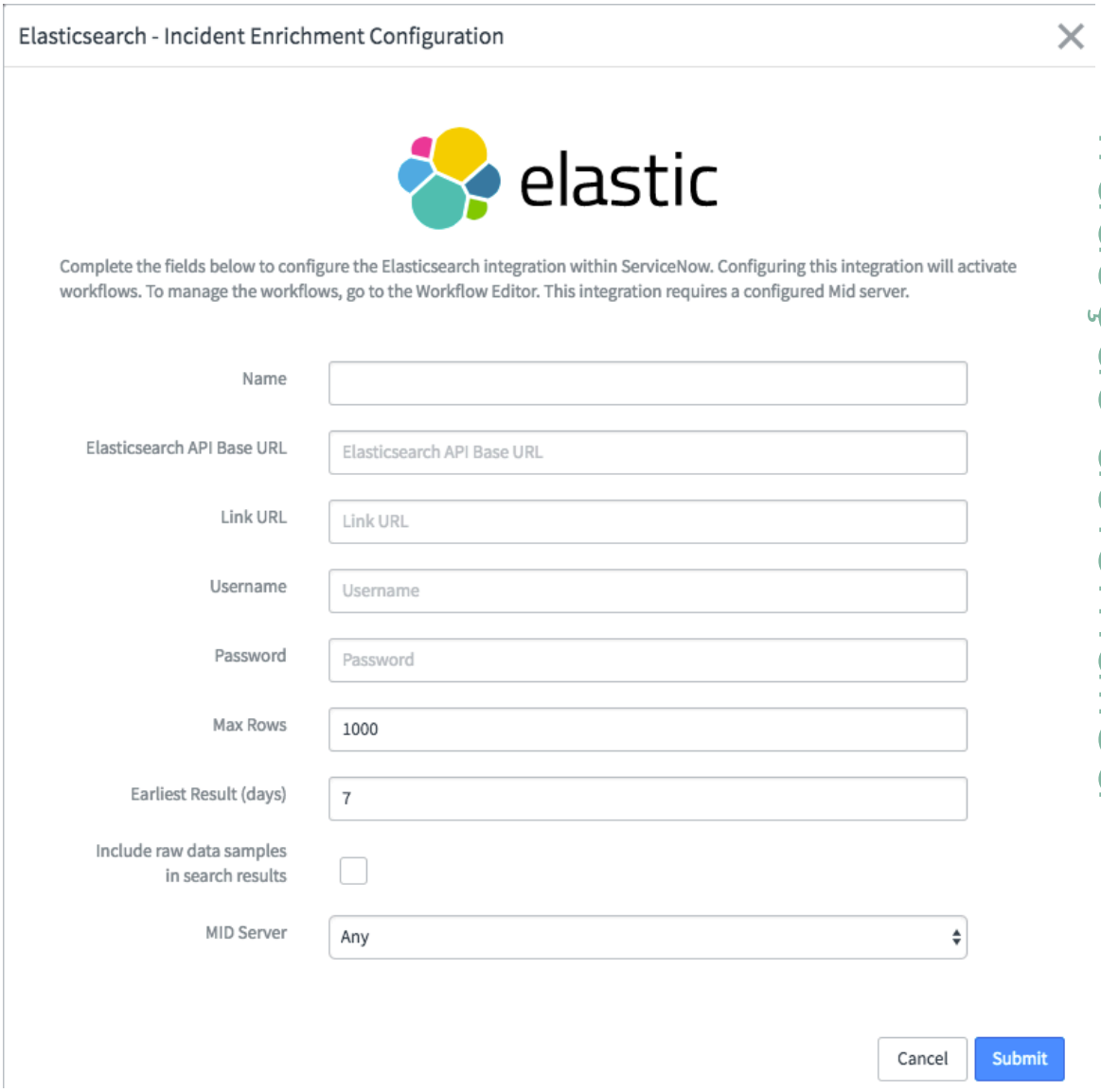
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Elasticsearch e obtenha a URL base da API no seu perfil do Elasticsearch.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Elasticsearch - Aprimoramento de incidentes, clique em **Novo**.



5. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL de Base da API Elasticsearch	A URL base que você adquiriu do site Elasticsearch.
URL do Link	[Opcional] Links para uma instância do Kibana, quando disponível
Nome de usuário	Seu nome de usuário Intel Elasticsearch.
Senha	Sua senha Intel Elasticsearch.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Resultados

Depois de configurada, a integração Elasticsearch - Incident Enrichment pode ser selecionada para publicar observáveis em listas de observação no Security Incident Response.

Integração do FireEye Endpoint Security

O FireEye Endpoint Security (série HX) ajuda as organizações a inspecionar e analisar quais contêm ameaças conhecidas e desconhecidas em qualquer endpoint.

Hoje, os invasores habilidosos ignoram as defesas tradicionais nas quais a maioria das equipes de segurança conta há anos para proteger seus endpoints. Mesmo quando uma defesa tradicional interrompe uma ameaça conhecida, ela não pode determinar o que essa ameaça estava tentando fazer. FireEye HX A Segurança de endpoint ajuda sua equipe de segurança a localizar e interromper ameaças avançadas conhecidas e desconhecidas contra seus endpoints.

A integração do Gold Standard Security Incident Response com FireEye HXtorna mais fácil e eficiente para os analistas de segurança investigar e corrigir incidentes de segurança em um instante, sem precisar navegar entre as ferramentas. Você pode usar a contenção de rede para executar ações de correção nos endpoints, implementar perfis para coletar detalhes específicos sobre o host e executar consultas ou ações específicas no endpoint.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

- Capacidade de executar ações de enriquecimento de host para coletar mais detalhes sobre o endpoint, como detalhes do host, estatísticas de rede, detalhes do usuário, detalhes do arquivo, detalhes do processo e detalhes do serviço.
- Capacidade de executar a Pesquisa de segurança empresarial para detectar possíveis observáveis mal-intencionados nos endpoints e tomar medidas de correção.
- Capacidade de coletar triagem e aquisição de dados para inspeção e análise detalhadas do endpoint.

Limitações

A seguir estão as limitações conhecidas desta integração:

1. O valor do campo Aplicação MID deve ser inserido manualmente.
2. Não é possível isolar o host e obter serviços em execução no agente Linux.
3. Remover isolamento não é compatível com o agente Linux.
4. A aquisição de triagem não é compatível com o agente Linux.
5. Os usuários precisam configurar links relacionados a Mostrar dados de aprimoramento. Ele não está disponível para uso imediato.
6. Para a pesquisa de detecções, somente cinco pesquisas ativas podem estar presentes de uma só vez. O restante será enfileirado e começará após a conclusão de qualquer uma das detecções em andamento.
7. As vistas estão disponíveis prontas para uso, que serão ativas falsas por padrão.
8. O hash não é compatível com Obter processos em execução.

Configurar sua instância do NowPlatform para integração com FireEye

Verifique e revise o procedimento de configuração a seguir para configurar a instância NowPlatform para integração FireEye.

Antes de Iniciar

Função necessária: administrador da Now Platform (sn_si.admin)

A seção a seguir lista as tarefas de configuração que precisam ser concluídas na instância do NowPlatform antes de instalar a aplicação para a integração do FireEye.

Verifique se você concluiu as tarefas a seguir antes de instalar a aplicação da ServiceNow Store.

Tarefa	Descrição
Verifique se você atribuiu as funções necessárias do NowPlatform e do Security Incident Response (SIR).	As seguintes funções são necessárias: **1.** É necessário um usuário com a função de administrador do sistema (admin) para instalar a aplicação da integração. **2.** É necessário um usuário com a função de administrador de incidentes de segurança (sn_si.admin) para configurar a integração, criar, ativar e remover perfis. **3.** É necessário um usuário com a função de analista de incidentes de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	(sn_si.analyst) para trabalhar com incidentes de segurança. Um usuário com esta função pode iniciar qualquer uma das capacidades disponíveis na integração.
Verifique se você instalou e configurou um MID Server.	Configure o MID Server: um MID Server em sua instância do NowPlatform é necessário para gerenciar arquivos e se conectar ao serviço FireEye implantado na rede da sua organização. Para obter mais informações sobre MID servers, consulte https://docs.servicenow.com
Verifique se as aplicações principais da ServiceNow necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação.	As aplicações a seguir devem ser instaladas e ativadas na ServiceNow Store antes de instalar esta aplicação. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas: **1.** Suporte do Security Incident Response **2.** Núcleo de suporte de segurança **3.** Security Support Common **4.** Resposta a incidentes de segurança **5.** Threat Intelligence Support Common **6.** Instalador do pacote Enterprise do Hub de integração da ServiceNow
Antes de habilitar a opção de aprovação para perfis, verifique se você criou um grupo de aprovação.	Um fluxo de trabalho de aprovação opcional está disponível para isolar máquinas host, restaurá-las na rede, obter arquivo e executar ações adicionais no endpoint. Se sua organização quiser um nível extra de controle sobre essas ações, habilite a opção Requer aprovação durante a configuração dos perfis. Na ausência de um perfil, se uma capacidade for invocada diretamente da Lista relacionada, as Aprovações poderão ser tratadas no módulo de configuração padrão do FireEye. Como administrador de segurança, você pode configurar a aprovação ao configurar os perfis e as configurações padrão. Um grupo de aprovação deve estar disponível na lista Grupos em sua instância.

Tradução automática

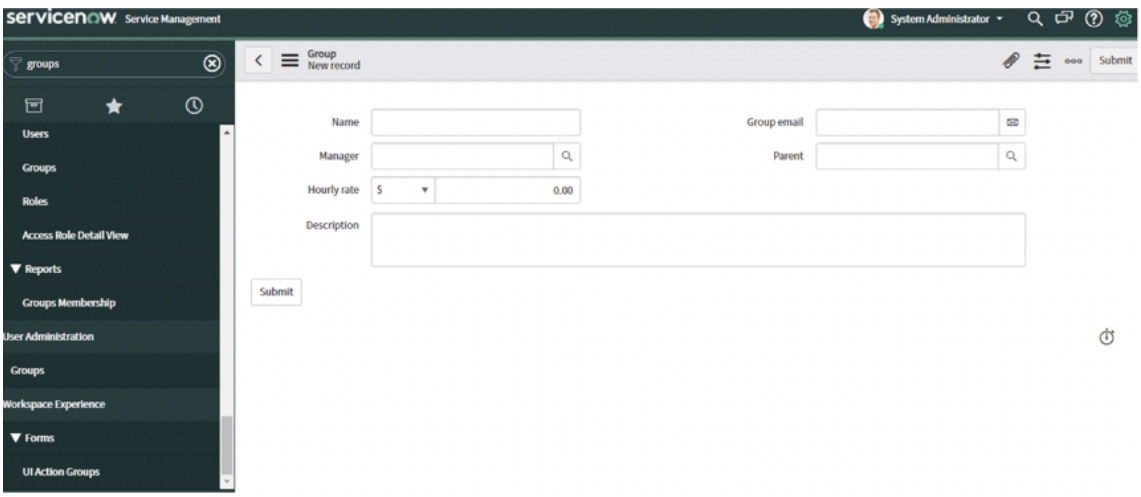
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Administração de usuários** > **Grupos**.
2. Clicar **Novo** na lista Grupos.
3. Preencha o formulário com os seguintes detalhes:

Campo	Descrição
Nome	Nome do grupo que é exibido quando uma solicitação de aprovação é enviada.
E-mail do grupo	(Opcional) Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo.
Gerente	(Opcional) Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	(Opcional) Nome do grupo primário, se associado a um primário.
Taxa por hora	(Opcional) O valor pago por cada hora trabalhada.
Descrição	(Opcional) Informações adicionais sobre o grupo.

4. Clicar **Enviar**.



O novo grupo é exibido na lista Grupos. Você criou com sucesso um grupo de aprovação. Adicione usuários ao seu novo grupo conforme necessário que possam aprovar as solicitações enviadas pelo analista de segurança. Um usuário herda funções de todos os grupos aos quais o usuário pertence. Você também pode atribuir funções diretamente a um usuário.

Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação deve navegar até Minhas aprovações na Now Platform. Como alternativa, os aprovadores podem encontrar as solicitações enviadas especificamente para a integração do FireEye em Aprovações do FireEye.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois
A próxima etapa é instalar e configurar a aplicação da ServiceNow Store.

Definição de configurações de carimbo de data/hora para aquisição de triagem

Configure e verifique as configurações do carimbo de data/hora antes do procedimento de instalação.

Antes de Iniciar
Função necessária: administrador de incidentes de segurança do NowPlatform (sn_si.admin)

Antes de instalar a aplicação FireEye, há alguns pré-requisitos que precisam ser realizados no FireEye.

A aquisição de triagem pode ser solicitada com uma entrada do campo "Carimbo de data/hora próximo" ou do campo "Padrão". Em torno do carimbo de data/hora solicita informações coletadas durante um período especificado antes do carimbo de data/hora até um período especificado após o carimbo de data/hora. O carimbo de data/hora é a hora em que ocorreu o evento que gerou o alerta. Se você selecionar Padrão, o dispositivo Endpoint Security solicitará informações do host para todos os dados em torno de um evento.

Quando um usuário de Segurança de endpoint solicita uma coleta de triagem com base em uma data e hora específicas, o agente retorna informações para uma janela de tempo especificada antes e depois do alerta. As configurações de carimbo de data/hora controlam o comprimento da janela para a coleta de triagem. As configurações de carimbo de data/hora se aplicam somente a eventos de URL de agente (Eventos de monitoramento de URL) e eventos de chave de registro (Eventos de chave de registro).

Você pode usar a guia Configurações de carimbo de data/hora para especificar o período de tempo antes e depois do carimbo de data/hora durante o qual as informações são coletadas. As configurações de carimbo de data/hora podem variar de 0 a 86.400 segundos. O padrão para ambas as configurações é 600 segundos.

Você pode usar a guia Configurações de carimbo de data/hora na página Configurações de triagem automática para especificar o período de tempo antes e depois do carimbo de data/hora durante o qual as informações são coletadas. O carimbo de data/hora é a hora em que ocorreu o evento que acionou o alerta.

Procedimento
1. Navegar até **IU da web de segurança de endpoint**.
2. Selecionar **Administrador** > **Configurações de triagem**.
3. Clicar **Configurações de carimbo de data/hora** guia no **Configurações de triagem automática** página.
4. Especifique o período de tempo antes e depois do carimbo de data/hora para o qual as informações são necessárias.
5. Insira o número de segundos antes do carimbo de data/hora especificado para o qual as informações são necessárias.
6. Insira o número de segundos após o carimbo de data/hora para o qual as informações são necessárias.
7. Clicar **Salvar**.

Nota: Você pode alterar todos os valores na página de volta para as configurações padrão clicando em **Redefinir para padrões**e clicando em Salvar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Área do espaço de aquisição**: a página Aquisições mostra a quantidade de espaço em disco restante para aquisições.
- **Definir limites de utilização de disco para aquisições:**
  - Triagens, aquisições de arquivos e aquisições de dados podem se acumular ao longo do tempo e usar uma quantidade crescente de espaço em disco. Para controlar isso, você pode alocar uma quantidade definida de espaço em disco para eles. Dez por cento do espaço em disco especificado é reservado para aquisições de triagem automática. Quando o espaço total de aquisição alocado é excedido, as triagens automáticas mais antigas são excluídas.
  - Quando o tamanho total do disco de aquisições concluídas excede um limite especificado, o dispositivo Endpoint Security exclui as aquisições concluídas mais antigas até que o espaço em disco suficiente seja liberado para colocar o total abaixo do limite especificado. As aquisições que ainda não foram concluídas não são afetadas.
  - O dispositivo Endpoint Security excluirá automaticamente as aquisições se um Administrador, Analista ou Investigador usar a IU da Web de Endpoint Security para excluir manualmente o agente associado.

  Para definir limites de utilização de disco para aquisições completas usando a IU da web:
- Navegue até **Endpoint Security Web UI**.
- Selecionar **Limites de utilização de disco** do **Administrador** menu.
- No **Limite do espaço de aquisição** Na área, especifique a quantidade máxima de espaço em disco (em GB) que pode ser usada para armazenar triagens, arquivos e aquisições de dados. Os valores e padrões válidos variam de acordo com o modelo do dispositivo Endpoint Security. Os valores apropriados para o seu modelo são mostrados na página Limites de utilização de disco.
- Clicar **Salvar**.

Nota: Todas as configurações mencionadas são respeitadas e, em caso de falhas ou erros, a Now Platform apenas retorna esses erros.

Instalar a aplicação e configurar uma origem para a integração

Instale e configure a aplicação da ServiceNow Store em sua instância da Now Platform.

Antes de Iniciar

Função necessária: administrador do NowPlatform (admin)

Nota: Um MID Server ativo é obrigatório para configurar uma origem.

Baixe a integração do Security Incident Response com a aplicação FireEye HX da ServiceNow Store e instale.

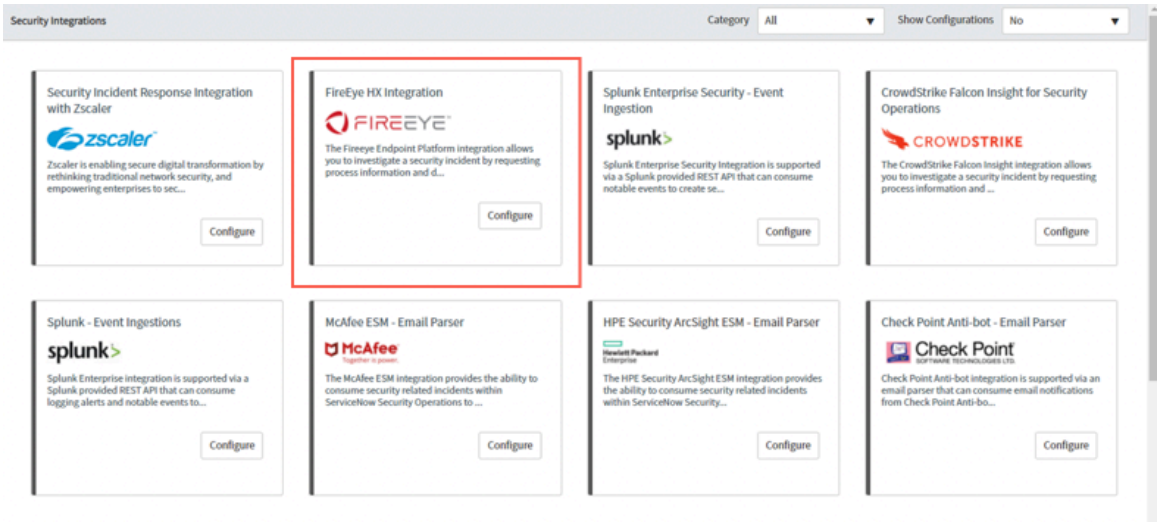
Depois de instalar a aplicação com sucesso, siga as etapas abaixo para configurá-la:

Procedimento

1. Navegar até **Integrações** > **Configurações de Integração**.
2. Selecione **Configurações de Integração** módulo para exibir as integrações disponíveis e localizar o **FireEye** bloco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



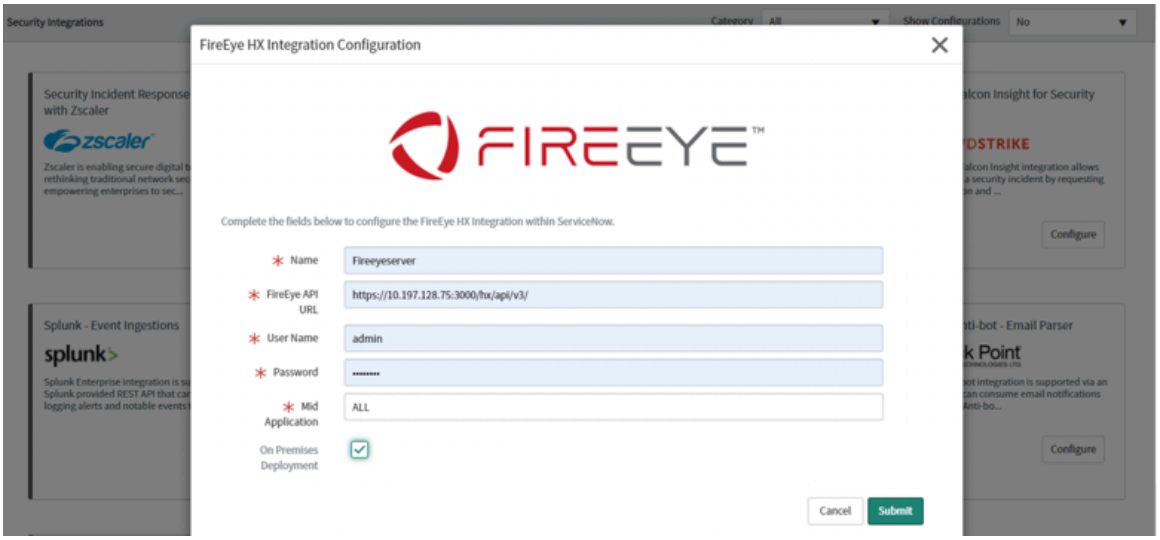
3. Clicar **Configurar** no bloco FireEye.

4. Forneça os seguintes detalhes para configurar a integração do FireEye:

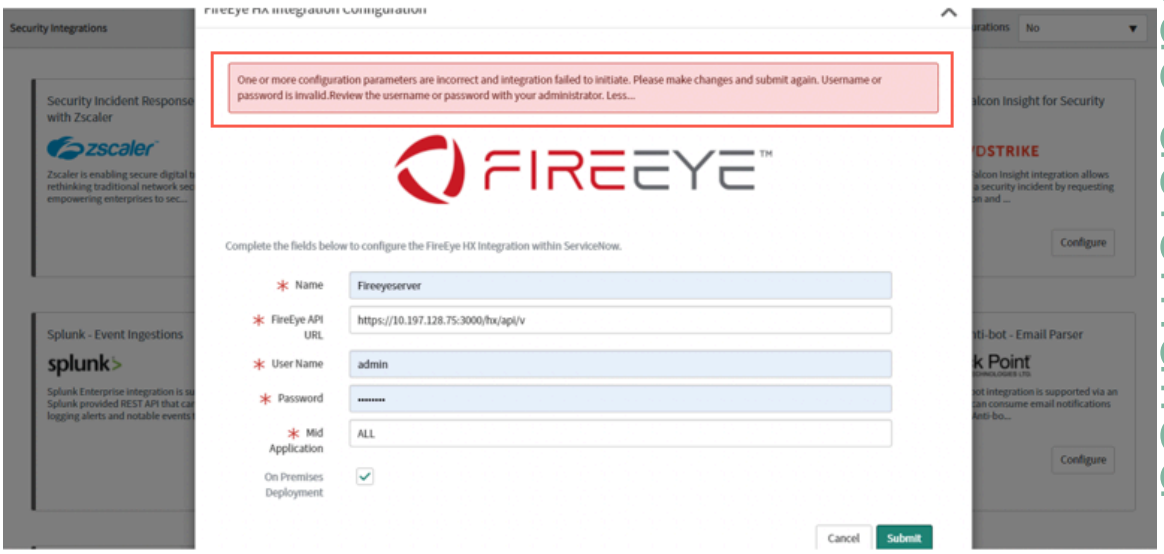
Campo	Descrição
Nome	Nome da configuração do FireEye. Este nome é usado para identificar a origem e as credenciais e configurações associadas. Esse nome ajuda a distinguir as credenciais e as contas e a identificar cada origem para evitar conflitos com perfis.
URL da API	URL base que hospeda a API FireEye.
Nome do usuário	Insira o nome de usuário da conta do FireEye.
Senha	Insira a senha da conta do FireEye.
Aplicação de MID	Aplicação de MID configurada em seu ambiente. O MID Server é necessário para processar arquivos zip para alguns dos recursos de enriquecimento. Por padrão, será TODOS. Os usuários devem fornecer um nome de aplicação válido manualmente.
Implantação no Local	O padrão é desabilitado. Se você estiver usando a versão baseada em nuvem do FireEye, verifique se a caixa de seleção está desmarcada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clicar **Enviar**.
   A lista Configurações do FireEye é exibida com o novo registro de configuração. Você concluiu a configuração de um servidor FireEye. Se você não puder se conectar ao FireEye ou suas credenciais estiverem incorretas, uma mensagem de erro de validação será exibida, conforme mostrado na figura a seguir. Verifique se suas credenciais estão corretas e tente novamente.



Tradução automática

Configurações padrão do FireEye

A seguir estão as definições de configuração adicionais após a conclusão da instalação.

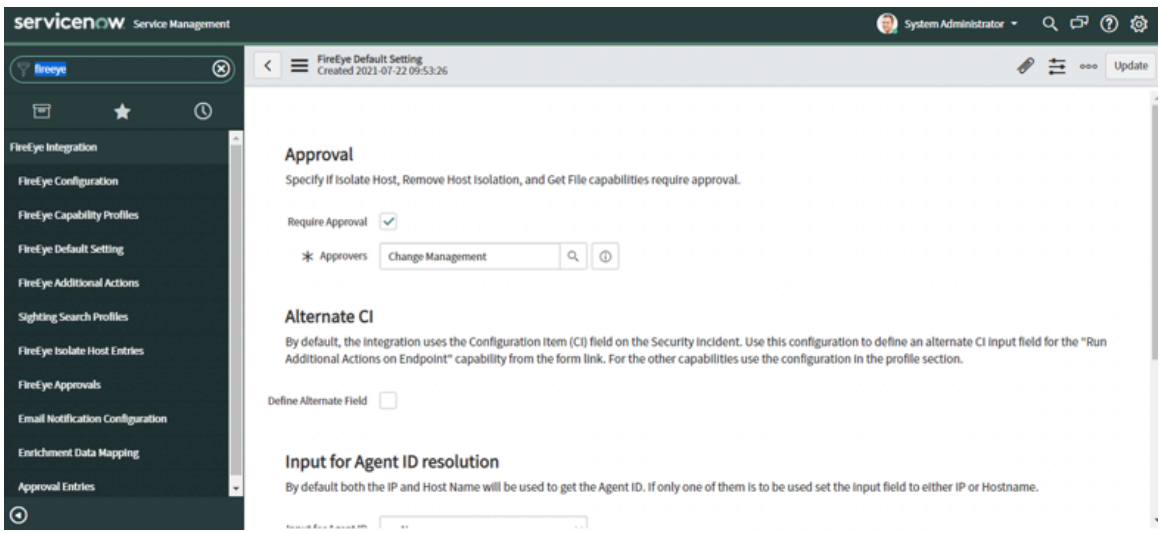
Depois de concluir a instalação, você encontrará o módulo Configurações padrão do FireEye na navegação à esquerda. Ele contém configurações padrão para diferentes funcionalidades do FireEye.

Configurações adicionais

A seguir estão as definições de configuração adicionais:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. **Aprovação**: Esta aprovação é especificamente para as capacidades Isolar host, Remover isolamento de host e Obter arquivo quando elas são acionadas diretamente da Lista relacionada e na ausência de perfis para elas. Se houver/(tiverem) perfis existentes para essas capacidades, a configuração de aprovação no perfil será respeitada.
   - **Requer aprovação:** Quando você habilita Requer aprovação, o campo Aprovadores fica disponível no formulário.
   - **Aprovadores**: Lista de grupos de aprovadores. Depois de enviar uma solicitação, é necessária a aprovação do grupo para concluir a solicitação.
2. **IC alternativo**: habilitar esta caixa de seleção fornecerá uma lista de campos disponíveis para passar um IC alternativo para a capacidade. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Esta configuração é aplicável somente para a capacidade "Executar ações adicionais no endpoint". Portanto, use esta configuração para definir um campo de entrada de IC alternativo somente para a capacidade "Executar ações adicionais no endpoint". Para as outras capacidades, use a configuração na seção de perfil. Se os perfis não definirem um IC alternativo, as capacidades selecionarão o campo de IC do formulário de Incidente de segurança.
3. **Entrada para resolução do ID do agente**: por padrão, o IP e o nome do host serão usados para obter o ID do agente. Se apenas um deles for usado, defina o campo de entrada como IP ou Nome do host.

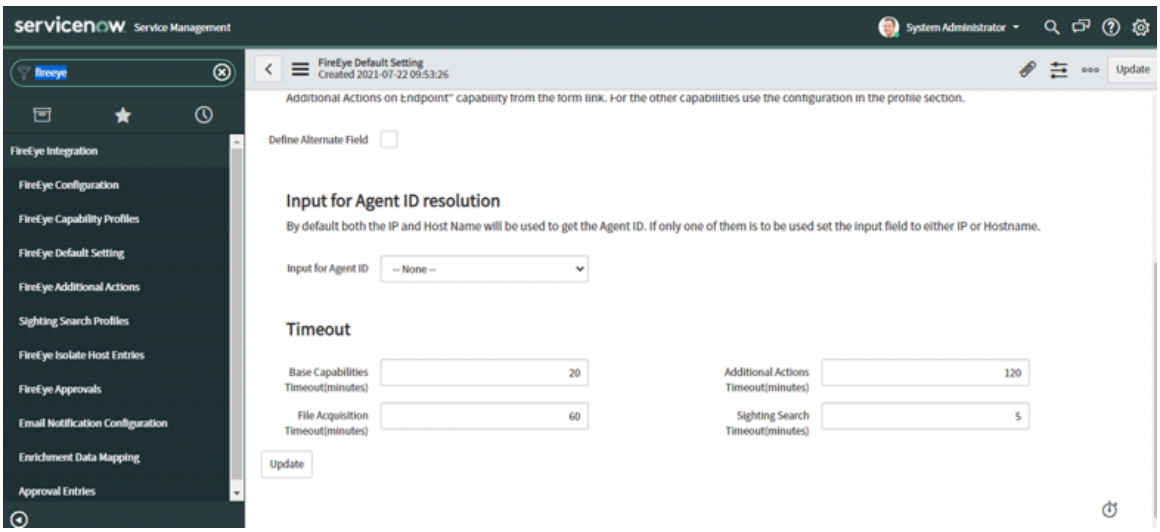


4. **Tempo limite**:
   - **Tempo limite das capacidades básicas (minutos):** As capacidades de Aprimoramento, Isolar Host e Remover Isolamento de Host falharão se nenhuma resposta for renderizada no tempo definido.
   - **Tempo limite de ação adicional (minutos):** A capacidade Executar ações adicionais no endpoint falhará se nenhuma resposta for renderizada no tempo definido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Tempo limite de aquisição de arquivo (minutos):** A capacidade Obter arquivo falhará se nenhuma resposta for renderizada no tempo definido.
- **Tempo limite da pesquisa de detecções (minutos):** A pesquisa será interrompida após o tempo definido.



Criar um novo perfil de capacidade para a integração do endpoint do FireEye

Crie um perfil e selecione os FireEye HX recursos que você deseja que o perfil execute.

Antes de Iniciar

Função necessária: administrador de incidentes de segurança do NowPlatform (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Os perfis são criados para agrupar capacidades e ajudariam os analistas a executar a investigação/correção com facilidade.

A seguir está a lista de capacidades que você pode adicionar ao(s) perfil(is):

1. Obter detalhes do host
2. Obter usuários conectados
3. Obter estatísticas de rede
4. Obter processos em execução
5. Obter serviços em execução
6. Obter arquivo
7. Isolar host
8. Remover isolamento

Você não pode agrupar as capacidades Obter arquivo, Isolar host e Remover isolamento de host com outras capacidades ao criar um perfil. Os perfis para eles devem ser criados individualmente. Por outro lado, Obter detalhes do sistema, Obter usuários conectados, Obter estatísticas de rede, Obter processos em execução e Obter serviços em execução podem ser combinados. Você pode criar perfis individualmente ou agrupando-os no todo ou em partes de acordo com sua necessidade. Depois que uma capacidade é incluída em um perfil, ela não pode ser incluída em outro perfil.

Para criar um novo perfil de capacidade, siga estas etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

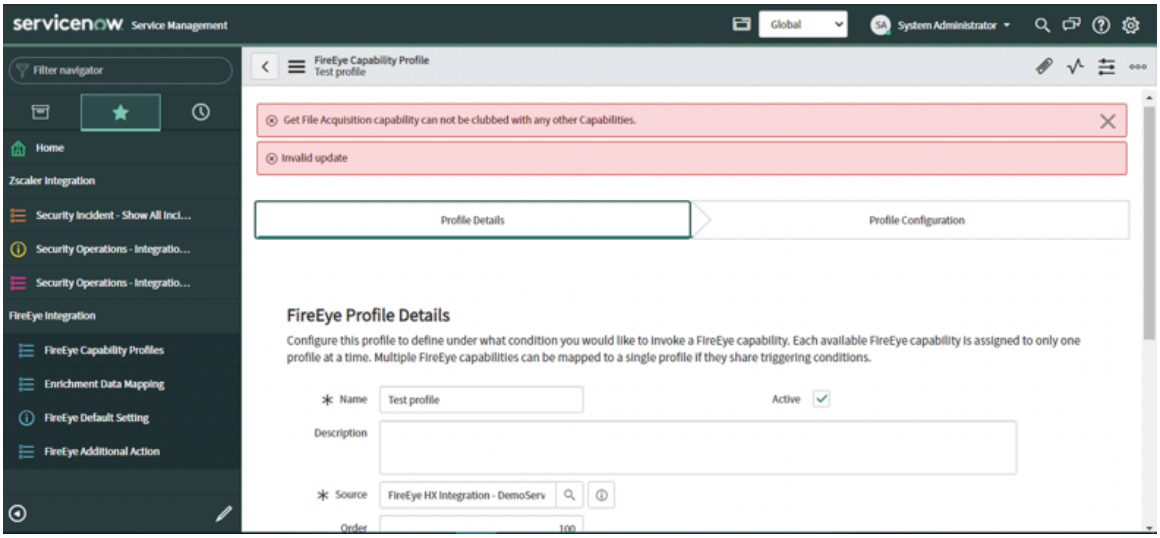
Procedimento

1. Navegar até **Integração do FireEye** > **Perfis de capacidade do FireEye**.
   A lista de perfis de capacidade é exibida.
2. Clicar **Novo**.
3. No formulário, preencha os campos.

Nome	Nome do perfil de capacidade FireEye HX. Este nome ajuda a identificar o tipo de perfil e descrevê-lo.
Descrição	Informações adicionais sobre o perfil que descrevem melhor o perfil.
Origem	Nome da origem FireEye HX. Somente origens configuradas estão disponíveis na lista de seleção.
Capacidades do FireEye HX.	Capacidades do perfil FireEye HX. Selecione os recursos desejados para este perfil na coluna Disponível e mova-os para a coluna Selecionado.
Ordem	Prioridade de fluxo. O padrão é 100. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	Isso indica que o perfil está ativo. Quando o perfil está ativo, ele é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem que você especificou na configuração.

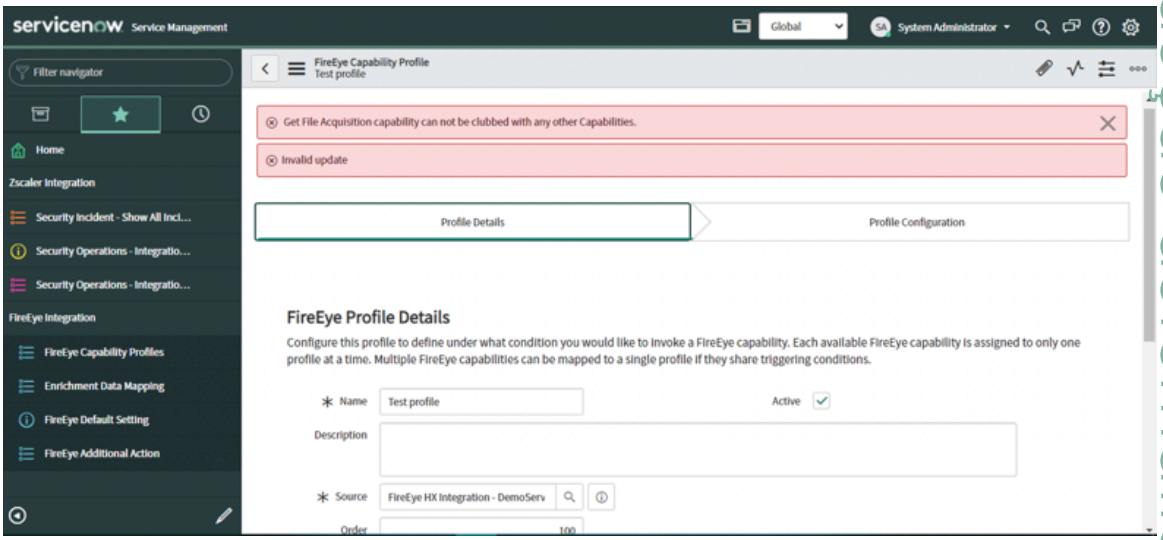
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A figura a seguir é um exemplo de um formulário preenchido para detalhes de perfil com a capacidade Obter detalhes do host.

4. Clicar **Avançar** para continuar para Configuração de perfil.



Nota: As capacidades Isolar host, Remover isolamento de host e Obter arquivo não podem ser combinadas com outras capacidades.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, talvez você prefira revisar os conceitos de configuração de perfis e condições de acionamento. Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração para um perfil.

Entenda como as condições do gatilho funcionam com um item de configuração

Depois de criar um perfil e selecionar os recursos do FireEye que você deseja que o perfil execute, defina as configurações do perfil para que ele seja executado somente quando um conjunto de condições específicas for atendido.

Você pode definir condições do gatilho para que o perfil seja executado automaticamente sempre que um incidente de segurança correspondente à condição do gatilho for criado. Se a condição do gatilho não estiver definida, esses perfis poderão ser executados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

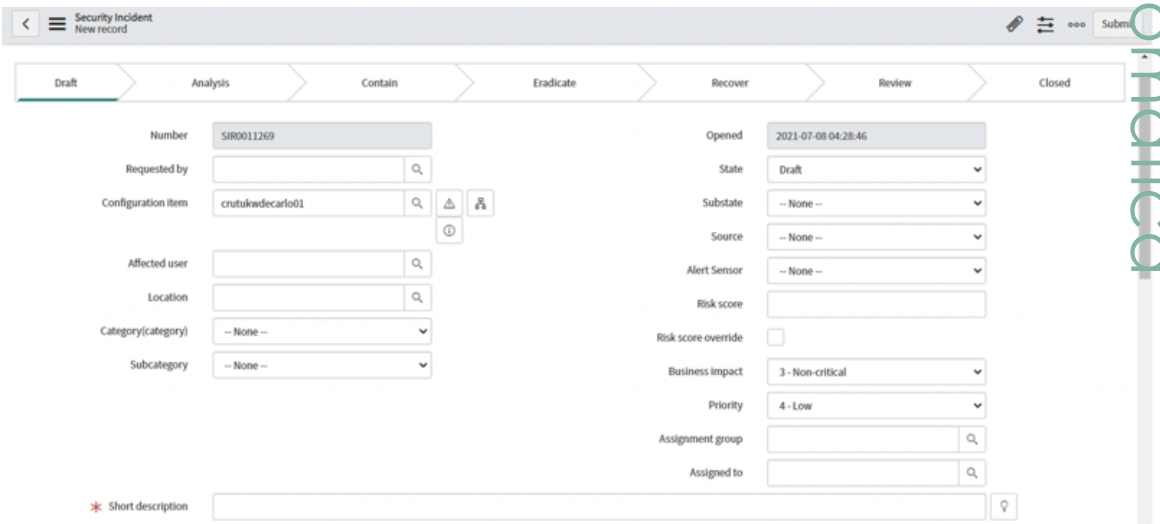
manualmente clicando no formulário "Executar perfil(is) de EDR" no incidente de segurança e selecionando o perfil.

Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos com as informações armazenadas no CMDB da Now Platform. Quando um incidente de segurança é criado e um perfil é executado automaticamente ou manualmente, o CMDB é pesquisado para recuperar o nome do host e/ou o endereço IP com base no valor do campo de IC. O nome do host e/ou o IP são usados para resolver o ID do agente em FireEye HX para identificar o endpoint.

Em um caso ideal, um valor correspondente é encontrado no banco de dados e os dados são coletados do console FireEye HX para o ativo correspondente. Os dados de várias capacidades são extraídos da sua instância da Now Platform e exibidos nas listas relacionadas de incidentes de segurança. Quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança que contenha o nome do host ou o IP a ser executado a resolução do ID do agente.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de IC alternativo para identificação de endpoint para garantir que você possa identificar o endpoint em FireEye HX. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como um backup, você garante que seus perfis sejam executados mesmo que o campo de IC não esteja preenchido no incidente de segurança associado após a criação do incidente.

Nota: Os campos de IC alternativo são considerados somente para capacidades que podem ser adicionadas a um perfil. Para todas as ações adicionais, o IC alternativo é selecionado na página de configurações padrão.



Configurar perfis e incidentes de segurança para a integração FireEye HX

Depois de criar um perfil e selecionar os FireEye HX recursos que você deseja que o perfil execute, defina as configurações para que o perfil possa ser invocado somente sob as condições definidas.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o perfil para que ele seja executado somente quando as condições especificadas forem atendidas. Selecione um campo de entrada alternativo para o campo Item de configuração (IC), se necessário, e defina as condições de filtragem para que o perfil possa ser acionado automaticamente quando um incidente de segurança que atender às condições do gatilho for criado.

Nota: Você pode navegar até o **Configuração de perfil** página somente depois de ter inserido o **Detalhes do perfil**.

Procedimento

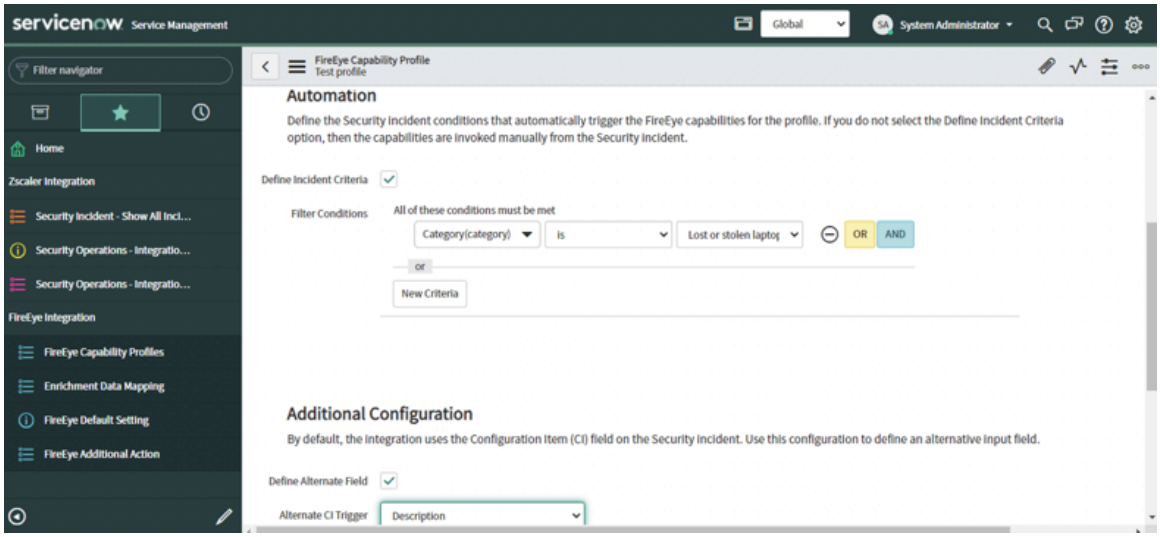
1. Navegar até **Integração do FireEye** > **Perfis de capacidade do FireEye**.
2. Clicar **Avançar** no **Detalhes do perfil** página depois de concluir a seção Detalhes do perfil.
3. Revise e configure as seguintes seções:
   - **Definir critérios de incidente (automação)**: defina as condições do incidente de segurança que acionariam automaticamente as capacidades FireEye HX do perfil. Se você não selecionar o **Definir critério de incidente** Se a opção, o perfil e as capacidades subjacentes poderão ser invocados manualmente a partir do incidente de segurança.
     - Selecionar **Definir critério de incidente** Opção para acionar automaticamente FireEye HX capacidades no perfil.
     - No **Condições do filtro**, selecione o campo obrigatório.
     - Você pode adicionar **Novos critérios** e também definem a condição OU ou E.

       Nota: Isolar host, Remover isolamento de host, Obter arquivo não podem ser acionados automaticamente.

   - **Configuração adicional**: quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança para consultar as FireEye HX APIs.
     - Selecione **Definir campo alternativo** Opção para definir um campo de entrada alternativo.
     - Selecione o campo de entrada em **Campo de gatilho de IC alternativo**.

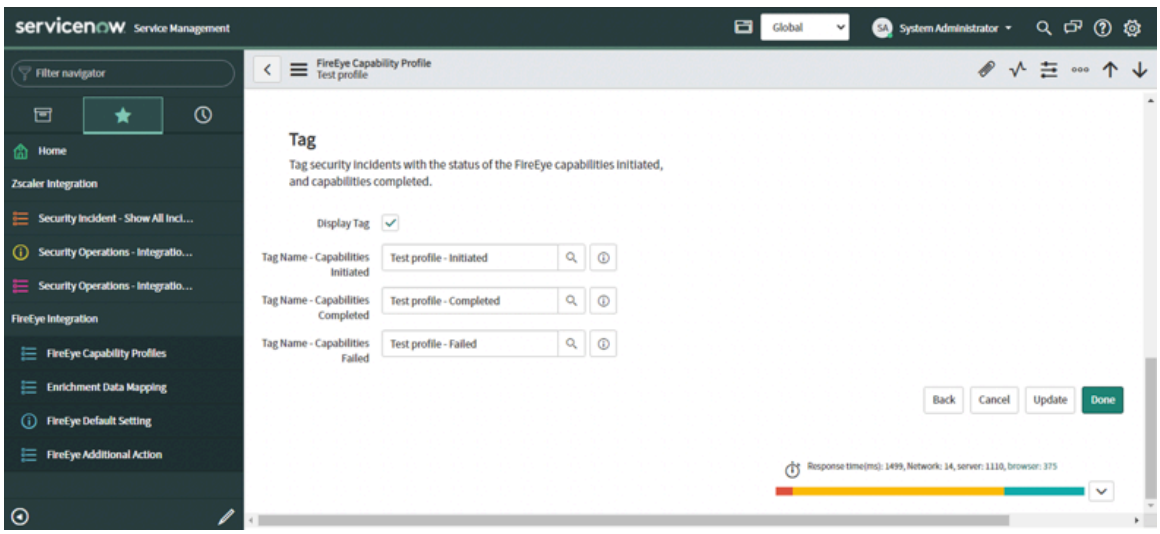
       Nota: Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



◦ **Marcadores**: opcionalmente, você pode marcar incidentes de segurança com os marcadores FireEye HX de perfil iniciado, perfil concluído e perfil com falha.

Selecione **Marcador de exibição** caixa de seleção para habilitar a marcação de incidentes de segurança, o nome do perfil é prefixado na habilitação do marcador. Por padrão, esta opção está desabilitada para todos os perfis.

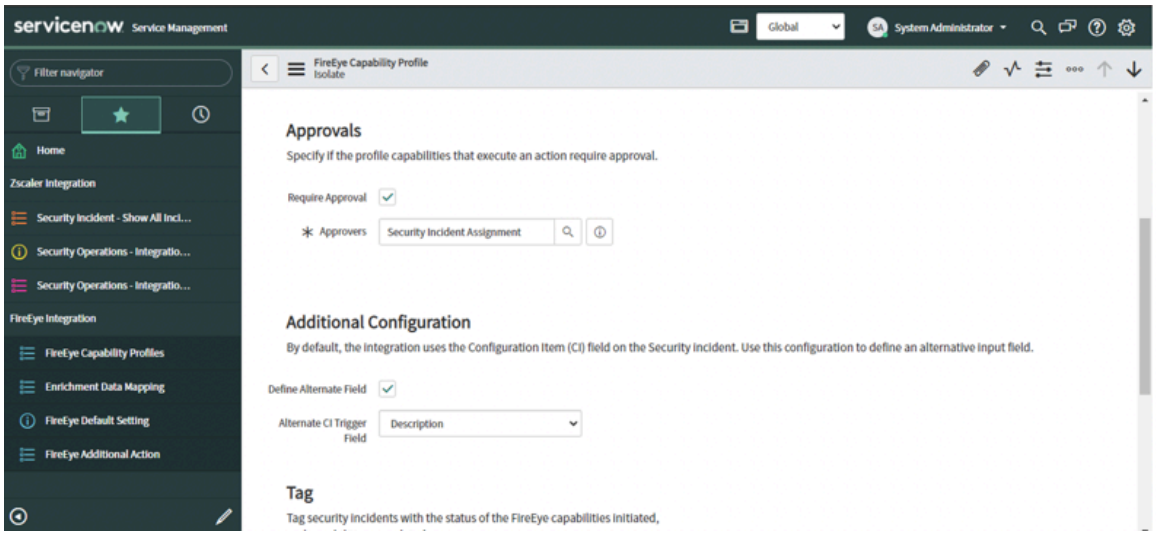


◦ **Aprovações**: selecione o **Requer Aprovação** caixa de seleção para fornecer um nível extra de controle ao usar os recursos FireEye HX para isolar máquinas host, restaurá-las na rede e obter os arquivos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A opção de aprovações na configuração do perfil aparece somente para as capacidades Isolar host, Remover isolamento de host e Obter arquivo.



4. Clique em **Concluído**.
5. Verifique FireEye HX condições do gatilho.

Verificar os filtros de condição do gatilho

Teste o perfil e verifique se os filtros de condição do gatilho que você configurou estão funcionando conforme o esperado.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

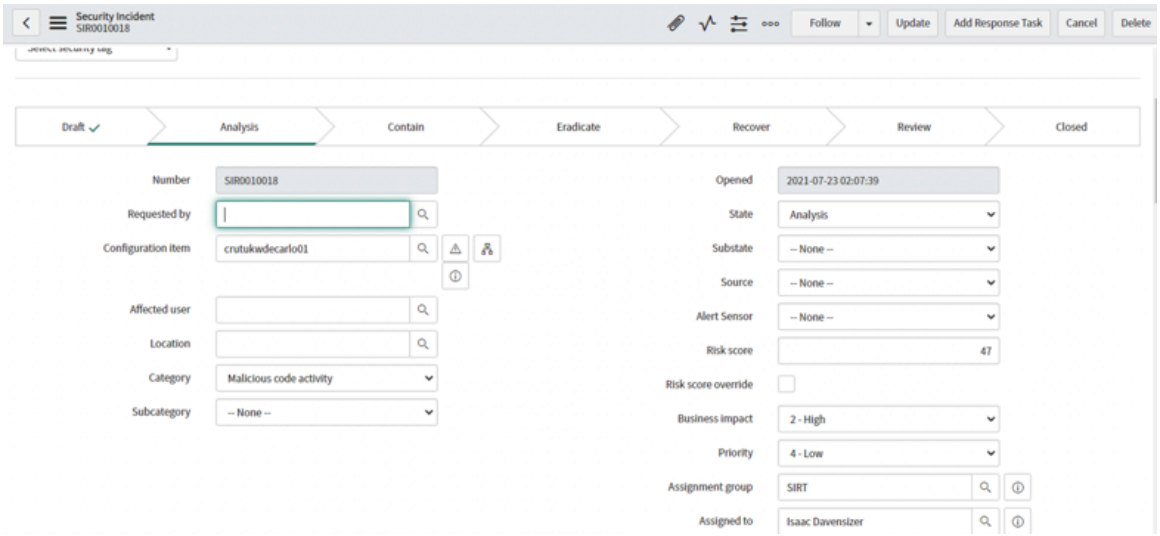
Depois de ativar o perfil, com base nas condições de gatilho configuradas, você pode exibir os resultados da consulta nos incidentes de segurança da Now Platform.

Procedimento

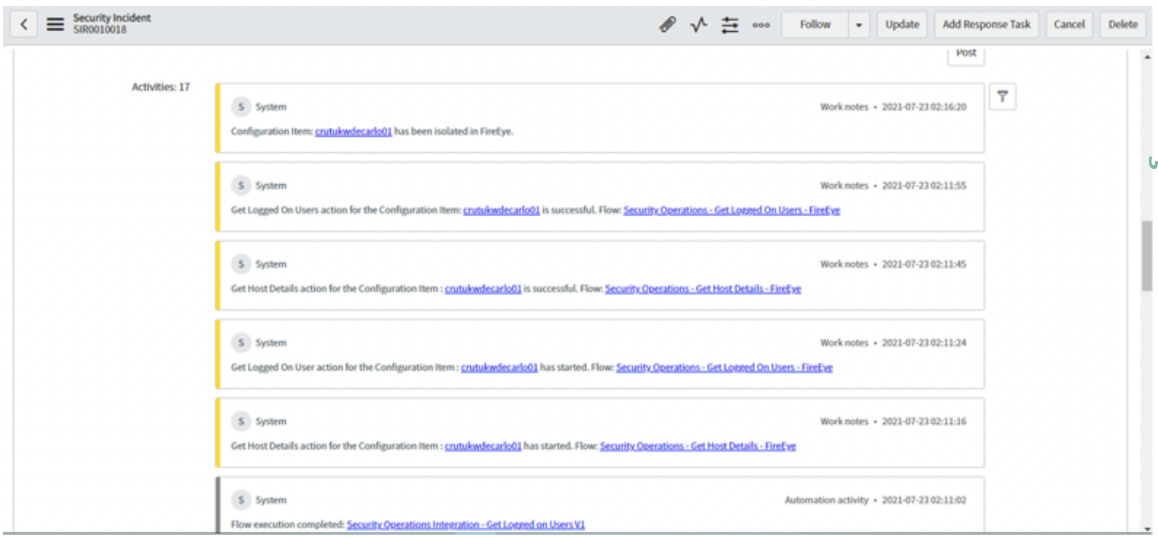
1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecionar **Novo** para criar um novo incidente de segurança.
3. Forneça as condições de filtro conforme fornecidas no perfil de capacidade para acionar o respectivo perfil.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clicar **Salvar**.



5. Revise as anotações de trabalho e a seção de atividades.

6. Exiba os marcadores de perfil iniciado, perfil concluído ou perfil com falha.

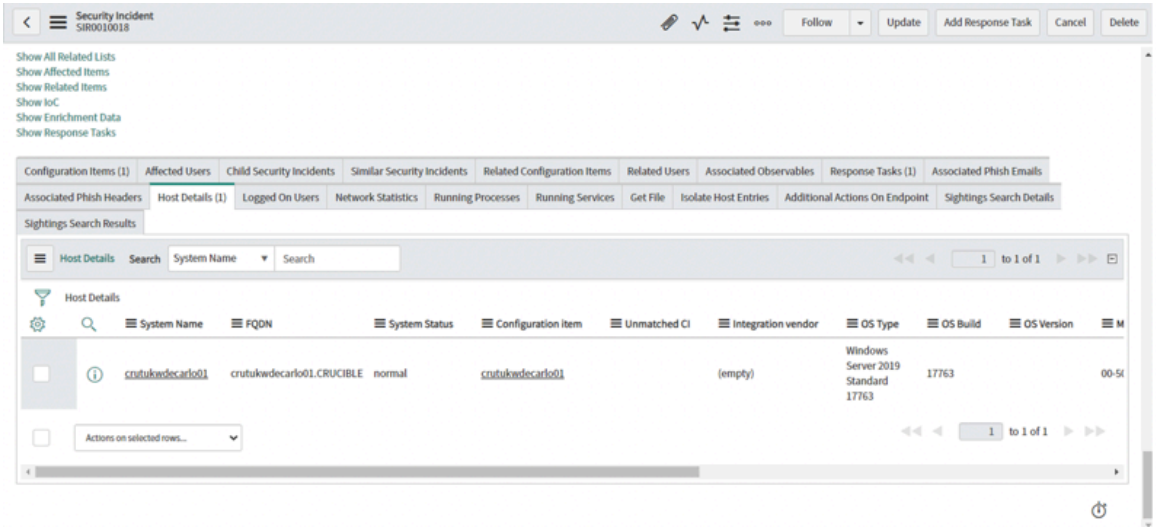
7. Clicar **Mostrar todas as listas relacionadas**.

8. Clique em qualquer lista relacionada (guia).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, Detalhes do host.



Acionar um perfil de capacidade do FireEye em Links relacionados

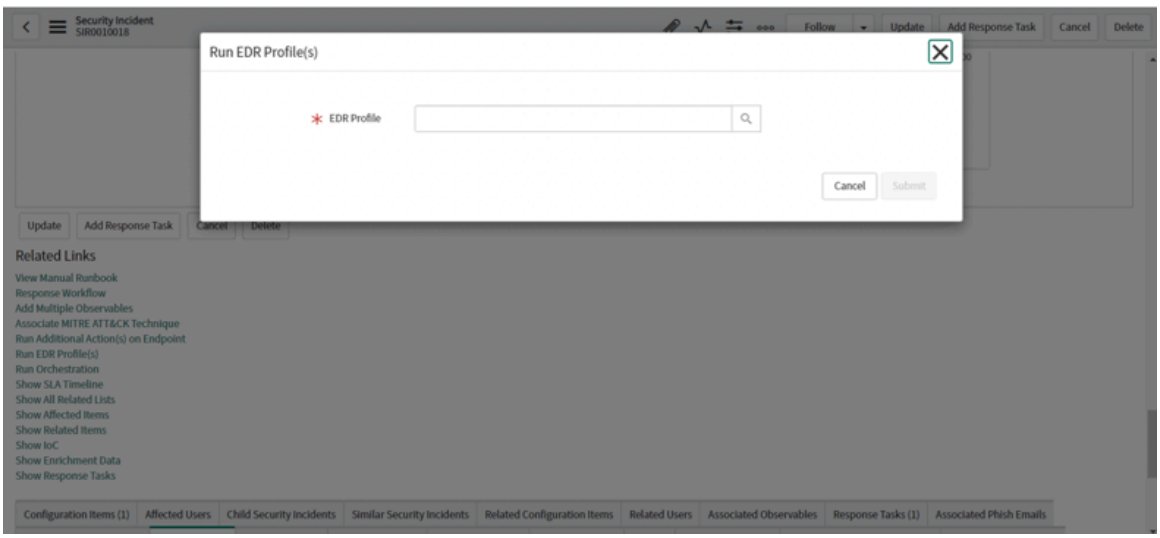
Acione um perfil de capacidade manualmente após revisar um incidente de segurança de links relacionados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

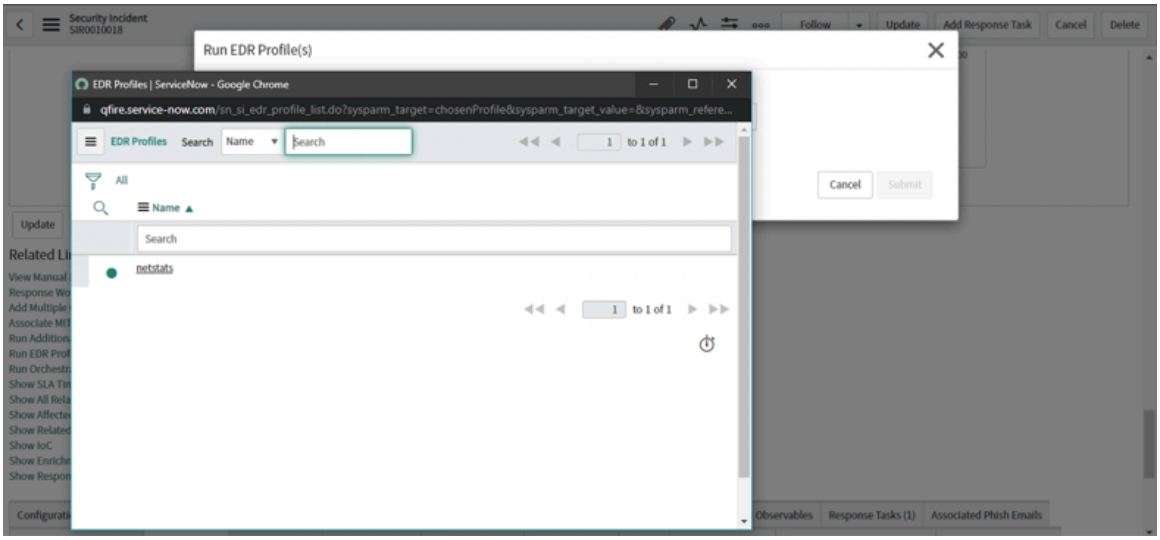
1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar.
3. Clicar **Executar perfis de EDR**na seção de links relacionados.

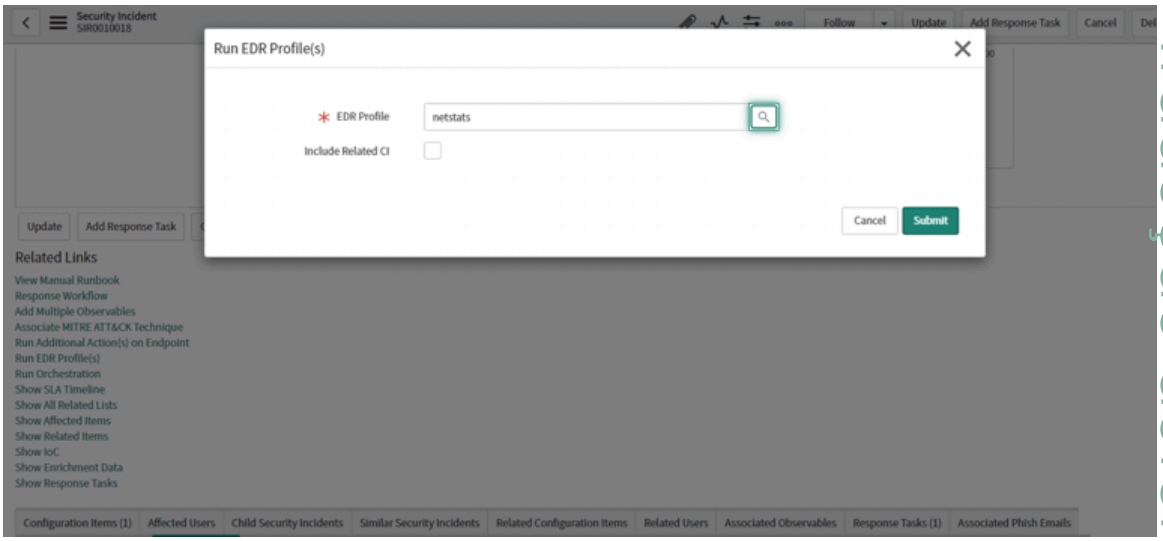


4. Navegue e selecione um perfil na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tradução automática

5. O perfil selecionado é acionado manualmente.
6. Revise as anotações de trabalho e a seção de atividades.
7. Exiba os marcadores e verifique as listas relacionadas aos dados.

Nota: Além de executar o perfil do IC ou do IC alternativo do incidente de segurança, você também pode executar o perfil dos valores de IC presentes na lista relacionada Item de configuração marcando a caixa de diálogo Incluir IC relacionado. Isso também buscará dados para os valores de IC presentes na lista relacionada. Como alternativa, você pode executar o perfil apenas para os valores de IC presentes na lista relacionada.

Acionar um perfil de capacidade do FireEye a partir da lista relacionada de item de configuração

Acione um perfil de capacidade manualmente na lista relacionada de itens de configuração.

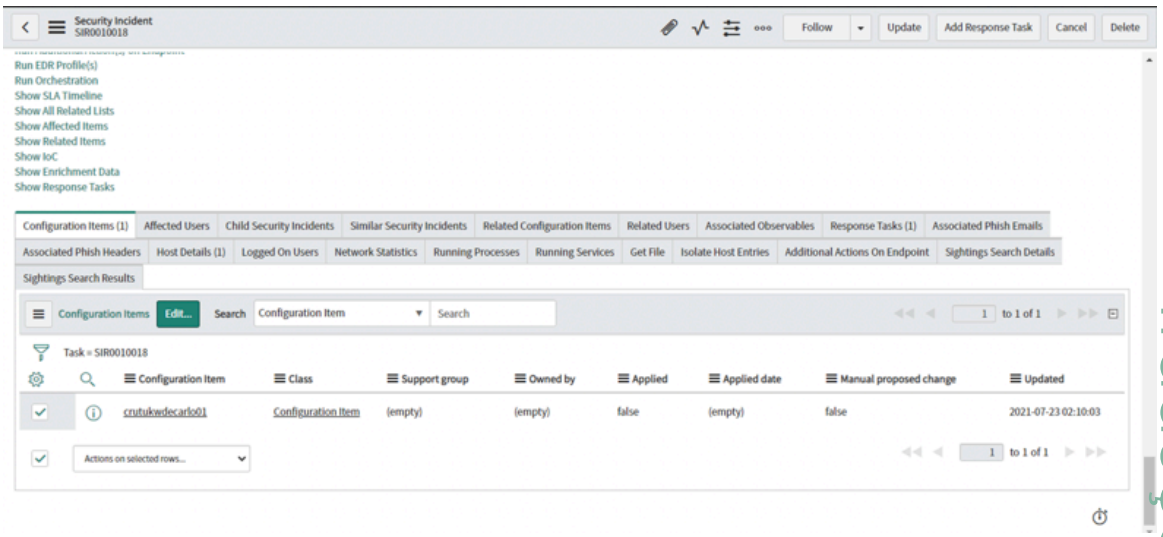
Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

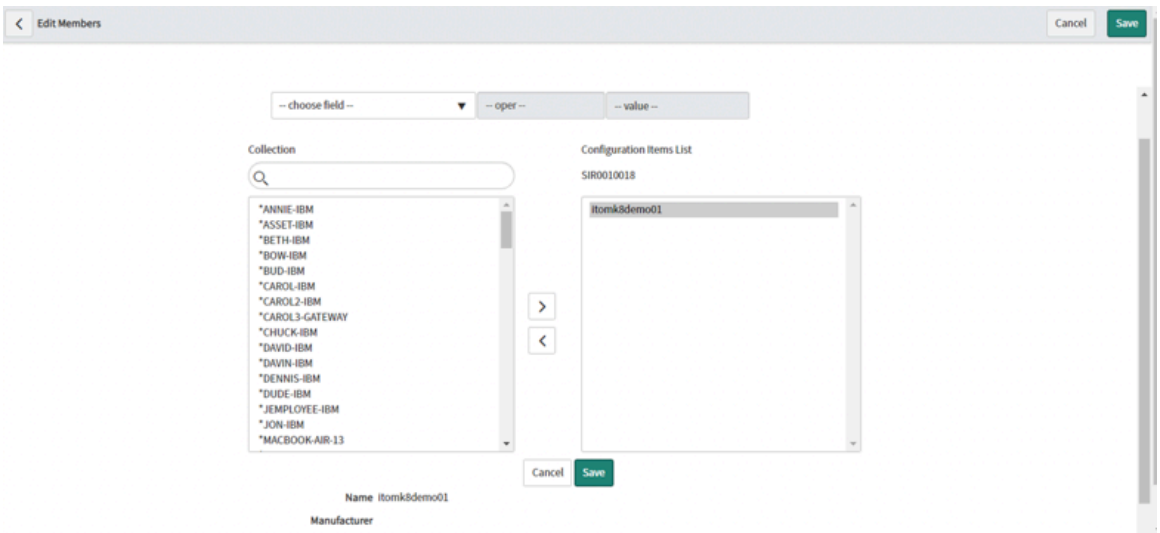
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações FireEye HX.
3. Clicar **Mostrar todas as listas relacionadas** na seção de listas relacionadas.
4. Clique no botão **Item de Configuração** lista relacionada.



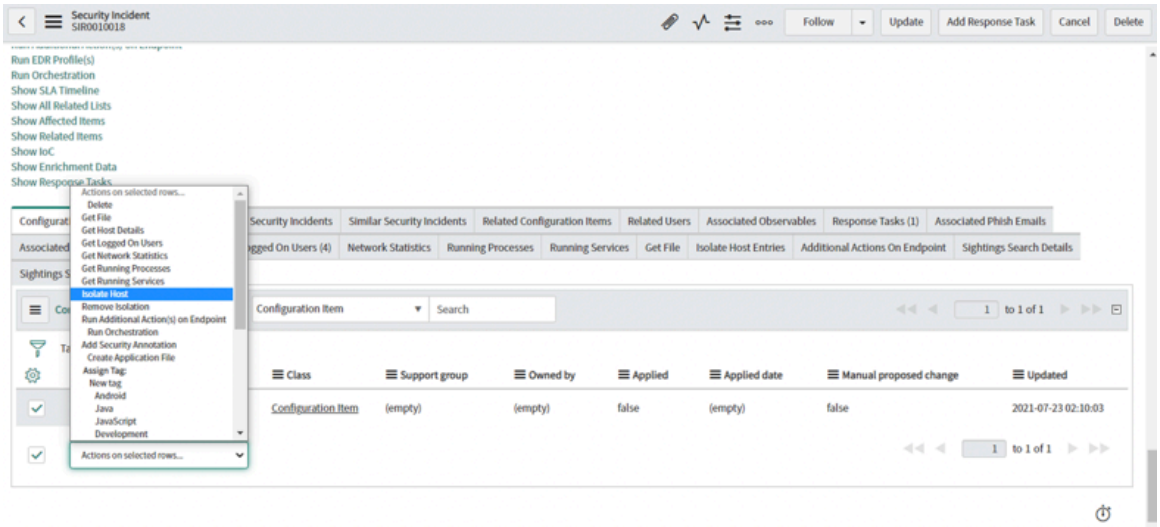
5. Clicar **Editar** para adicionar os itens de configuração disponíveis, se os valores ainda não estiverem presentes, e clique em **Salvar**.



6. Selecione o(s) item(ns) de configuração adicionado(s) e, nas linhas Ações nas linhas selecionadas, selecione uma capacidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. A capacidade selecionada é acionada manualmente.

8. Revise as anotações de trabalho e a seção de atividades.

9. Exiba os marcadores e verifique os dados nas listas relacionadas.

Capacidade de obter arquivo do FireEye

As solicitações de aquisição de arquivo instruem um Endpoint Security Agent a obter um arquivo do endpoint do host. As aquisições de arquivos são usadas para análise estática ou dinâmica de comprometimentos potenciais ou verificados, bem como para retenção de evidências durante investigações de ameaças internas. A capacidade Obter arquivo deve ser criada como um perfil separado.

Antes de Iniciar

Função necessária: administrador

Acionando Obter perfil de arquivo e criar um perfil de capacidade FireEye HX com **Obter arquivo** capacidade.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.

2. Selecione o incidente de segurança que você deseja revisar.

3. Clicar **Executar perfis de EDR**na seção de links relacionados.

4. Navegue e selecione Obter perfil de arquivo na lista de perfis disponíveis.

5. Forneça o **Nome do arquivo** e **Caminho do arquivo**.

> **Nota:** Insira o nome do arquivo para o qual você deseja adquirir. Especifique um nome de caminho preciso ou outra variável de ambiente do Windows baseada em caminho apropriada. Você deve especificar a letra da unidade ou os nomes do caminho. Endpoints diferentes podem ter mapeamentos de unidade diferentes. Se você especificar explicitamente um nome de pasta, poderá terminar o caminho com uma barra invertida. No entanto, a barra invertida final não é obrigatória.

6. Clicar **Enviar**.

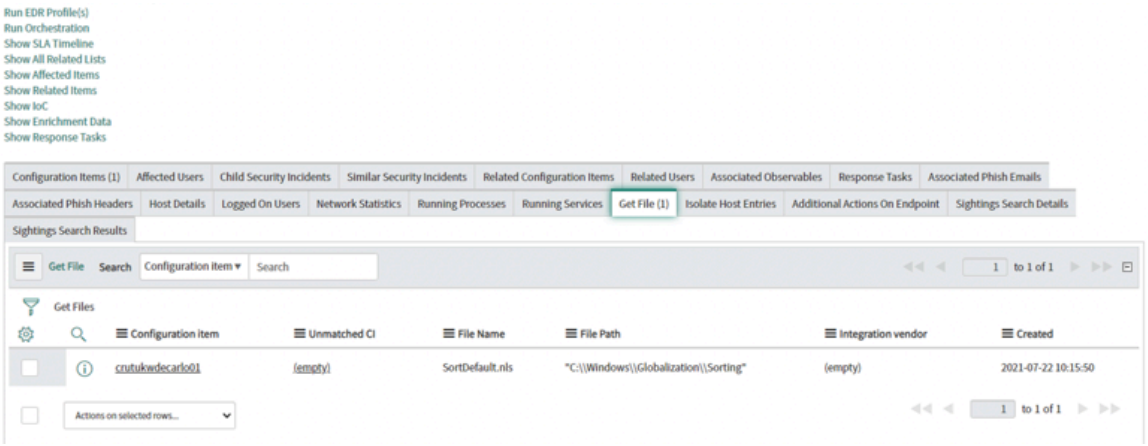
7. Revise as anotações de trabalho e a seção de atividades.

8. Exibir os marcadores e verificar os resultados no **Obter arquivo** lista relacionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O perfil Obter arquivo agora é acionado manualmente.



Para revisar uma aquisição de arquivo baixada:

- Abra o arquivo .zip de aquisição de arquivo.
- Insira a senha necessária para abrir o arquivo. Para exibir a senha, passe o mouse sobre o link de download no Console FireEye HX. Siga as etapas abaixo para exibir a senha:
  - Faça login no console do FireEye HX.
  - Navegar até **Aquisições** e filtrar por Tipo de aquisição – Arquivo.
  - Selecione o registro desejado.

    Nota: Você poderá ver os detalhes do arquivo adquirido na guia à direita.

  - Passe o mouse sobre **Baixar** link disponível na parte superior para obter a senha.

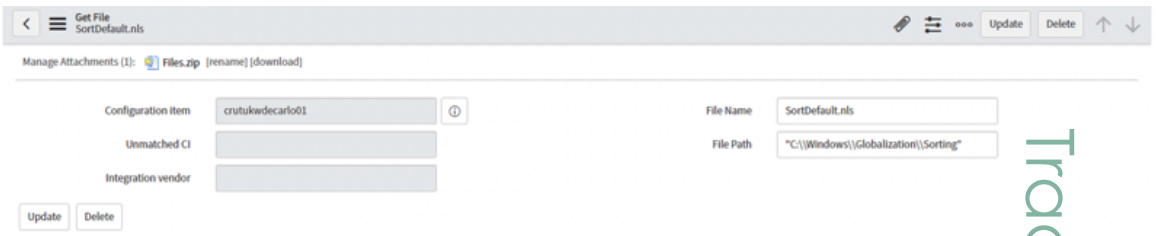
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

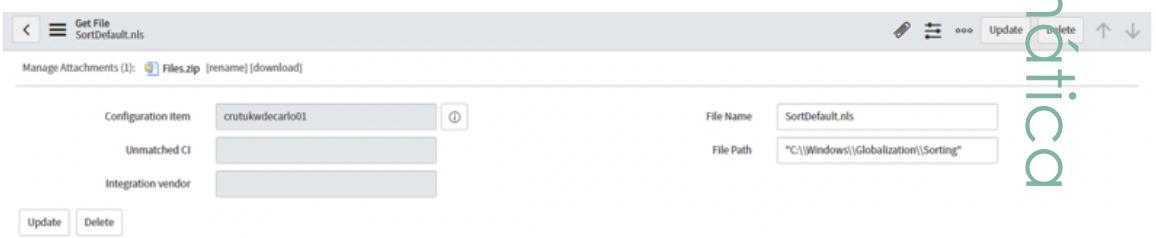
- Abra e revise os arquivos dentro do arquivo .zip usando qualquer editor de texto ou XML.

Nota:

- É recomendável que o arquivo recuperado seja adicionado como um observável manualmente, para que possa ser rastreado como uma evidência contra o incidente de segurança. Isso também ajudará a exibir os arquivos no futuro, quando a senha for esquecida ou alterada.
- O tamanho máximo de arquivo compatível com a ação Obter arquivo é de 1024 MB e este valor pode ser configurado alterando **com.glide.attachment.max_size**, e o tempo limite padrão é de 60 minutos, que pode ser configurado na página FireEye HX Configurações padrão.



- Obter arquivo também pode ser acionado a partir da lista relacionada de itens de configuração.



Tradução automática

Ações adicionais do FireEye no endpoint

A integração do FireEye oferece suporte à execução de ações adicionais além das ações padrão ouro.

Essas ações são compostas por Aquisição de triagem e Aquisições de dados. Duas aquisições de dados prontas para uso são compatíveis:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Script de detalhes investigativos abrangentes
- Script de detalhes investigativos padrão

Além disso, a aquisição por triagem também é compatível com o pronto para uso. Todos esses três são criados por padrão junto com a origem. Os clientes também podem criar suas próprias ações, ou seja, aquisições de dados do módulo de ações adicionais do FireEye.[1] O tamanho máximo de arquivo compatível com as ações adicionais do FireEye é 1024 e esse valor pode ser configurado alterando **com.glide.attachment.max_size**, e o tempo limite padrão é de 120 minutos, que pode ser configurado na página de configuração padrão do FireEye.

Script de detalhes investigativos abrangentes

Permite a coleta de todos os artefatos forenses e investigativos do endpoint, mas é a opção mais cara. Essa configuração é ideal para situações em que haverá apenas uma janela para coletar dados do endpoint em questão e a capacidade de adquirir mais dados não pode ser garantida posteriormente. Portanto, use esta ação com cuidado.

Script de detalhes investigativos padrão

Habilita as opções mais comuns para coletar artefatos forenses e investigativos de um endpoint. Deve ser a ferramenta de resposta primária quando você suspeita que um endpoint pode estar comprometido e precisa executar uma análise profunda desse endpoint. Tem como objetivo encontrar um equilíbrio entre a coleta dos dados mais relevantes e valiosos e, ao mesmo tempo, evitar as opções caras que podem ser coletadas posteriormente, quando uma investigação mais aprofundada for necessária.

Aquisição de triagem

As coleções de triagem contêm informações de dentro do cache de lookback, bem como informações adicionais de auditoria forense, como histórico de download de URL, histórico de download de arquivo, listagens de processos e portas e informações do sistema padrão. Você pode querer examinar essas informações quando o tráfego de rede anômalo for detectado e quiser mais visibilidade sobre as ações do endpoint.

Manutenção de scripts de aquisição de dados no FireEye

As solicitações de aquisição de dados (às vezes chamadas de solicitações de resposta em tempo real) permitem que você adquira todos os dados necessários de um único endpoint em execução. Usando a página Scripts de aquisição de dados no FireEye, você pode criar, editar, copiar e excluir os scripts de aquisição de dados usados para solicitações de aquisição de dados.

Como acessar a página de scripts de aquisição de dados no FireEye

Para acessar a página Scripts de aquisição de dados:

1. Navegue até Endpoint Security interface do usuário da web.
2. Selecione Scripts de aquisição de dados no menu do administrador.

Como criar um script no FireEye

Para criar um script de aquisição de dados:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecionar **Scripts de aquisição de dados** > **Administrador** menu da interface do usuário da Web do Endpoint Security.
2. Clicar **Criar script**.
3. Insira um nome para o novo script no **Nome do script** campo.
4. Opcionalmente, insira uma descrição do script.
5. Selecione o sistema operacional ao qual o script se aplica. Você só pode selecionar um único sistema operacional na caixa de diálogo Criar script.
6. Clicar **Criar** para iniciar a definição do script.
7. Selecione um tipo de dados de aquisição no **Adicionar um tipo de aquisição**caixa suspensa e clique em **Adicionar**. As opções para o tipo de aquisição solicitado aparecem à direita da lista de scripts.
8. Forneça valores para as opções de tipo de aquisição ou use os valores padrão que já estão selecionados. A IU da Web não avisa ou remove tabulações, espaços ou caracteres indesejados (como \n) em suas especificações.
9. Repita as duas etapas anteriores para solicitar dados adicionais para o script de aquisição de dados. Alguns tipos de dados de aquisição estão disponíveis apenas uma vez para um script, enquanto outros podem ser especificados mais de uma vez. Depois de adicionar um tipo de aquisição a um script, a lista de tipos de aquisição disponíveis no **Adicionar um tipo de aquisição**A caixa suspensa se ajusta corretamente.
10. Para remover um tipo de dados de aquisição do script, clique no ícone x ( ) na guia de aquisição no lado esquerdo da página.

Nota: Esta integração não é compatível com **Permitir edições antes de adquirir** ao criar scripts. Portanto, certifique-se de que a caixa de seleção esteja desmarcada.

Exportando um script do FireEye

Você pode exportar um script de aquisição de dados para um arquivo JSON. Para exportar um script de aquisição de dados:

1. Selecionar **Scripts de aquisição de dados** > **Administrador** da interface do usuário da Web do Endpoint Security.
2. Selecione Scripts de aquisição de dados no menu do administrador.
3. Selecione o script que você deseja exportar no lado esquerdo da página.
4. selecionar **Ações** > **Exportar script**.
5. Um arquivo JSON é baixado para o seu computador. O nome do arquivo JSON inclui o sistema operacional para que você possa determinar facilmente quais scripts são para qual sistema operacional.

Como criar uma nova ação de aquisição de dados na Now Platform

Para criar uma nova ação, siga estas etapas:

1. Navegar até **Integração do FireEye** > **Ações adicionais do FireEye**. A lista Ações adicionais do FireEye é exibida.
2. Clicar **Novo**. O formulário da nova ação é exibido.
3. Preencha o formulário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Nome da ação do FireEye que é executada. Este nome ajuda a identificar o tipo de ação e descrevê-lo.
Aquisição	Uma aquisição obtém os dados a serem analisados. Este é um campo somente leitura e o padrão é Aquisição de dados.
Origem	Nome da origem do FireEye. Somente origens configuradas estão disponíveis na lista de seleção.
Capacidade	Este é um campo somente leitura e está preenchido com a capacidade Executar ação(ões) adicional(is)
Tipo de aquisição	Tipo de ação de aquisição que precisa ser obtido e analisado.
Ativo	Isso indica que a Ação está ativa.
Requer Aprovação	Quando você habilita a opção Requer aprovação, o campo Aprovadores fica disponível no formulário. Depois de enviar uma solicitação, é necessária a aprovação do grupo para concluir a solicitação.
Marcador de exibição	Tipo de sistema operacional, como Windows, Mac e Linux, para adicionar scripts. **Nota:** Somente um tipo de SO é compatível no momento. Você pode criar uma ação por sistema operacional. Para outros sistemas operacionais, crie novas ações conforme necessário.
Scripts	O script importado do FireEye precisa ser fornecido para o tipo de SO selecionado. Somente um script pode ser adicionado a cada tipo de SO.

4. Clicar **Enviar**.

Como acionar aquisições de dados a partir do incidente de segurança

As ações adicionais criadas podem ser executadas por meio do link relacionado chamado **Executar ações adicionais no endpoint** sobre o incidente de segurança.

Nota: **Permitir edições antes de adquirir** A funcionalidade FireEye não é compatível com as Ações adicionais no endpoint.

Criar e configurar um perfil para pesquisa de detecções com a integração do FireEye

Configure o perfil de pesquisa de detecções usando o procedimento a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador de incidentes de segurança do NowPlatform (sn_si.admin)

Sempre que uma origem for criada, as configurações de pesquisa de detecções individuais para cinco tipos (Arquivo, IPs (v4), MD5, SHA1 e SHA256) serão criadas e inativas por padrão. Você deve torná-lo ativo antes de usar a Pesquisa de detecções. Cada tipo de observável tem uma consulta de pesquisa diferente para recuperar detecções. Estaríamos iniciando uma pesquisa diferente para cada tipo de observável. A pesquisa de vários observáveis para uma pesquisa de detecções não é possível no FireEye, pois isso executaria uma operação E nos observáveis, e o resultado poderia ser impreciso.

Nota: Para a pesquisa de detecções, somente cinco pesquisas ativas podem estar presentes de uma só vez. O restante será enfileirado e começará após a conclusão de qualquer uma das detecções em andamento.

Se você quiser criar um novo perfil de pesquisa de detecções, siga as etapas abaixo para criar um:

Procedimento

1. Navegar até **Integrações** > **Configuração da Pesquisa de detecções**.
2. Clicar **Novo**.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do perfil de capacidade.
Pesquisa salva	Isso executará uma pesquisa salva, ou seja, o campo de Nome deve corresponder ao nome da pesquisa salva.
Origem da pesquisa de detecções	Define a origem configurada para a integração.
Pesquisar	Adicione uma cadeia de caracteres de pesquisa nativa para formar uma consulta.
Ativo	A consulta será executada somente se estiver ativa.
Tipo de observável	Define o tipo de categoria de observável.
Máximo de observáveis por pesquisa	O número de observáveis antes da consulta de pesquisa é dividido em várias consultas. Defina este valor como 1 para esta integração.
Parâmetros de pesquisa de detecções	Use os parâmetros de pesquisa de detecções para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado.

4. Clicar **Enviar** para concluir a configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Invocar pesquisa de detecções a partir de um incidente de segurança

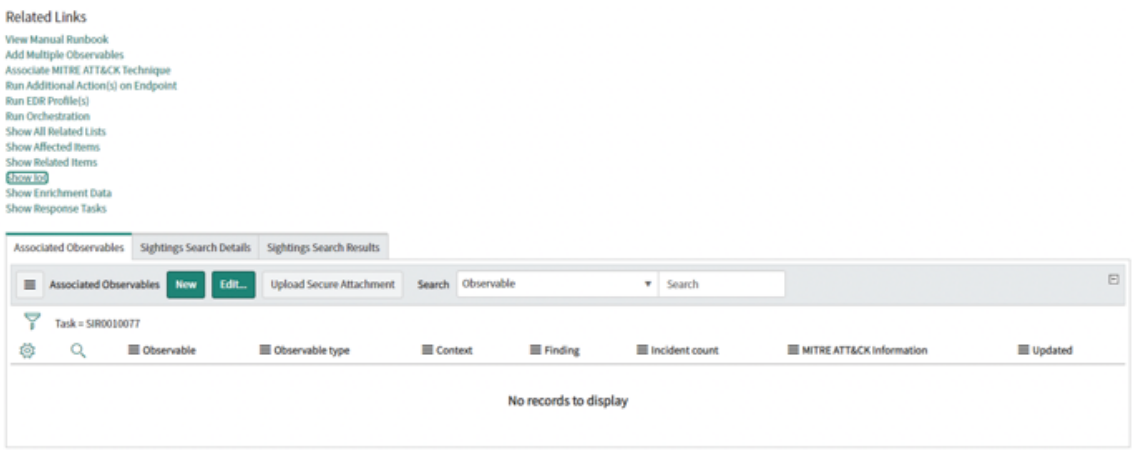
Invoque a pesquisa de detecções de um incidente de segurança SIR seguindo o procedimento abaixo.

Antes de Iniciar

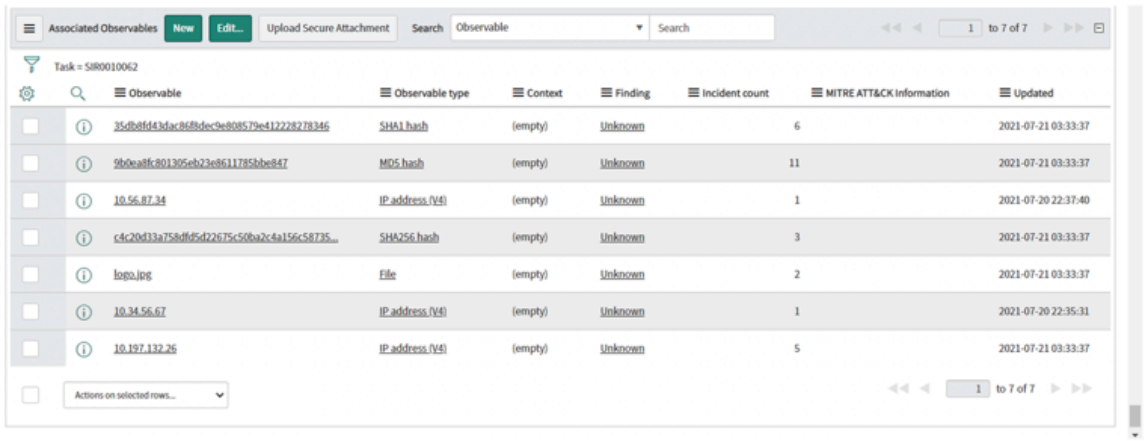
Função necessária: administrador da Now Platform (sn_si.admin)

Procedimento

1. Navegue até Incidentes de segurança.
2. Abra qualquer SIR existente ou crie um novo SIR.
3. Clique em Mostrar IoC em Links relacionados.
4. Clicar **Observáveis Associados** listas relacionadas.



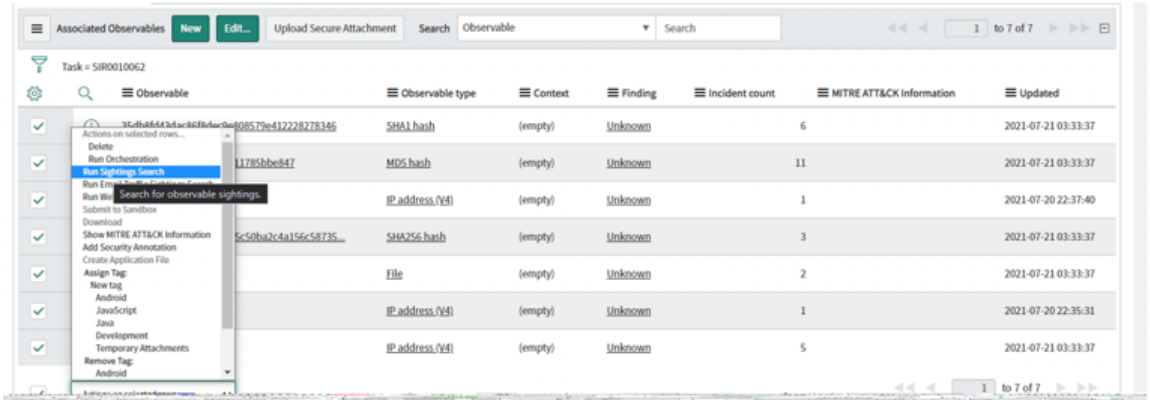
5. Adicione observáveis existentes ou crie um novo observável.



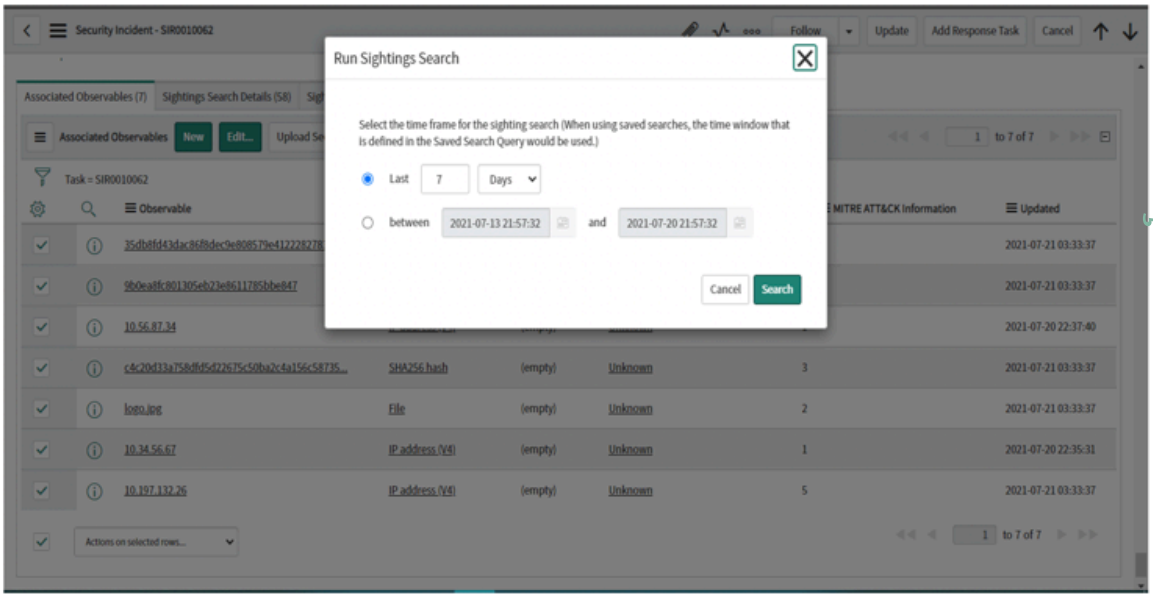
6. Selecione os observáveis e, em Ações nas linhas selecionadas, clique em **Executar Pesquisa de detecções**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



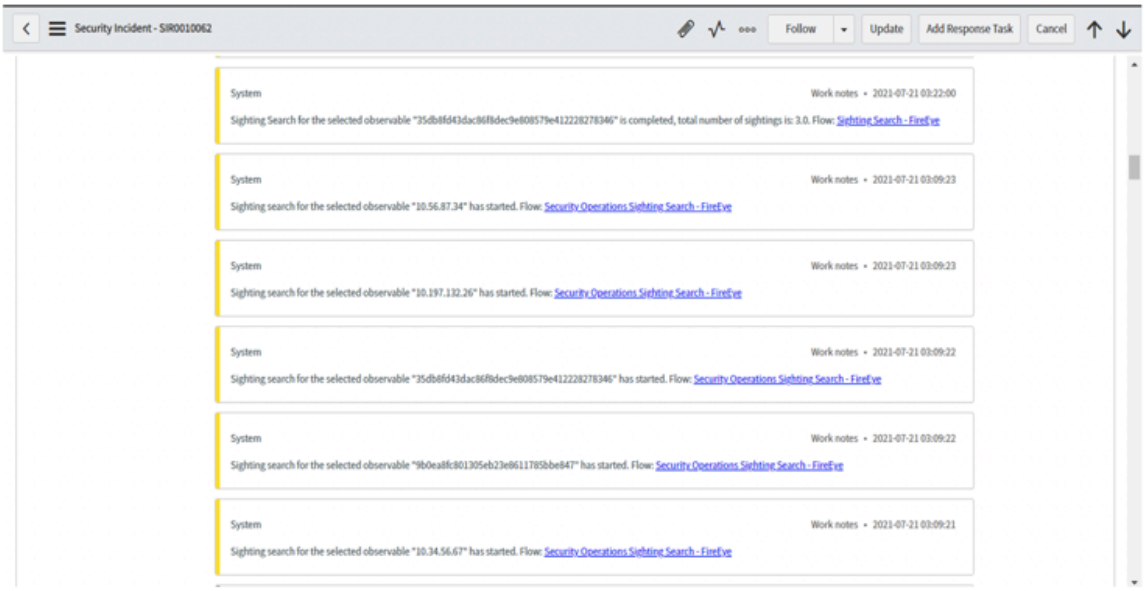
7. Ignore as entradas na próxima caixa de diálogo que solicita dados de tempo. Há valores padrão preenchidos. No entanto, a pesquisa é realizada em tempo real e os valores de tempo são ignorados para esta integração.



8. Verifique o status das anotações de trabalho.

Tradução automática

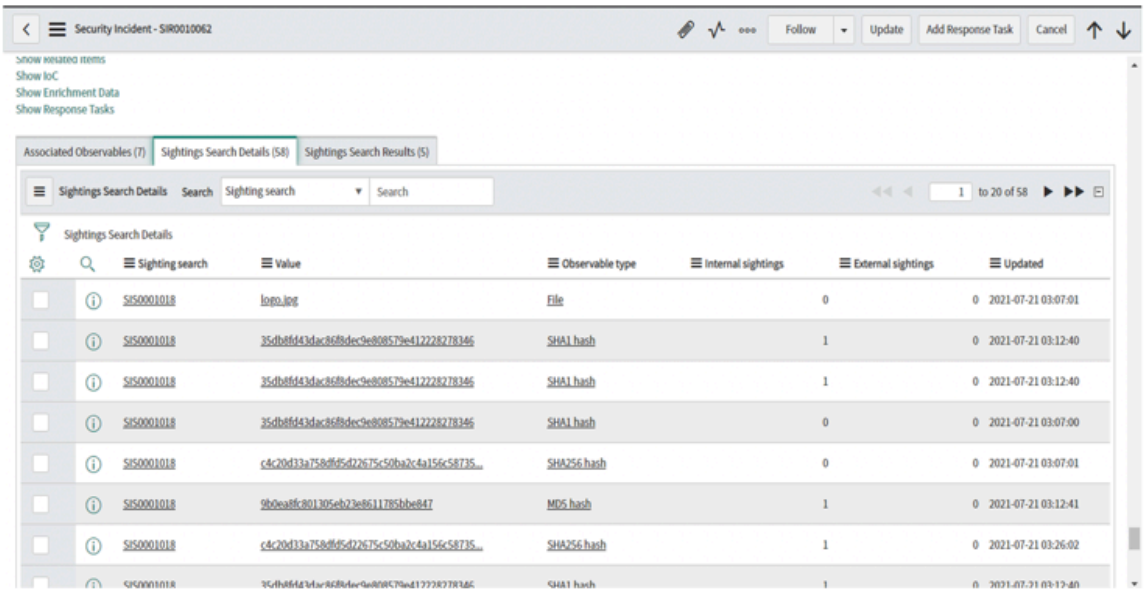
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

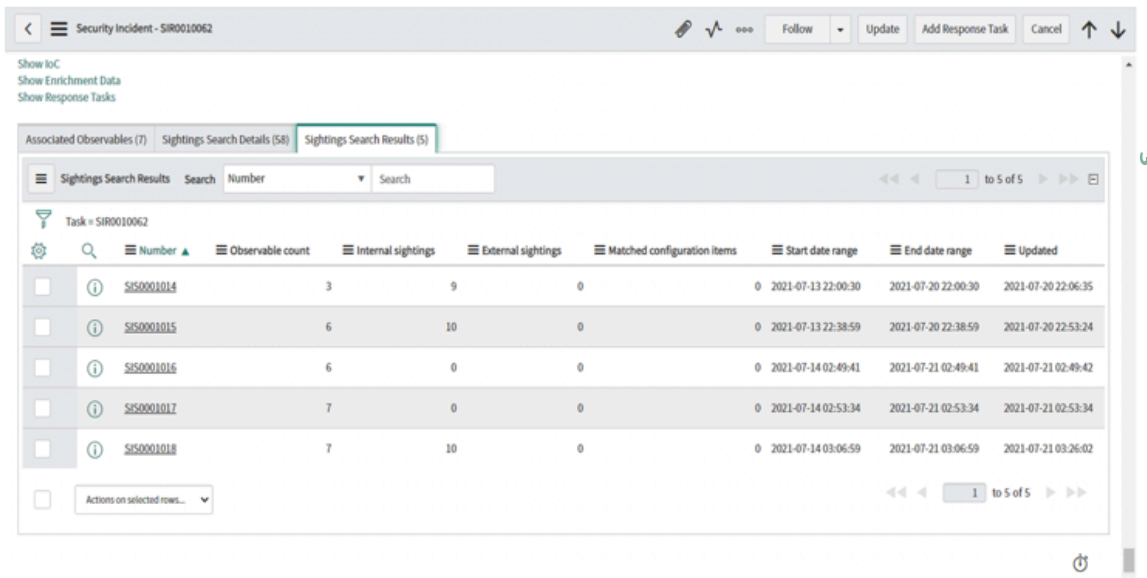


9. Ao concluir a pesquisa, verifique os resultados e os detalhes nas listas relacionadas.
10. Clique em **Detalhes de Pesquisa de detecções** guia para obter detalhes e **Resultados da pesquisa de detecções** guia para resultados de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tradução automática

Integração de Have I been pwned?

A integração Operações de segurança Have I been pwned? permite que você envie pesquisas em nomes de domínio e endereços de e-mail para determinar se os dados pessoais do usuário foram comprometidos por violações de dados.

Explorar

Integrações do Security Incident Response

Configurar

- Configuração de integração de Operações de segurança Have I been pwned?
- Ativar a integração das Operações de segurança Have I been pwned?

Usar

Executar pesquisas em observáveis Pesquisa de ameaças - Have I been pwned? fluxo

Desenvolver

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Configuração de integração de Operações de segurança Have I been pwned?

Have I been pwned? é um recurso gratuito usado para avaliar se alguém pode ter sido colocado em risco devido a sua conta on-line ter sido comprometida ou "pwned" em uma violação de dados. Ele se integra facilmente com Operações de segurança.

Antes de poder usar a integração Have I been pwned?, você deve ativar o plug-in. Se necessário, você também pode atualizar sua certificação SSL X509.

Os plug-ins Security Incident Response, Inteligência contra ameaçase Operações de segurança Have I been pwned? são necessários para implementar a integração Operações de segurança Have I been pwned?.

Pesquisa de ameaças - Have I been pwned? fluxo

O fluxo Pesquisa de ameaças - Have I been pwned? executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por Have I been pwned?, eles serão verificados quanto a malware e os resultados serão retornados.

Função necessária: sn_si_admin

Este fluxo é acionado pelo Integração de Operações de segurança - Capacidade de pesquisa de ameaças quando você executa uma pesquisa de ameaças em um ou mais observáveis e a implementação Have I been pwned? é selecionada. Para obter mais informações, consulte Executar pesquisas em observáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de I Been Pwned

Para obter informações sobre as atividades usadas por este fluxo, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Ativar a integração das Operações de segurança Have I been pwned?

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo a integração Operações de segurança Have I been pwned?. Antes de poder usar a integração Have I been pwned?, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser instalado e ativado para que você possa usar a integração Operações de segurança Have I been pwned?.

Função necessária: sn_si_admin

Procedimento

Baixe a integração do ServiceNow Store.
Esta integração oferece suporte a uma API aberta e não requer configuração adicional. Have I been pwned? agora pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Informações relacionadas

Executar pesquisas em observáveis

Atualizar seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor de terceiros ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira a URL do endpoint na barra de endereço do navegador.
   Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM no sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou na área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

> **Nota:** Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Como substituir um certificado SAML expirando .

HPE Security ArcSight ESM - Integração do analisador de e-mail

A integração do HPE Security ArcSight ESM - Analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do ESM para criar incidentes de segurança.

Configurar integração do HPE Security ArcSight ESM - Analisador de e-mail

A integração do HPE Security ArcSight ESM - Analisador de e-mail usa notificações por e-mail do ESM para gerar fluxos de trabalho de enriquecimento e de resposta.

Antes de Iniciar

Função necessária: sn_si_admin

Tradução automática

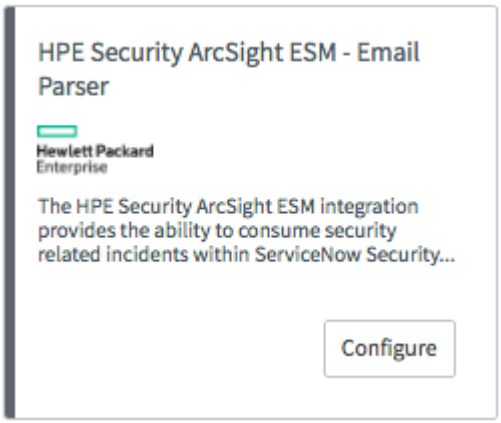
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Um modelo de analisador de e-mail do HPE Security ArcSight ESM é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. A atualização do analisador o ativa.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão HPE Security ArcSight ESM - Analisador de e-mail, clique em **Configurar**.
3. Na caixa de diálogo **HPE Security ArcSight ESM - Configuração do analisador de e-mail**, clique no link **Configurar analisador de e-mail**.
4. Clique no link do **ArcSight ESM** para editar as configurações no analisador de e-mail de modelo fornecido.
   No mínimo, preencha o campo O `e-mail é de`. Para criar seu próprio analisador de e-mail, consulte Criar analisadores de e-mail em Operações de segurança.
5. Marque a caixa **Ativo**.
6. Clique em **Atualizar** no formulário **Analisador de e-mail**.
   O analisador de e-mail está ativo. Você não precisa retornar às **Configurações de integração**.

HPE ArcSight Logger - Integração de enriquecimento de incidentes

A integração HPE ArcSight Logger - Incident Enrichment pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	**Configurar** • Introdução ao HPE ArcSight Logger - Incident Enrichment integration • Criar registros de configuração de pesquisa de detecções
Usar	**Desenvolver**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Executar uma pesquisa de detecções
- Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções
- Operações de segurança - Fluxo de trabalho de pesquisa de detecções do Arcsight Logger
- Exibir detalhes da pesquisa de detecções
- Exibir resultados da pesquisa de detecções

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Fazer ou responder a perguntas na comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Introdução ao HPE ArcSight Logger - Incident Enrichment integration

HPE ArcSight Logger transmite dados em tempo real e os categoriza em logs específicos e se integra facilmente com Operações de segurança. Antes de poder usar a integração HPE ArcSight Logger - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL da API e as credenciais de login.

Antes de Iniciar

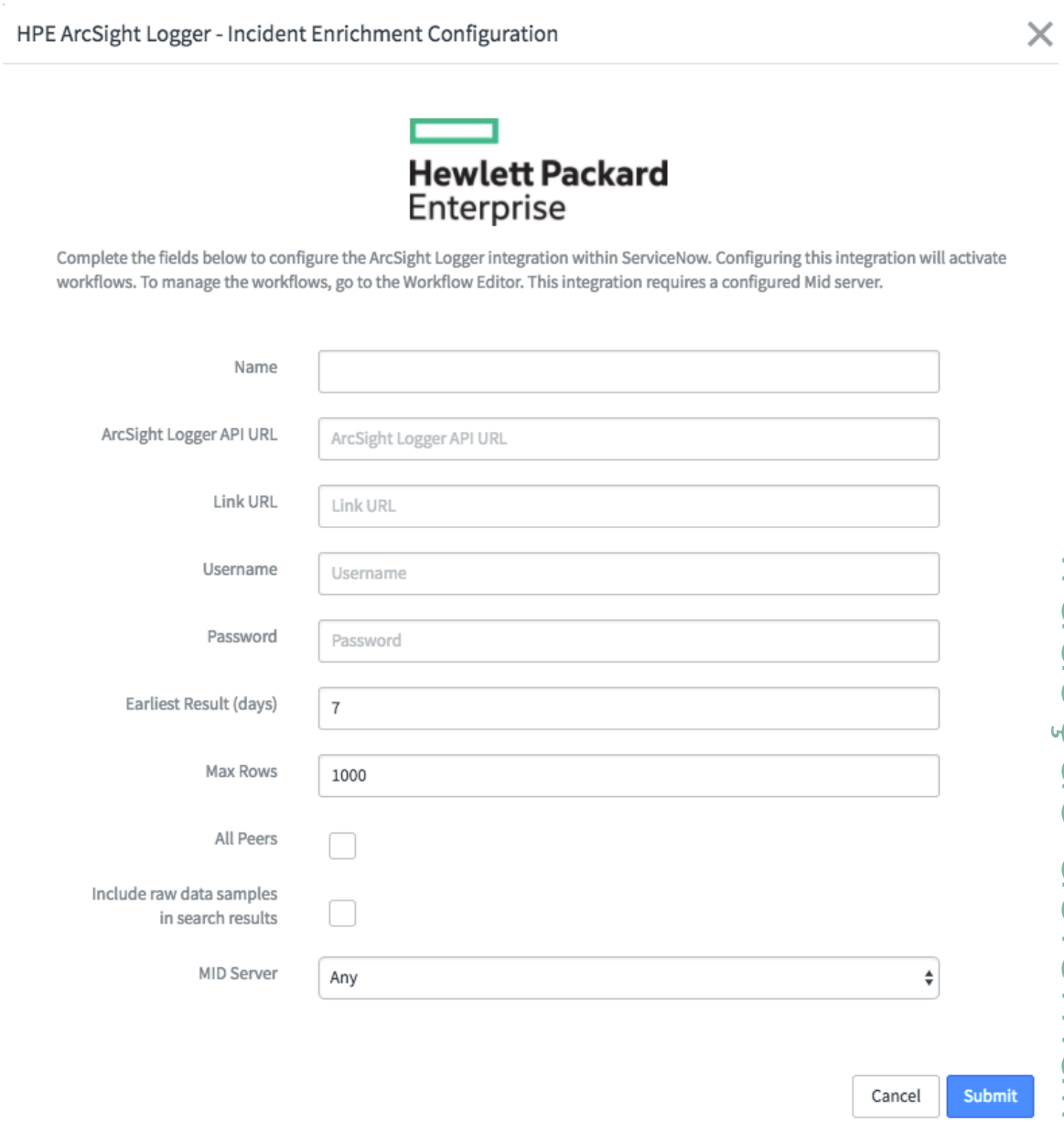
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão HPE ArcSight Logger - Aprimoramento de incidentes, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

4. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL base da API do ArcSight Logger	A URL base que você adquiriu no site do HPE Security ArcSight Logger.
URL do Link	[Opcional] A URL do link que vincula a uma instância do HPE Security ArcSight Logger, quando disponível.
Nome de usuário	Seu nome de usuário Intel HPE ArcSight Logger.
Senha	Sua senha Intel HPE ArcSight Logger.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Todos os Pares	O padrão é desmarcado e pesquisa somente o agente de log local ao qual você está conectado. Quando marcada, ela pesquisa todos os agentes de log que estão conectados entre si.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração de Análise híbrida

A aplicação Análise híbrida faz parte de uma comunidade online aberta na qual os usuários analisam arquivos e URLs em busca de ameaças. Você compartilha resultados e utiliza pesquisas da comunidade para obter respostas a incidentes mais eficazes. Quando integrada ao produto Now Platform Operações de segurança, a inteligência contra ameaças compartilhada fornece informações adicionais sobre a gravidade de observáveis específicos.

A integração Análise híbrida executa pesquisas de ameaças nos seguintes observáveis:

- Hashes de arquivo
- Endereços IP
- URLs

O fluxo verifica se há novos observáveis conforme eles chegam em incidentes de segurança. Se os observáveis forem de um tipo reconhecido pela integração de API, os observáveis serão avaliados. Os observáveis determinados como mal-intencionados são marcados.

Instalar e configurar Análise híbrida

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que a aplicação Análise híbrida se integre corretamente a Now Platform Operações de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador (admin) instala o aplicativo e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Operações de segurança e atribui a função sn_si.analyst.
Obtenha uma chave de API.	Visite o site de Análise híbrida para obter informações sobre chaves de API e para criar uma conta: Site de análise híbrida . A configuração requer que você insira as chaves de API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Madrid e as versões posteriores da família, o plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações. As Operações de segurança aplicações a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas: **1.** Estrutura de integração de segurança **2.** Security Support Common **3.** Orquestração de suporte de segurança **4.** Resposta a incidentes de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .

Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

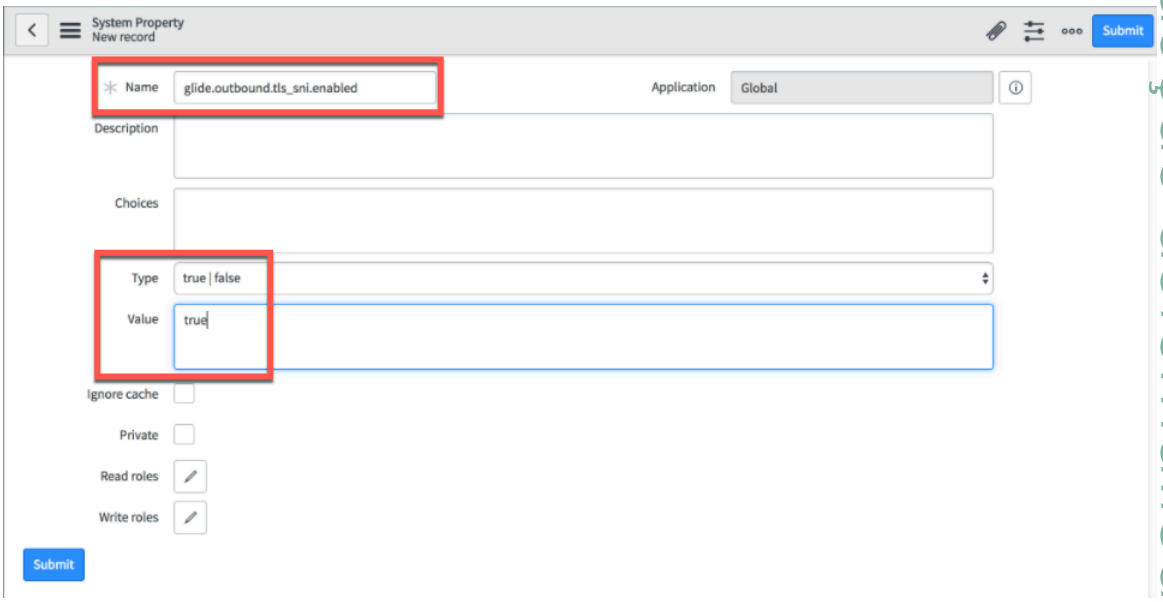
Por Que e Quando Desempenhar Esta Tarefa

Execute as etapas a seguir para atualizar as propriedades do sistema e instalar e configurar a integração.

Procedimento

1. No filtro de navegação, insira `sys_properties.list` e pressione **Enter**.
   A lista **Propriedades do sistema** é exibida.
2. Clique em **Nova**.
   Um novo registro é exibido.
3. Preencha os campos ou selecione os valores listados na tabela a seguir e clique em **Enviar**.

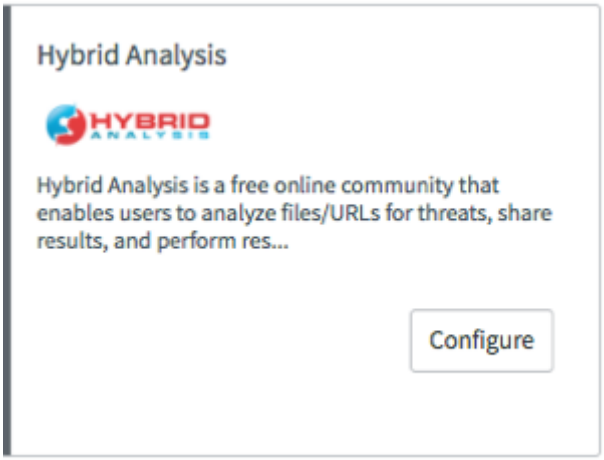
Nome do campo	Valor
Nome	`glide.outbound.tls_sni.enabled`
Tipo	Selecionar **verdadeiro I falso**
valor	`verdadeiro`



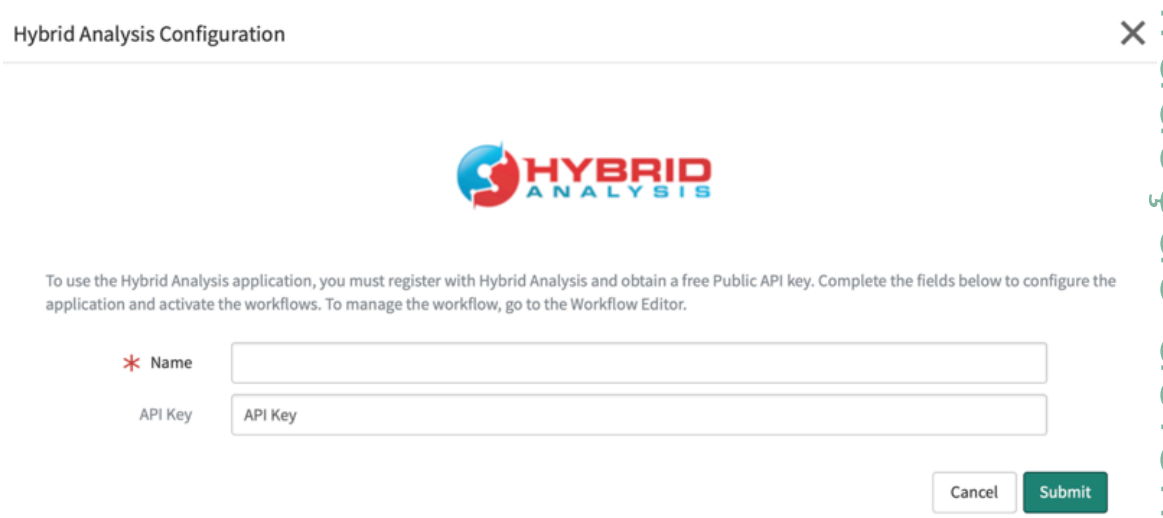
4. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.
5. Depois que a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Análise híbrida.
6. Clique em **Configurar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Na caixa de diálogo **Configuração de análise híbrida**, insira a chave de API que você obteve no site Análise híbrida e clique em **Enviar**.



8. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, a chave de API Análise híbrida pode ser inválida.

Verificar resultados esperados para Análise híbrida

Os observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Localize os resultados da pesquisa no incidente de segurança para verificar se a pesquisa de ameaças foi executada com sucesso. Exiba também dados brutos e execute pesquisas de ameaças em observáveis secundários.

Antes de Iniciar

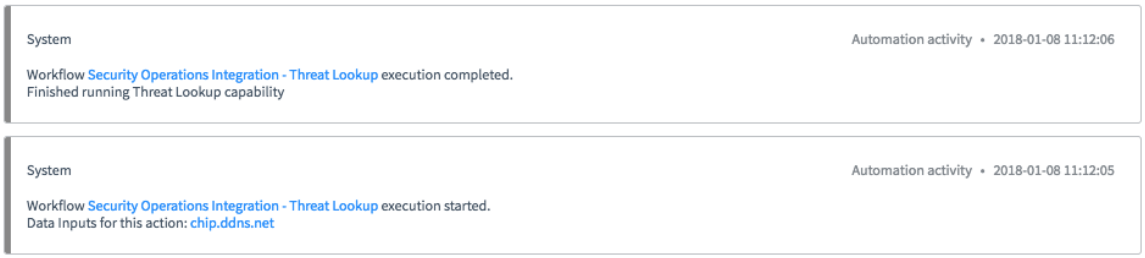
Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o registro de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

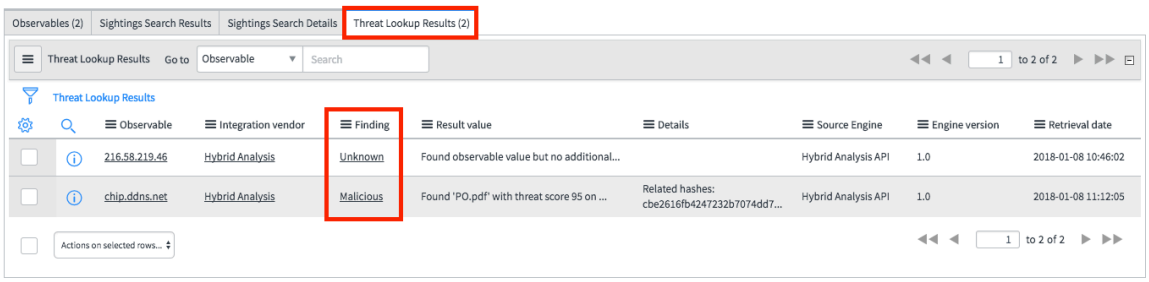


   Depois que a aplicação é configurada, o fluxo é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações sobre como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

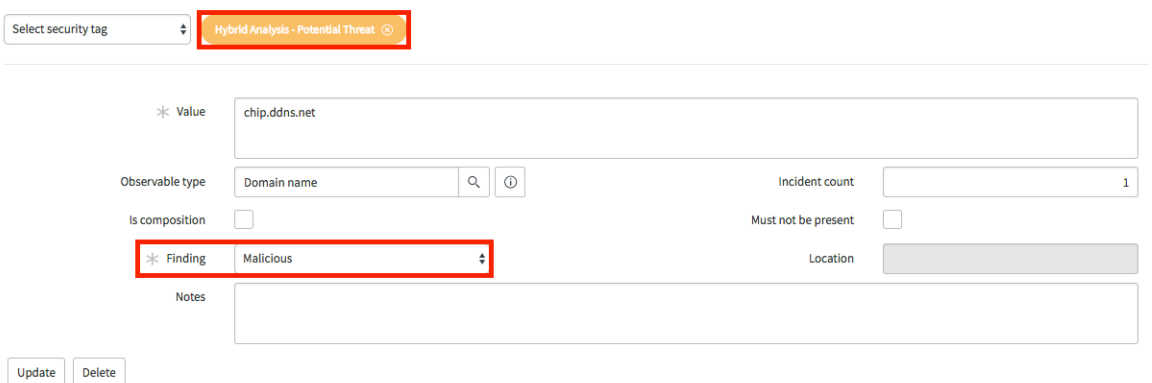
3. Navegue até a parte inferior do registro de incidente de segurança e clique no link relacionado **Mostrar todas as listas** relacionadas para exibir os resultados.

   Nota: As imagens nas etapas a seguir são mostradas com a configuração **Formulários com guias** ativa nas Configurações do sistema. No canto superior direito da faixa superior, clique no ícone de engrenagem Configurações. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se Formulários **com guias** e **Com o formulário** estão selecionados.



   A guia **Resultados da pesquisa de ameaças** exibe os resultados da pesquisa na parte inferior do registro de incidente de segurança. Observe que a coluna **Descoberta** exibe `Desconhecido` para registros não determinados como mal-intencionados. Para resultados correspondentes a maliciosos, a coluna **Descoberta** exibe `Mal`-intencionado .

4. Na coluna **Observável**, clique em um observável para abrir o registro.



Tradução automática

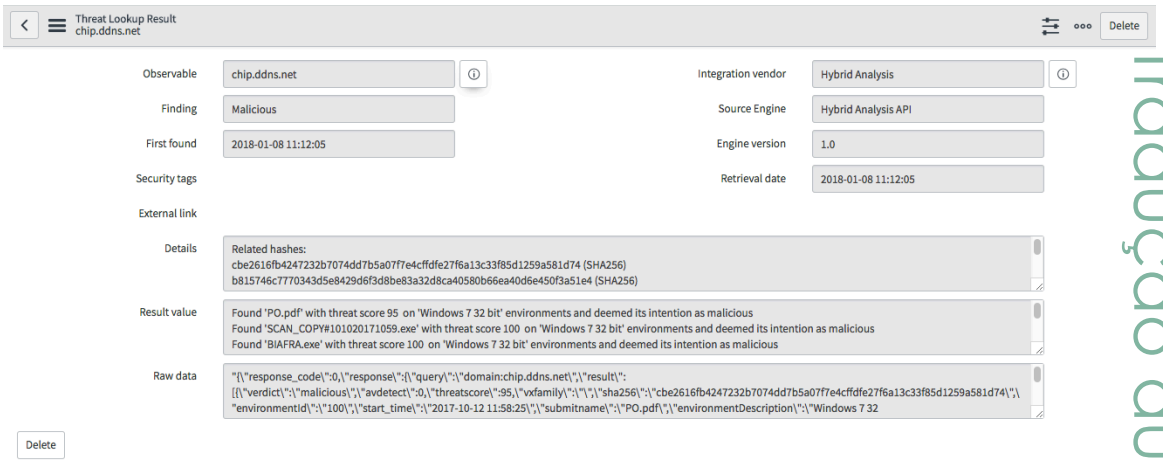
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para pesquisas correspondentes a mal-intencionadas, o campo **Descoberta** exibe `Mal-intencionado` e o observável é marcado com a origem Inteligência contra ameaças que o considerou mal-intencionado, neste caso, a integração Análise híbrida.

5. Opcional: Siga as etapas para exibir dados brutos, exibir uma lista de observáveis secundários e executar uma pesquisa de ameaças em observáveis secundários selecionados.

   a. Navegue de volta para o incidente de segurança e, na guia **Resultados da pesquisa de ameaças**, clique no ícone de informações azul ao lado de um observável.

   b. Na janela que é exibida, clique em **Abrir registro** para exibir os dados.
   A partir de todos os observáveis visíveis nos dados brutos exibidos na pesquisa, a integração Análise híbrida também cria observáveis secundários ou relacionados.



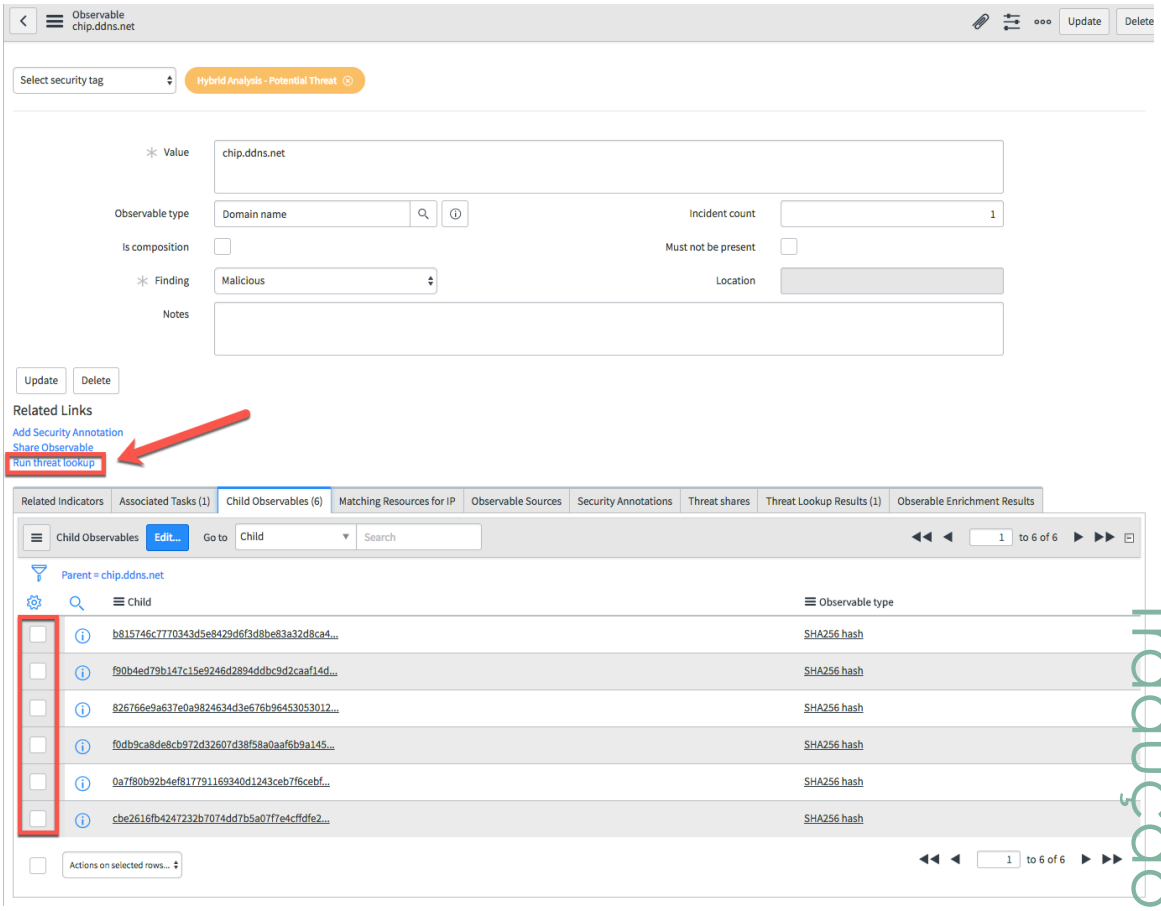
   O link criado pela API, os dados brutos e outras informações são exibidos.

   c. Navegue de volta para o incidente de segurança e clique no link relacionado **Mostrar IoC**.
   Os observáveis secundários são exibidos na guia **Observáveis secundários** no incidente de segurança, porque a pesquisa encontrou uma conexão existente entre esses observáveis relacionados e o observável enviado inicialmente.

   d. Clique no campo ao lado de um observável na coluna **Secundário** para selecioná-lo e, em seguida, no link relacionado **Executar pesquisa de ameaças** para realizar uma pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Na caixa de diálogo exibida, verifique se a integração Análise híbrida está selecionada e clique em **Enviar**.

f. Nas anotações de trabalho, verifique se a pesquisa foi executada com sucesso e, na guia **Resultados da pesquisa de ameaças** do incidente de segurança, localize os resultados da pesquisa dos observáveis secundários.

Trouble?
Se você não vir os resultados na guia **Resultados da pesquisa de ameaças**, verifique se o observável é de um tipo compatível com a pesquisa pela integração.

(Opcional) Anexar manualmente um observável para Análise híbrida

Você pode anexar observáveis manualmente quando quiser executar pesquisas de ameaças em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

Antes de Iniciar

Verifique se o observável é de um tipo compatível com a integração. A integração executa pesquisas nos seguintes tipos de observáveis:

- Hashes de arquivo
- Endereços IP
- URLs

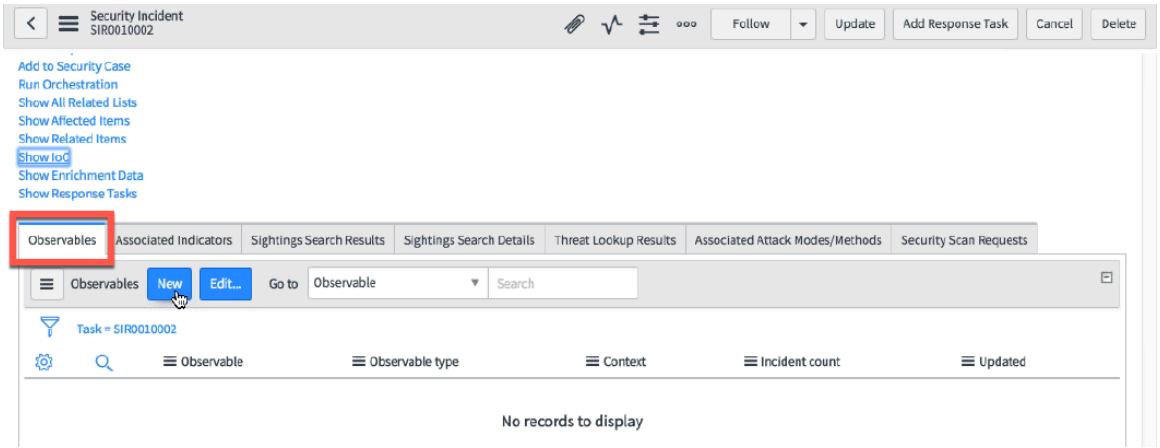
Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

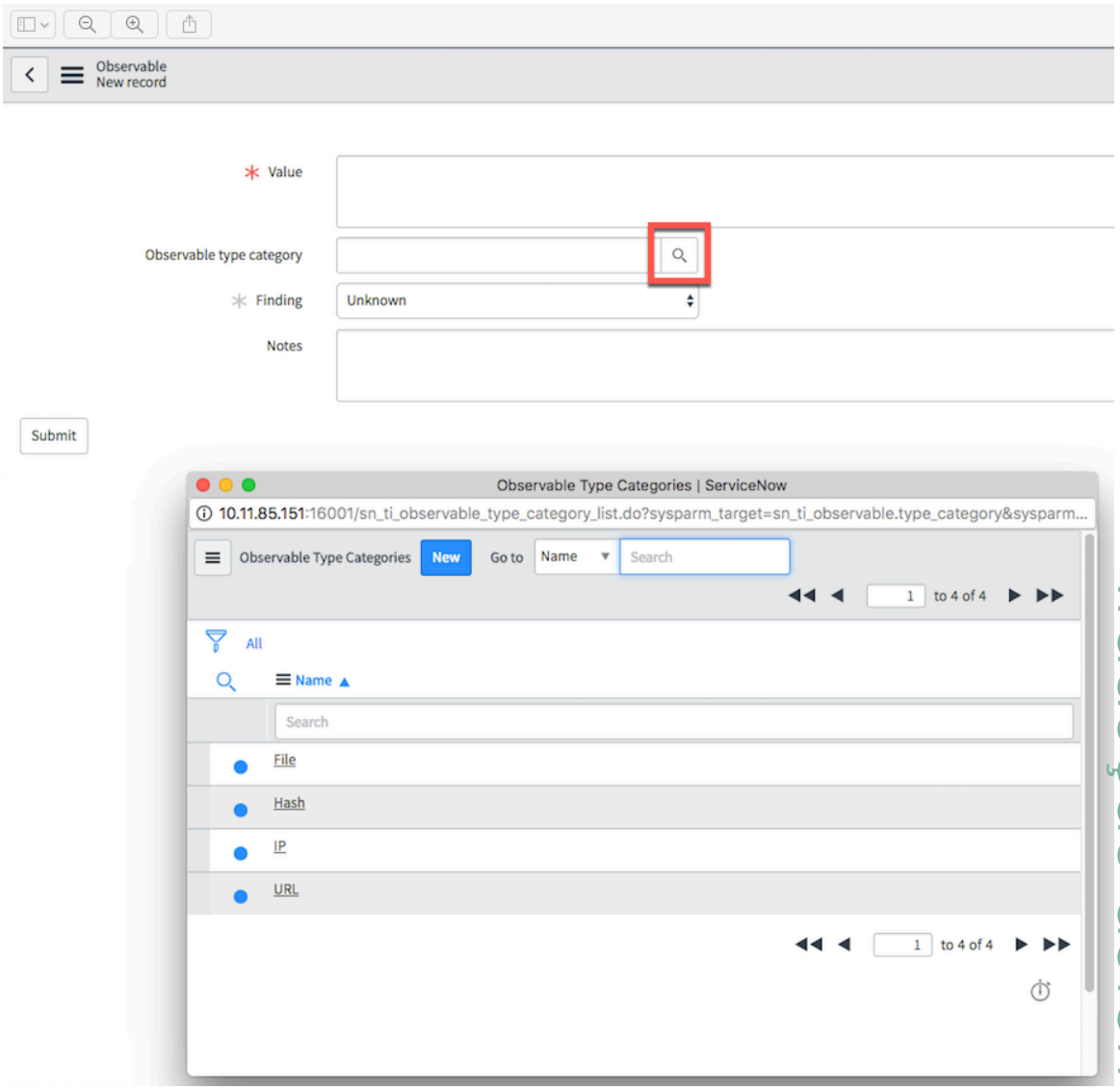
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes** e abra um incidente de segurança ao qual você deseja anexar o observável.
2. No incidente de segurança aberto, clique no link **Mostrar IoC**em **Links relacionados**.



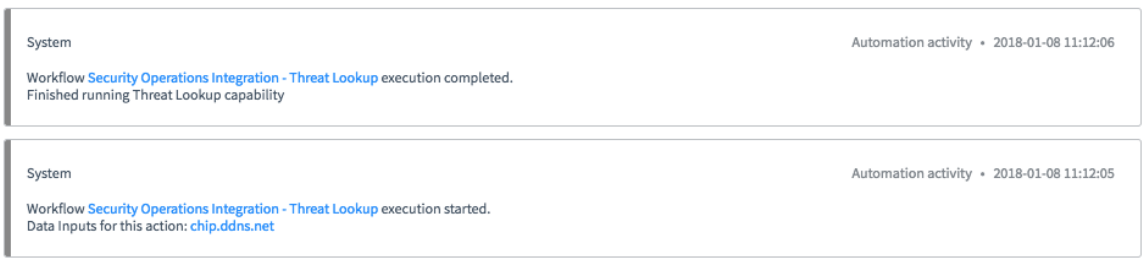
3. Na guia **Observáveis**, clique em **Novo**.
   O formulário Observável é exibido.
4. No campo **Valor**, insira um observável (hash de arquivo, endereços IP ou URL).
5. Clique no ícone de pesquisa e, na caixa de diálogo **Categorias de tipo de observável**, clique no tipo de observável desejado na lista para preencher o campo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



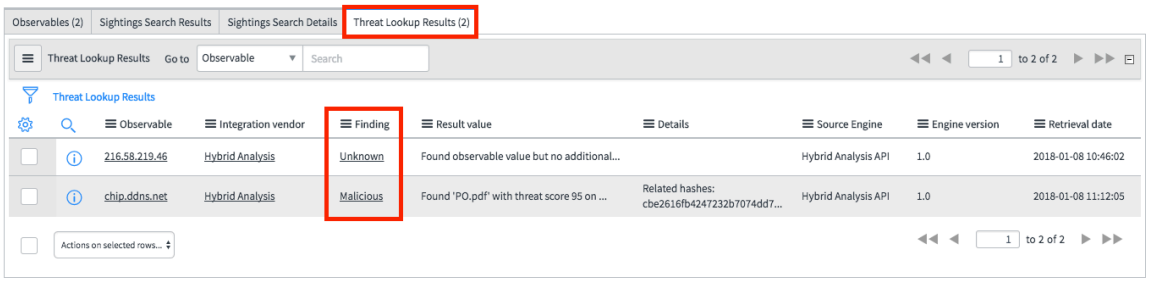
6. Clique em **Enviar**.
   O fluxo é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção de anotações de trabalho no registro de incidente de segurança.
7. Navegue até o seu incidente de segurança e revise as anotações de trabalho.



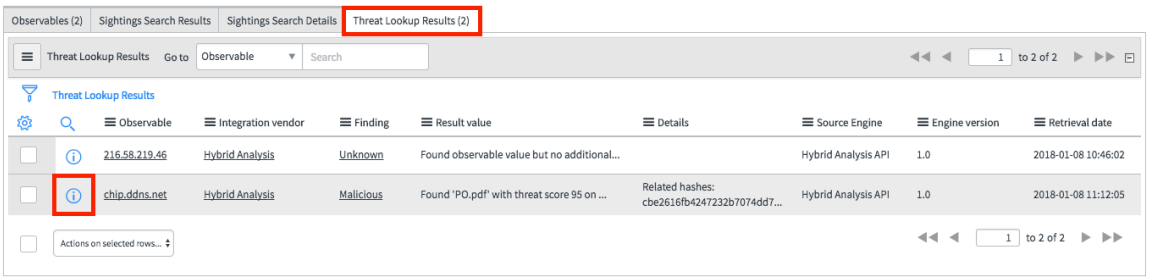
8. Na parte inferior do registro, clique no link relacionado **Mostrar todas as listas** relacionadas.
9. Clique na guia **Resultados da pesquisa de ameaças** para exibir os resultados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Na coluna **Observável**, clique no ícone de informações azul ao lado de um determinado observável para obter mais informações e dados brutos.



11. Na caixa de diálogo exibida, clique em **Abrir registro** para exibir os dados brutos e mais detalhes.
Como alternativa, você também pode anexar um observável existente ao registro de incidente de segurança.

12. Opcional: Com a guia **Observáveis** selecionada, clique em **Editar**.

13. Opcional: No formulário **Editar membros** exibido, mova um observável existente da **Coleção** para a **Lista de observáveis** e clique em **Salvar**.
Você retorna ao incidente de segurança.

14. Na coluna da extrema esquerda, selecione os observáveis nos quais deseja executar a pesquisa e, na lista de seleção **Ações em linhas selecionadas...**, selecione **Executar pesquisa de ameaças**.
Uma mensagem é exibida na parte superior do registro informando que a solicitação está sendo processada. Verifique se a pesquisa foi executada com sucesso.

Trouble?
Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

IBM QRadar Offense Ingestion Integração

A integração IBM QRadar Offense Ingestion permite que você busque automaticamente IBM QRadar infrações e as converta em incidentes de segurança e habilite ações de resposta automatizadas.

Esta integração é compatível com o seguinte:

- Descoberta de IBM QRadar infrações que são candidatas a incidentes de segurança.
- Buscando eventos ou fluxos recentes associados a uma infração.
- Rastreie atualizações importantes para infrações periodicamente.
- Mapeamento de campos de infração, evento e fluxo para campos de incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Exibição preliminar dos campos mapeados.
- Configure ingestões programadas de infrações para criar incidentes de segurança periodicamente.
- Encerre as infrações quando os incidentes de segurança forem encerrados.

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de infração IBM QRadar

Antes de executar a integração em sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Operações de segurança em sua instância Now Platform.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se você não instalou a aplicação [IBM QRadar de ServiceNow Store para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize o bloco IBM QRadar.
3. Para configurar a aplicação, clique em **Novo**.
4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo **Configuração de ingestões de infração** exibida, preencha os campos.

Campo	Descrição
Nome	Nome do console IBM QRadar ou da instância IBM QRadar usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis.
URL base da API do IBM QRadar	URL do host para sua instância IBM QRadar. **Nota:** Você precisa inserir apenas o URL e o número da porta aqui. Por exemplo, https://ibm-qradar.com:8443. Se o número da porta for 443, ele não precisará ser inserido explicitamente.
URL do painel do IBM QRadar	O URL do painel IBM QRadar ou do console. Este URL é usado para construir automaticamente os hiperlinks para infrações no painel IBM QRadar. Insira somente a URL do host, por exemplo, https://qradar.com. Não inclua .jsp no URL, por exemplo, https://qradar.com/console/qradar/jsp/QRadar.jsp é um formato inválido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se a URL do painel não estiver disponível, insira a URL base da API IBM QRadar aqui.
IBM QRadar Versão da API	As versões 10 e superiores são compatíveis.
IBM QRadar Token de serviço autorizado da API (no local)	O IBM QRadar token de serviço autorizado é usado para autenticação. O token de serviço autorizado deve ter a função de usuário **administrador** e o perfil de segurança de **administrador**. Para gerar o token de serviço autorizado, siga estas etapas: ◦ No console IBM QRadar, navegue até a guia **Administrador** e clique em **Serviços autorizados**. ◦ Se existir um token de serviço autorizado válido, verifique a data de vencimento e use este token. Se um token de serviço autorizado não estiver disponível, siga estas etapas: ◦ No IBM QRadar, navegue até a guia **Administrador** e clique em **Serviço autorizado**. ◦ Clique em **Adicionar serviço autorizado** e crie um token com a função de usuário **administrador** e o perfil de segurança de **administrador**. Certifique-se de especificar uma data de vencimento para um longo período de validade.
IBM QRadar Token de serviço autorizado da API (para QRoC)	Se você estiver usando o IBM QRadar on Cloud (QRoC), use a aplicação de autoatendimento para gerar o token de serviço autorizado com função de usuário administrador e perfil de segurança de administrador para autenticação.
Implantação no Local	O padrão é desabilitado. Se esta opção estiver habilitada, você deverá especificar um Nome da aplicação MID. Se você estiver usando IBM QRadar na nuvem (QRoC), verifique se a caixa de seleção está desmarcada.
Nome da aplicação MID	Especifique uma aplicação de MID Server que esteja configurada em seu ambiente. Se você não tiver uma aplicação de MID Server configurada, deverá criar uma nova

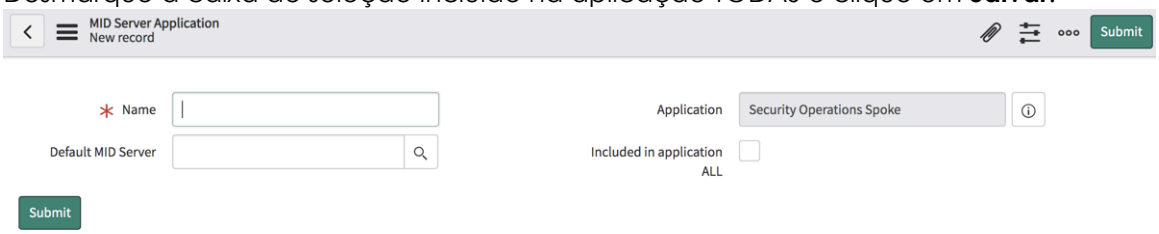
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	aplicação de MID Server para esta integração. **Nota:** A aplicação do MID Server pode ser configurada somente por usuários com a função de administrador do sistema.

Para criar uma nova aplicação do MID Server, siga estas etapas:

- Navegar até **MID Server** > **Aplicações** e clique em **Novo**.
- Insira um nome para a aplicação do MID Server e selecione um MID Server a ser usado como padrão.
- Desmarque a caixa de seleção Incluído na aplicação TODAS e clique em **Salvar**.

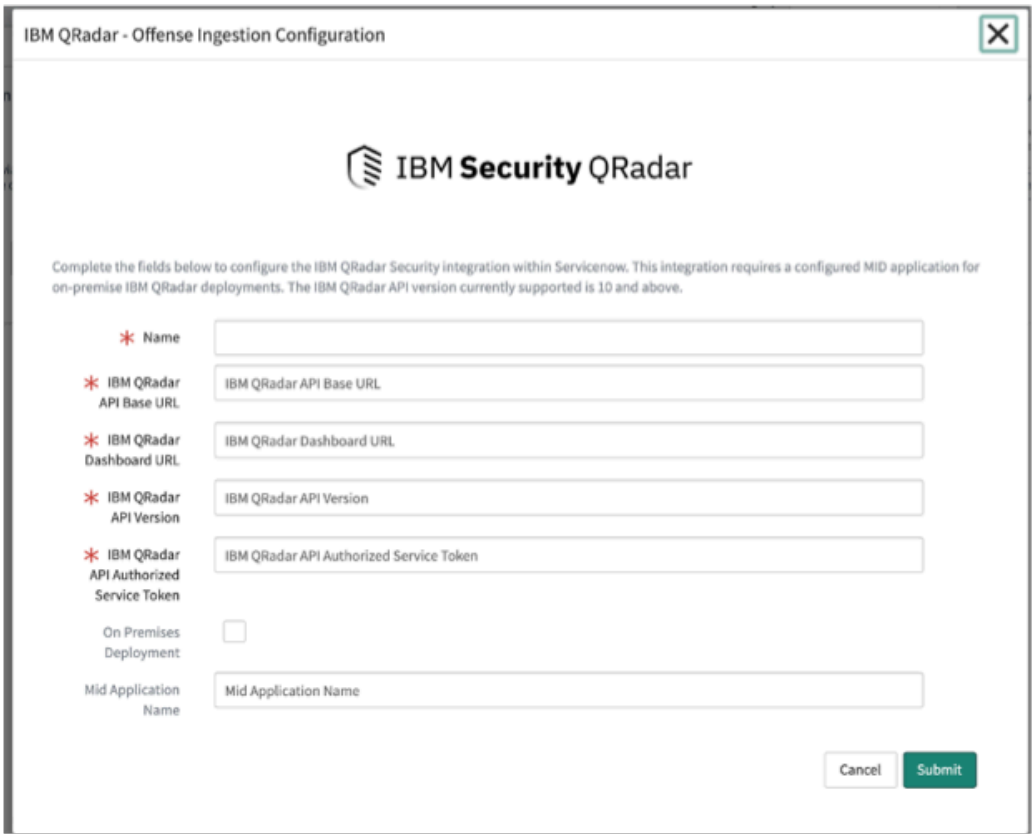


- Clique em **Editar**. Na página **Editar Membros**, selecione todos os MID Servers disponíveis, mova-os para a Lista de MID Servers e clique em **Salvar**. Dependendo da disponibilidade, um dos MID Servers configurados com a aplicação MID Server será usado.

6. Insira os detalhes da configuração e especifique a aplicação do MID Server que você criou.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A origem que você configura no formulário **Configuração de ingestão de infração do IBM QRadar** pode ser reutilizada para vários Now Platform perfis, desde que cada perfil ingira infrações.

7. Clique em **Enviar**.
   Depois de ser validada e enviada com sucesso, cada configuração de servidor IBM QRadar é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.

   Nota: Se você encontrar alguns problemas com o recurso de segmentação de domínio IBM QRadar, entre em contato com o Suporte ao cliente IBM QRadar para obter assistência.

O que Fazer Depois
Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar o perfil.

Configure sua instância Now Platform® para a integração de ingestão de infração IBM QRadar

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação a partir do ServiceNow Store.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As funções a seguir são necessárias para a instalação, configuração e uso da integração em sua instância Now Platform®. • Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®: ◦ Nomeia, cria e edita perfis de infração. ◦ Seleciona e mapeia IBM QRadar campos de dados de infração para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão de infração contínua. ◦ Habilita atualizações de infração quando um incidente SIR é criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e como atribuir funções a usuários, consulte Funções no site de documentação de produtos da Servicenow .
Verifique se você está usando as seguintes versões: • IBM QRadar versão 7.3.2 ou posterior. • IBM QRadar API versão 10 ou posterior. Versões anteriores não são compatíveis.	Se você tiver acesso ao console IBM QRadar, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.
Verifique se você instalou e configurou uma aplicação do MID Server.	Aplicação do MID Server configurada. Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço IBM QRadar se o servidor IBM QRadar estiver implantado em sua rede corporativa. Consulte o site de documentação de produtos da ServiceNow para obter informações sobre MID Servers.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Se você estiver usando o serviço em nuvem IBM QRadar, um MID Server não será necessário.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Ingestão de eventos e alertas para Operações de segurança: esta aplicação requer: ◦ com.glide.hub.integration.runtime => Tempo de execução do IntegrationHub da ServiceNow ◦ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in Event and Alert Ingestion. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

O que Fazer Depois
Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação IBM QRadar da ServiceNow Store para a integração.

Criar um perfil para IBM QRadar integração de ingestão de infração

Como um usuário com a função sn_si.admin, você cria um perfil de infração em sua instância Now Platform e determina quais infrações criam incidentes de segurança. Antes que Now Platform Security Incident Response (SIR) incidentes de segurança sejam criados a partir de infrações, os valores de campos de infrações são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será criado.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
De uma perspectiva de integração usando as APIs disponíveis, IBM QRadar infrações são ingeridas automaticamente no ambiente Operações de segurança da sua instância Now Platform, dependendo do tipo de perfil definido. Os fluxos de trabalho de integração ingerem diferentes tipos de infrações, como tentativas de acesso não autorizado e malware, por exemplo. Essas infrações são ingeridas com base nos perfis que você configura no ambiente Operações de segurança da sua instância. Todas as infrações são ingeridas inicialmente para um tipo de infração configurado em um perfil. As infrações ingeridas podem ser filtradas para especificar quais infrações criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

somente para infrações identificadas como de alto risco. Antes que um perfil seja ativado e crie incidentes de segurança a partir de infrações ingeridas, os valores de campos individuais nas infrações são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização.

Os nomes dos perfis de infração na sua instância Now Platform devem ser exclusivos. Você pode criar várias configurações para várias origens e também pode criar vários perfis para uma única origem.

Criar perfis para ingerir IBM QRadar infrações

Você pode configurar um perfil para ingerir infrações.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para uma infração em sua instância Now Platform, navegue até **Integração do IBM QRadar** > **Perfil do IBM QRadar**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

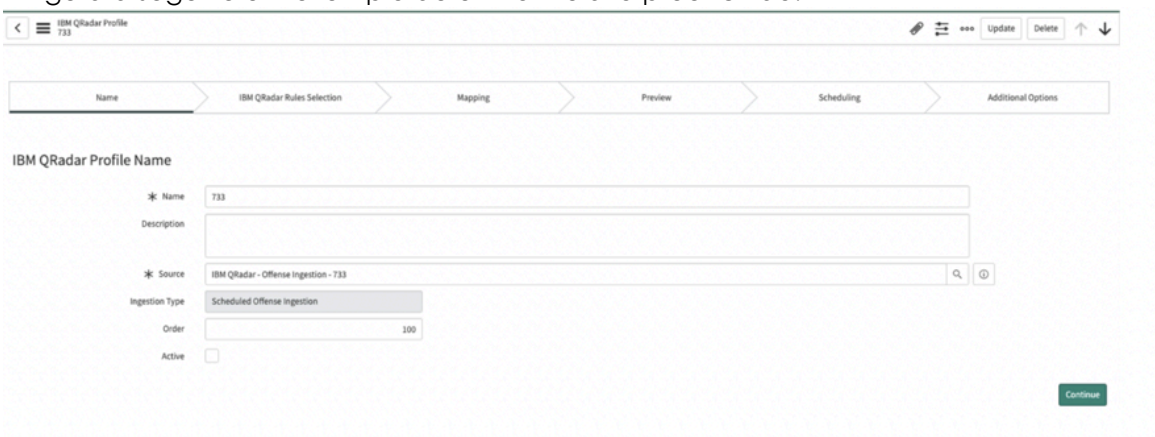
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e nomes de perfil duplicados não serão salvos. Os nomes de perfil em sua instância Now Platform devem ser exclusivos.
Ativo	A caixa de seleção está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo e a ingestão não ocorrerá. **Nota:** Você deve concluir todas as seções no perfil antes de torná-lo ativo.
Origem	O servidor IBM QRadar que você configurou para ingerir infrações. Se você tiver vários servidores IBM QRadar configurados, selecione o servidor apropriado para os tipos de infração que serão ingeridos para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem as mesmas condições de acionamento. O fluxo de traba-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	lho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

A próxima etapa é selecionar as infrações para ingestão.

Selecionar IBM QRadar regras

Com base na Origem IBM QRadar, selecione uma ou mais regras IBM QRadar para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba as regras IBM QRadar disponíveis em sua instância da Now Platform para que você saiba quais regras IBM QRadar ativas para as quais você deseja ingerir e criar incidentes de segurança.

Em IBM QRadar, você pode identificar regras por sua origem como regras do sistema, de substituição e de usuário. Por padrão, a origem de uma regra está vinculada a uma regra do sistema. Quando você modifica uma regra do sistema em IBM QRadar, sua origem é definida como Substituir.

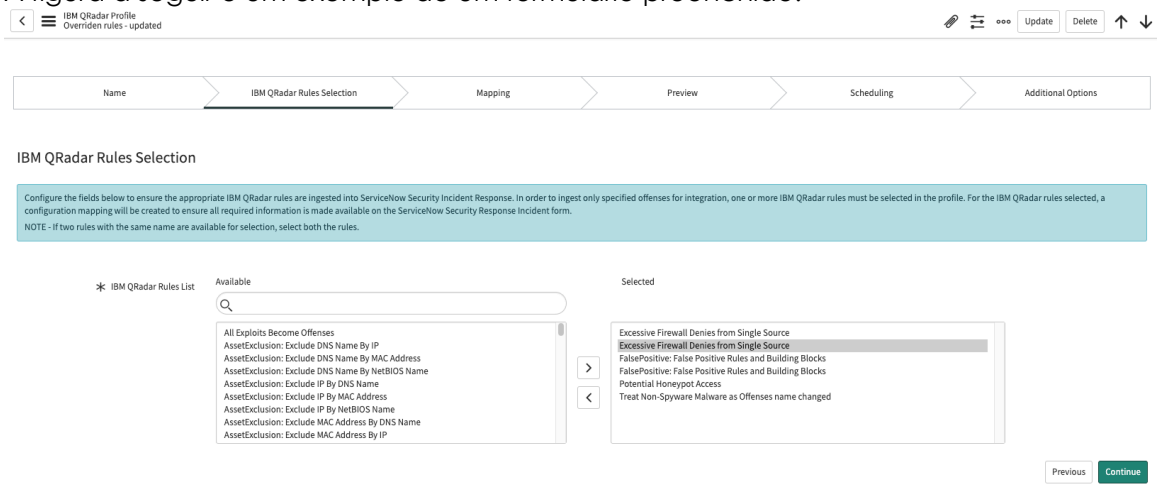
Clique na lista no campo IBM QRadar Lista de regras. Uma lista de regras IBM QRadar ativas que estão presentes no Console IBM QRadar é exibida. Selecione uma ou mais regras na lista e mova-as para a coluna **Selecionada**. As infrações acionadas por uma ou mais das IBM QRadar regras selecionadas são ingeridas neste perfil.

Regras com o mesmo nome: na instância Now Platform, uma lista de regras ativas ou habilitadas é exibida. Se você modificar uma regra do sistema ativa ou habilitada em IBM QRadar, uma nova regra de substituição será criada. Isso resulta na exibição de duas regras com o mesmo nome no Now Platform. Quando este cenário ocorrer, selecione as regras para ingerir e criar incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A figura a seguir é um exemplo de um formulário preenchido:



Clique em **Continuar** para prosseguir para a próxima etapa no assistente.

Mapeamento de campos de infração para a integração IBM QRadar

Depois de selecionar as regras, a próxima etapa é mapear campos de infração, evento ou fluxo para os campos no formulário de incidente de segurança.

Visão geral

Para a etapa de mapeamento, você deve primeiro ingerir amostras de infrações para uma ou mais regras IBM QRadar selecionadas. Em seguida, você deve garantir que todos os dados de campo de infração relevantes estejam mapeados para o local apropriado no formulário de incidente SIR e visualizar o incidente SIR na seção de visualização.

O mapeamento dos campos de infração de amostra envolve o seguinte:

- Buscando e preenchendo os dados de amostra: consulte Ingestão da amostra IBM QRadar de infrações.
- Mapeamento dos campos de infração para o incidente de segurança: consulte Mapeamento de campos de infração IBM QRadar para campos de resposta a incidentes de segurança.

Ingestão da amostra IBM QRadar de infrações

Você pode ingerir amostras de infrações para uma ou mais regras IBM QRadar selecionadas.

Antes de Iniciar

Função necessária: sn_si.admin

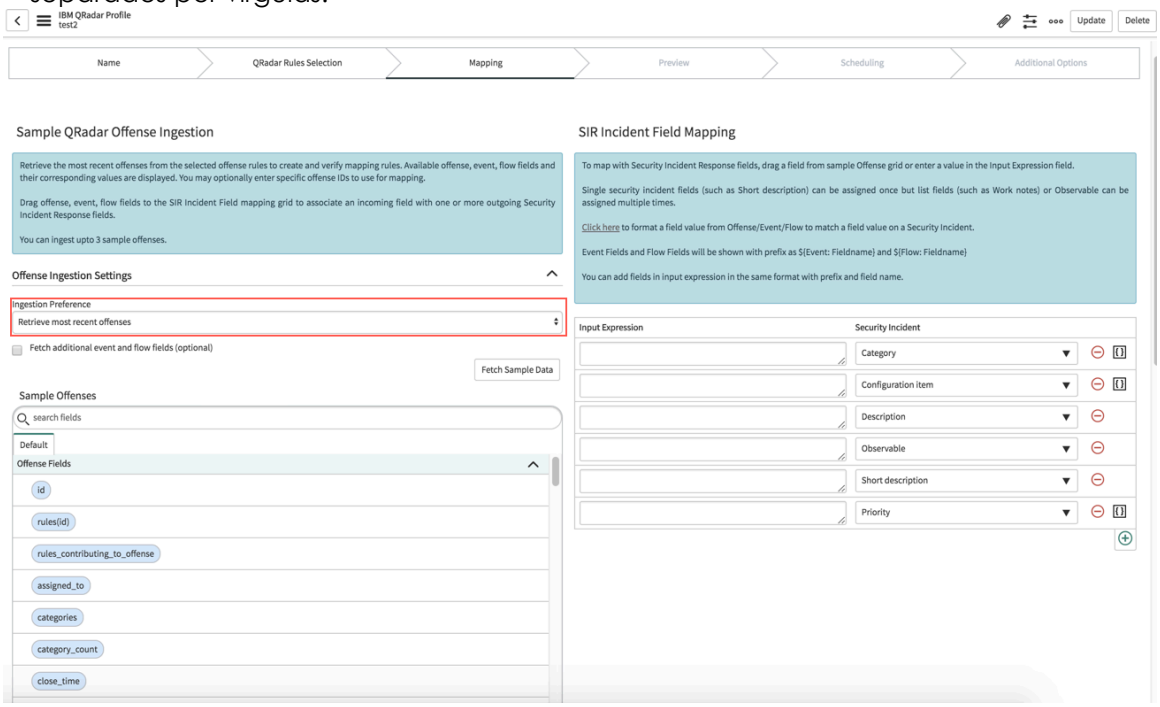
Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair as três infrações de amostra mais recentes ou fornecer os IDs de infração exclusivos para as infrações específicas que deseja usar para sua experiência de mapeamento.
   Na lista de seleção **Preferência de ingestão**, selecione uma das seguintes opções:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Recuperar infrações mais recentes: as três infrações mais recentes das regras selecionadas são recuperadas.
- Selecionar infrações com base no ID de infrações: especifique o ID de infração para as infrações a serem recuperadas. Você pode especificar no máximo 3 IDs de infração separados por vírgulas.



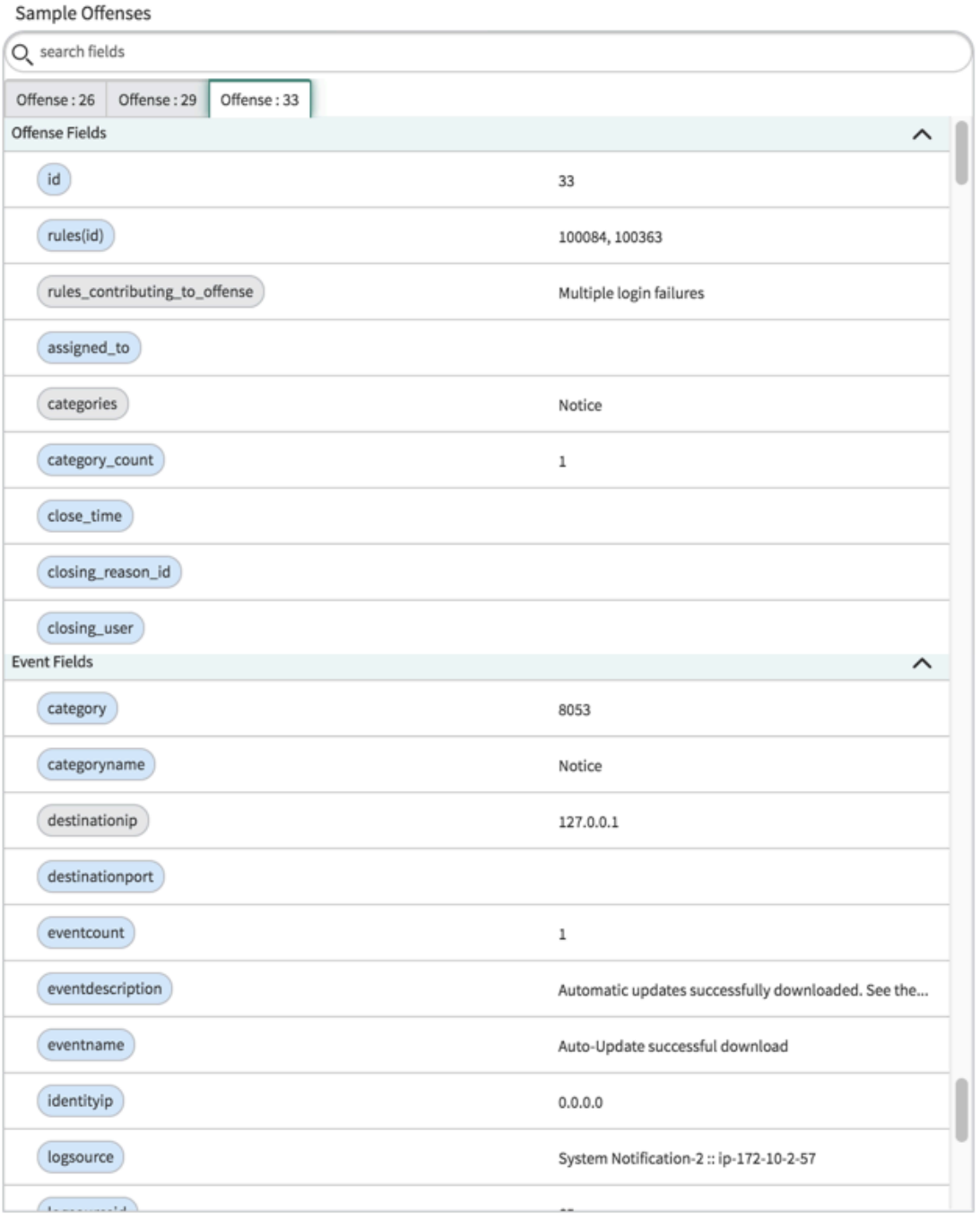
3. Clique em **Buscar dados de amostra** para extrair os dados de infração de amostra mais recentes do console IBM QRadar para as regras de infração selecionadas.

   Os campos de infração e os resultados dos valores são exibidos como guias individuais. Uma infração pode ser acionada por três tipos de regras:

   - Evento: nesta regra, os logs de eventos são verificados e, se os critérios especificados forem atendidos, uma infração será criada.
   - Fluxo: os dados e o tráfego da rede são verificados e, se determinadas condições forem atendidas, uma infração será criada.
   - Comum: neste caso, você pode especificar condições para eventos ou fluxos e uma ou ambas as condições forem atendidas, uma infração será criada.

   A extração de exemplos de infrações pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela. Dependendo da regra ou regras que acionaram a infração, junto com os campos de infração, os campos de evento ou fluxo são preenchidos conforme mostrado na figura abaixo:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

Nota: Os campos de evento ou fluxo exibidos pertencem ao primeiro evento ou campo de fluxo que acionou a infração com base no evento correspondente ou na regra de fluxo.

4. A seguir estão os campos de infração personalizados criados para esta integração. Os campos de infrações padrão, além desses campos personalizados, estão disponíveis para mapeamento.
   - rules_contributing_to_offense: IBM QRadar regras que contribuíram para a infração com base no ID da regra.
   - users: nomes de usuário para a infração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

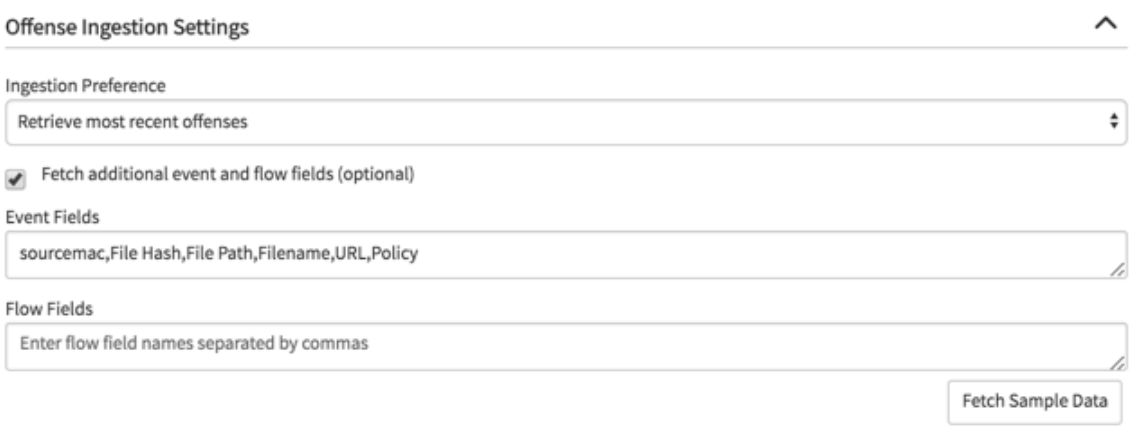
- remote_destination_ip: os IPs de destino remoto da infração.

  Com base nos IDs de destino local da infração, os seguintes campos de endereço de destino local personalizado estão disponíveis:

  - local_destination_address (domain_id)
  - local_destination_address (event_flow_count)
  - local_destination_address (first_event_flow_seen)
  - local_destination_address (ID)
  - local_destination_address (last_event_flow_seen)
  - local_destination_address (local_destination_address_ids)
  - local_destination_address (tamanho)
  - local_destination_address (rede)
  - local_destination_address (offense_ids)
  - local_destination_address (local_destination_ip)

- Os seguintes endereços de origem estão disponíveis com base nos IDs de origem da infração:
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (ID)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (grandeza)
  - source_addresses (rede)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

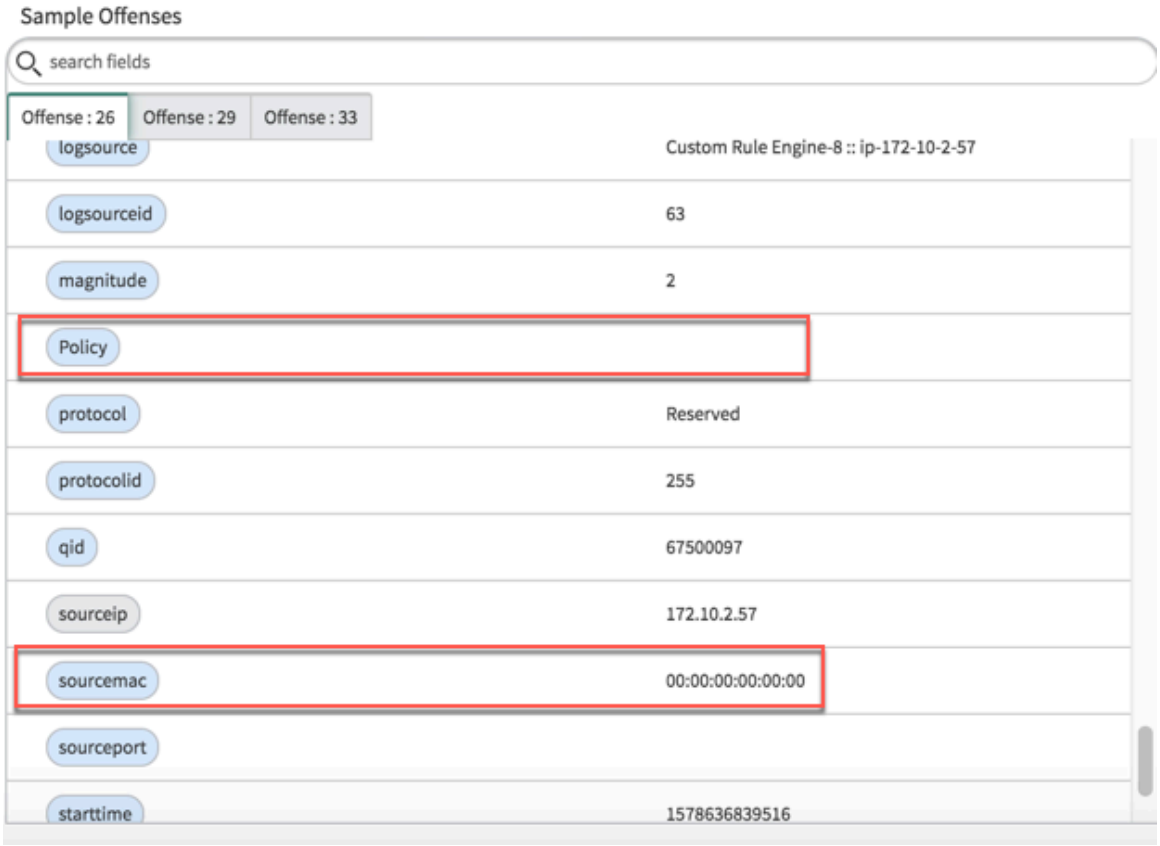
Marque a caixa de seleção **Buscar campos adicionais de evento e fluxo (opcional)**. Você pode buscar dados de evento e fluxo de amostra de qualquer evento personalizado e campos de fluxo ativos e válidos. Especifique os campos personalizados separados por vírgulas, conforme mostrado abaixo:



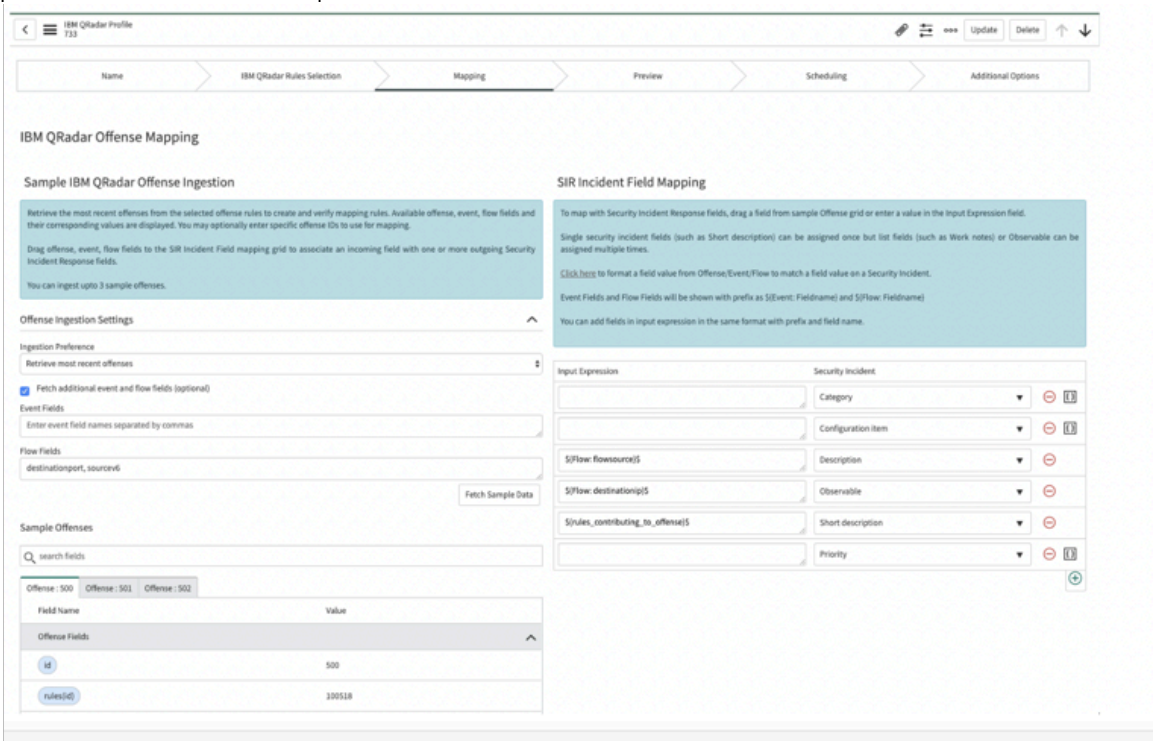
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clique **em Buscar dados de amostra**. Os campos de fluxo ou evento especificados junto com seus valores (se disponíveis) são anexados à seção Evento ou Fluxo, conforme mostrado abaixo:



Depois de buscar os dados de amostra, os valores correspondentes a esses campos são preenchidos no lado esquerdo do formulário.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de obter os dados de amostra, a próxima etapa é mapear os campos de infração para o incidente de segurança.

Mapeamento de campos de infração IBM QRadar para campos de resposta a incidentes de segurança

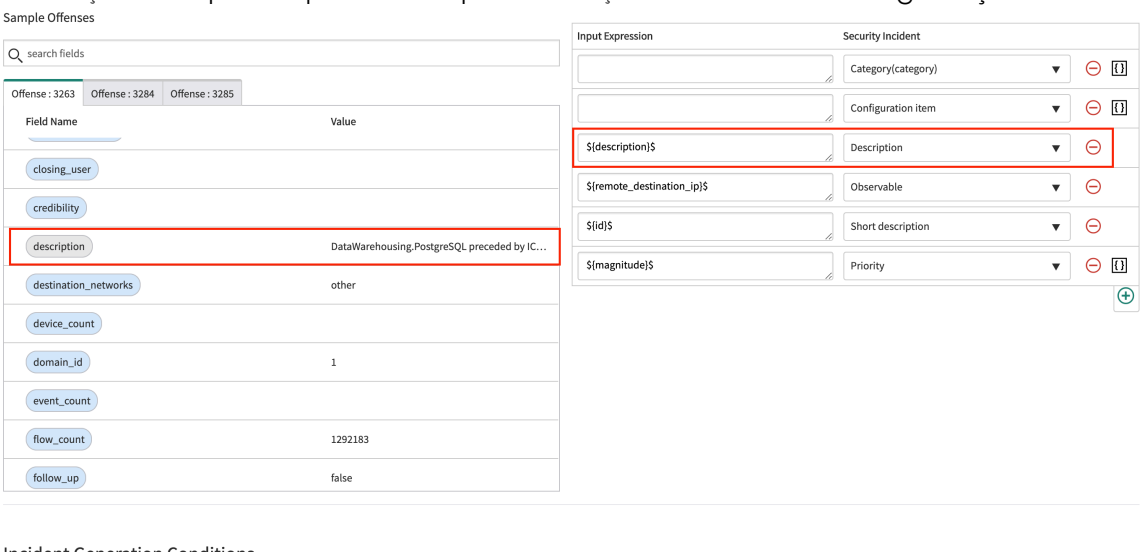
Mapeie campos de infração, evento e fluxo individuais para campos em um Now Platform SIR incidente de segurança.

Mapeamento de campo de infração

Como um usuário com a função sn_si.admin, use os campos da seção Amostra de infrações à esquerda e mapeie-os para os campos de incidente de segurança na coluna Mapeamento de campo de incidente de SIR. Edite a configuração de mapeamento arrastando os campos de infração, evento ou fluxo do lado esquerdo e soltando-os na seção de mapeamento de incidente ServiceNow SIR à direita. O mapeamento à direita associa o campo de infração de entrada a um campo de incidente de segurança de saída.

1. Depois de obter os dados de amostra, a próxima etapa é mapear os campos de infração, evento ou fluxo para o incidente de segurança. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
2. Arraste o nome do campo, por exemplo, `descrição`e solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

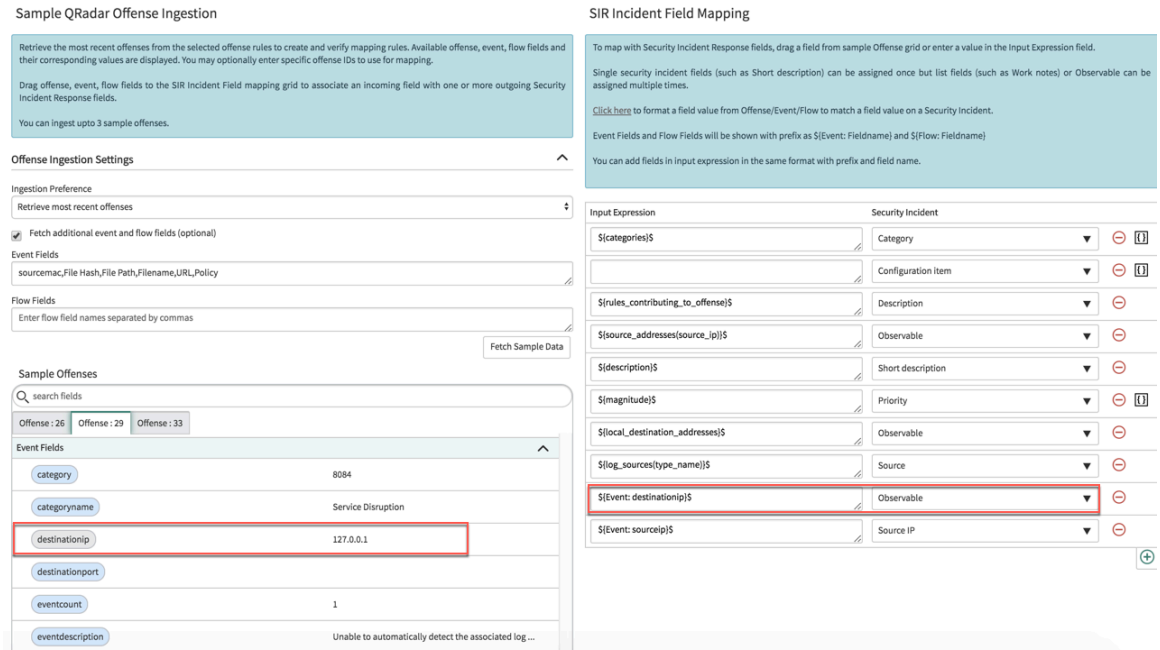
   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, a `descrição` é mapeada para o campo `Descrição` no incidente de segurança.



Nota: Se você inserir o nome do campo de fluxo ou evento manualmente na seção Expressão de entrada, deverá adicionar um prefixo como *`${Event:eventfield}$`* ou *`${Flow:flowfield}$`* antes do nome do campo que está sendo mapeado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Para ajudá-lo a garantir que nenhum campo de infração, evento ou fluxo seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação de cores dos campos de infração ajuda a rastrear os valores de infração que você já mapeou conforme eles ficam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de violação importante restante permanece não mapeada.

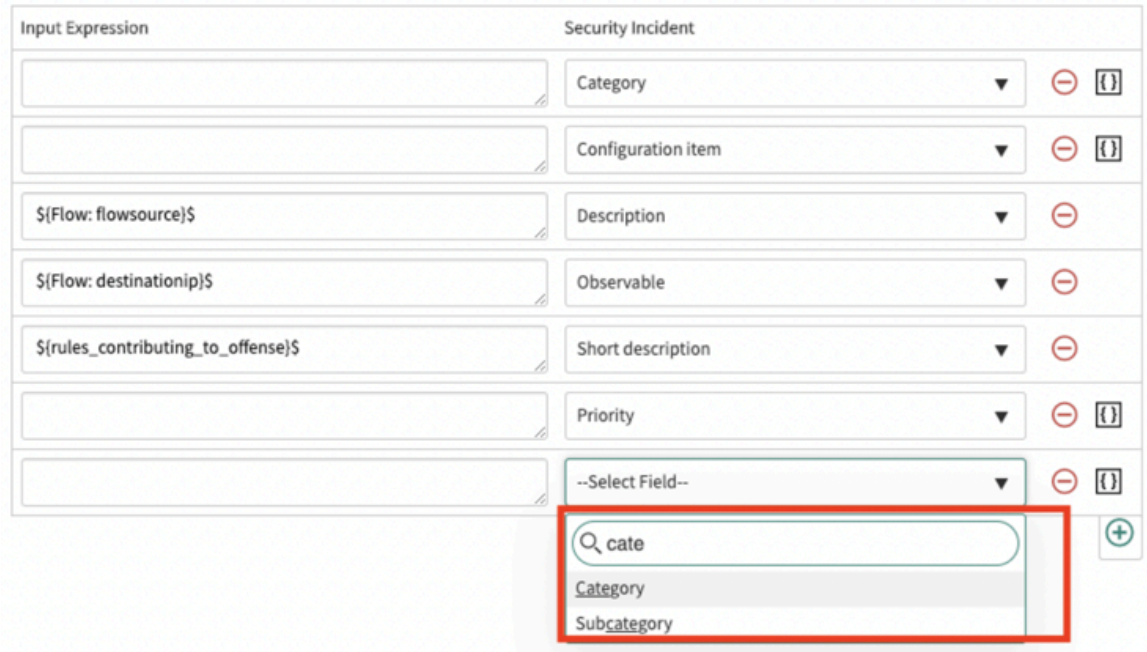
Os campos em azul claro à esquerda indicam que um campo de infração ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar uma infração, evento ou campo de fluxo de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas:
   a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de adição (+). Um novo campo é exibido.
   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

      Na lista de seleção expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, a categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores para os campos de infração no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente SIR já mapeados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, selecione o campo de infração e arraste-o e solte-o em um campo de incidente de segurança apropriado à direita.

4. Remova campos usando o ícone - ao lado do nome do campo na seção de mapeamento de campo de incidente SIR.

5. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.

Campos de infração com vários valores

- Os campos de incidente de segurança, como os campos **Categoria** e **Usuário** (por exemplo, Usuário afetado, Atribuído a) disponíveis com o produto base, não são compatíveis com vários valores.
- Os seguintes campos IBM QRadar são compatíveis com vários valores:
  - *categorias*
  - *redes_de_destino*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- *rules_contributing_to_offense*
- *usuários*

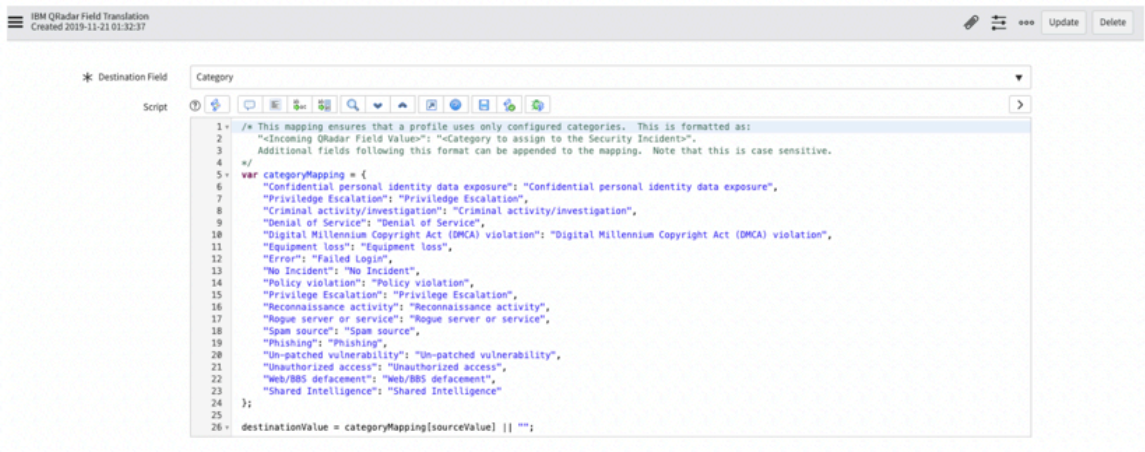
Se você precisar mapear os campos acima para quaisquer campos Security Incident Response, além dos campos de tipo IC e Observável, você deverá criar novos campos Security Incident Response do tipo **Lista** e usá-los para mapeamento.

Nota: Por padrão, somente os campos do tipo **Lista** de não referência são compatíveis.

Formatar tradução do campo

Em determinados casos, os valores do campo de infração em IBM QRadar podem não ser convertidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de Malware e Infecção de Vírus pode ter valores de campos diferentes para a categoria de origem, mas ambos os valores podem ser convertidos para uma Atividade de Código Mal-Intencionado comum no campo Categoria no incidente de segurança SIR usando o Formato Funcionalidade de tradução de campo.

Para usar o editor de script, clique no {0}. O editor de script é exibido.



Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças e retornar à página Mapeamento.

Condições de geração de incidentes

Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para que possa especificar quais infrações devem criar incidentes de segurança e quais infrações devem ser filtradas, por exemplo, infrações de baixa prioridade. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que uma violação de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até a seção **Condições de geração de incidente** no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

   O Construtor de condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

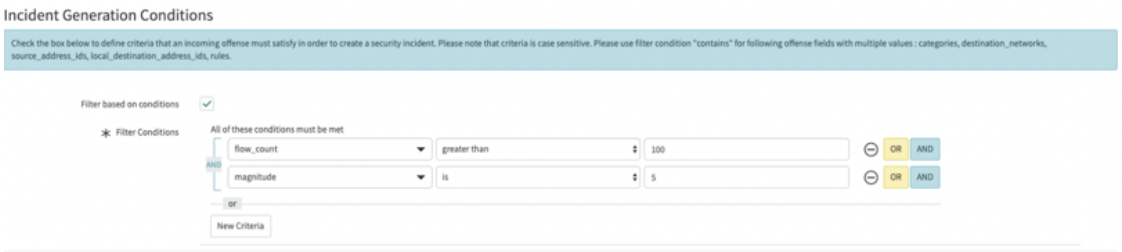
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As opções nas listas de seleção do primeiro campo no construtor de Condições de filtro correspondem aos campos que são exibidos na seção Amostra de ingestão de infração do QRadar para as infrações que você ingeriu. Esses campos são dinâmicos e mudam dependendo das infrações que você ingere. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores da infração IBM QRadar. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console IBM QRadar e revisar suas infrações para as palavras-chave.

Nota: As *categorias*, *target_networks*, *source_address_ids*, *local_destination_address_ids*,*remote_destination_ips*, *rules_contributing_to_offense*e campos de infração de *usuários* podem ter vários valores (já que os valores são armazenados em matrizes). Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar a condição de filtro " *contém*" para esses campos para garantir que os dados sejam filtrados corretamente.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   - Se **E** for selecionado, todas as condições deverão ser atendidas.
   - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.
4. (Opcional) Na segunda linha, defina uma segunda condição de filtro.

A imagem a seguir é um exemplo com duas condições que devem ser atendidas antes que os incidentes de segurança sejam criados.



Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Esse tipo de filtragem de condição de geração de incidente ajuda a restringir as infrações e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a regra subjacente ou os filtros em IBM QRadar. Se critérios de filtragem adicionais forem definidos, somente as infrações que corresponderem a todos os critérios serão mapeadas para os incidentes.

Nota: Se algum dos nomes de campo de infração tiver caracteres especiais, como aspas (“), hifens ('), sublinhados (-) ou e comercial (@), talvez esses caracteres precisem ser substituídos para fins de filtragem, mas um sufixo numérico será anexado a diferencie campos com nomes de infração duplicados. Por exemplo, se o primeiro campo de violação for `alerts.alert` e o segundo campo de violação for `alerts@alerts`, esses campos não poderão ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de infração e o campo é renomeado para `alerts@alert(1)` quando exibido na lista Condições de filtro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Critérios de agregação de infração para lidar com infrações semelhantes e evitar incidentes duplicados

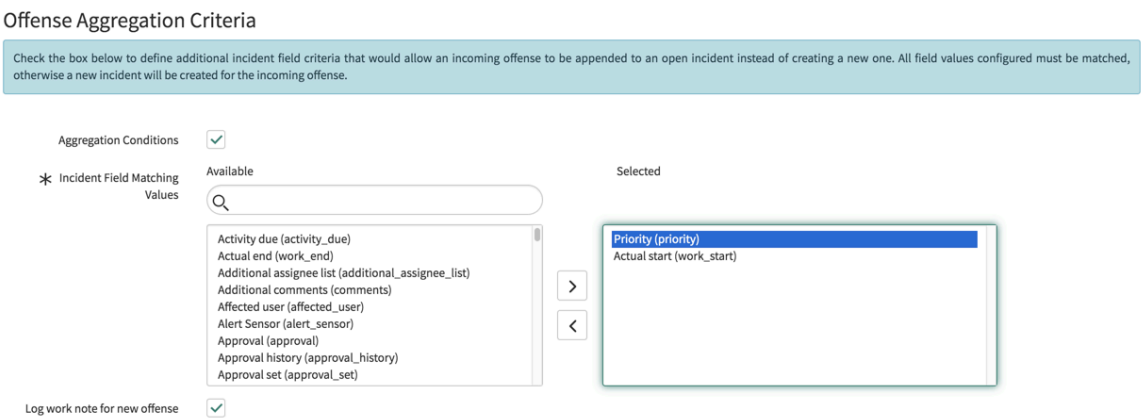
Defina critérios de agregação de infração adicionais que agregam uma infração de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes, potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de infração relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

1. Role até a seção Critérios de agregação de infração no formulário e marque a caixa de seleção **Condições de agregação** para habilitar essa opção.

   As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

2. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes em seu Now Platform e mova-os para a lista Selecionado.

   Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de infração mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de infração não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para mapeamento de campos de vários valores.



   Se uma nova infração corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, a nova infração será adicionada automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todas as infrações agregadas adicionadas em uma lista relacionada em um incidente de segurança. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que essas infrações estão sendo agregadas a incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.

3. (Opcional) Para registrar uma anotação de trabalho para uma nova infração que foi adicionada recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra que uma nova infração foi adicionada junto com um link para os detalhes da infração e quaisquer outros detalhes

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que possam ter sido adicionados ao campo de anotação de trabalho em sua seção de mapeamento.

Você mapeou com sucesso valores de uma infração IBM QRadar para campos em um incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidente. Você também anexou infrações a incidentes de segurança existentes quando os valores do campo de infração correspondem aos critérios de agregação configurados.

4. Clique em **Continuar** para continuar com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Visualizar o incidente de segurança da integração IBM QRadar

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de infração que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

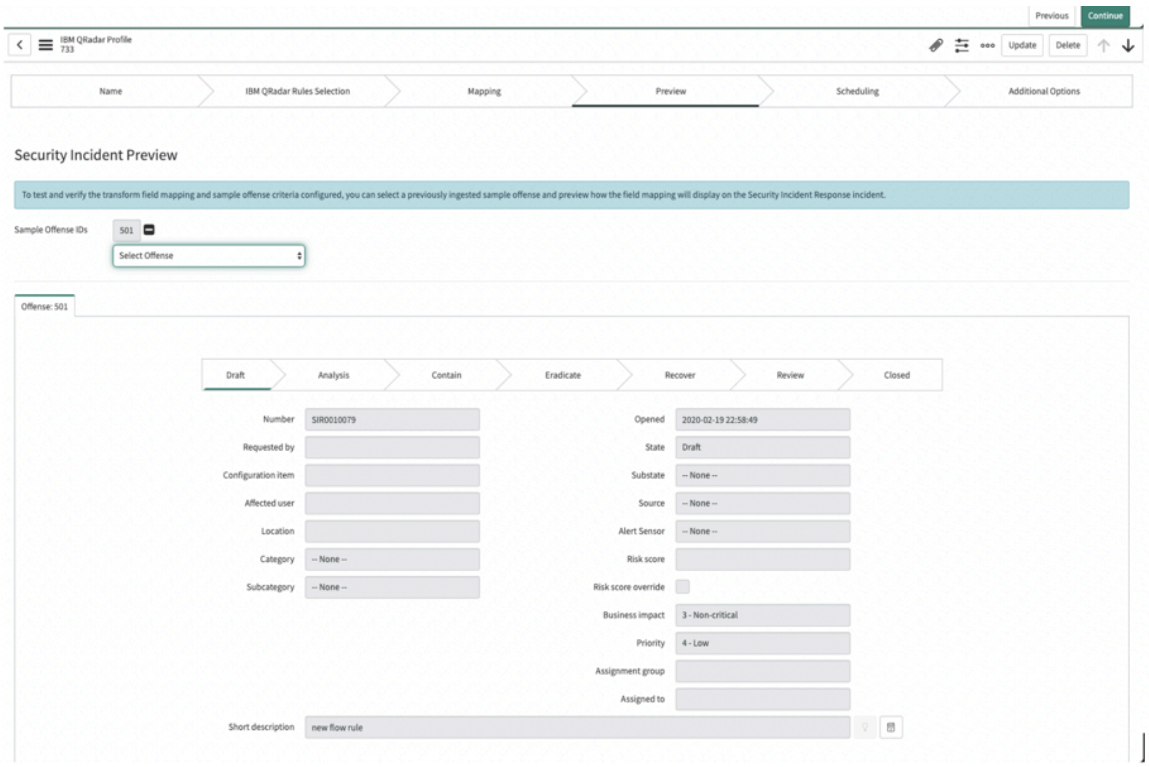
Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Na lista de seleção Amostra de IDs de infração, selecione um item.
   O incidente de segurança é exibido. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de infração no incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

O que Fazer Depois
Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campos no incidente de segurança, a próxima etapa será definir a programação.

Definir programação para a integração IBM QRadar

Você pode definir a programação para a ingestão de infração. Durante esta etapa, você pode verificar as configurações padrão para a recuperação da infração ou modificar a programação conforme necessário. Esta etapa também permite que você recupere infrações históricas usando um intervalo de datas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode escolher se deseja ingerir quaisquer infrações históricas durante a etapa de Programação. Você também escolhe com que frequência pesquisará novas infrações futuras e infrações atualizadas que correspondam à configuração do perfil.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de infração IBM QRadar pode ser afetado pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a redução da sobrecarga de pesquisa no servidor IBM QRadar com o desejo de ser notificado assim que possível quando uma infração for criada ou atualizada. Um valor

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo infrações novas e atualizadas

Quando a programação de pesquisa é definida, o trabalho agendado extrai infrações novas e atualizadas que foram extraídas anteriormente, mas não atenderam aos critérios de filtragem de incidentes. Isso oferece a flexibilidade de criar incidentes com base em critérios que podem não estar presentes quando uma infração é criada pela primeira vez, mas se tornam disponíveis após a ocorrência de uma atualização, por exemplo, durante a fase de investigação. Depois que um incidente é criado para uma violação específica, suas atualizações subsequentes são ignoradas, pois espera-se que a violação esteja sendo tratada como um incidente de segurança ativo ServiceNow. No entanto, todas as outras infrações que foram ingeridas anteriormente, mas não atenderam aos critérios de geração de incidentes, continuarão a ser extraídas e verificadas em relação aos critérios de geração de incidentes até que se tornem parte de um incidente ativo.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando as infrações são extraídas do console IBM QRadar.

Opção	Descrição
Campo de ingestão de infração contínua selecionado	Infração contínua Com base na configuração padrão, a instância Now Platform extrai do servidor IBM QRadar para infrações novas e atualizadas a cada cinco minutos. Os incidentes de segurança serão criados se forem encontradas infrações e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar a sobrecarga de pesquisa de ingestão para obter os dados mais atuais, cinco minutos é a configuração padrão. No entanto, este valor pode ser modificado para até um minuto, se necessário.
◦ Ingestão de infração contínua selecionada ◦ Definir tempo de ingestão da infração inicial	Tempo de ingestão inicial Se você quiser programar a ingestão inicial em um horário específico, siga estas etapas: ◦ Selecione os campos Ingestão de infração contínua e Definir tempo de ingestão da infração inicial. ◦ Especifique o tempo no campo Tempo de ingestão da infração inicial de entrada. A ingestão inicial ocorrerá no horário especificado aqui. As ingestões subsequentes serão baseadas na programação definida

Tradução automática

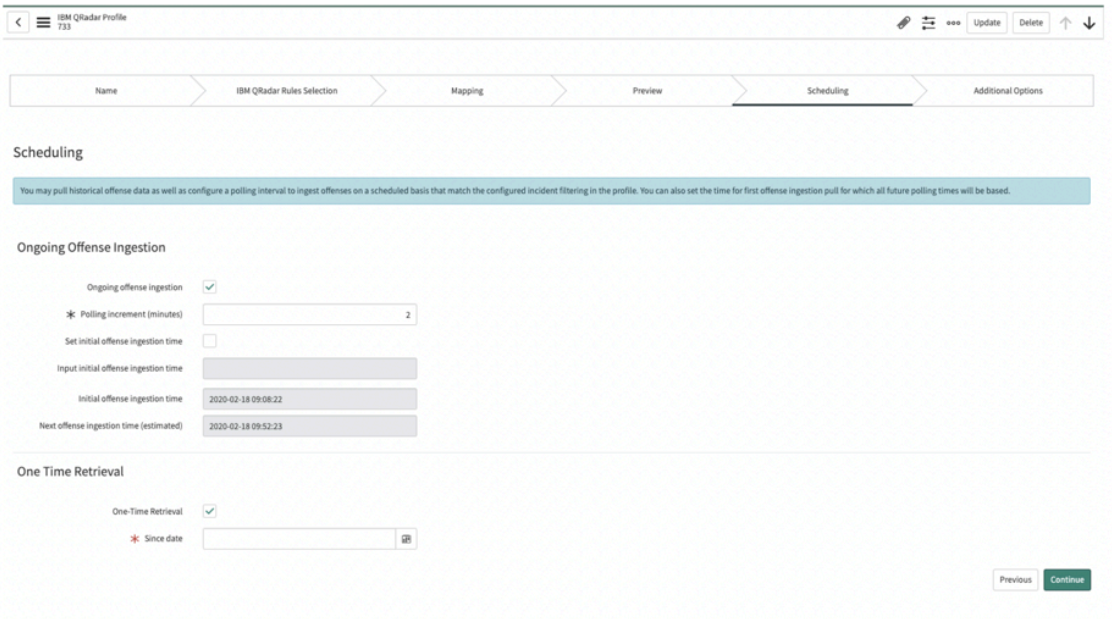
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	no campo Incremento de pesquisa (minutos). Como um exemplo para programar um horário de ingestão de infração inicial, se você tiver uma verificação de segurança diária IBM QRadar que é executada uma vez por dia às 4h no horário local, você pode configurar o perfil de infração correspondente em sua instância Now Platform para ser executado às 4:05 Hora local AM para capturar a falha de segurança imediatamente e criar um incidente de segurança. Inserir<date> `04 05 00` no campo Ingestão de infração inicial. No campo Incremento de pesquisa (minutos), insira<date> `1440` (24 horas) para programar a próxima ingestão de infração por 24 horas a partir da ingestão de infração inicial. O tempo de ingestão da infração inicial e o tempo de ingestão da próxima infração são exibidos nos campos. A ingestão inicial ocorrerá às 4h05. As ingestões subsequentes serão baseadas no intervalo de pesquisa. Nesse caso, como o incremento de pesquisa é de 24 horas, a próxima ingestão ocorrerá no dia seguinte às 4h05.
Campo de recuperação única selecionado	Recuperação Única Use esta configuração se quiser que uma extração única inclua ofensas históricas. Quando esta configuração é definida, um perfil é usado uma vez para recuperar infrações de eventos históricos que são baseados em um intervalo de datas. À direita do campo Data desde, clique no ícone de calendário. No calendário exibido, selecione a data em que deseja começar a extrair infrações. Começando com o valor de data Desde, as infrações são recuperadas até a data atual. Observe que você pode retroceder até sete dias a partir da data atual. Esta funcionalidade não tem como objetivo recuperar quantidades significativas de infrações históricas de IBM QRadar por motivos de arquivamento, mas sim uma quantidade mínima de infrações em curso que estão sendo trabalhadas ativamente no momento da ativação do perfil. Depois que as infrações forem extraídas, esta configuração não recuperará mais infra-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ções para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todas as infrações encontradas para o intervalo inserido.



3. Clique em **Continuar** para navegar até a página Opções adicionais.

Automatizar atualizações de infração e fechamento com base no status do incidente SIR

A integração IBM QRadar tem uma interface bidirecional que permite que ambas as infrações criem incidentes de segurança, bem como a capacidade de atualizar as infrações depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como número do incidente de segurança, atribuição grupo, URL do incidente de segurança e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração para atualizar as infrações quando o incidente de segurança for criado.

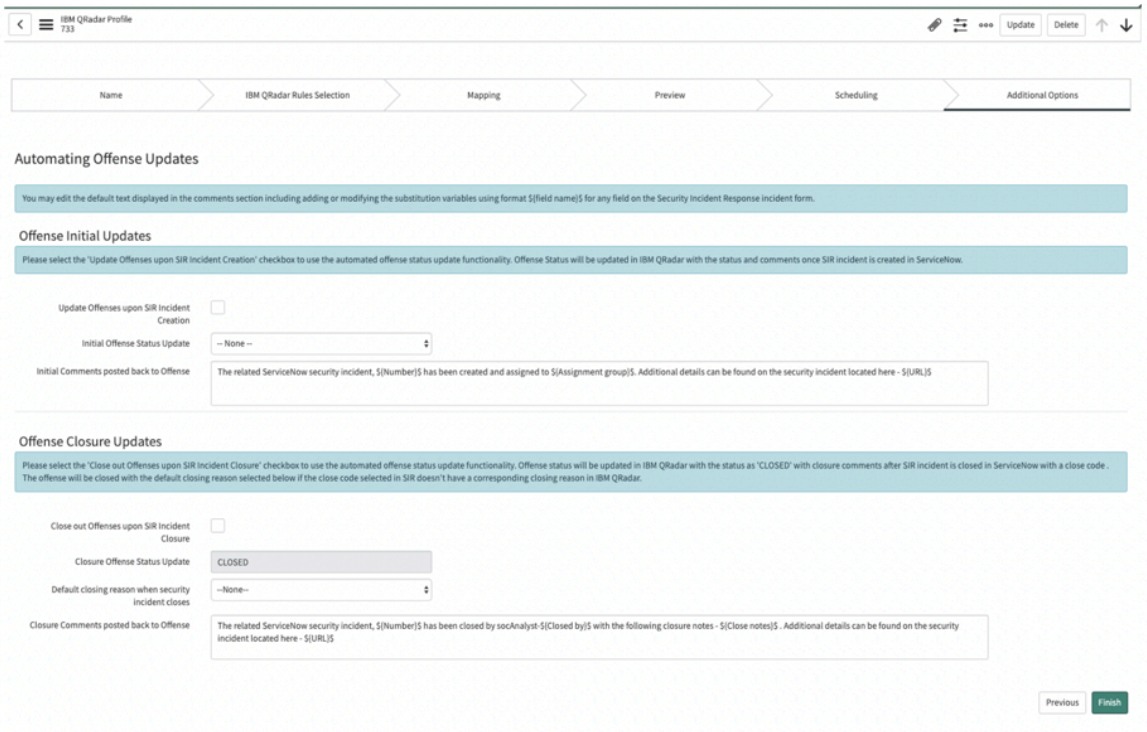
Opção ou campo	Descrição
Atualizar infrações após a criação do incidente de SIR	Selecione esta opção se quiser atualizar o status da infração e adicionar comentários adicionais quando um incidente de segurança for criado a partir da infração. Isso pode ocorrer para as infrações de gatilho iniciais que criam o incidente de segurança, bem como para as infrações agregadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
Atualização do status de infração inicial	Você pode selecionar: ◦ Aberto: o status da infração é definido como **Aberto** e um comentário é adicionado indicando que um incidente de segurança foi criado para a infração. ◦ Oculto: o status da infração está definido como **Oculto** e esta infração está oculta no painel IBM QRadar.
Comentários iniciais retornados para a infração	Com base na fase selecionada, os comentários iniciais definidos no console IBM QRadar são exibidos aqui.
Encerrar infrações após o fechamento do incidente de SIR	Selecione esta opção se quiser usar a opção de fechamento automatizado de infração. Quando o incidente de segurança é encerrado em ServiceNow com um código de encerramento relevante, o status da infração é atualizado em IBM QRadar para **Encerrado** com comentários de fechamento. **Nota:** O código de fechamento especificado para o incidente de segurança deve corresponder ao motivo de fechamento especificado no painel IBM QRadar. A infração será encerrada em IBM QRadar somente se um motivo de fechamento correspondente for encontrado. Se um motivo correspondente não for encontrado, a infração será encerrada com um código de encerramento padrão.
Comentários de fechamento retornados para a infração	Os comentários de fechamento definidos no painel IBM QRadar são exibidos aqui.
Motivo de fechamento padrão quando o incidente de segurança é fechado	O motivo padrão a ser usado quando um incidente de segurança é encerrado. Quando um incidente de segurança é encerrado, um código de encerramento (ou o motivo do encerramento) é especificado no registro do incidente de segurança. Se o código de encerramento não corresponder ao motivo de encerramento especificado em o painel IBM QRadar e você tentar fechar o incidente de segurança, uma mensagem de erro será exibida. Nesses casos, o motivo de fechamento padrão especificado aqui é usado quando o incidente de segurança é fechado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Concluir** para concluir a configuração e mover o perfil para o estado **Aguardando**.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair infrações do console IBM QRadar com base em sua programação.

IBM QRadar definições de configuração de integração

Use esta opção para modificar as IBM QRadar propriedades do sistema padrão de integração de ingestão.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Integração do IBM QRadar** > **Configurações de integração do IBM QRadar**.

Configurações de integração do IBM QRadar

Nome da Propriedade	Descrição
Imponha um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_qradar.max_si_per_day	Especifica o número máximo de incidentes de segurança que podem ser criados em 24 horas. • Tipo: inteiro • Valor padrão: 1000
Impor um limite ao número de infrações que podem ser agregadas a um único incidente. sn_sec_qradar.max_aggregation_per_si	O limite de agregação de infrações para um incidente de segurança. Por exemplo, se houver 102 infrações, as primeiras 100 serão agregadas ao incidente de segurança_1 e as 2 restantes ao incidente de segurança_2.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de integração do IBM QRadar

Nome da Propriedade	Descrição
	• Tipo: inteiro • Valor padrão: 100
Esta propriedade define o período de tempo do AQL para buscar eventos/fluxos recentes para uma infração específica. sn_sec_qradar.on_demand_recent_days_limit	Especifica o número de dias para buscar eventos ou fluxos recentes para uma infração específica. • Tipo: inteiro • Valor padrão: 7
Esta propriedade limita o número de eventos recentes obtidos para uma infração específica. sn_sec_qradar.on_demand_event_limit	Especifica o número de eventos recuperados para uma infração. Os eventos mais recentes são recuperados primeiro com base no carimbo de data/hora do evento. • Tipo: inteiro • Valor padrão: 100
Esta propriedade limita o número de fluxos recentes obtidos para uma infração específica. sn_sec_qradar.on_demand_flow_limit	Especifica o número de fluxos recuperados para uma infração. Os fluxos mais recentes são recuperados primeiro com base no carimbo de data/hora do fluxo. • Tipo: inteiro • Valor padrão: 100
Esta propriedade define o valor de tempo limite (segundos) para o AQL que busca fluxos/eventos recentes para uma infração específica. sn_sec_qradar.on_demand_timeout	• Tipo: inteiro • Valor padrão: 300
Tempo limite de IDs de pesquisa (segundos) para registros na fila para pesquisa de AQLs de uma infração. sn_sec_qradar.sid_ttl	O tempo limite do AQL para uma violação na fila antes de criar um incidente de segurança. Por exemplo, se houver 90 infrações, as primeiras 50 infrações serão processadas para dados de AQL no primeiro lote e as 40 infrações restantes no lote subsequente no mesmo intervalo de pesquisa. • Tipo: inteiro • Valor padrão: 300
Limite para controlar o número de pesquisas que podem estar em execução em IBM QRadar ao mesmo tempo que é acionado pela integração programada	Especifica o número de infrações que você busca em um único lote em um intervalo de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de integração do IBM QRadar

Nome da Propriedade	Descrição
job.sn_sec_qradar.records_threshold_in_que_for_agl	• Tipo: inteiro • Valor padrão: 50
Este é o número de dias para limpeza das tabelas de integração. sn_sec_qradar.queue_item_expire	A seguir estão as tabelas de integração: • sn_sec_qradar_events — Eventos do IBM QRadar • sn_sec_qradar_flows — Fluxos do IBM QRadar • sn_sec_qradar_offense_updates — Atualizações de infração do IBM QRadar • sn_sec_qradar_offense_to_task — Infração do IBM QRadar para tarefa • Tipo: inteiro • Valor padrão: 30
Limite de infração por execuções de trabalho agendadas por perfil em recuperação única ou ingestão contínua. sn_sec_qradar.max_offense_limit_per_run	Especifica o número de infrações que você busca na Now Platform em uma única recuperação. • Tipo: inteiro • Valor padrão: 1000
Defina esta propriedade para ativar o recurso Atualizações de infração. sn_sec_qradar.get_offense_updates	**Nota:** Habilitar esta configuração pode causar um atraso na criação de um incidente de segurança. • Tipo: verdadeiro | falso • Valor padrão: falso

Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Opcional: copiar um perfil IBM QRadar

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar os perfis para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

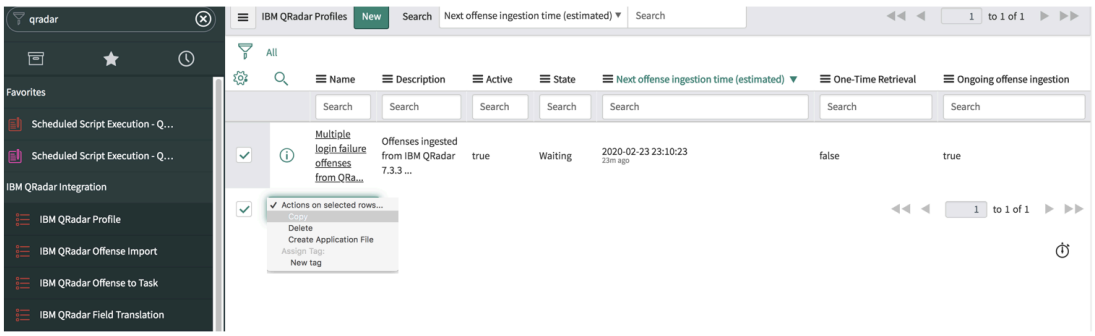
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

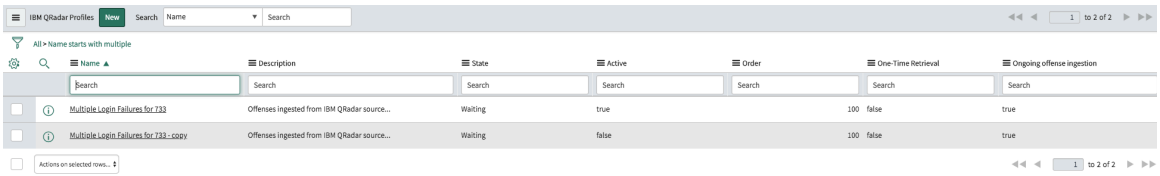
Procedimento

1. Navegar até **Todos** > **Integração do IBM QRadar** > **Perfil do IBM QRadar**.
2. Na lista Perfis do IBM QRadar exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (`verdadeiro`), a cópia está desabilitada neste ponto (`falso`). Você pode preferir editar valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.

Nota: Se você selecionar uma origem diferente para o perfil, deverá selecionar novas regras (Selecionar IBM QRadar regras) para o perfil. Mas se você usar a mesma origem e selecionar novas regras, as infrações de amostra serão apagadas.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativo** está definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Separação de domínios e ingestão de infração IBM QRadar

O Domain Separation é compatível com a ingestão de IBM QRadar infrações. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, emissão de relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

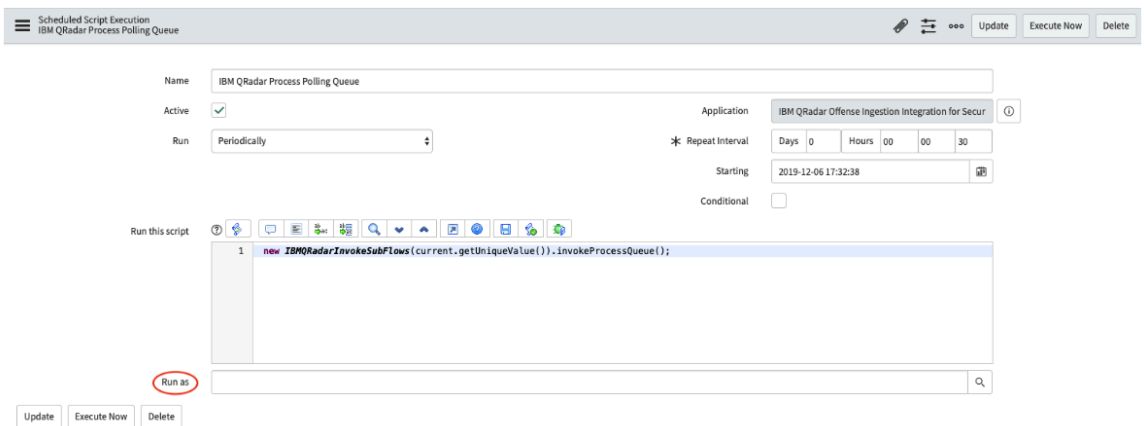
Como o Domain Separation funciona na ingestão de infração IBM QRadar

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com a função *sn_si.admin* no respectivo domínio.

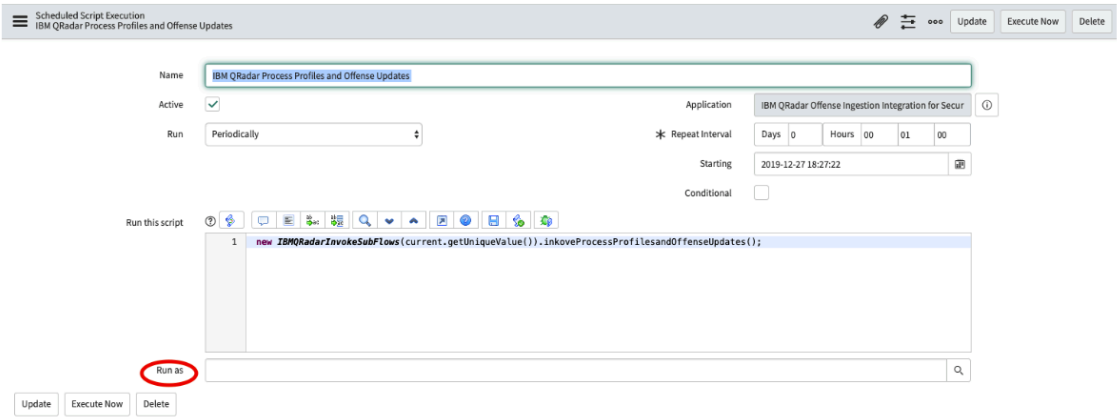
> **Nota:** Ao criar o perfil, use o seletor de domínio para selecionar o domínio específico. Não crie o usuário no domínio primário e altere posteriormente o domínio do perfil. Você deve ter um usuário específico para cada domínio do seu perfil com a função *sn_si.admin*. Use este usuário para criar ou modificar configurações no perfil.

- Desabilite os trabalhos agendados existentes.
- Replique a IBM QRadar Fila de pesquisa de processo, os IBM QRadar Perfis de processo e os trabalhos agendados de Atualizações de infração para cada domínio.
- Altere **Executar como** do usuário do sistema para o usuário com a função *sn_si.admin* no respectivo domínio e execute o trabalho agendado.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Informações relacionadas

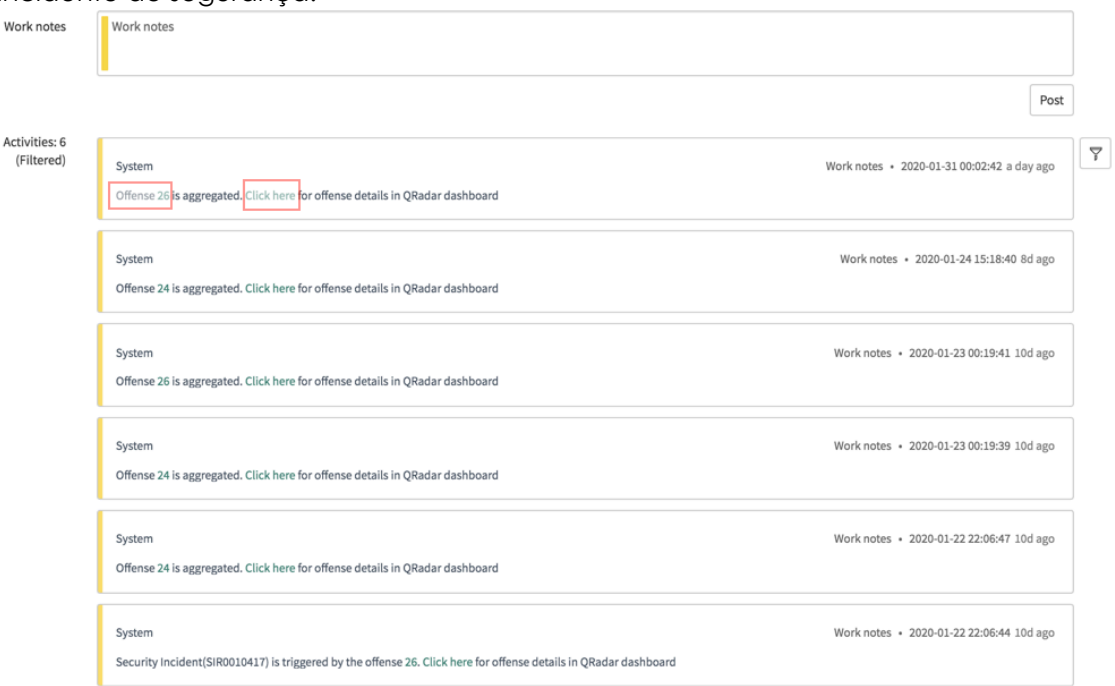
Domain Separation para provedores de serviço

Formulário do Security Incident Response após ingestão de infração

Depois que uma infração IBM QRadar é ingerida, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro do incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada com detalhes da infração que acionou o incidente de segurança.

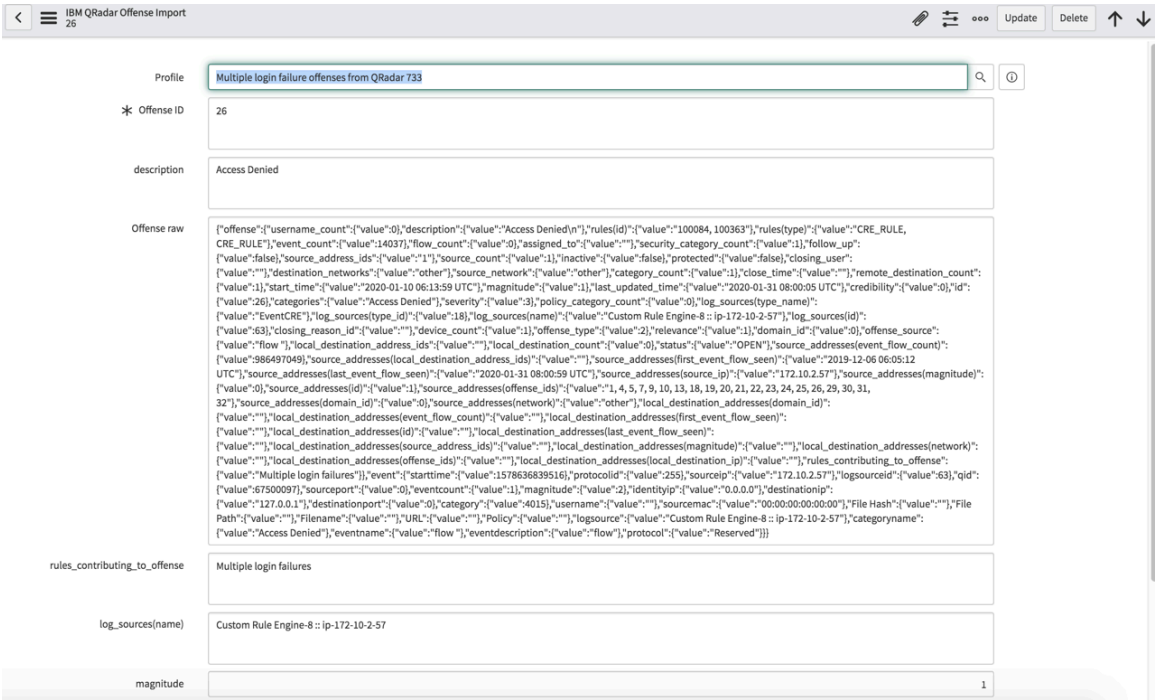


Clique no link da infração para navegar até o registro do incidente de segurança interna. O hiperlink **Clique aqui** leva você para o painel IBM QRadar, onde você pode exibir os detalhes da infração.

Se você selecionou a opção **Registrar anotação de trabalho para nova infração** nos Critérios de agregação de infração conforme descrito em Mapeamento de campos de infração IBM QRadar para campos de resposta a incidentes de segurança, uma anotação de trabalho será publicada quando a infração for agregada.

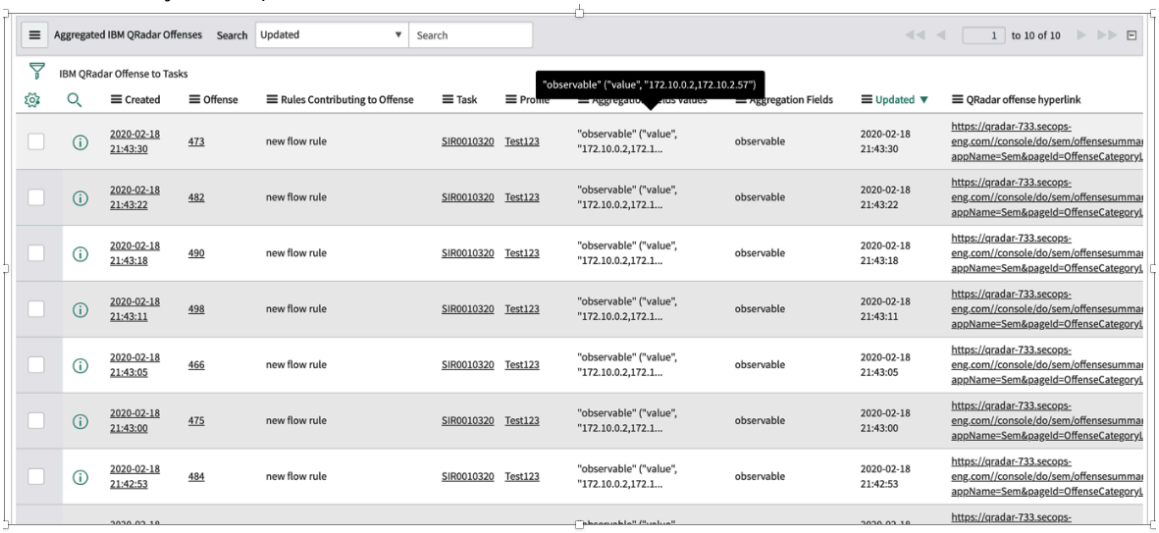
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Infrações agregadas

Clicar **Listas relacionadas** > **Infrações agregadas do IBM QRadar** para exibir as infrações agregadas ao incidente de segurança. Clique no hiperlink de infração do QRadar para exibir a infração no painel IBM QRadar.

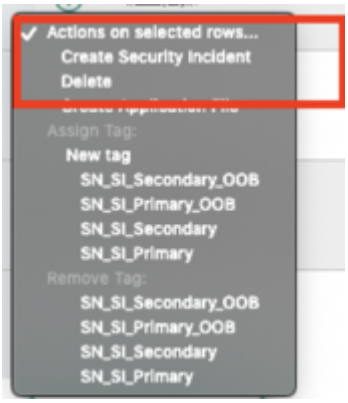


Criar incidente de segurança: selecione uma infração na lista, clique no menu **Ações** e clique em **Criar incidente de segurança**. Esta opção cria um incidente de segurança para a infração e esta infração é desagregada do incidente de segurança primário.

Excluir registro de infração: selecione uma infração na lista, clique no menu **Ações** e clique em **Excluir**. Esta opção exclui o registro de infração.

Tradução automática

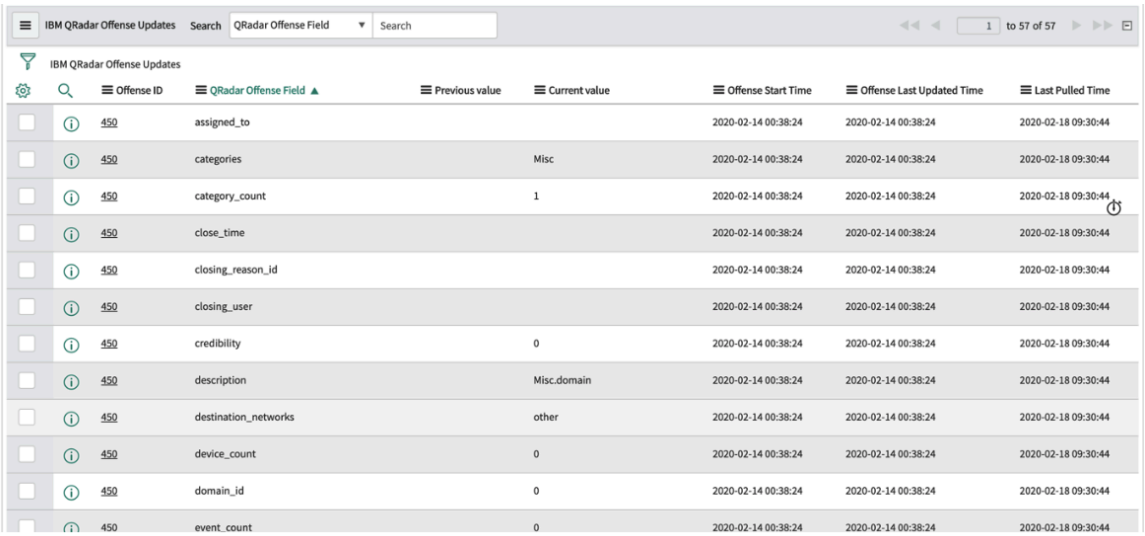
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Atualizações de infração do IBM QRadar

Mostra os campos de infração padrão e personalizados e rastreia as mudanças na infração durante cada intervalo de pesquisa. Isso é útil, pois você pode exibir todas as atualizações de infração diretamente sem navegar até o painel IBM QRadar. Todas as mudanças nos valores são exibidas nos campos Valor anterior e Valor atual.

Para habilitar o recurso de atualizações de infração, navegue até **Integração do IBM QRadar** > **Configurações de integração do IBM QRadar** e habilite **Defina esta propriedade para ativar o recurso Atualizações de infração**. Por padrão, essa configuração está desabilitada.

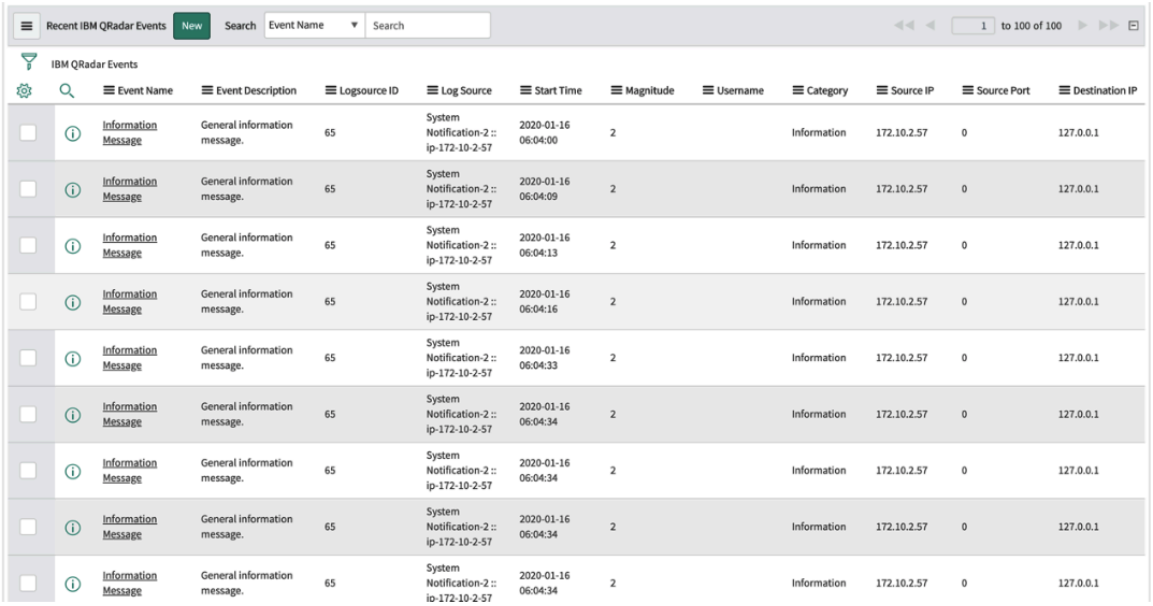


Eventos recentes do IBM QRadar

Clique na opção **Buscar eventos recentes do IBM QRadar** em **Links relacionados** para exibir os eventos IBM QRadar mais recentes.

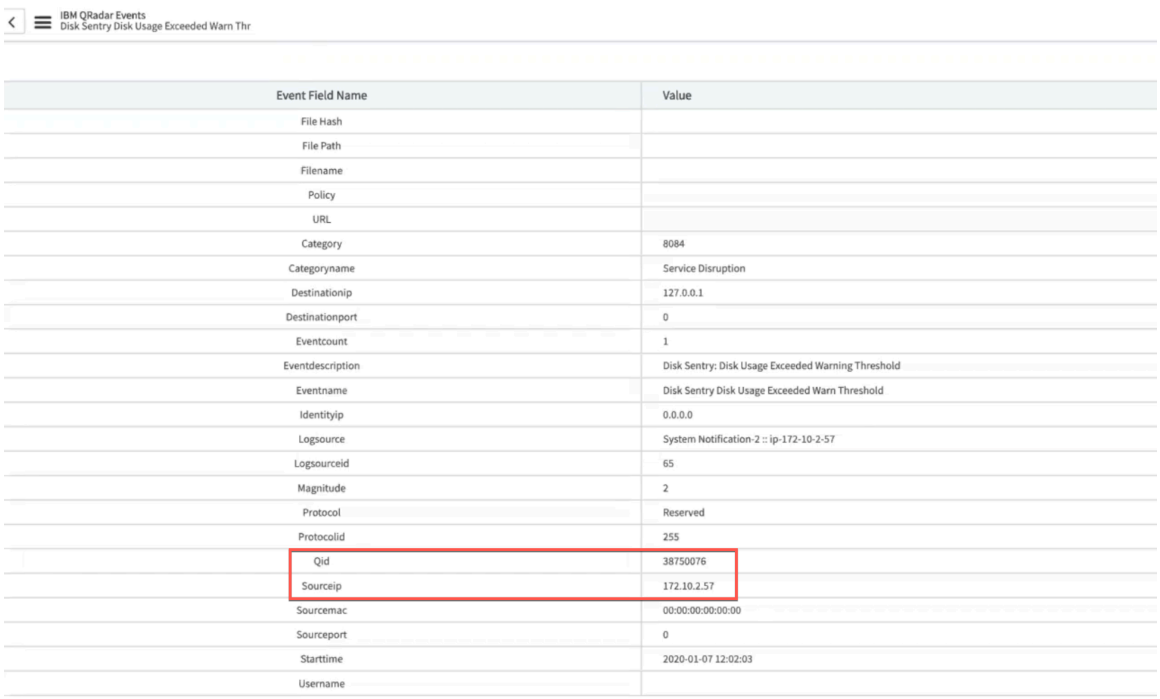
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, um número máximo de 100 eventos é exibido. Você pode modificar esta configuração padrão no IBM QRadar definições de configuração de integração.

Nota: A imagem acima mostra os campos de evento padrão associados à infração. Se você configurou e mapeou campos de evento personalizados (consulte Mapeamento de campos de infração IBM QRadar para campos de resposta a incidentes de segurança), poderá exibi-los na Exibição de lista clicando no link Nome do evento.

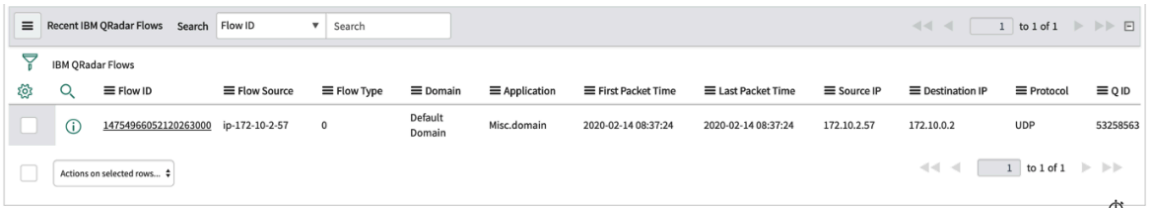


Fluxos recentes do IBM QRadar

Usando o Integration Hub e o Flow Designer, vários fluxos, subfluxos e ações estão disponíveis com a integração IBM QRadar. Quando você clica na opção **Buscar fluxos recentes do IBM QRadar** em Links relacionados, os fluxos mais recentes são recuperados. Para exibir esses fluxos, clique em **Fluxos recentes do IBM QRadar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, um número máximo de 100 fluxos é exibido. Você pode modificar esta configuração padrão no IBM QRadar definições de configuração de integração.

Nota: A imagem acima mostra os campos de fluxo padrão associados à infração. Se você configurou e mapeou campos de fluxo personalizados (consulte Mapeamento de campos de infração IBM QRadar para campos de resposta a incidentes de segurança), poderá exibi-los na Exibição de lista clicando no link do ID de fluxo.

Uso do Flow Designer e do Hub de integração com integração de ingestão de infração do IBM QRadar

Usando o Flow Designer e a funcionalidade do Hub de integração, vários subfluxos e ações foram criados como parte da integração de ingestão de infração IBM QRadar.

Os seguintes IBM QRadar subfluxos estão disponíveis:

- Validação de conexão e credencial: usado no bloco de configuração para validar o host e as credenciais na configuração inicial.
- Recuperação de regras do IBM QRadar: usada na seção Regras da configuração do perfil para recuperar todas as regras ativas em IBM QRadar. Este subfluxo é acionado de forma assíncrona.
- Buscar dados de infrações de amostra do IBM QRadar: usado na seção Mapeamento da configuração do perfil para buscar dados de amostra. Este subfluxo é acionado de forma assíncrona.
- Atualizações de status de infração do IBM QRadar: é acionado por um trabalho agendado a cada minuto e atualiza a infração em IBM QRadar quando o incidente de segurança é criado ou encerrado.
- Processar perfis de infrações de fila e trabalho agendado: é acionado por um trabalho agendado a cada minuto para extrair infrações por perfil com base no intervalo de pesquisa. Isso extrai as infrações e as enfileira na tabela de pesquisa para processamento adicional.
- Processar fila de pesquisa e pesquisa em lotes: é acionado por um trabalho agendado a cada 30 segundos para processar a fila da tabela de pesquisa.
- Buscar fluxos recentes do IBM QRadar: isso é acionado a partir do link do formulário de incidente de segurança para obter os fluxos de infração mais recentes.
- Buscar eventos recentes do IBM QRadar: isso é acionado a partir do link do formulário de incidente de segurança para obter os eventos de infração mais recentes.

Para exibir esses subfluxos, faça login como um usuário com a função `sn_si.admin` e navegue até **Flow Designer** > **Designer**. Clique no link Nome de qualquer um dos subfluxos listados acima para exibir o subfluxo em detalhes.

Solução de problemas de IBM QRadar integração de ingestão de infração

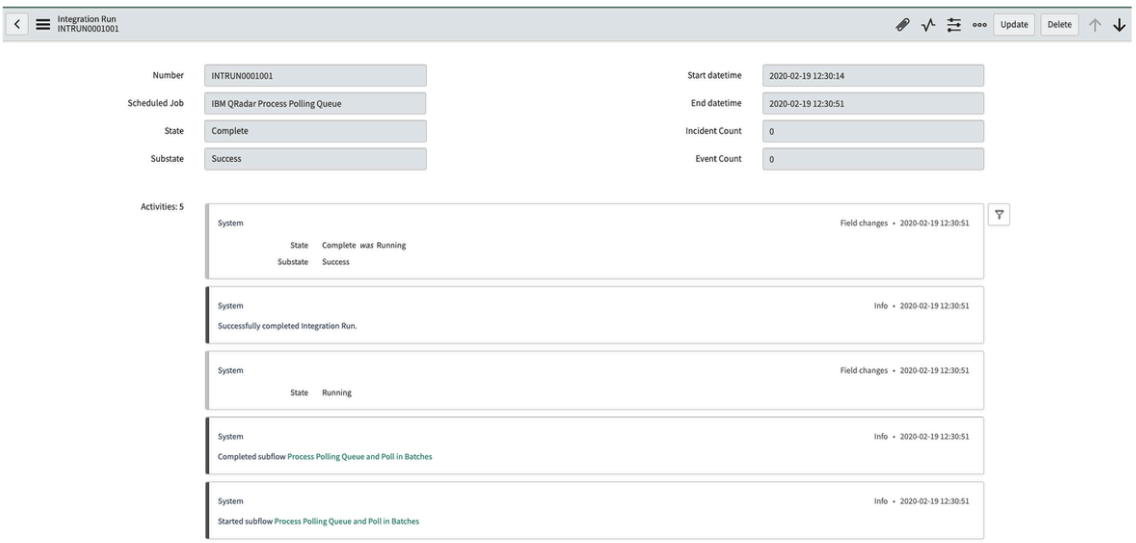
Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas à ingestão de IBM QRadar infração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Execução de integração: quando um trabalho agendado começa a ser executado, um registro de execução de integração com logs, erros e avisos é exibido. O número de infrações extraídas e o número de incidentes criados em uma execução de trabalho agendada também são exibidos. Usuários com a função sn_si.analyst podem ver se houve falha na extração de erros/perfis durante a execução da integração.

  As anotações de trabalho na execução de integração fornecem links para os subfluxos executados. Usuários com a função sn_si.analyst podem verificar a tabela `sn_event_ingestion_integration_run` em busca de erros ocorridos. Para solucionar quaisquer problemas de integração, você deve primeiro verificar a execução da integração. Os erros são registrados como anotações de trabalho nos registros de execução de integração para cada execução de trabalho agendado.



- Problemas de SSL: ao se conectar a IBM QRadar instâncias de nuvem, certifique-se de que a instância tenha um certificado de CA válido que não tenha expirado. Você pode importar o RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Consulte https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 para obter detalhes.
- Perfil incompleto: ao configurar o perfil, na seção Opções adicionais (Automatizar atualizações de infração e fechamento com base no status do incidente SIR), você deve clicar no botão **Concluir** para garantir que o perfil seja movido para o estado Aguardando, indicando que está aguardando a ingestão.
- Validar perfil: para validar se a integração está funcionando corretamente, verifique os estados do perfil, a data da última extração do perfil, a tabela de importação de infração, os registros da tabela de infração para tarefa.
- Configuração do MID Server: se você estiver instalando a aplicação IBM QRadar no local, após configurar o MID Server, deverá criar uma aplicação de MID Server. O nome da aplicação do MID server deve ser usado no bloco de configurações de integração em vez do nome do MID server.

  Nota: O tempo limite de serviço do MID padrão é de 30 segundos. Para ver instruções sobre como desabilitar o período de tempo limite, consulte <link>. Observe que esta é uma mudança em todo o sistema e pode afetar outras integrações.

- Atualizações de infração: se você tiver habilitado a propriedade *sn_sec_qradar.get_offense_updates* e observar um atraso na criação de incidentes

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de segurança, desabilite a propriedade. Não habilite esta propriedade quando o intervalo de pesquisa for baixo e a carga de infrações no QRadar for alta, pois isso aumenta a carga da fila.

- Evento ausente, dados de fluxo, remote_ip ou dados de usuários em um incidente de segurança: se você observar que eventos, dados de fluxo, remote_ip ou dados de usuários estão ausentes em um incidente de segurança, aumente o tempo limite (segundos) do parâmetro *sn_sec_qradar.sid_ttl*. O aumento da duração atrasa a criação do incidente de segurança até que os AQLs concluam a análise de cada violação.
- Tempos limites: se você exibir erros de tempo limite nos logs da aplicação, revise e modifique as seguintes ações do Flow Designer:

Ações do Flow Designer

Parâmetros	Ação
Buscar exemplos de infrações `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);`	Revise e atualize a duração em milissegundos.
Buscar exemplos de infrações `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);`	Adicione um parâmetro para *executeAction* e insira a duração em milissegundos.
Buscar infrações para registros de perfil e fila na tabela de pesquisa `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);`	Revise e atualize a duração em milissegundos.
Wrapper para REST de conexão de teste `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);`	Adicione um parâmetro para *executeAction* e insira a duração em milissegundos.
Wrapper para validar REST de credenciais de API `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);`	Adicione um parâmetro para *executeAction* e insira a duração em milissegundos.
Etapa REST para atualizações de infração do IBM QRadar `var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, entradas,60000);`	Revise e atualize a duração em milissegundos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

IBM QRadar - Incident Enrichment Integration

A integração IBM QRadar - Incident Enrichment pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.

Explorar

Integrações do Security Incident Response

Configurar

- Introdução ao IBM QRadar - Incident Enrichment integration
- Criar registros de configuração de pesquisa de detecções

Usar

- Executar uma pesquisa de detecções
- Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções
- Operações de segurança - Fluxo de trabalho de pesquisa de detecções do QRadar
- Exibir detalhes da pesquisa de detecções
- Exibir resultados da pesquisa de detecções

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Fazer ou responder a perguntas na comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Introdução ao IBM QRadar - Incident Enrichment integration

IBM QRadar é um produto de gestão de eventos e informações de segurança empresarial (SIEM) que se integra facilmente com Operações de segurança. Antes de poder usar a integração IBM QRadar - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL Base de API e a Chave de API apropriadas.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

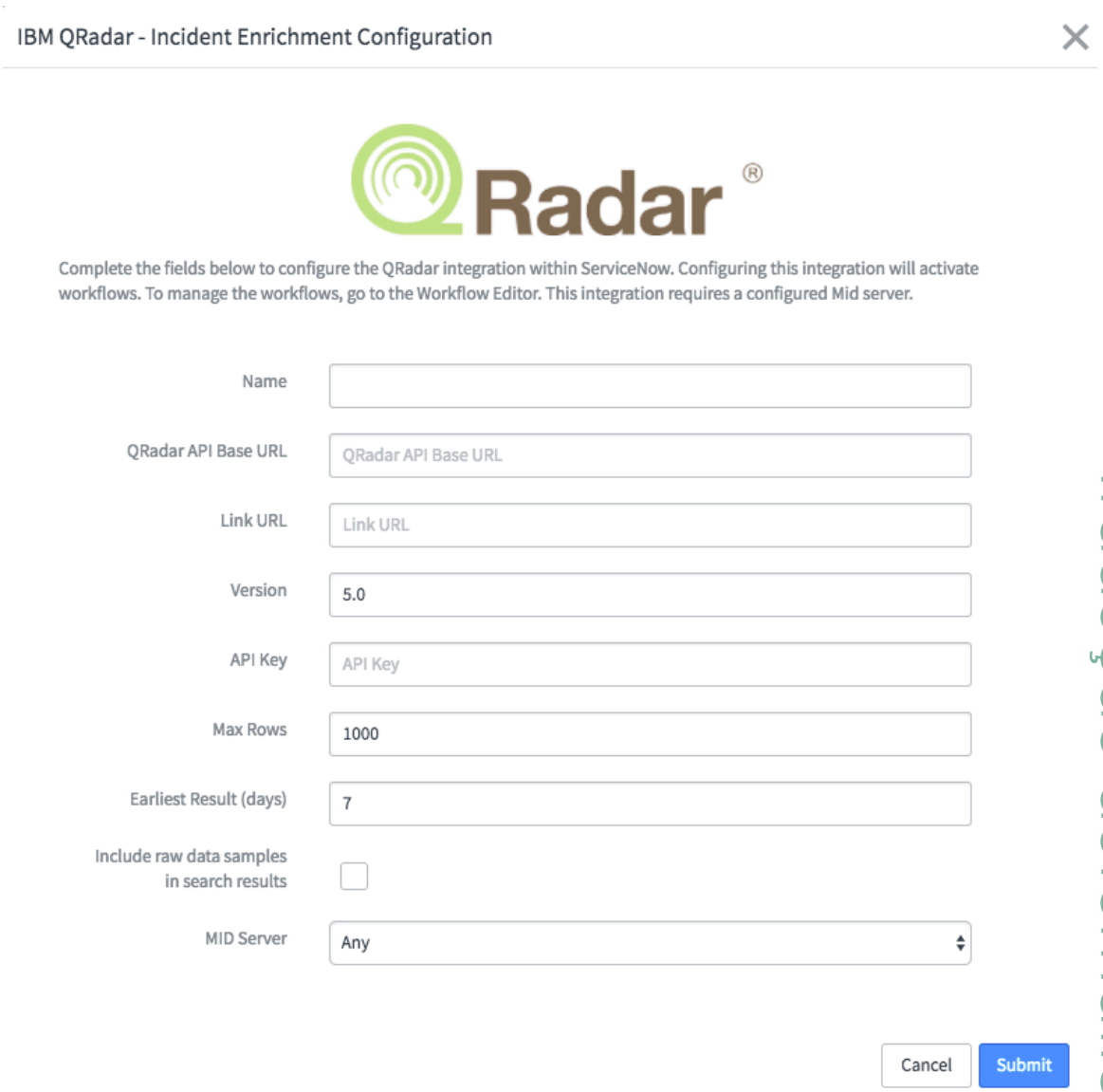
1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse IBM QRadar e obtenha a URL base da API e a chave de API no seu perfil IBM QRadar.
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As integrações de segurança disponíveis aparecem como uma série de cartões.

4. No cartão IBM QRadar - Aprimoramento de incidentes, clique em **Novo**.



5. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL de Base de API do QRadar	A URL base que você adquiriu do site IBM QRadar.
URL do Link	[Opcional] A URL do link que vincula a uma instância IBM QRadar, quando disponível.
Versão	A versão IBM QRadar ; 5.0 é o padrão.
Chave de API	A chave de API que você obteve do site IBM QRadar.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

LogRhythm Visão geral

A flexibilidade de mapeamento desta integração fornece a um analista visibilidade para eventos e dados de alarme relacionados que podem ser integrados em Now Platform incidentes de segurança para investigação e correção adicionais.

Os perfis de alarme são criados em sua instância Now Platform para personalizar como diferentes LogRhythm campos de alarme são exibidos em um incidente de segurança Now Platform. É fornecido um mapeamento padrão de campos de alarme, que pode ser editado para atender às necessidades específicas do cliente.

A figura a seguir é um exemplo de um ambiente do cliente. Quando um evento aciona a criação de um incidente de segurança na instância Now Platform®, uma solicitação é enviada da sua instância Now Platform® para extrair alarmes do console do cliente LogRhythm por meio de um MID Server ou mesmo sem ele.

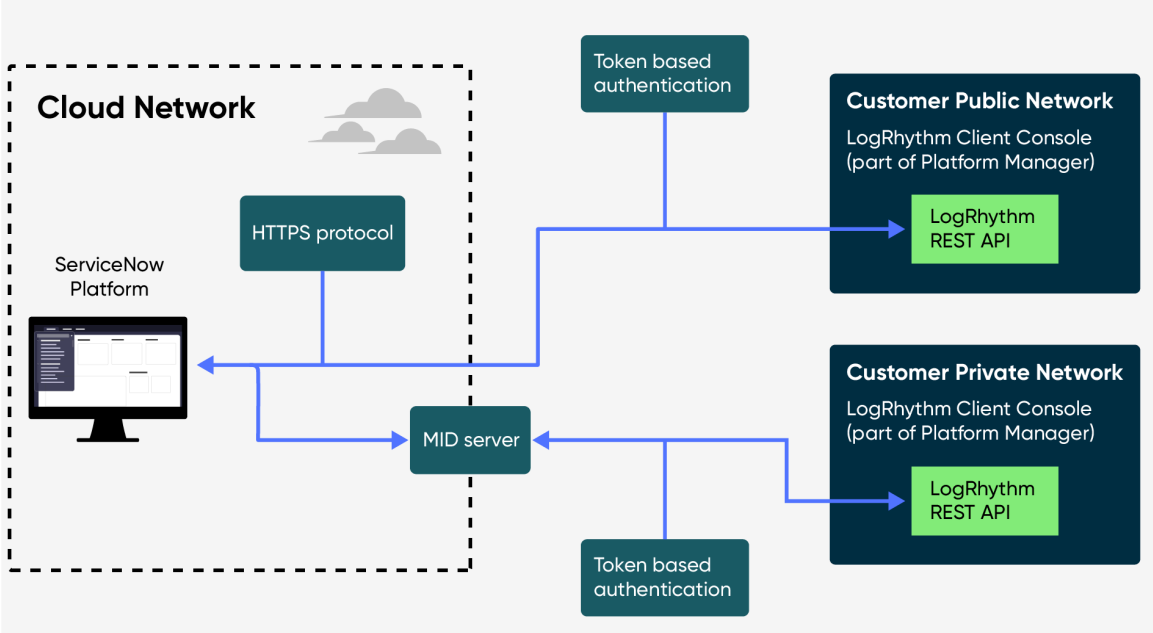
A chave de REST API é usada pelo Now Platform® para autenticar com o LogRhythm Console do cliente. Esta conexão permite que sua instância Now Platform extraia alarmes LogRhythm individuais com base em perfis configurados.

A REST API é usada para coletar detalhes da mensagem não acessados pela REST API.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração com LogRhythm



Principais recursos

Esta integração inclui os seguintes recursos principais:

- Flexibilidade para criar vários perfis de alarme para diferentes tipos de alarme, como phishing e malware.
- Mapeamento de arrastar e soltar de valores de campo de alarme LogRhythm] para campos de incidentes de segurança SIR associados.
- Uma visualização do layout de incidente de segurança SIR com base em alarmes de amostra LogRhythm.
- Ingerir alarmes históricos, bem como alarmes futuros contínuos em intervalos configuráveis.
- Fechamento de alarme LogRhythm automatizado após fechamento de SIR incidente. Um URL para o incidente SIR, bem como um ID de incidente, são fornecidos para facilitar a referência.

Versões compatíveis do Now Platform

Esta integração é compatível com o Quebec ou versões posteriores do Now Platform®.

Versões compatíveis do LogRhythm

Esta integração é compatível com LogRhythm 7.8 ou posterior. As versões anteriores não são compatíveis devido a limitações de API.

Nota: Os tópicos a seguir estão numerados. Para uma instalação sem problemas e para ajudá-lo a verificar os resultados esperados, siga os tópicos na ordem em que são apresentados.

Configurar a REST API para LogRhythm

Você usa a chave de REST API LogRhythm para coletar detalhes adicionais do evento para campos de alarme individuais. A chave de API fornece detalhes que não estão disponíveis usando a LogRhythm REST API.

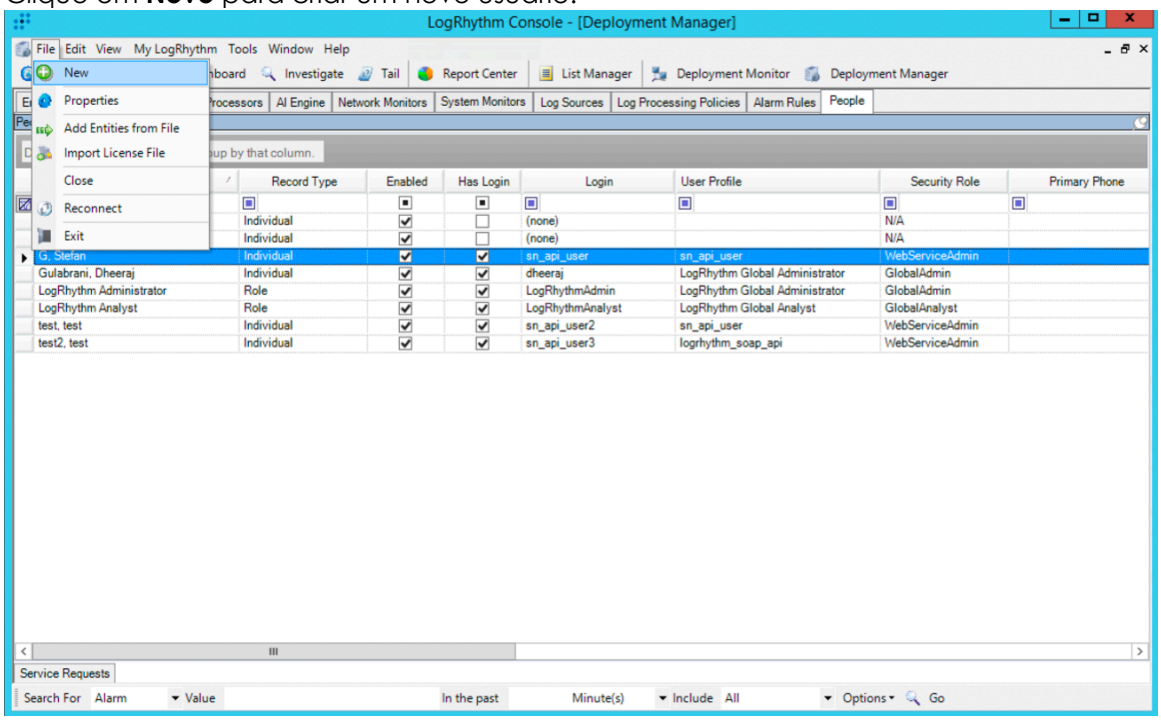
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

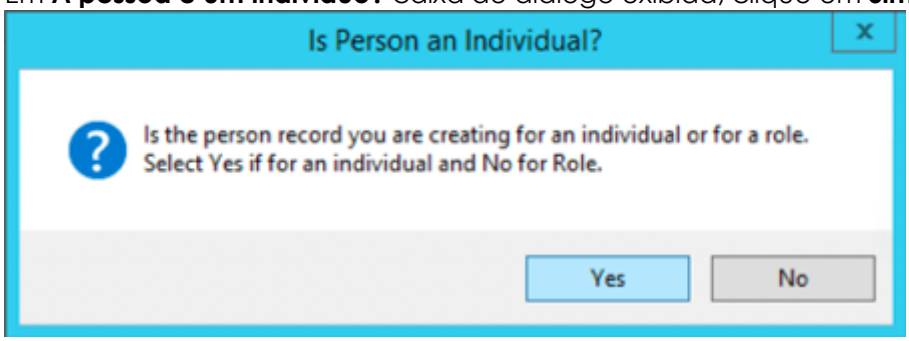
Antes de Iniciar
Função necessária: LogRhythm Administrador do Console do cliente/Gerente de plataforma

Por Que e Quando Desempenhar Esta Tarefa
Esta tarefa é realizada no LogRhythm Console do cliente. Configure a LogRhythm REST API antes de instalar o plug-in do ServiceNow Store.

Procedimento
1. Navegue até o LogRhythm Console do cliente e selecione o menu **Arquivo**.
2. Clique em **Novo** para criar um novo usuário.



3. Em **A pessoa é um indivíduo?** caixa de diálogo exibida, clique em **Sim**.

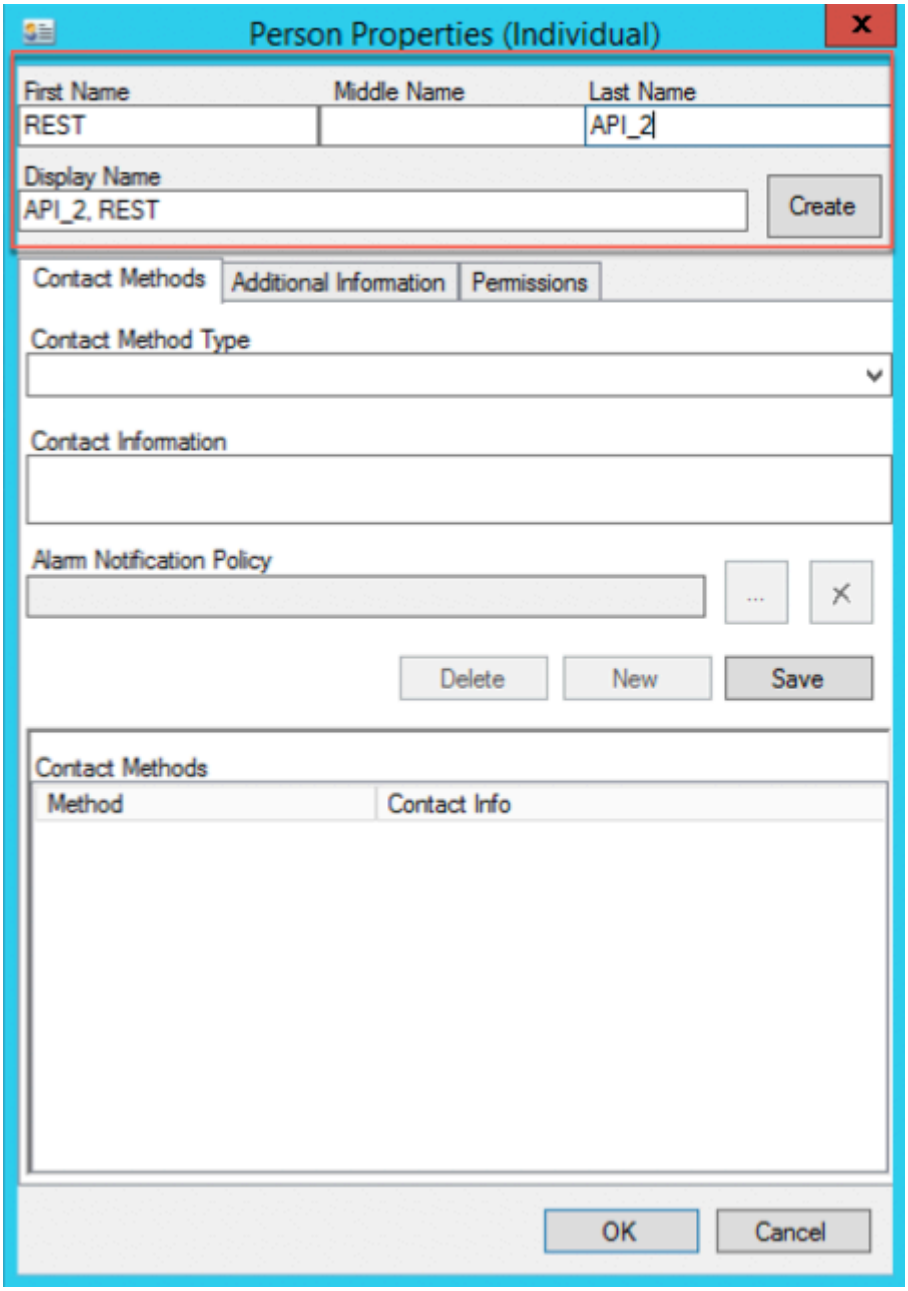


4. Na caixa de diálogo Propriedades da pessoa exibida, preencha os campos Nome.

   Use um nome diferente para a LogRhythm REST API do que você usou para criar a REST API, por exemplo, `REST API_2`.

Tradução automática

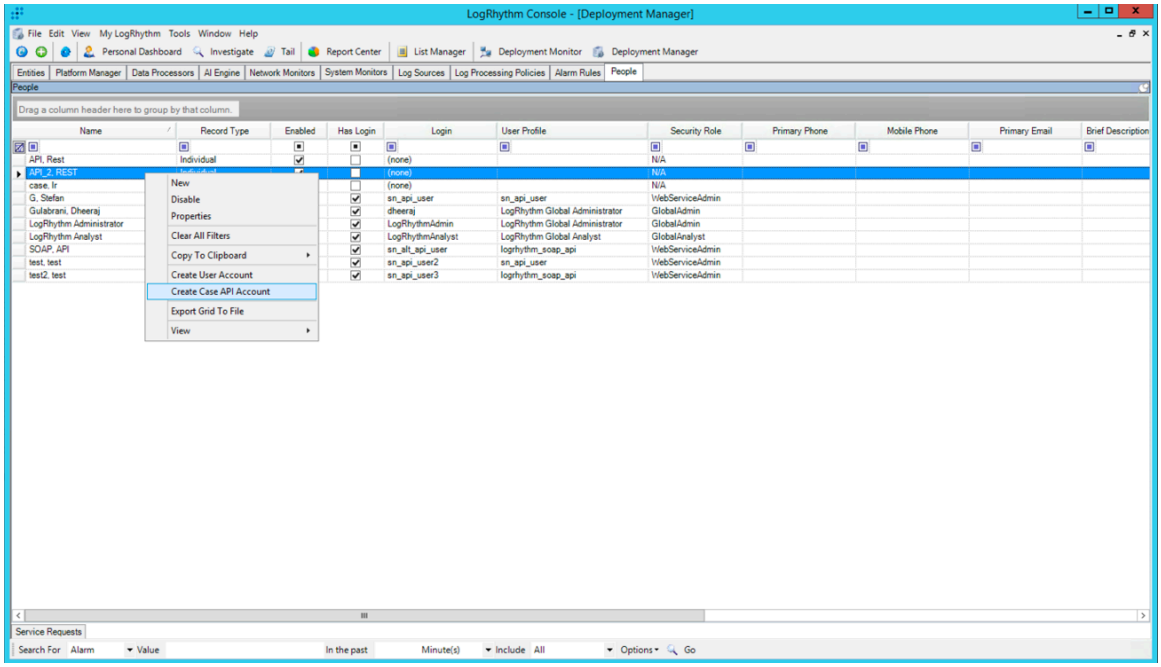
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **OK**.
6. Clique com o botão direito do mouse na nova listagem na coluna Nome (**API_2_REST**) e, na lista de seleção, selecione **Criar conta de API de caso**.

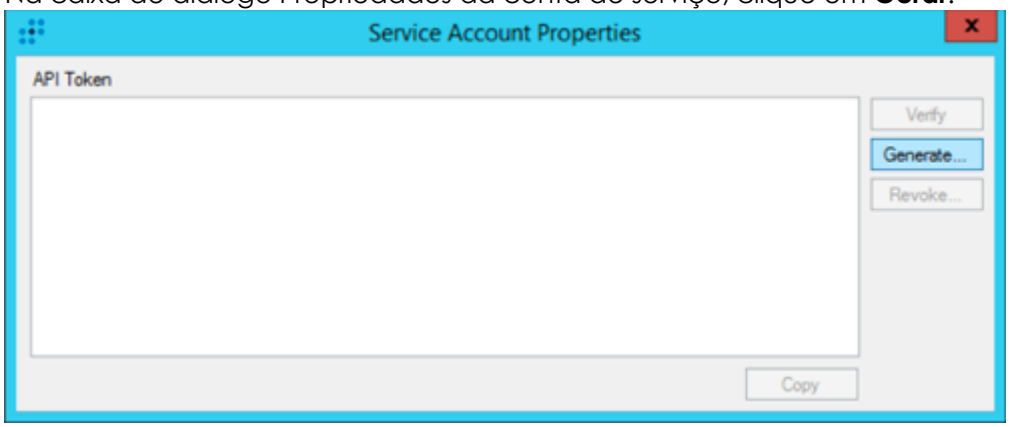
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

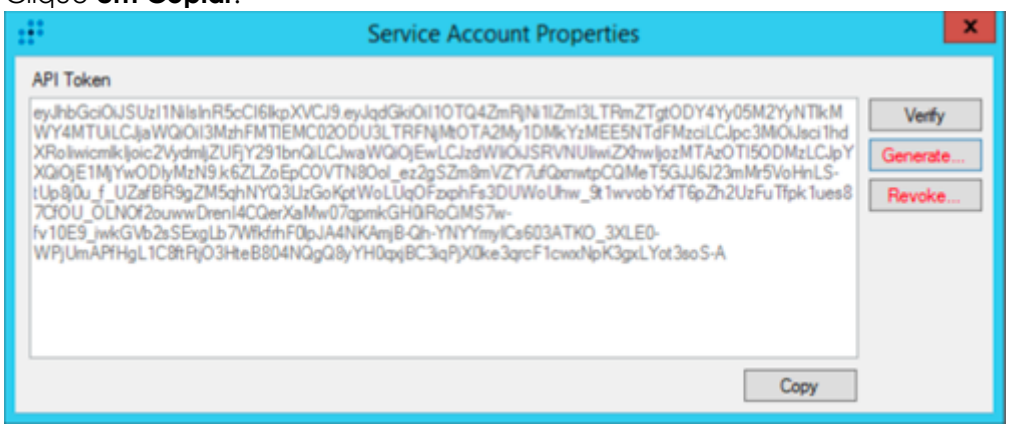


Nota: A API de caso não é usada, mas as credenciais da conta da API de caso e da LogRhythm REST API são as mesmas.

7. Na caixa de diálogo Propriedades da conta de serviço, clique em **Gerar**.



8. Clique **em Copiar**.



Agora você configurou a LogRhythm REST API. Você cola a cadeia de caracteres copiada na etapa anterior na sua instância Now Platform no campo LogRhythm Token de REST API durante as etapas de configuração listadas em Instalar o plug-in e configurar LogRhythm.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Agora você está pronto para Instalar o plug-in e configurar LogRhythm.

Instalar o plug-in e configurar LogRhythm

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que a aplicação se integre corretamente com Operações de segurança no Now Platform®.

Antes de Iniciar

Função necessária: administrador

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas. A versão LogRhythm mais recente é 7.8 ou posterior.

Nota: Seus perfis de alarme existentes não serão mais compatíveis com a versão LogRhythm mais recente, portanto, você precisa criar novos perfis de alarme e executar as configurações necessárias.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o plug-in da aplicação e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O (sn_si.admin) supervisiona as seguintes tarefas: ◦ Nomeia, cria e edita perfis de alarme. ◦ Mapeia e filtra alarmes: identifica LogRhythm alarmes específicos que criam incidentes de segurança e configura como esses campos de alarme são mapeados para um Now Platform® incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Ingere alarmes históricos e programa alarmes extraídos. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Esta função também tem acesso ao módulo Operações de segurança. • O analista de incidentes de segurança (sn_si.analyst) responde a incidentes de segurança que são criados com base nas configurações de perfil de alarme.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Obtenha um nome de usuário e senha de API LogRhythm e verifique se você está usando a versão LogRhythm 7.8 ou posterior.	Visite o site do produto para obter informações sobre chaves de API e para criar uma conta: Site do LogRhythm Enterprise . As contas de usuário, credenciais e certificados devem ser configurados corretamente antes de instalar a aplicação. A integração requer LogRhythm versão 7.8 ou posterior e as LogRhythm REST APIs. Consulte Configurar a REST API para LogRhythm.
Verifique se você instalou e configurou um MID Server.	Um MID Server é necessário em seu ambiente Now Platform. Consulte o site de documentação do produto da ServiceNow para obter informações sobre como instalar e configurar MID Servers.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Rome e as versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .

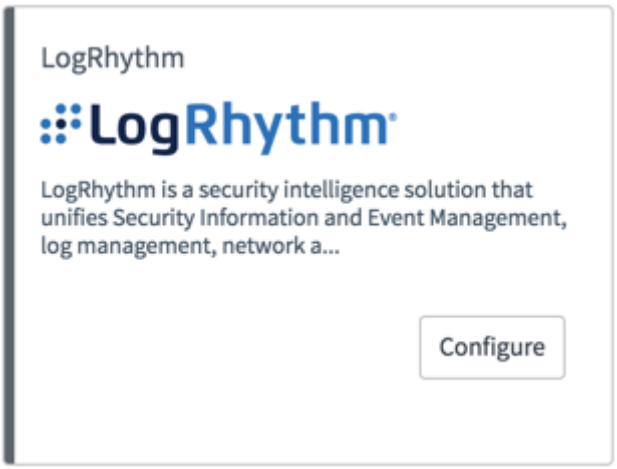
Importante: Se você tiver problemas de conectividade com o console do cliente LogRhythm, consulte Verificar conectividade para LogRhythm.

Tradução automática

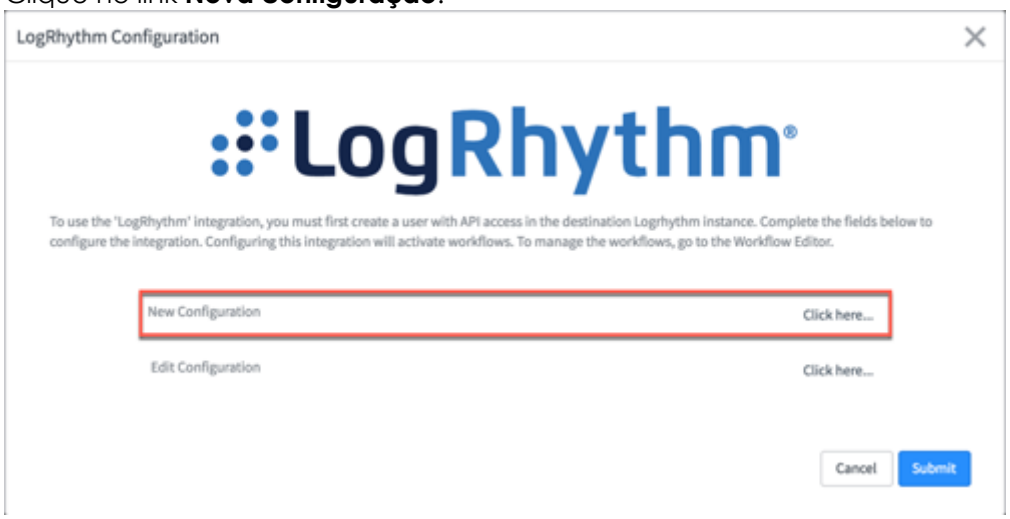
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.
2. Quando a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco LogRhythm.
3. Clique em **Configurar**.



4. Clique no link **Nova configuração**.



5. No formulário, preencha os campos:

Configuração da LogRhythm

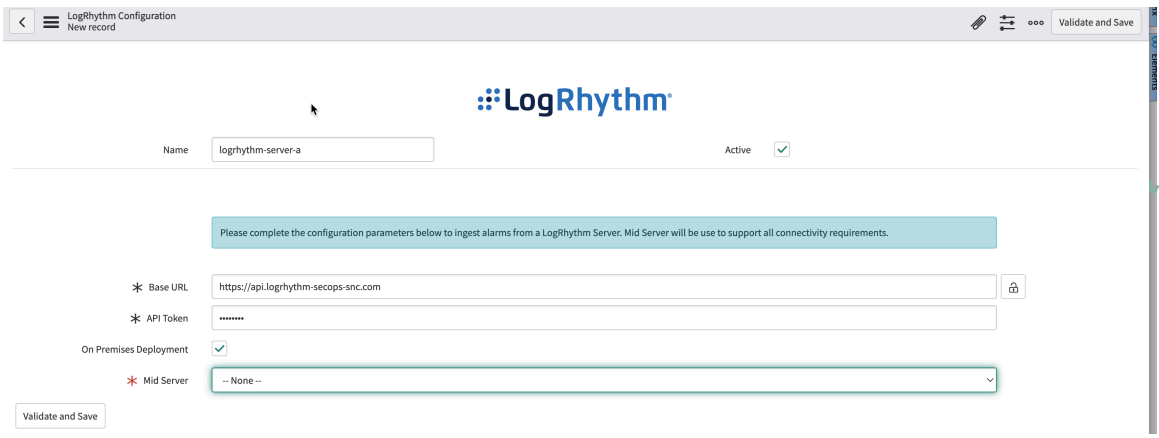
Campo	Descrição
Nome	LogRhythm nome do servidor, por exemplo, `logrhythm-server-a`.
URL base	URL base que hospeda a LogRhythm REST API. O MID Server permite o acesso à rede onde o Console do cliente LogRhythm está hospedado. Este URL é onde o servidor LogRhythm está hospedado nessa rede. Clique no ícone de cadeado no lado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	direito para editar o campo e inserir o texto para um URL, por exemplo, `https://logrhythm.secops-eng.com:8501/`.
Token de API	Insira o token que está associado à REST API que você criou no LogRhythm Console do cliente.
Implantação no local	Opção para selecionar se for uma implantação LogRhythm no local.
MID Server	MID Server específico que está configurado em seu ambiente. Somente os MID Servers que estão ativos e foram validados estão disponíveis nesta lista de seleção.

A figura a seguir é um exemplo de um formulário preenchido.



6. Clique **em Validar e salvar**.
   Depois que a validação for concluída com sucesso, uma mensagem será exibida e a página LogRhythm Configurações será recarregada. A próxima etapa é criar um perfil de alarme.

O que Fazer Depois

Depois de concluir com sucesso a validação, a próxima etapa é para Como criar um perfil de alarme para LogRhythm.

Como criar um perfil de alarme para LogRhythm

Em um perfil de alarme que você cria e nomeia, você especifica quais alarmes deseja extrair do LogRhythm Console do cliente. Você também define como eles são mapeados para campos em um Now Platform incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Com base no perfil de alarme configurado, um perfil de alarme pode ingerir todos os tipos de alarmes prontos para uso, mas você pode usar critérios de filtro para ingerir tipos específicos de alarmes. Usando esta integração Now Platform, todas as regras de alarme configuradas ou específicas com base no perfil criado são ingeridas. Regras de alarme, como somente alarmes de nível de alto risco, podem ser filtradas para especificar quais alarmes devem criar incidentes de segurança. Antes que os incidentes de segurança sejam

Tradução automática

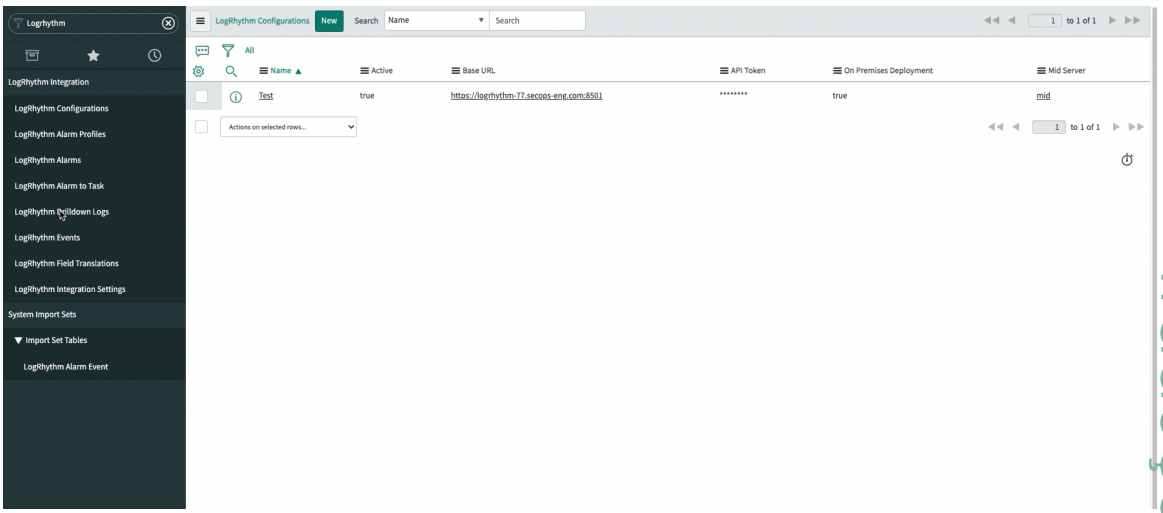
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

criados, os valores de campos individuais nos alarmes filtrados são mapeados para os campos correspondentes no incidente de segurança Now Platform. Esta configuração é feita por meio de um perfil de alarme em sua instância Now Platform.

Procedimento

1. Navegar até **Todos** > **Integração com LogRhythm**.
2. Selecione o módulo **Perfis de alarme da LogRhythm** para exibir a lista **Perfis de alarme**.

Perfil do Alarme



3. Para criar um novo perfil de alarme, clique em **Novo**.
   Um novo formulário de perfil de alarme é exibido. Na parte superior da página na barra de andamento, a opção **Nome** está selecionada. Esta barra rastreia seu andamento durante a configuração.
4. No formulário, preencha os campos.

Perfil do Alarme

Campo	Descrição
Nome	Nome do perfil de alarme. Este nome ajuda a identificar os tipos de alarme, como acesso não autorizado (VPN), malwareou phishing.
Descrição resumida	Texto curto para informações adicionais sobre o perfil do alarme, que pode incluir o tipo de alarmes ou uma categoria de alarme. Uma descrição de exemplo: todos os alarmes associados a tentativas de acesso não autorizadas do Powershell e Sudo.
Origem	Servidor de origem na lista de seleção. A lista consiste em LogRhythm configurações que você já definiu, por exemplo, `logrhythm-server-a`. Consulte Instalar o plug-in e configurar LogRhythm.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	Prioridade do perfil de alarme. Este campo indica a ordem na qual os perfis de alarme são executados quando dois ou mais perfis de alarme compartilham as condições de acionamento.
Ativo	Por padrão, esta opção não está selecionada. Depois de concluir todas as etapas de configuração do perfil de alarme e clicar em **Concluir**, você será solicitado a marcar esta caixa de seleção para ativar o perfil de alarme. Quando o perfil de alarme está ativo, ele extrai alarmes do LogRhythm Console do cliente automaticamente.

5. Clique em **Continuar** para salvar seus dados e prosseguir para o formulário Mapeamento.

   Se a validação for bem-sucedida, a página será recarregada e o formulário **Mapeamento** será exibido. Você não pode prosseguir com a configuração até ter validado com sucesso sua conexão e credenciais.

Informações relacionadas

Mapeamento de LogRhythm alarmes para o incidente de segurança

Mapeamento de LogRhythm alarmes para o incidente de segurança

Depois de selecionar a origem LogRhythm que você deseja ingerir, você precisa mapear campos de alarme LogRhythm individuais para os campos de incidente de segurança Now Platform.

O mapeamento de alarmes inclui as seguintes tarefas:

- Mapear LogRhythm alarmes. Para esta tarefa, você lista e ingere (Pull) alarmes de amostra usando os IDs de alarme ou os alarmes mais recentes do console do cliente LogRhythm.
- Os campos de alarme de amostra são categorizados em três grupos:
  - Campos dealarme: os campos de alarme que estão disponíveis e seus valores correspondentes são exibidos.
  - Campos de evento: os campos de evento que estão disponíveis e seus valores correspondentes são exibidos.
  - Campos de Detalhamentode log: os campos de log de detalhamento que estão disponíveis e os valores correspondentes são exibidos.
- Cada ID de alarme que você extraiu é exibido como uma guia. Nas guias ID do alarme, verifique se todos os campos de alarme críticos da seção Ingestão de amostra de alarme à esquerda do formulário estão mapeados para a seção Mapeamento de campo de incidente SIR à direita do formulário.
- Depois de mapear os alarmes para o campo Mapeamento de campo de incidente SIR, você pode ver a categoria de alarme também sendo exibida no campo Expressão de entrada. Por exemplo, `${Alarm: alarmid}$`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode modificar a configuração adicionando ou removendo campos no incidente de segurança. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida.
- Você pode filtrar alarmes para especificar quais alarmes são ingeridos na aplicação SIR. Você pode filtrar os alarmes diretamente ou usar as categorias de alarme para detalhar sua pesquisa com base em Alarmes, Eventos ou DetalhamentoDeLogs.
- Use o editor de script se quiser formatar valores para os campos Prioridade e Categoria no incidente de segurança.

A próxima etapa é Mapear LogRhythm campos de alarme para campos de incidente de segurança.

Informações relacionadas

Mapear LogRhythm campos de alarme para campos de incidente de segurança

Use o editor de script para formatar valores LogRhythm

Filtrar alarmes para LogRhythm

Tradução automática

Mapear LogRhythm campos de alarme para campos de incidente de segurança

Você mapeia campos de alarme individuais para os campos de incidente de segurança. O mapeamento pré-configurado pode ser editado e a codificação de cores fornecida para os campos ajuda a monitorar os alarmes já mapeados. Esta etapa ajuda a visualizar como suas edições afetam os campos no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin
Se você não estiver familiarizado com os alarmes LogRhythm, navegue até o Console do cliente LogRhythm e revise alguns exemplos de IDs de alarme. Para o exemplo a seguir, LogRhythm alarmes `9468` e `9474` foram usados para mapear os alarmes para o incidente de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Usando este formulário, você mapeia as regras de alarme LogRhythm à esquerda para os campos de incidente de segurança à direita.

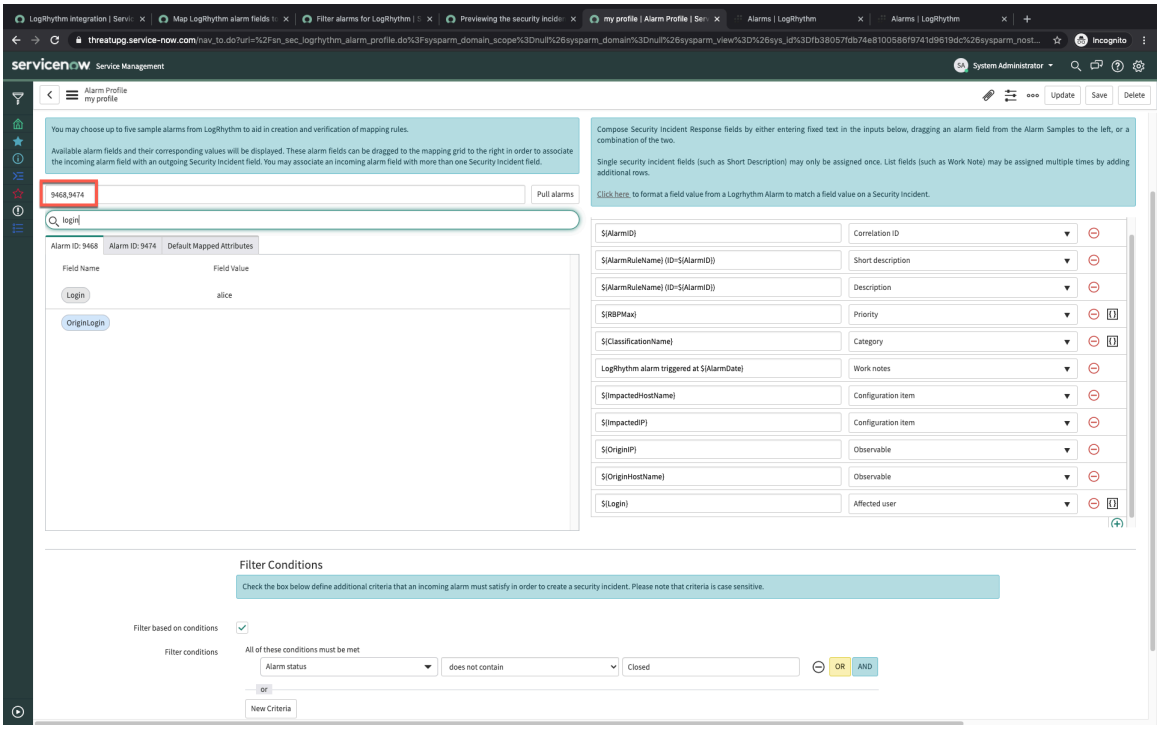
A figura a seguir mostra o mapeamento padrão de alarmes pré-configurados para cada perfil de alarme. Este mapeamento padrão pode ser editado e, com este formulário, você personaliza os campos que preenchem o incidente de segurança. Depois de concluir este mapeamento, você pode ver como adicionar ou remover campos de alarme pode afetar os valores de campo no incidente de segurança.

No lado esquerdo deste formulário na figura a seguir, as regras de alarme LogRhythm são descritas. Os valores dessas regras de alarme são mapeados para os campos de incidente de segurança no lado direito do formulário.

Procedimento

1. Depois de criar um perfil de alarme para o LogRhythm, clique em **Mapeamento** na barra de andamento.
2. No campo **Ingestão de amostra de alarme**, insira até cinco amostras LogRhythm de IDs de alarme separadas por vírgulas (`9468,9474`).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Ao lado do campo de alarme, clique em **Extrair alarmes**.

A extração de alarmes de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

Depois que as IDs de alarme de amostra são enviadas e extraídas com sucesso do servidor LogRhythm, os campos de alarme e seus valores correspondentes são exibidos nas guias.

Nota: Depois que um ID de alarme é extraído com sucesso, o Now Platform pode retornar a seguinte mensagem: `Os seguintes novos campos estarão disponíveis para filtragem em breve. Recarregue este perfil em alguns minutos se a filtragem com base nesses campos for necessária. itenspacotesem, itenspacotesfora`.

Esta mensagem ocorre quando o único alarme que foi extraído contém nomes de campo não processados anteriormente pelo Now Platform. Esses campos estão disponíveis para mapeamento, no entanto, se esta mensagem for exibida, recarregue o formulário para que esses campos sejam exibidos e disponíveis nas listas de seleção de filtro do construtor de condições quando você estiver pronto para definir as condições de filtragem.

A ingestão desses alarmes de amostra na configuração do perfil de alarme ajuda a evitar o mapeamento de campos de alarme para o incidente de segurança que não contém valores. Ele também alinha os campos de alarme com valores para os campos apropriados no incidente de segurança. Esta etapa garante que todos os campos de alarme críticos sejam mapeados e que não haja valores de campos ausentes no incidente de segurança.

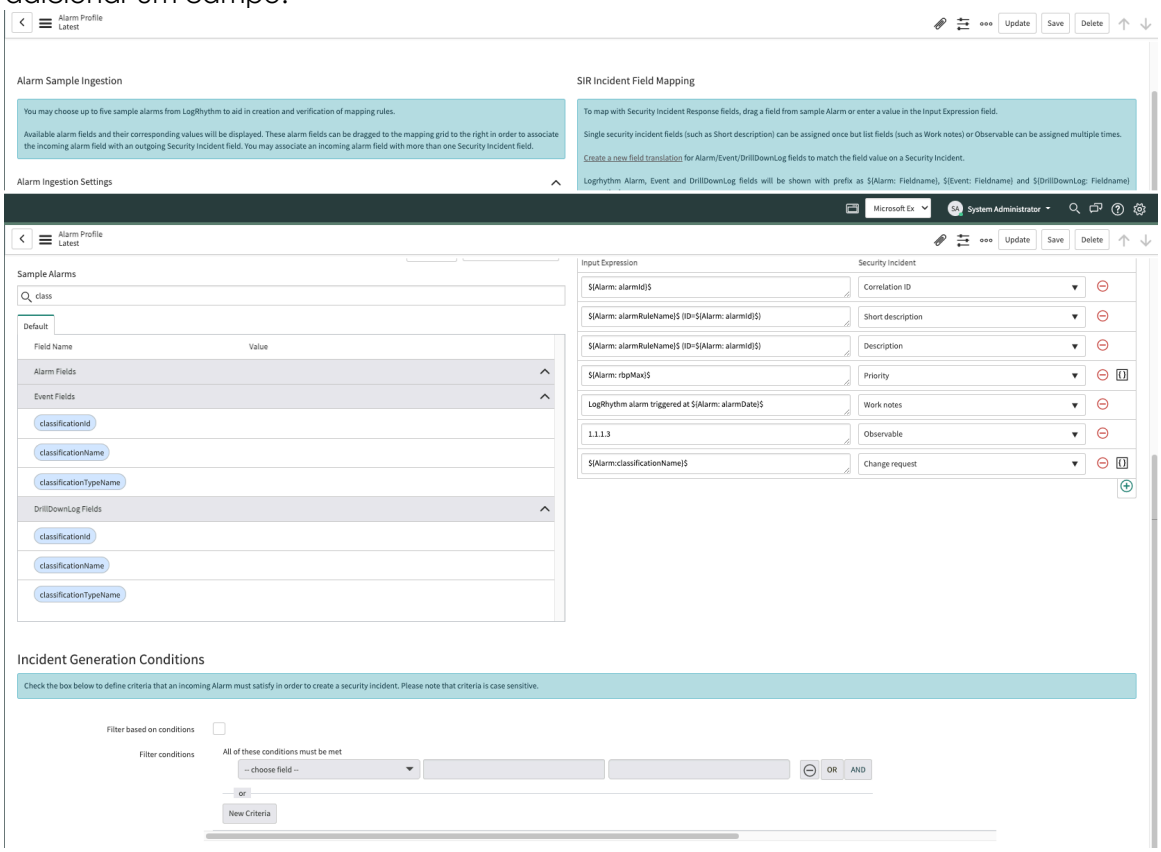
Para ajudá-lo a garantir que nenhum alarme seja ignorado ou duplicado no processo de mapeamento, os campos de alarme são codificados por cores. Um campo de alarme azul claro (`Account`, `AlarmRuleID`, `AlarmStatus`etc.) indica que um campo ainda não foi selecionado para mapeamento para um incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um campo cinza (`AlarmDate`, `AlarmID`e `AlarmRuleName`) indica que um campo já foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento porque, em determinados casos, um campo de alarme pode ser mapeado para mais de um campo em um incidente de segurança. Por exemplo, os campos `Observáveis` e `Anotação de trabalho` podem ter mais de um valor.

4. Para limpar os dados de alarme de amostra, clique em **Limpar dados de alarme de amostra**.
5. Para editar a configuração padrão no incidente de segurança, siga estas etapas para adicionar um campo:



   a. No canto inferior direito do formulário, clique no ícone de mais.
   Um novo campo é exibido.

   b. Na coluna Incidente de segurança, selecione um campo disponível na lista de seleção.

   Na lista de seleção expandida, alguns dos campos estão sombreados. Por exemplo, a `categoria` tem um plano de fundo cinza, o que indica que ela foi mapeada no incidente de segurança. Semelhante à codificação de cores para campos de alarme LogRhythm, essa codificação de cores para os campos de incidente de segurança garante que os valores dos campos de alarme não sejam mapeados inadvertidamente para o mesmo campo de incidente de segurança.

   Na ilustração acima, a regra de alarme `${Alarm:classificationName}$` já está mapeada para o campo `Categoria` no incidente de segurança neste perfil.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O campo Observável pode ser mapeado para mais de campos no mesmo incidente de segurança para que vários observáveis possam ser exibidos. Da mesma forma, os campos `Item de configuração` e `Anotações de trabalho` podem ser mapeados para exibir vários valores.

No lado Ingestão de amostra de alarme do formulário, o azul indica que um campo de regra de alarme não foi mapeado. Cinza indica que ele foi mapeado. Na lista de seleção no lado Mapeamento de campo de incidente SIR do formulário, branco indica que um campo não foi mapeado. Cinza indica que um campo foi mapeado. Use esta codificação de cores para ajudá-lo a rastrear seu mapeamento de campo.

Na ilustração acima, `o usuário afetado` foi selecionado na lista de seleção como um novo campo no incidente de segurança.

c. Na seção Ingestão de amostra de alarme no lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o ID do alarme desejado no campo Expressão de entrada.

Na ilustração acima, `Login` foi selecionado.

d. Arraste-o para o campo limpo e solte-o.
Na coluna esquerda da seção Mapeamento de campo de incidente SIR, o novo valor do campo `Usuário afetado` é exibido. Nesse caso, o valor de `Login` do alarme LogRhythm é exibido no campo `Usuário afetado` no incidente de segurança.

6. Como alternativa, para inserir manualmente um valor para campos na coluna Expressão de entrada, coloque o cursor no campo de expressão de entrada e insira um valor de alarme desejado.

Por exemplo, na ilustração acima, outro campo foi adicionado (`Grupo de atribuição`) ao formulário de incidente de segurança, e `a Atribuição de incidente de segurança` foi inserida manualmente no campo.

7. Continue editando o mapeamento pré-configurado conforme necessário.
Se você precisar converter valores de LogRhythm campos de alarme para valores que são compatíveis com os campos no incidente de segurança, você pode usar o editor de script. Consulte Use o editor de script para formatar valores LogRhythm.

O que Fazer Depois
Depois de concluir o mapeamento de campo, a próxima etapa é para Filtrar alarmes para LogRhythm.

Filtrar alarmes para LogRhythm

Definir critérios de filtragem para alarmes depois de mapear campos ajuda a determinar quais alarmes devem ser ingeridos na aplicação SIR. A filtragem de alarmes ajuda a reduzir significativamente o número de alarmes que você ingere quando o perfil de alarme está ativado.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Use as condições de filtragem na parte inferior do formulário de mapeamento para filtrar alarmes específicos ou limitar a ingestão somente para alarmes que atendam a determinados critérios no nível de campo. A filtragem reduz significativamente o número

Tradução automática

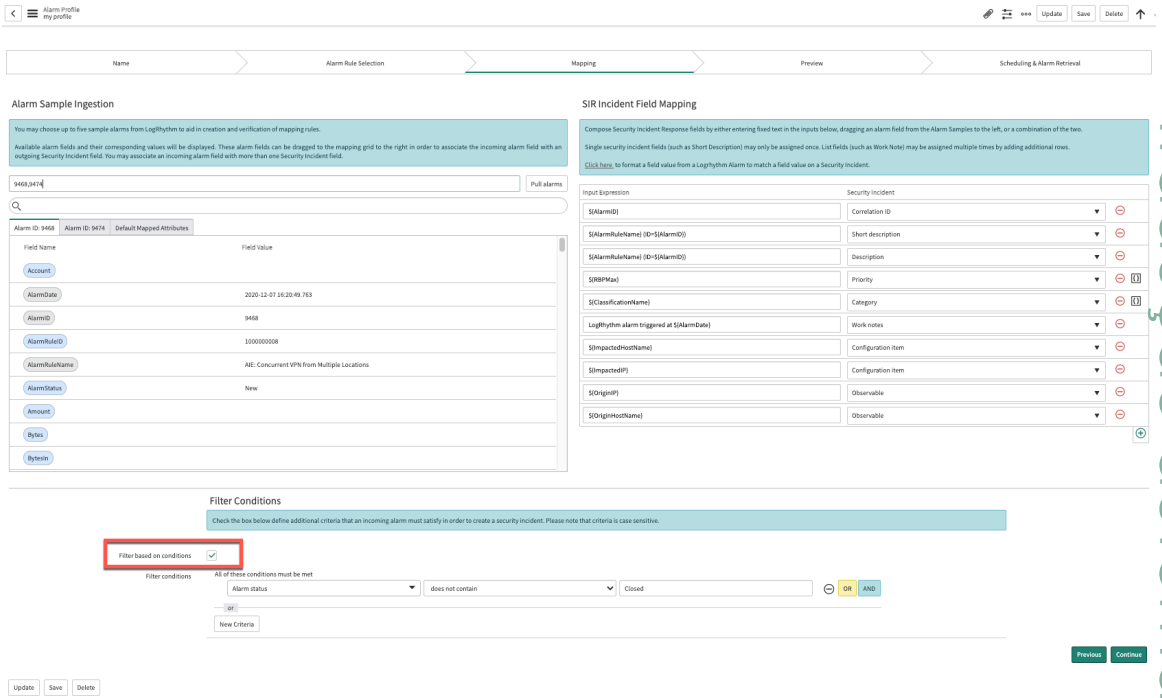
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de alarmes que você ingere quando o perfil do alarme é ativado. Use a filtragem para ingerir uma quantidade gerenciável de alarmes que a equipe do Centro de operações de segurança (SOC) pode suportar.

Nota: O exemplo a seguir mostra uma configuração de filtro padrão na qual o `status do alarme-não-contém-fechado` é a configuração padrão. Este filtro extrai somente alarmes ativos e essa configuração reduz o número de alarmes extraídos. As etapas a seguir ilustram como adicionar outro filtro útil que inclui somente alarmes com os valores de severidade ou prioridade mais altos.

Procedimento

1. Para editar os critérios de filtragem, marque a caixa de seleção **Filtrar com base nas condições**.

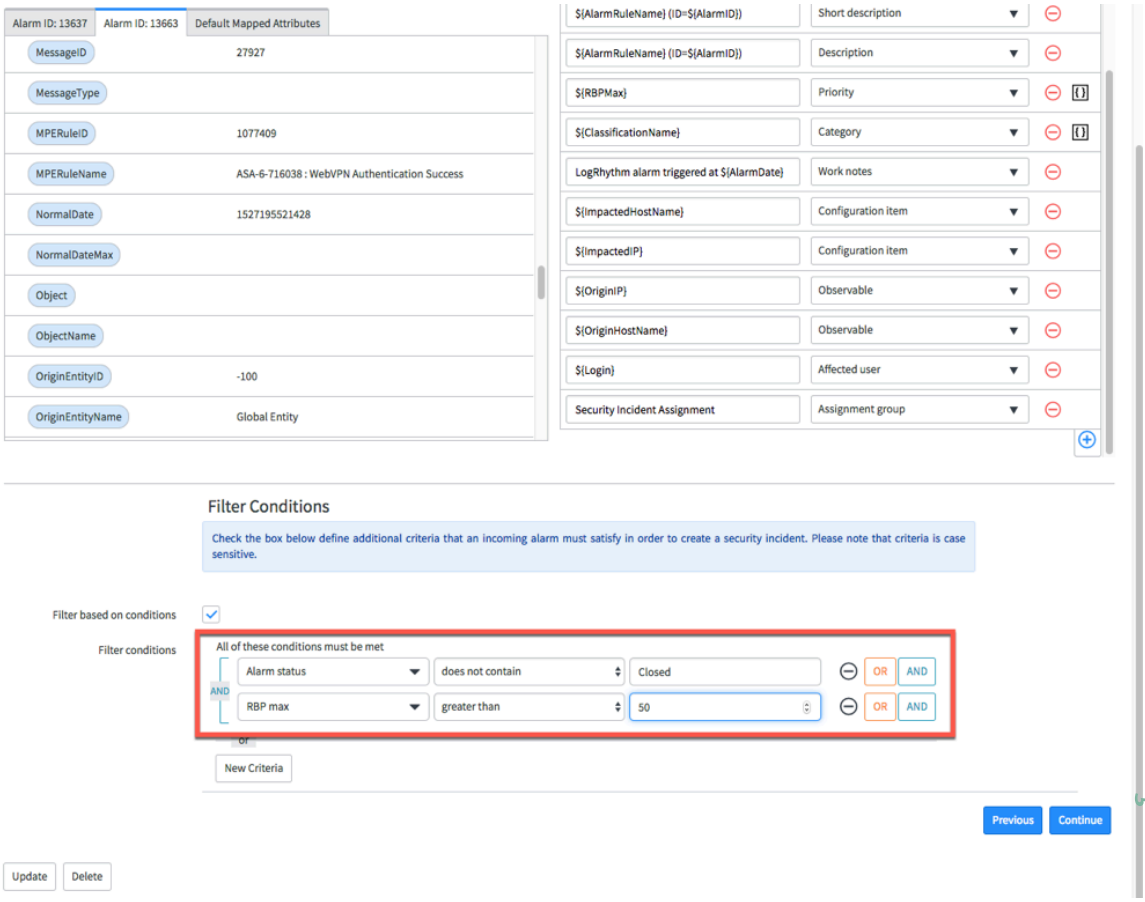


2. À direita do campo **Condições do filtro**, clique em **OU** ou **E**.
3. Na nova linha exibida, selecione as condições de filtragem nas listas de seleção.

   A imagem a seguir mostra um filtro adicional adicionado aos critérios nos quais a prioridade baseada em risco (`RBP máx`) é maior que `50`. Com esta configuração de filtro, somente LogRhythm alarmes com um valor de prioridade baseado em risco maior que 50 são extraídos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Depois de verificar que todos os campos de alarme críticos LogRhythm estão mapeados para o incidente de segurança Now Platform e definir critérios de filtragem para limitar a ingestão de alarmes, escolha um para continuar a configuração.

Opção	Descrição
Continuar ou Visualizar	O formulário Visualizar do incidente de segurança com sua configuração de mapeamento é exibido. A **visualização** está selecionada na barra de andamento. A próxima etapa é exibir o incidente de segurança com seus alarmes mapeados.
Atualizar	Salve seus dados e retorne à lista de **perfis de alarme**.
Anterior	O registro do perfil do alarme é exibido.
Excluir	Exclua este perfil de alarme e a lista **Perfis** de alarme será exibida.

O que Fazer Depois

A próxima etapa é visualizar os campos mapeados no incidente de segurança. Consulte Visualização do incidente de segurança com valores de alarme LogRhythm mapeados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualização do incidente de segurança com valores de alarme LogRhythm mapeados

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou para os campos no incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de alarme críticos LogRhythm que deseja exibir no incidente de segurança.

Função necessária: sn_si.admin.

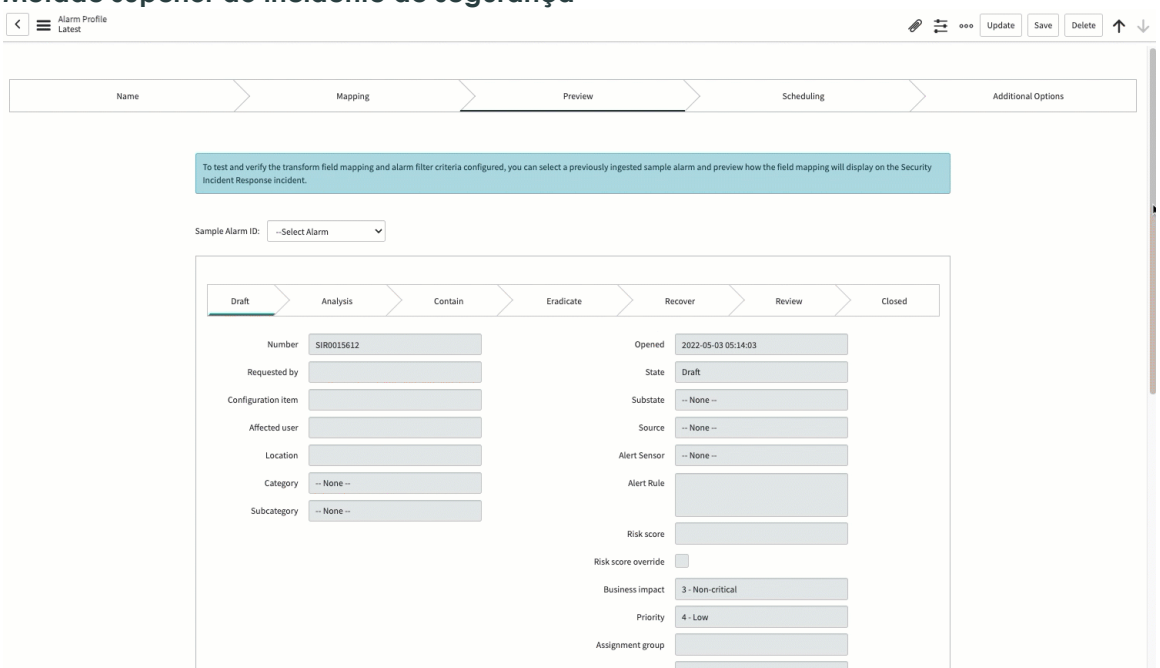
Incidente de segurança

Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.

Um exemplo da visualização de todo o incidente de segurança Now Platform é exibido nas duas imagens a seguir. Este exemplo da visualização do incidente de segurança é preenchido com os LogRhythm campos de alarmes mapeados do alarme de amostra `13663`.

Na figura a seguir, os campos `Item de configuração`, `Usuário afetado`, `Prioridade`, `Grupo de atribuição`e `Descrição resumida` do incidente de segurança são preenchidos.

Metade superior do incidente de segurança



Na metade inferior do formulário de incidente de segurança, o campo `Descrição` está preenchido. Na seção Itens relacionados, os campos `Item de configuração`, `Observável`e Anotação de `trabalho` são preenchidos com valores. Se vários valores para esses campos forem mapeados, cada valor será exibido no incidente de segurança, porque cada um desses campos pode aceitar mais de um valor.

Condições de erro na visualização

As seguintes mensagens de aviso podem ser exibidas ao visualizar o incidente de segurança. Se um alarme de amostra não passar nos critérios de filtragem, o incidente de segurança inteiro não será preenchido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valor de entrada não encontrado

Se o ID do alarme estiver incluído nas condições de filtragem, uma mensagem de aviso ainda poderá ser exibida se valores de entrada específicos não forem encontrados para determinados campos mapeados. Para fins do exemplo a seguir, na visualização do registro, suponha que não haja nenhum valor no campo `Atribuído a`, embora ele tenha sido mapeado.

Para este tipo de mensagem, no registro de Mapeamento, verifique se o valor de entrada está correto. Nesse caso, a pessoa no campo `Atribuído a` no incidente de segurança está incorreta na instância Now Platform. Quando este alarme é ingerido e cria um incidente de segurança com esta condição, os campos com este valor de entrada (`Abel Tuter`) são deixados em branco no incidente de segurança.

As mensagens restantes em azul são informativas e indicam que esses campos não têm valor a ser exibido na visualização. Esta visualização permite que o administrador de incidentes de segurança configure o perfil do alarme para verificar se esses campos não devem ter valor na fase de criação inicial, porque, em determinados casos, os campos de incidentes de segurança podem ser preenchidos automaticamente posteriormente. Outros erros de mapeamento também são exibidos.

Quando estiver satisfeito com o mapeamento e a visualização do incidente de segurança, escolha um para continuar a configuração.

Opção	Descrição
Clique em **Continuar** ou **Programação** na barra de andamento.	Avance para o formulário **Programação e recuperação de alarme**. **A programação e a recuperação de alarmes** estão selecionadas na barra de andamento. A próxima etapa é programar a recuperação do alarme.
Clique **em Anterior**.	Retorne ao perfil de alarme e continue o mapeamento.
Insira outro ID de alarme na lista de seleção **ID de alarme de amostra** na parte superior do formulário de visualização.	A lista de seleção de **ID de alarme de amostra** é exibida para cada ID de alarme inserido. Você pode selecionar até cinco alarmes. Esta opção permite que você visualize outro LogRhythm ID de alarme em um incidente de segurança.

Depois de visualizar o incidente de segurança e estar satisfeito com os resultados, a próxima etapa é Programar e recuperar LogRhythm alarmes.

Programar e recuperar LogRhythm alarmes

Depois de visualizar o incidente de segurança com os LogRhythm alarmes que você selecionou e mapeou, você está pronto para programar a recuperação do alarme. Depois de concluir esta etapa, o perfil do alarme estará pronto para ser ativado.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

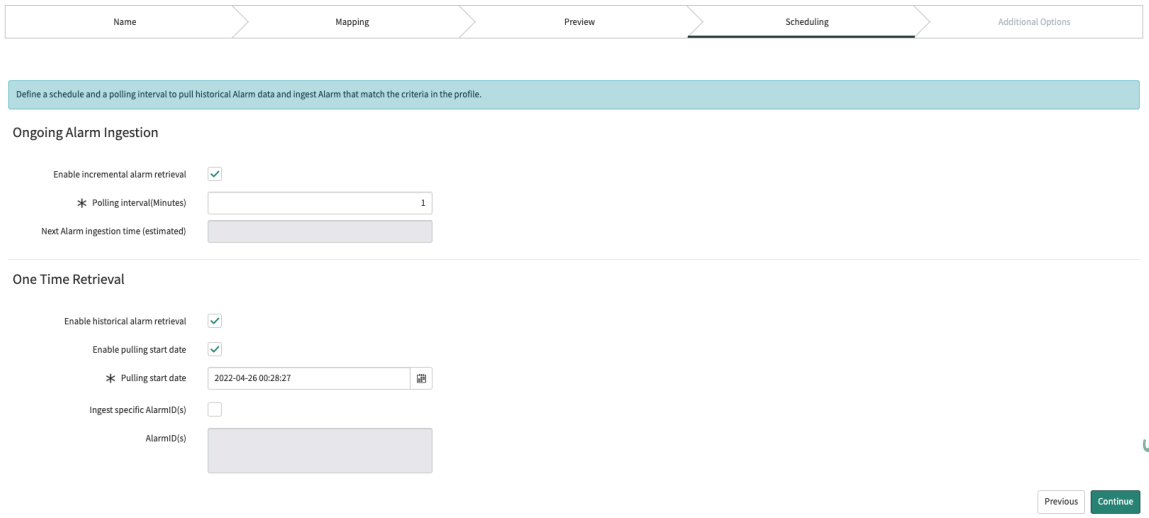
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A programação permite que você modifique a programação e os tipos de alarmes selecionados para recuperação. Você filtra os alarmes que ingere com base em um intervalo de datas ou em IDs de alarme específicos. Com esta etapa, você determina se deseja ingerir alarmes históricos e com que frequência pesquisa alarmes futuros que correspondam à configuração do perfil de alarme.

Procedimento

1. Clique na etapa **Programação** na barra de andamento.



2. Escolha uma das seguintes opções para configurar a recuperação do alarme.

Opção	Descrição
Habilitar recuperação de alarme incremental	O padrão é selecionado. Selecione esta opção para recuperar alarmes incrementais.
Intervalo de pesquisa (em minutos)	A instância Now Platform extrai do Console do cliente LogRhythm novos alarmes a cada minuto. Se alarmes mapeados forem encontrados e os critérios de filtragem forem correspondidos, os incidentes de segurança serão criados. Esta configuração pode ser alterada, no entanto, a configuração padrão balanceia a ingestão de alarmes em relação à carga do servidor e recupera os dados mais atuais.
Próximo período de ingestão de alarmes (estimado)	Exibe quando a próxima ingestão programada ocorreria para o perfil de alarme atual. Este é apenas um tempo estimado.
Habilitar recuperação de alarme histórico	O padrão é limpo. Nenhum dado histórico foi extraído.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Se selecionado, os seguintes campos serão exibidos. Escolha um para configurar a recuperação por data ou ID de alarme. Habilitar data de início da extração O padrão é limpo. Selecione esta opção para habilitar a extração de data. Data de início da extração O padrão é limpo. Selecione esta opção para definir a data de início da extração. Clique no ícone de calendário para inserir uma data e hora. Os alarmes são extraídos a partir da data e hora que você insere até a data atual. Ingerir ID(s) de alarme específico(s) O padrão é limpo. Selecione esta opção para ingerir IDs de alarme específicos. ID(s) de Alarme(s) Insira IDs de alarme específicos. Você extrai os alarmes especificados e pode inserir vários IDs de alarme separados por vírgulas. **Nota:** Depois que uma extração única histórica de alarmes é concluída, esta caixa de seleção é desmarcada. Você precisará marcar esta caixa de seleção novamente antes de executar outra extração única de alarmes históricos.

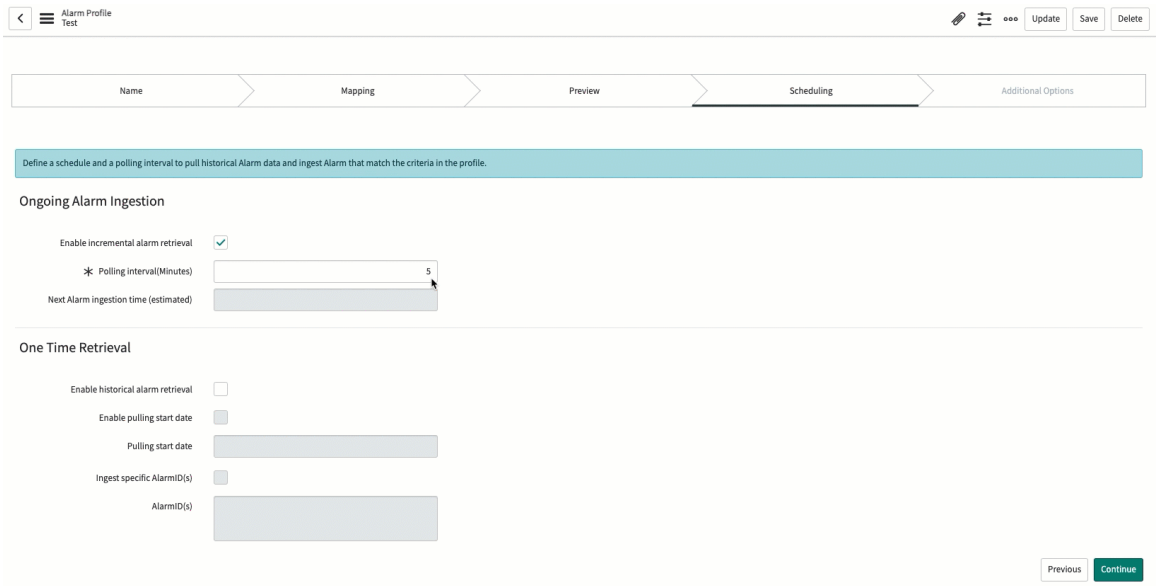
3. Para editar a recuperação do alarme histórico, siga estas etapas para inserir uma data para a recuperação do alarme ou um ID de alarme específico.

   a. Selecione **Habilitar data**de **início da extração e selecione Data de início da extração**.

   b. No campo **Data de início da extração**, clique no calendário exibido, selecione a data seguida da marca de seleção verde para salvar sua entrada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A data é exibida.

c. Como alternativa, selecione a opção **Ingerir IDs de alarme específicos** e, no campo **AlarmID(s)**, insira os IDs de alarme específicos dos dados históricos para recuperar IDs de alarme específicos.

Você pode inserir até cinco alarmes separados por vírgulas.

d. Clique em **Atualizar**.

4. Escolha uma das seguintes opções para continuar editando ou concluir a configuração.

Opção	Descrição
Atualizar	Salve seus dados e permaneça no formulário.
Opções adicionais (na barra de andamento)	Para ir para a etapa Opções adicionais.
Anterior	Retorne à etapa de Exibição.
Excluir	Exclua este perfil de alarme e a lista de perfis de alarme será exibida.

O que Fazer Depois

Depois de configurar os detalhes de Ingestão de alarmes contínuos e Recuperação única, a próxima etapa é Opções adicionais para LogRhythm alarmes.

Opções adicionais para LogRhythm alarmes

A integração LogRhythm Enterprise oferece a capacidade de atualizar ou fechar automaticamente os alarmes LogRhythm com base nos incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Quando você habilita a opção Atualizações iniciais do alarme, os alarmes são atualizados automaticamente nos comentários do LogRhythm com as atualizações do alarme inicial. Da mesma forma, quando você habilita a opção Atualizações de fechamento de alarme, os alarmes são fechados automaticamente no LogRhythm junto com o Código de fechamento SIR e os comentários de fechamento.

O LogRhythm ID do alarme está conectado ao Now Platform ID do incidente de segurança durante todo o curso do ciclo de vida do incidente. Essa correlação permite que ocorra um fechamento simultâneo e automatizado de incidente/alarme de segurança. Quando o registro de incidente de segurança Security Incident Response (SIR) é fechado, há um comentário publicado no alarme no console da web LogRhythm. Este comentário indica que o alarme foi encerrado com base no fechamento do Now Platform incidente de segurança. O número do incidente e um URL que vincula de volta ao incidente de segurança para referência também estão incluídos na seção de comentários no alarme LogRhythm.

Procedimento

1. Clique na etapa **Opções adicionais** na barra de andamento.
2. Para usar a atualização automatizada de alarmes para a criação de incidentes de SIR, escolha uma das seguintes opções para configurar a recuperação do alarme.

Opção	Descrição
Atualizar alarmes da LogRhythm após a criação de incidente de SIR	O padrão é limpo. Selecione esta opção para atualizar automaticamente os alarmes LogRhythm quando o incidente de SIR for criado.
Comentários iniciais retornados para o alarme da LogRhythm	Indica os comentários iniciais que são publicados para o alarme LogRhythm. Edite o texto padrão que é exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente SIR. Por exemplo, `O incidente de segurança da ServiceNow relacionado, ${Number}$, foi criado e atribuído a ${Grupo de atribuição}$. Detalhes adicionais podem ser encontrados sobre o incidente de segurança localizado aqui - ${URL}$.`

3. Para usar a atualização automatizada de alarme para o fechamento do incidente SIR, escolha uma das seguintes opções para configurar a recuperação do alarme.

Opção	Descrição
Fechar alarmes da LogRhythm após o fechamento do incidente de SIR	O padrão é limpo. Selecione esta opção para fechar automaticamente os alarmes LogRhythm quando o incidente SIR for fechado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Comentários de fechamento retornados para o alarme da LogRhythm	Indica os comentários de fechamento publicados para o alarme LogRhythm. Edite o texto padrão que é exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente SIR. Por exemplo, `O incidente de segurança relacionado à ServiceNow, ${Number}$, foi encerrado pelo analista do SOC-${Closed by}$ com as seguintes notas de fechamento: ${Closed by}$. Detalhes adicionais podem ser encontrados sobre o incidente de segurança localizado aqui - ${URL}$.`

4. Clique em **Concluir** para salvar o perfil do alarme.

Trouble?
Se você não vir anotações indicando que o alarme foi encerrado com sucesso no incidente de segurança, revise as anotações de trabalho para obter mais informações sobre como prosseguir para corrigir o problema. Além disso, verifique a conexão do servidor. Se você confirmar que o Now Platform incidente de segurança foi encerrado e o servidor não expirou, talvez seja necessário fechar manualmente o alarme no LogRhythm Console da web.

Configurações adicionais para a integração LogRhythm

Use as configurações de integração LogRhythm para modificar o sistema predefinido e as propriedades de solução de problemas de acordo com seus requisitos.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Integração com LogRhythm** > **Configurações da Integração com LogRhythm**.
2. Configure as propriedades do sistema de acordo com seus requisitos.
3. No formulário, preencha os campos.

LogRhythm Propriedades do sistema de integração

Campo	Descrição
Isso aplicará o filtro antes que os dados sejam salvos nas tabelas da ServiceNow.	Opção para determinar se você deseja aplicar o filtro antes que os dados sejam armazenados nas tabelas da ServiceNow. Por padrão, o valor é definido como Sim.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
O número máximo de incidentes de segurança que pode ser criado em um dia	Opção para definir o número máximo de incidentes de segurança que podem ser criados em um dia. Por padrão, o valor é definido como 2000.
LogRhythm A ingestão periódica pode ter mais de 1000 alarmes, portanto, a paginação é usada para ingerir os alarmes. Limite por página permitido para buscar o número de alarmes por página.	Opção para definir o número máximo de alarmes a serem recuperados em uma única página. Por padrão, o valor é definido como 100.
Excluir registros da tabela "Origem para tarefa" mais antigos do que o número especificado de dias.	Opção para excluir registros da tabela Origem para tarefa quando o número de dias especificado tiver sido violado. Por padrão, o valor é definido como 30.

4. Configure as propriedades de solução de problemas de acordo com seus requisitos.
5. No formulário, preencha os campos.

Propriedades de solução de problemas de integração da LogRhythm

Campo	Descrição
Depurar ingestão programada: habilita os logs do sistema no nível de depuração para a ingestão feita pelo trabalho agendado. Isso registrará em log todas as mensagens/exceções geradas pela ingestão programada ao extrair alarmes/ logs de detalhamento/eventos de LogRhythm.	Opção para habilitar logs do sistema no nível de depuração para ingestão realizada pelo trabalho agendado. Por padrão, o valor é definido como Não.
Depurar mapa de transformação: habilita os logs do sistema no nível de depuração para o mapa de transformação. Isso registrará todas as mensagens geradas por mapas de transformação ao criar o incidente de segurança da importação de alarme. Isso também habilitou a ação de IU na tabela de importação de alarme para executar novamente o mapa de transformação.	Opção para habilitar logs do sistema no nível de depuração para o Mapa de Transformação. Por padrão, o valor é definido como Não.
Ingestão de amostra de depuração no perfil de alarme: habilita os logs do sistema no nível de depuração para ingestão de amostra. Isso registrará todas as mensagens geradas enquanto as amostras são ingeridas.	Opção para habilitar logs do sistema no nível de depuração para ingestão de amostra. Por padrão, o valor é definido como Não.
Visualização de depuração no perfil do alarme: habilita os logs do sistema no nível de depuração para a visualização do perfil do alarme. Isso registrará todas	Opção para habilitar logs do sistema no nível de depuração para Visualização de perfil de alarme.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
as mensagens geradas enquanto a visualização é renderizada para o alarme de amostra.	Por padrão, o valor é definido como Não.
Depurar chamadas REST de saída: a habilitação desta propriedade permitirá o registro em log no nível de depuração na tabela Logs do sistema para todas as chamadas REST (solicitação e resposta) com ou sem MID Server de LogRhythm.	Opção para habilitar o registro em log de nível de depuração na tabela Logs do sistema para todas as chamadas REST com ou sem MID Server de LogRhythm. Por padrão, o valor é definido como Não.

6. Clique em **Salvar**.

Use o editor de script para formatar valores LogRhythm

Além dos campos mapeados diretamente dos valores de alarme extraídos e dos valores de alarme inseridos manualmente, você pode usar o editor de script para formatar valores de campos no incidente de segurança durante a etapa de mapeamento, que é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

O editor de script muda os valores de um alarme LogRhythm para que os valores mapeados para os campos `Prioridade` e `Categoria` no incidente de segurança sejam compatíveis.

Por Que e Quando Desempenhar Esta Tarefa

Em determinados casos, se os valores de alarme LogRhythm forem mapeados para os campos `Prioridade` e `Categoria` no incidente de segurança, convém editar os valores mapeados. Se você quiser converter o valor de um alarme LogRhythm para um valor que seja compatível com os campos `Prioridade` ou `Categoria` no incidente de segurança, use o editor de script.

Procedimento

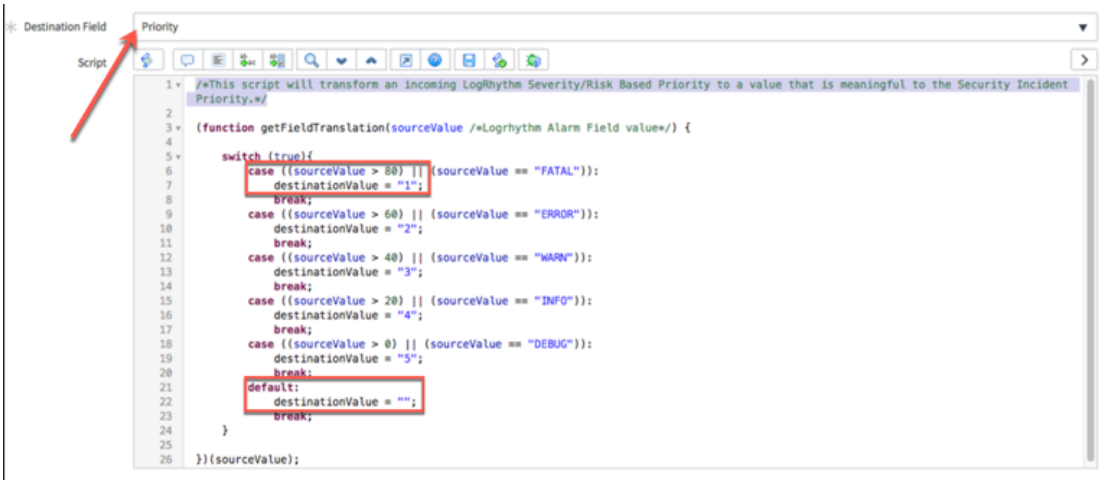
1. Com o formulário de mapeamento exibido, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete `[{}]` para abrir o editor de script.

   Os valores padrão são incluídos para os campos `Prioridade` e `Categoria` no incidente de segurança. Você pode editar esses valores.

   Para este exemplo, no editor aberto, verifique se **Prioridade** é exibido na lista de seleção **Campo de destino**, conforme mostrado na figura a seguir. Observe que este campo é a prioridadedo incidente de segurança , não a LogRhythmprioridadebaseada em risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

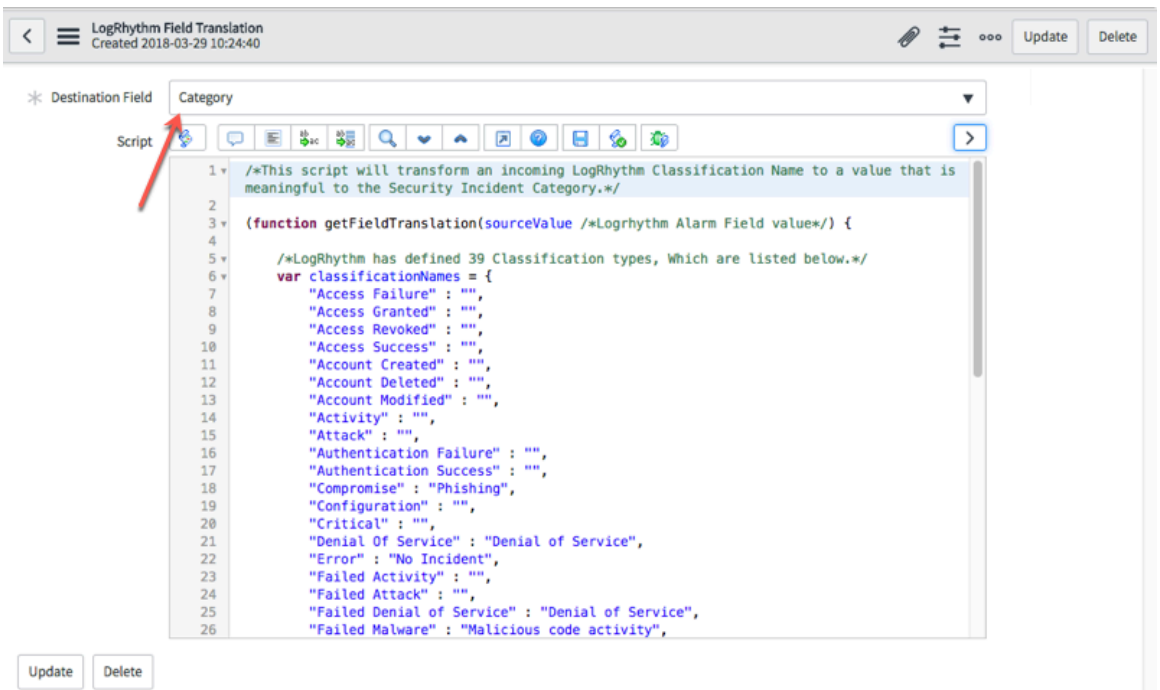


Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo `Prioridade`. Para um alarme LogRhythm, por exemplo, uma pontuação de prioridade baseada em risco é atribuída a um valor entre 0 e 100. No entanto, no Now Platform, o campo de prioridade em um incidente de segurança aceita valores entre 1 e 5. Conforme ilustrado na figura anterior, uma inclusão de script converte os valores do campo de alarme LogRhythm para os valores apropriados compatíveis com o campo no incidente de segurança no Now Platform.

Neste exemplo do campo `Prioridade`, se o valor do alarme LogRhythm for `80` ou maior, `1` será exibido no campo de incidente de segurança (`Prioridade`). Este valor se traduz em uma prioridade `Crítica` no incidente de segurança. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

2. Insira as mudanças e clique em **Atualizar** para salvar suas mudanças.
   A tabela LogRhythm Tradução de Campo é exibida.
3. Feche a tabela para retornar ao formulário Mapeamento.

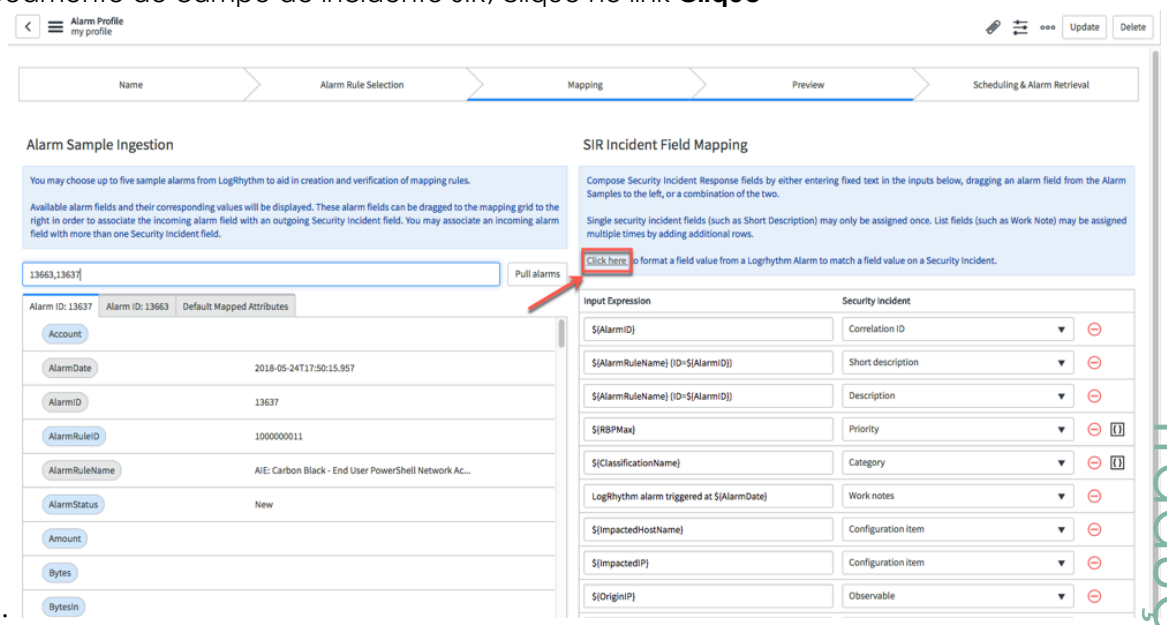
A figura a seguir mostra o editor de script com a `Categoria` selecionada na lista de seleção Campo de destino.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

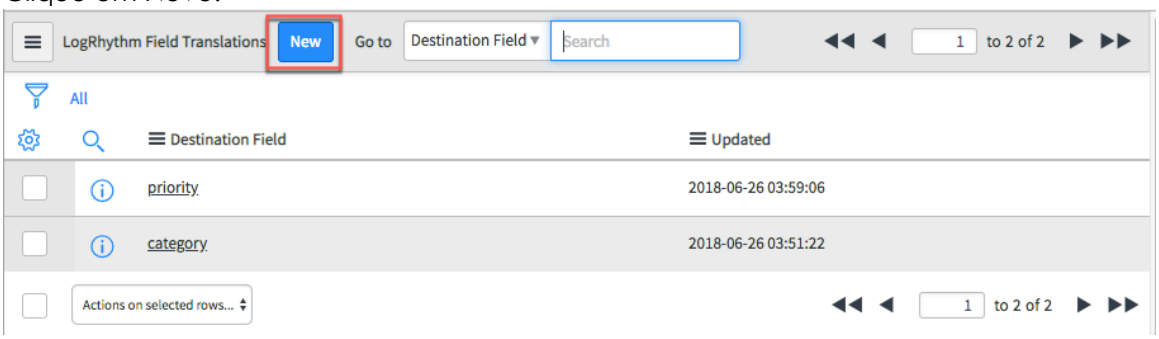
4. Se você quiser adicionar um novo campo à lista de Traduções de Campo, siga estas etapas para adicionar um novo registro.

   a. Com o formulário de mapeamento exibido, na seção Mapeamento de campo de incidente SIR, clique no link **Clique aqui**.



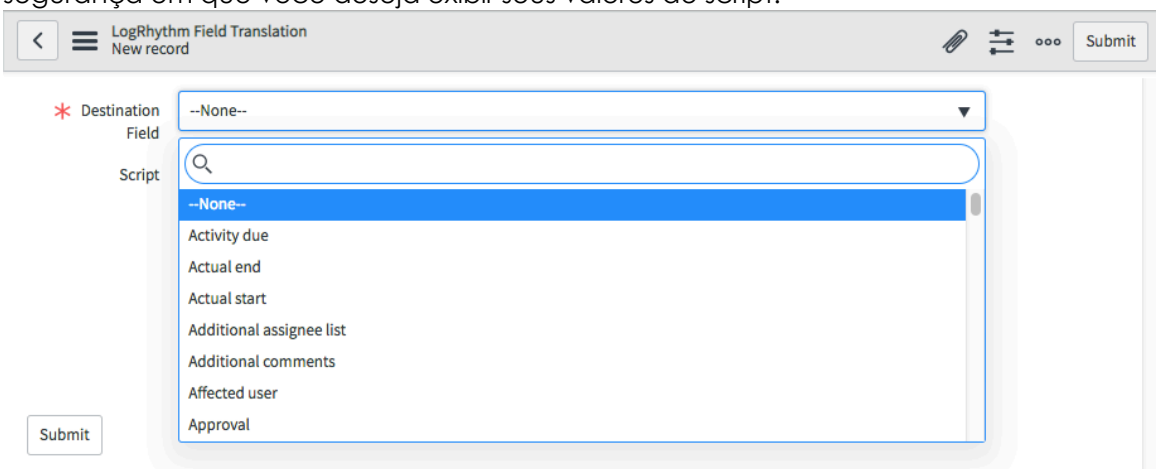
   A lista LogRhythm de tradução de campo com os campos de destino de `prioridade` e `categoria` é exibida.

   b. Clique em Novo.



   Um novo registro é exibido.

   c. Na lista de seleção Campo de destino, selecione um campo de destino no incidente de segurança em que você deseja exibir seus valores de script.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Clique em **Enviar**.
O editor de script é exibido.

e. Insira as mudanças no editor e clique em **Enviar** para salvar suas mudanças.
A tabela LogRhythm Traduções de campo com seu novo registro é exibida.

5. Feche a tabela para retornar ao formulário Mapeamento.

Copiar um perfil de alarme para LogRhythm

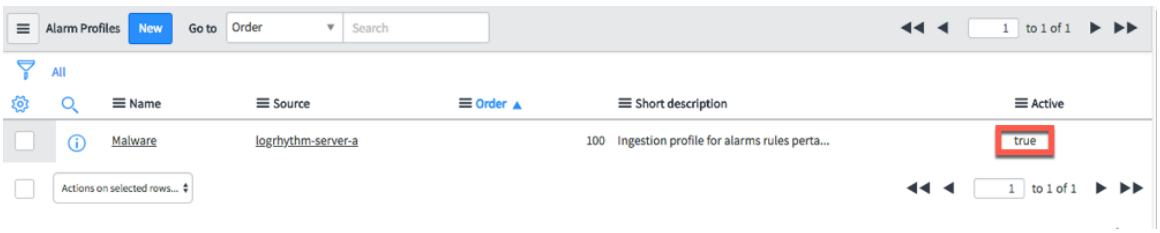
Copie um perfil existente e suas configurações associadas em vez de criar um novo perfil de alarme. Se você estiver criando vários perfis de alarme para diferentes tipos de alarmes e quiser reutilizar as configurações de um perfil existente, poderá copiar os perfis de alarme para economizar tempo. Este processo é opcional.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é definido como inativo para que não seja ativado acidentalmente antes de concluir a configuração.

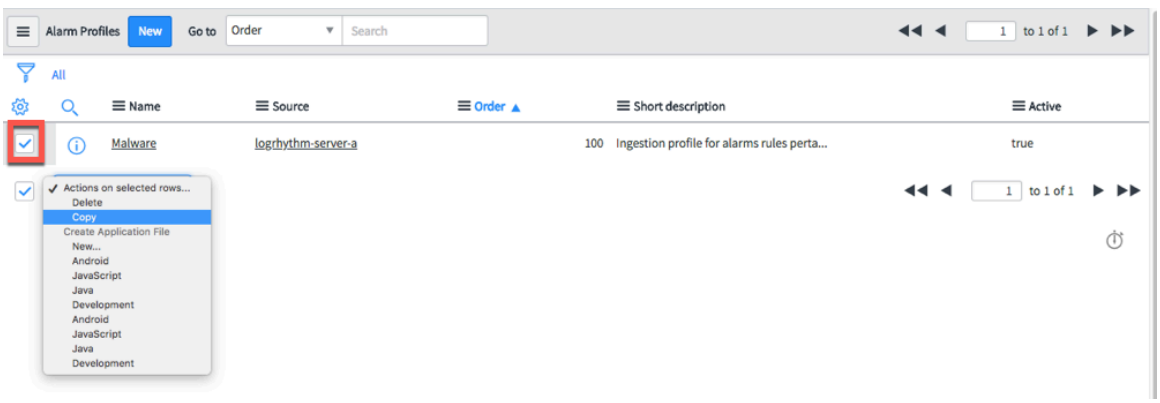
Procedimento
1. Navegar até **Todos** > **Integração com LogRhythm** > **Perfis de alarme LogRhythm**.

Na lista exibida, observe que a coluna `Ativo` indica se o perfil está ativo (`verdadeiro`).



2. No campo à esquerda da coluna **Nome**, selecione o nome do registro.

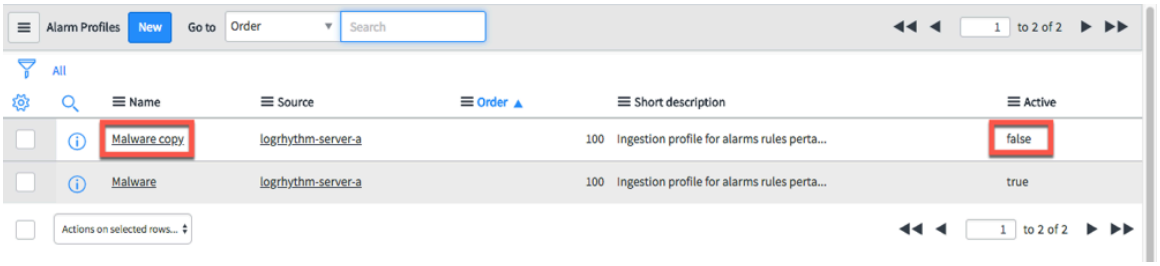
3. Na lista de seleção **Ações em linhas selecionadas**, selecione **Copiar**.



Na lista **Perfis de alarme**, a cópia e o perfil original são exibidos. Embora o registro original esteja ativo, a cópia está inativa neste ponto (`falso`). Depois de configurá-lo, você ativa este perfil copiado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode editar valores do perfil copiado e renomeá-lo para que as regras de alarme extraídas se apliquem ao novo perfil. Você será solicitado a ativar o novo perfil quando as etapas de configuração forem concluídas.

Desabilitar fechamento automatizado de alarme para LogRhythm

Desabilite a capacidade de fechamento de alarme automatizado se você não quiser mais exibir as informações de fechamento do incidente de segurança no LogRhythm Console da web. Depois de desativado, o Now Platform não fecha mais os alarmes no console da web LogRhythm. Este processo é opcional.

Antes de Iniciar

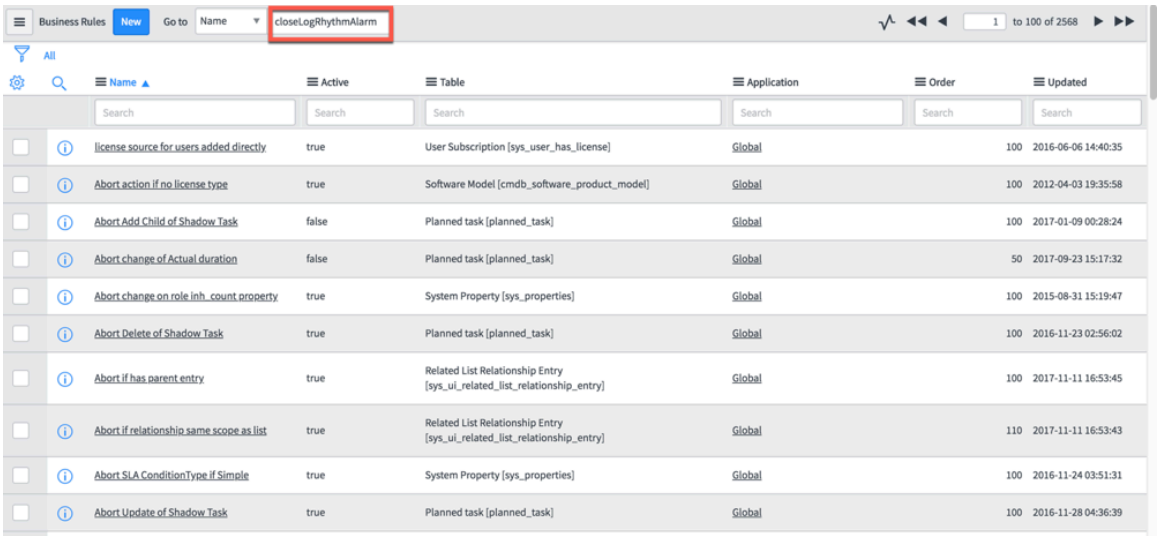
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Depois de desabilitado, as anotações de status e outras informações de fechamento no incidente de segurança não são mais exibidas no LogRhythm Console da web.

Procedimento

1. Navegar até **Todos** > **Definição do sistema** > **Regras de negócio** e selecione o módulo **Regras de negócio**.
2. Se não for exibido na lista **Regras de negócio**, insira **LogRhythm Close Alarm On SI Closure** no campo de pesquisa e pressione **Enter**.



3. Na coluna **Nome**, clique no **link Alarme de fechamento da LogRhythm no fechamento de SI** para abrir o registro.
4. No registro exibido, desmarque a caixa de seleção **Ativo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Atualizar**.
   A capacidade de fechamento de alarme automatizado agora está desabilitada.

Exibir LogRhythm eventos de detalhamento

Exiba os eventos brutos ou de base relacionados a um alarme LogRhythm no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

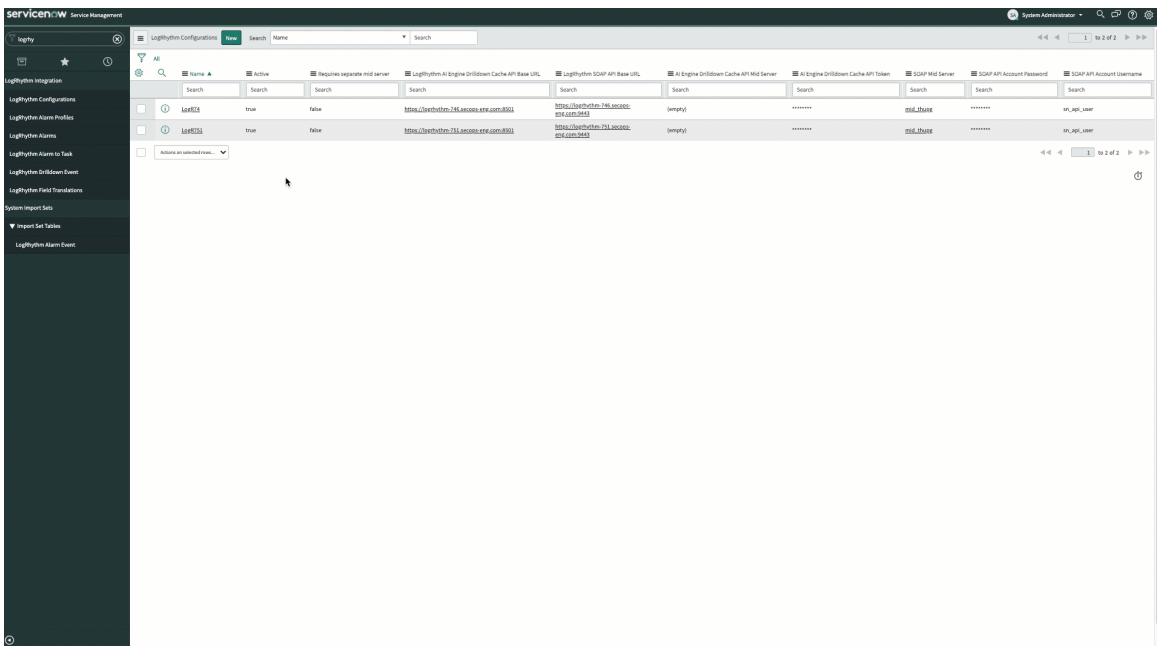
Por Que e Quando Desempenhar Esta Tarefa

Como analista de segurança, você pode exibir os eventos brutos ou de base relacionados a um alarme LogRhythm sem precisar voltar para o console LogRhythm. Você pode fazer isso acessando uma lista relacionada que contém todos os eventos de detalhamento no incidente SIR.

Procedimento

Navegar até **Todos** > **Integração com LogRhythm** > **Eventos de detalhamento da LogRhythm**.

A ilustração a seguir mostra como navegar até o módulo **Eventos de detalhamento da LogRhythm**, classificar a lista de eventos por **Agrupar por ID de alarme**e clicar no incidente de segurança associado. No incidente de segurança, você pode encontrar a guia **Eventos de detalhamento da LogRhythm** nos links relacionados.



Solução de problemas de integração do LogRhythm

Solucionar problemas de conectividade e ingestão de alarmes.

Consulte os seguintes tópicos para solução de problemas:

- Verificar conectividade para LogRhythm
- Execução de script e log do sistema para LogRhythm

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar conectividade para LogRhythm

Verifique sua conexão com o Console do cliente LogRhythm enviando solicitações de ondulação para testar a LogRhythm REST API. O processo de verificação é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Para verificar se a conexão com o LogRhythm Client Console está funcionando corretamente depois de configurar as LogRhythm REST APIs, envie duas solicitações de curva do computador que hospeda o MID Server que você configurou em Instalar o plug-in e configurar LogRhythm.

A LogRhythm REST API usa WSSE para autenticação, o que requer alguns scripts externos para funcionar com Curl e Postman.

A LogRhythm REST API usa um token para autenticação, portanto, você pode fazer a chamada de validação real que a integração usa. O "0" no final do URL é um LogRhythm ID de alarme. A LogRhythm REST API com uma configuração padrão requer a porta 8501. Este número de porta deve ser incluído no URL que você planeja usar para o teste.

Procedimento

Atualizar a URL<LogRhythm REST url> e token<api token> na solicitação de curvatura a seguir e envie-a para validar a LogRhythm REST API: **Curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Autorização: Portador** " "https://<cache drilldown url> /lr-drilldown-cache-api/detalhamento/0"
Para uma conexão bem-sucedida com a LogRhythm REST API, você deve receber um HTTP 404, mas o corpo da resposta contém o `ID do alarme: 0 não encontrado`.

Execução de script e log do sistema para LogRhythm

Se você estiver solucionando um problema de ingestão de alarme, poderá substituir o intervalo de pesquisa padrão de cinco minutos para exibir os resultados imediatamente. Neste cenário, chame a execução do script manualmente para executar a pesquisa. Esta execução é opcional.

Antes de Iniciar

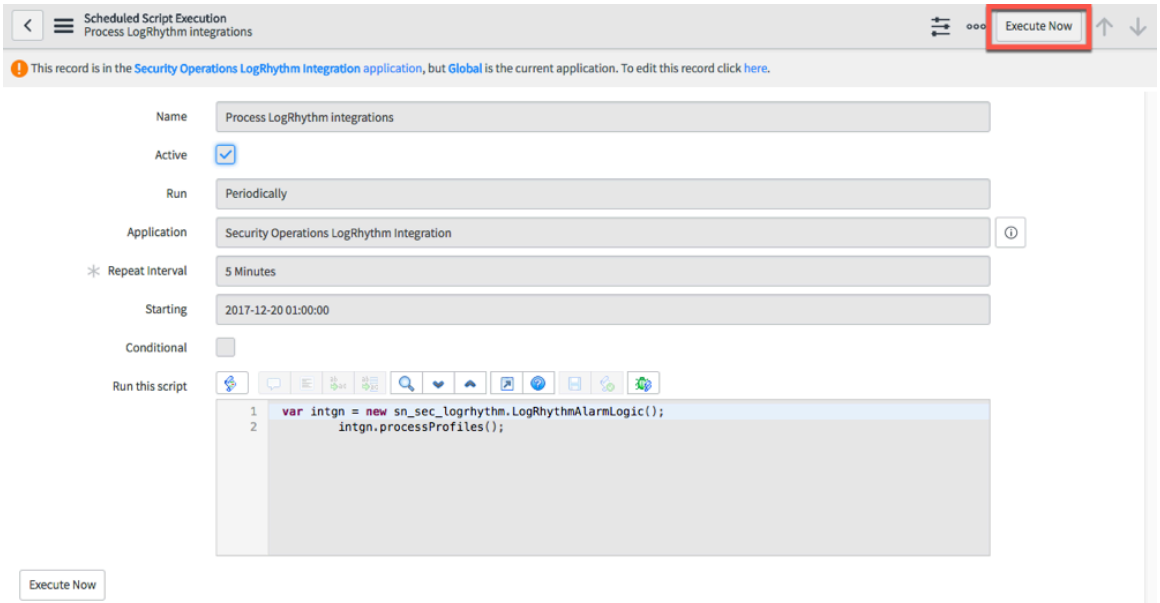
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Trabalho agendado** > **Trabalhos agendados** e selecione o módulo **Trabalhos agendados**.
2. Clique no registro de trabalho de integrações Processar LogRhythm.
3. No registro de Execução de script agendada exibido, clique em **Executar agora**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você precisar de mais ajuda na solução de problemas, poderá acessar o log do sistema para as consultas LogRhythm.

4. Para outros problemas gerais de solução de problemas, siga estas etapas para acessar os logs do sistema.

   a. Navegar até **Log do sistema** > **Todos** e selecione **Todos**.

   b. Defina o filtro (`Ir para`) como **Origem** e insira `sn_sec_logrhythm`.

   c. Pressione **Enter**.
   Todas as mensagens geradas pela integração são exibidas nesta tabela. As mensagens listadas podem fornecer informações sobre os processos em execução da integração e podem ajudá-lo na solução de problemas.

Integração de McAfee ePO

A capacidade McAfee ePO de detecção e resposta de endpoint (EDR) de integração que ajuda os analistas do Centro de Operações de Segurança (SOC) a identificar ameaças cibernéticas e reparar os danos causados por arquivos mal-intencionados.

Visão geral

Há dois conjuntos de capacidades McAfee ePO usadas nesta integração, as capacidades que invocam ações, como isolar um host e iniciar uma verificação de malware, e as capacidades que executam consultas para coletar detalhes do sistema e eventos de ameaça. Ambos os tipos de capacidades, as ações e as consultas, são invocados a partir da instância Now Platform®. Você pode agrupar esses recursos para que sejam executados automaticamente quando ocorrer um tipo específico de evento de segurança ou invocá-los manualmente a partir de um Now Platform® incidente de segurança.

As seguintes capacidades McAfee ePO estão disponíveis para esta integração.

Obter detalhes do sistema

Reúna detalhes do sistema que incluem detalhes do sistema operacional.

Iniciar verificação de malware

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com base na configuração e programação da verificação, inicie uma verificação de um endpoint afetado.

Isolar/Desfazer isolamento de host

Remova um sistema do acesso à rede para investigação e restaure o acesso à rede.

Listar eventos de ameaça

Reúna o status de conformidade e os eventos de ameaça mais atuais.

Principais recursos

Esta integração inclui os seguintes recursos principais.

- Oferece suporte ao acionamento automatizado de McAfee ePO consultas baseadas nas condições do incidente.
- Oferece suporte à inicialização de McAfee ePO capacidades manualmente a partir de Now Platform® Security Incident Response (SIR) incidentes de segurança que executam ações sob demanda.
- A flexibilidade de criar vários perfis para acionar diferentes tipos de capacidades McAfee ePO e Now Platform® Operações de segurança. Esses perfis reúnem informações de eventos de ameaça ou executam ações com base nas condições de categorias de incidentes específicas, como malware.
- Valide a configuração do seu perfil com uma visualização dos McAfee ePO resultados em SIR incidentes de segurança.
- Se a marcação estiver habilitada, os marcadores de segurança identificarão quais McAfee ePO capacidades são iniciadas inicialmente por um fluxo de trabalho e quando as consultas ou ações são concluídas com sucesso.
- Uma trilha de auditoria completa das consultas e ações McAfee ePO é publicada nas anotações de trabalho em incidentes de segurança SIR, e os comandos do Now Platform® são registrados no console do McAfee ePO.
- Oferece suporte a vários McAfee ePO consoles.

ServiceNow Plug-ins

O plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações.

As Operações de segurança aplicações a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Estrutura de integração de segurança
2. Security Support Common
3. Orquestração de suporte de segurança
4. Resposta a incidentes de segurança
5. Espaço de resposta a incidentes de segurança

Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Configure sua instância Now Platform para a integração McAfee ePO.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O plug-in de extensão ServiceNow

O plug-in ServiceNow Security Operations Extension for McAfee ePO# é necessário para esta integração. Instale este plug-in ServiceNowMcAfee ePO no console []. Para obter mais informações, consulte Configure sua instância Now Platform para a integração McAfee ePO.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao servidor McAfee ePO (console). Consulte o site de documentação de produtos da ServiceNow para obter mais informações sobre MID Servers.

Versões compatíveis do McAfee

A integração é compatível com as versões 5.9.1 e 5.10 de McAfee ePO. Ele oferece suporte ao McAfee Agent: MA 5.5.1.388 Para obter mais informações sobre os produtos da McAfee e o ePolicy Orchestrator, consulte o site do produto da McAfee .

A integração é compatível com a versão 10.5 do produto McAfee Endpoint Security Threat Prevention. Se você não estiver executando a versão 10.5, consulte o administrador McAfee ePO para ver se sua versão pode oferecer suporte a verificações sob demanda por meio de ações de marcador.

McAfee ePO marcadores de segurança são usados nesta integração. Você deve criar esses marcadores no console McAfee ePO. Para obter mais informações sobre esses marcadores, consulte Configure o console McAfee ePO para integração com Security Incident Response (SIR).

Referências

Referência	Identificador de documento	Título do Documento
1	Site do produto da McAfee	Site do produto da McAfee
2	Documentação de produto de negócios da McAfee para ePolicy Orchestrator Cloud	Documentação de produto da McAfee
3	ServiceNow Site da documentação do produto	Site de documentação do produto da ServiceNow

Para obter uma check-list para acompanhar o andamento da configuração, instalação e verificação dos resultados da integração, consulte Check-list para a integração McAfee ePO.

Para uma instalação sem problemas da aplicação e para ajudá-lo a verificar os resultados esperados, siga os tópicos na ordem em que são apresentados.

Informações relacionadas

Arquitetura de integração para McAfee ePO

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquitetura de integração para McAfee ePO

O tópico a seguir é uma visão geral da arquitetura do sistema e lista os principais recursos da integração. Esta seção também fornece informações sobre as etapas de configuração que você deve concluir na instância Now Platform e no console do McAfee ePolicy Orchestrator (McAfee ePO) antes de instalar a aplicação a partir do ServiceNow Store.

Termos-chave para a integração McAfee ePO

Os termos a seguir são usados em toda a documentação de instalação e configuração da integração.

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais, como Security Incident Response (SIR), Gestão de serviços de TI (ITSM) e outros produtos são criados.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento de incidentes de segurança desde a descoberta e análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Plug-in

Plug-ins são componentes de software que fornecem recursos e funcionalidades específicas em sua instância Now Platform. Para obter mais informações sobre a instalação e a configuração dos plug-ins de integração, consulte Instalar a aplicação e configurar um servidor para a integração McAfee ePO.

ePolicy Orchestrator (McAfee ePO)

O console do usuário onde você gerencia os serviços, produtos e configurações da McAfee.

Plug-in de extensão da McAfee

Este ServiceNow plug-in de extensão é necessário para esta integração. Este plug-in reside no console McAfee ePO e conecta o console McAfee ePONow Platform à instância [].

Capacidade

Uma atividade automática iniciada em sua instância Now Platform que é executada no console McAfee ePO para conduzir consultas de aprimoramento e executar ações em seus ativos.

Perfil

Configurações para capacidades McAfee ePO que você configura para especificar quando e sob quais condições as capacidades conduzem consultas de aprimoramento e executam ações em seus ativos.

MID server

Uma aplicação que facilita a comunicação e a movimentação de dados entre o Now Platform e aplicações, fontes de dados e serviços externos.

ServiceNow administrador (admin)

Um usuário com esta função baixa e instala os plug-ins SIR e McAfee ePO na sua instância Now Platform. Um usuário com esta função também atribui a função de administrador de incidentes de segurança conforme necessário.

ServiceNow Administrador de incidentes de segurança (sn_si.admin)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um usuário com esta função executa a configuração da integração McAfee ePO com o produto Security Incident Response (SIR) em sua instância Now Platform, conforme necessário. Um usuário com esta função também atribui a função de analista de incidentes de segurança conforme necessário.

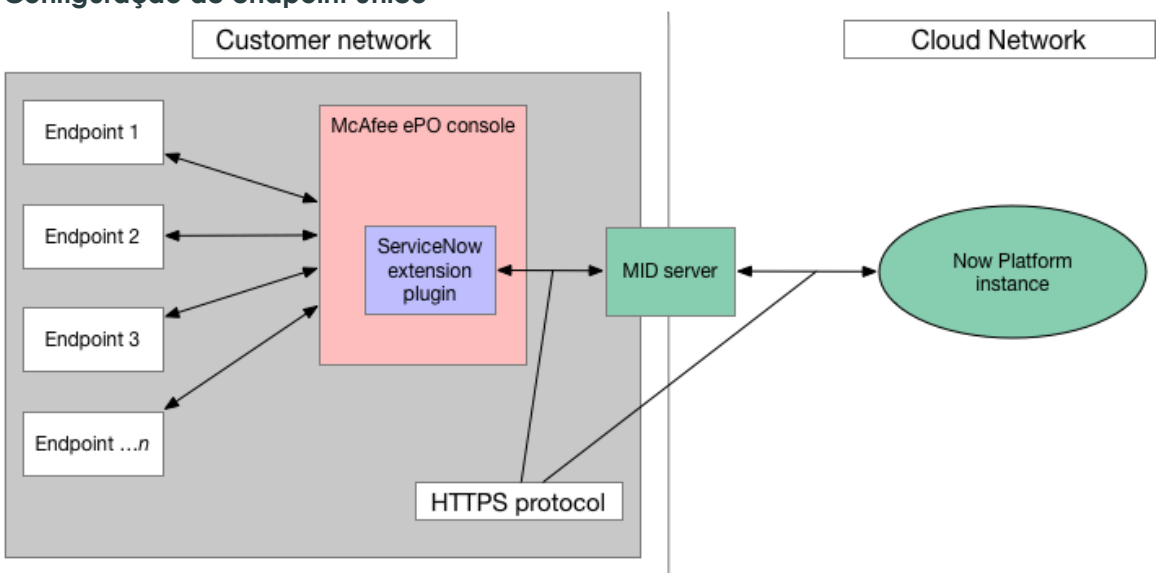
ServiceNow analista de incidentes de segurança (sn_si.analyst)

Um usuário com esta função interage e analisa incidentes de segurança no produto SIR.

Conexão do sistema e fluxo de dados

A figura a seguir é um exemplo de um ambiente do cliente. Um Now Platform MID Server é necessário para que sua instância Now Platform possa se conectar a um servidor McAfee ePO (console) por meio de um plug-in de extensão ServiceNow. Depois de conectado, você invoca capacidades do seu Now Platform para iniciar verificações de malware, isolar máquinas host e restaurá-las na rede, recuperar resultados da última verificação e coletar detalhes do sistema em seus ativos. Quando esses recursos retornam resultados de seus ativos que correspondem aos seus critérios de pesquisa, os dados são extraídos por meio do MID Server para sua instância Now Platform. Os dados são exibidos nas listas relacionadas de um incidente de segurança Now Platform Security Incident Response (SIR). A figura a seguir ilustra o fluxo de dados para um grupo de endpoints gerenciados por um console McAfee ePO.

Configuração de endpoint único

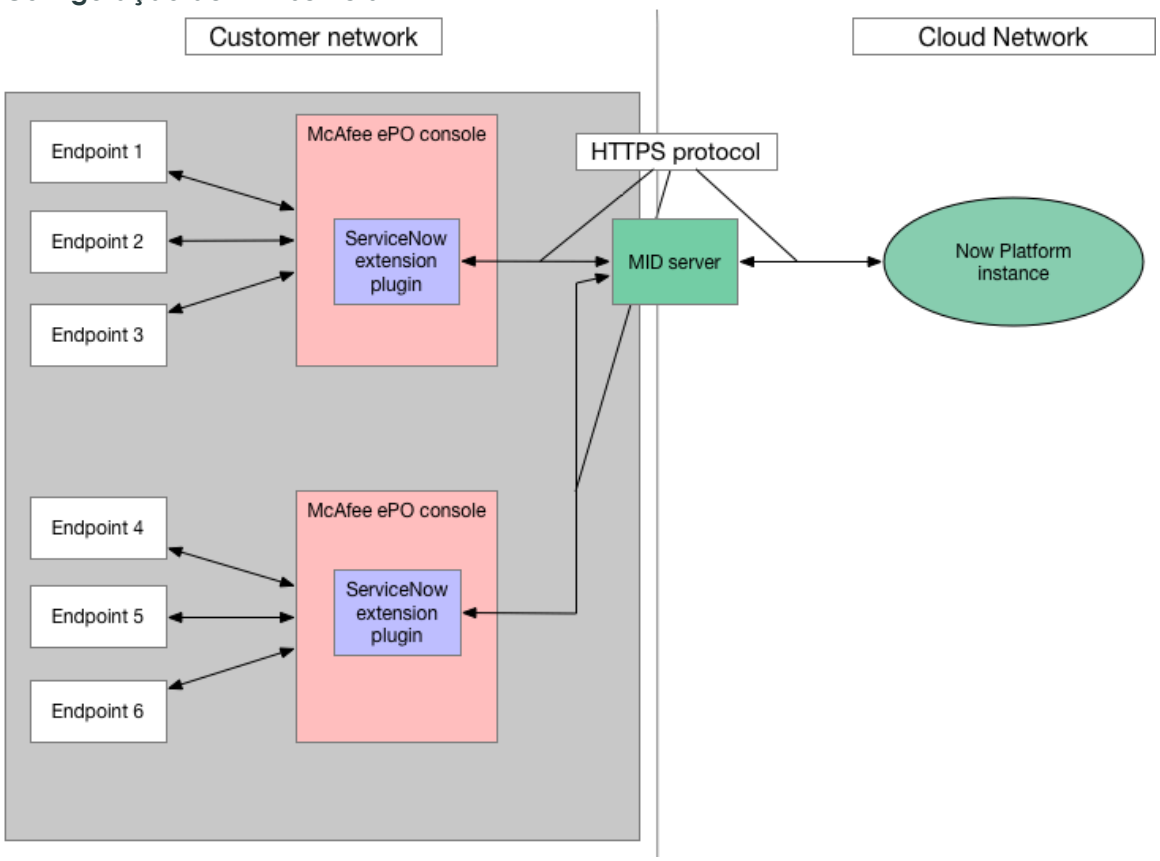


Conforme mostrado na figura a seguir, esta integração pode oferecer suporte a mais de um console McAfee ePO. Você pode ter um grupo de endpoints gerenciados por um console McAfee ePO e outro grupo de endpoints gerenciados por outro console McAfee ePO. Os dados de vários McAfee ePO consoles são extraídos por meio de um único MID Server. No entanto, você também pode preferir configurar vários MID Servers, se exigido pela sua organização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de MID servers



Fluxos de trabalho para a integração McAfee ePO

Esta integração inclui os seguintes fluxos de trabalho. Esses fluxos de trabalho são pré-configurados e projetados especificamente para esta integração. Você pode editar esses fluxos de trabalho para atender às necessidades da sua organização, conforme necessário. Para obter informações mais gerais sobre fluxos de trabalho e como usar o editor de fluxo de trabalho, consulte Introdução a fluxos de trabalho .

- Integração do McAfee EPO com o Security Operations - Obter detalhes do host
- Integração do McAfee EPO com o Security Operations - Iniciar verificação de malware
- Integração do McAfee EPO com o Security Operations - Isolar host
- Integração do McAfee EPO com o Security Operations - Listar eventos de ameaça
- Integração do McAfee EPO com o Security Operations - Remover isolamento

Conexão de sistemas externos

A integração requer que o MID Server se comunique por meio da conexão do protocolo HTTPS com o console McAfee ePO.

Check-list para a integração McAfee ePO

Use esta check-list para se orientar em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem os resultados esperados para a integração.

Antes de Iniciar

Função necessária: as funções são listadas para cada etapa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe o andamento da configuração, instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada linha da tabela lista as tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

Procedimento

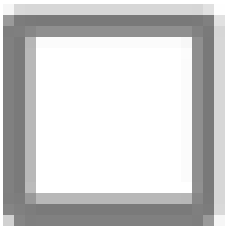
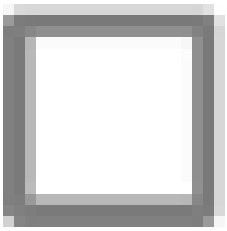
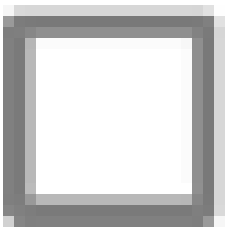
Siga as etapas na tabela na ordem em que são apresentadas.

Check-list

Item	Descrição
☐	Como um usuário com a função de administrador Now Platform®, configure sua instância Now Platform®. **a.** Atribua as funções Now Platform® e Security Incident Response. **b.** Verifique se todos os ServiceNow Security Incident Response e outros plug-ins compatíveis com a integração estão instalados e ativados para a versão do Now Platform. **c.** Instale e configure um MID Server em sua instância Now Platform®. **d.** Crie um grupo de aprovação se quiser processar as solicitações enviadas pelo analista de incidentes de segurança para o host isolado e iniciar ações de verificação de malware. Para obter mais informações, consulte Configure sua instância Now Platform para a integração McAfee ePO.
☐	Como administrador McAfee ePO, configure o console McAfee ePO. **a.** Verifique se você está usando a versão 5.9 do McAfee ePO. **b.** Instale o plug-in de extensão ServiceNowMcAfee ePO no console []. **c.** Verifique se você criou marcadores de segurança no console McAfee ePO para o host isolado e inicie as ações de verificação de malware. Para obter mais informações, consulte Configure o console McAfee ePO para integração com Security Incident Response (SIR). Para obter mais informações e obter o arquivo do plug-in de extensão, na sua instância Now Platform, navegue até **Conhecimento** > **Artigos** > **Todos** e, no campo Pesquisar, insira `ServiceNow Security Operations Extension para McAfee ePO`.
☐	Como um usuário com a função de administrador Now Platform, instale a aplicação McAfee ePO a partir do ServiceNow Store, configure um servidor e conecte-se ao console McAfee ePO. Para obter mais informações, consulte Instalar a aplicação e configurar um servidor para a integração McAfee ePO.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Como um usuário com a função de administrador de incidentes de segurança Now Platform, edite os nomes dos marcadores de segurança na sua instância Now Platform® para que eles correspondam aos nomes dos marcadores que você criou no console McAfee ePO. Para obter mais informações, consulte Editar marcadores de segurança no Now Platform para a integração McAfee ePO.
	Como um usuário com a função de administrador de incidentes de segurança, crie um perfil para capacidades McAfee ePO. Para obter informações sobre perfis, consulte McAfee ePO perfis de capacidade de integração. Para obter as etapas necessárias para criar um perfil, consulte Criar um perfil de capacidade para a integração McAfee ePO.
	Como um usuário com a função de administrador de incidentes de segurança, configure um perfil e teste incidentes de segurança. **a.** Revise as informações sobre condições e configurações de gatilho. **b.** Configure um perfil. **c.** Teste e visualize incidentes de segurança. **d.** Localize os resultados da pesquisa e outros detalhes nas listas relacionadas ao incidente de segurança. **e.** Crie e configure diferentes tipos de perfis e teste incidentes de segurança para cada tipo. Para obter informações sobre condições de gatilho e o campo de IC alternativo, consulte Definição de condições de acionamento com um campo de item de configuração (IC) para um perfil McAfee ePO. Para obter as etapas necessárias para configurar um perfil, testar e visualizar incidentes de segurança e exemplos de tipos de perfil, consulte os exemplos a seguir Configurando perfis para a integração McAfee ePO.
	Como um usuário com a função de analista de incidentes de segurança Now Platform, envie solicitações adicionais para verificações de malware e eventos de ameaça de lista. Para obter mais informações, consulte Acionar o perfil McAfee ePO manualmente a partir de um incidente de segurança. No Now Platform, como um usuário com uma função de aprovação ou, como membro de um grupo de aprovação, aprove solicitações para isolar o isolamento de host e remover o isolamento. Para obter mais informações sobre como processar solicitações de aprovação, consulte Criar um grupo de aprovação.

Você concluiu com sucesso as etapas de configuração, instalou e configurou a aplicação e verificou os resultados esperados para a integração.

Configure sua instância Now Platform® para a integração McAfee ePO

A seção a seguir lista as tarefas de configuração que você precisa concluir na instância Now Platform® antes de instalar a aplicação para a integração McAfee ePO.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar requisitos

Função necessária: Now Platform administrador (admin). Revise as informações a seguir antes de sua instância Now Platform® para a integração McAfee ePO.

A tabela a seguir é uma lista de requisitos de configuração para a aplicação. Verifique se você concluiu essas tarefas antes de instalar a aplicação para a integração do ServiceNow Store.

Configurar tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR).	As seguintes funções são necessárias: • Um usuário com a função de administrador do sistema (admin) para instalar a aplicação. • Um usuário com a função de administrador de incidentes de segurança (sn_si.admin) configura a aplicação e cria, ativa e remove perfis. • Um usuário com a função de analista de incidentes de segurança (sn_si.analyst) trabalha com incidentes de segurança. As tarefas incluem o início manual de perfis a partir de incidentes de segurança. Se a opção de aprovação for selecionada em um perfil durante a etapa de configuração, os usuários com essa função também enviarão solicitações para isolar hosts e devolvê-los à rede.
Verifique se você está usando a versão 5.9 do McAfee ePO.	A integração é compatível com a versão 10.4.3 do McAfee ePolicy Orchestrator.
Verifique se você instalou o plug-in de extensão ServiceNowMcAfee ePO no console [].	Instale o plug-in McAfee ePOServiceNow no console []. Para obter mais informações e obter o arquivo do plug-in, na sua instância Now Platform, navegue até **Conhecimento** > **Artigos** > **Todos** e, no campo Pesquisar, insira ServiceNow Security Operations Extension para McAfee ePO .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar tarefa	Descrição
	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Espaço de resposta a incidentes de segurança **3.** Estrutura de integração de segurança **4.** Security Support Common **5.** Orquestração de suporte de segurança Para obter mais informações sobre como instalar as aplicações principais das Operações de segurança, consulte e .
Verifique se você instalou e configurou um MID Server.	Um MID Server instalado e configurado é necessário em sua instância Now Platform®. Consulte o site de documentação de produtos da ServiceNow para obter mais informações sobre MID Servers.
Se você quiser habilitar o processo de aprovação para perfis, verifique se criou um grupo de aprovação para processar solicitações.	Há um processo de aprovação opcional disponível para isolar máquinas host e restaurá-las na rede. Se esta opção estiver habilitada, a aprovação prévia será necessária antes que as máquinas host sejam isoladas e restauradas para sua rede. Se sua organização quiser um nível extra de controle sobre essas ações, habilite a opção **Requer aprovação** durante a etapa de configuração de um perfil. Por padrão, a autoridade de aprovação é atribuída ao administrador de incidentes de segurança Now Platform® (sn_si.admin). Esta autoridade pode ser reatribuída a um grupo de aprovação. Dentro do grupo, qualquer membro tem permissão para aprovar ou rejeitar solicitações. Você seleciona um grupo de aprovação ativo durante a etapa de configuração da configuração do seu perfil. Para obter mais informações, consulte Criar um grupo de aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o console McAfee ePO para integração com Security Incident Response (SIR)

A seção a seguir lista as etapas de configuração que você deve concluir no console do McAfee ePO antes de instalar a aplicação do ServiceNow Store para a integração.

Antes de Iniciar

Função necessária: McAfee ePO administrador

Como um usuário com a permissão de administrador McAfee ePO, verifique se você instalou o plug-in de extensão `Servicenow.zip` no console McAfee ePO. Este plug-in de extensão é necessário para a integração. Para obter mais informações e obter o plug-in, em sua instância Now Platform, navegue até **Conhecimento** > **Artigos** > **Todos**. No campo Pesquisar, insira ServiceNow Security Operations Extension para McAfee ePO.

Por Que e Quando Desempenhar Esta Tarefa

O plug-in de extensão ServiceNow conecta sua instância Now PlatformMcAfee ePO ao console []. Esta conexão permite que você faça referência aos marcadores de segurança que você cria no console McAfee ePO para o host isolado e inicie ações de verificação de malware para os perfis de capacidade na sua instância Now Platform.

Os marcadores de segurança no console McAfee ePO devem corresponder aos marcadores de segurança nos registros de capacidade da instância Now Platform.

As etapas a seguir mostram como instalar o plug-in de extensão, criar um marcador de segurança no console do McAfee ePO e atribuir uma ação ao marcador. Para obter mais informações sobre os marcadores de segurança no console McAfee ePO, consulte o site de documentação de produtos da McAfee .

Nota: Os números na seção a seguir são do console McAfee ePO.

Procedimento

1. Se você não instalou o plug-in de extensão ServiceNowMcAfee ePO no console [], siga estas etapas para instalá-lo.

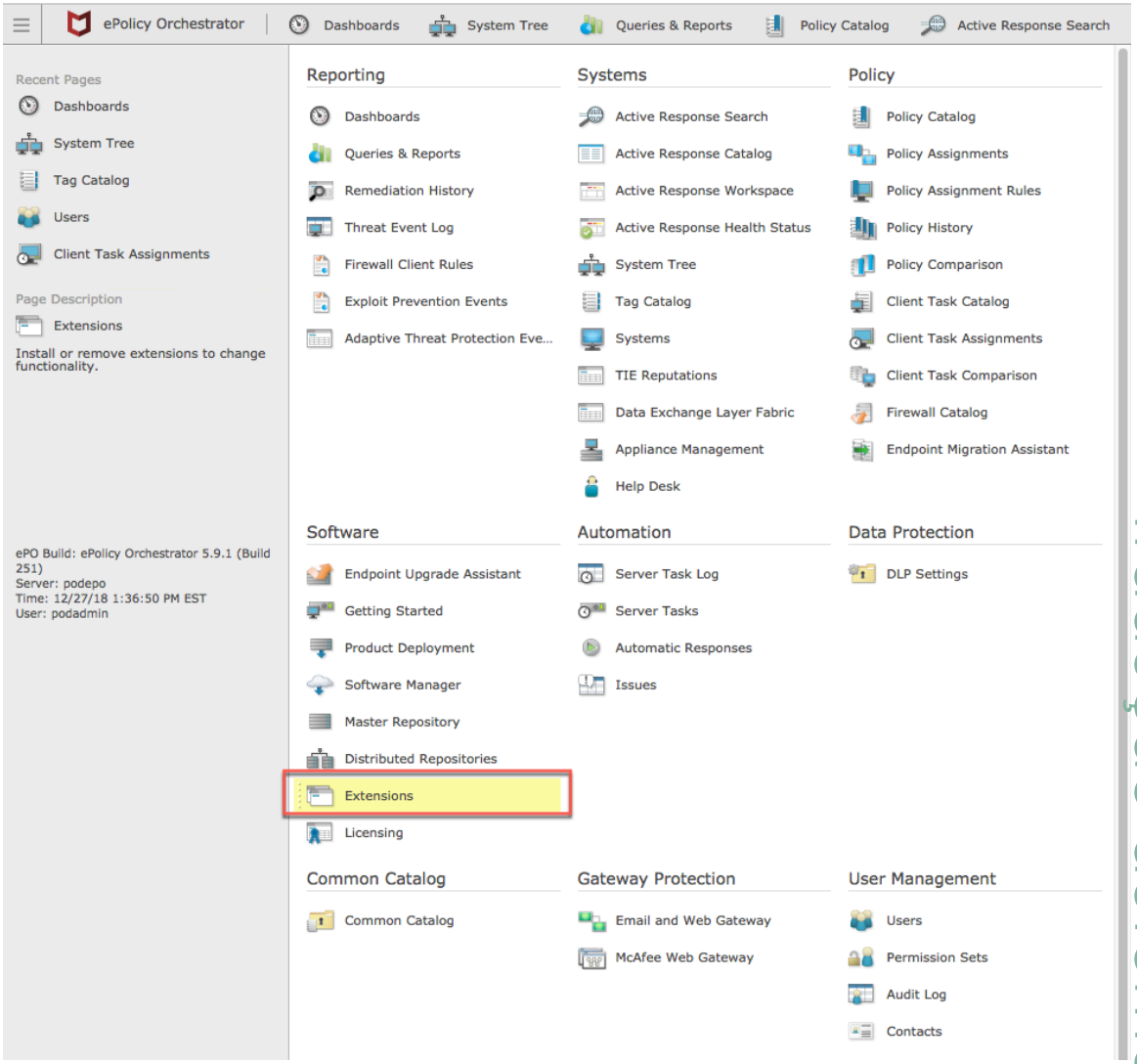
   a. Faça login no console do McAfee ePO com seu nome de usuário e senha da McAfee.

2. Se a página mostrada na figura a seguir não for exibida, no canto superior esquerdo da faixa da página inicial, clique no ícone de menu para exibi-la.

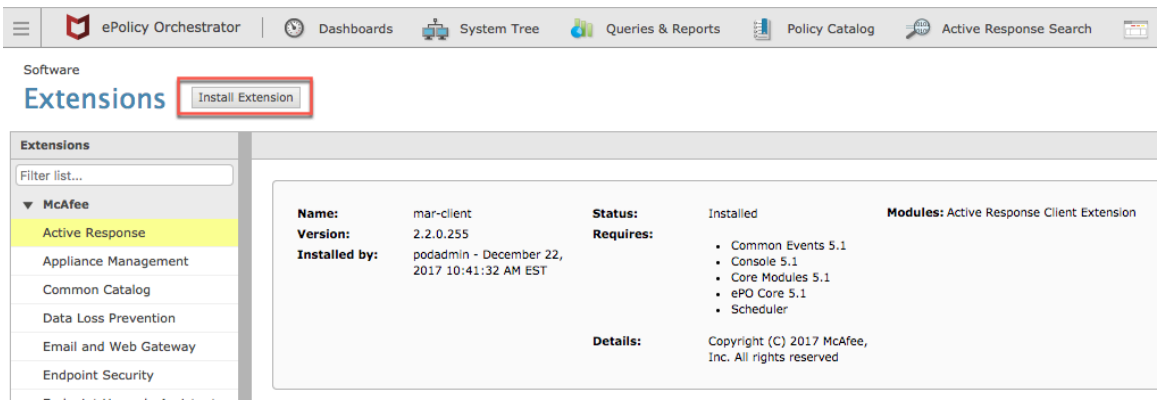
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na seção Software, clique no link **Extensões**.



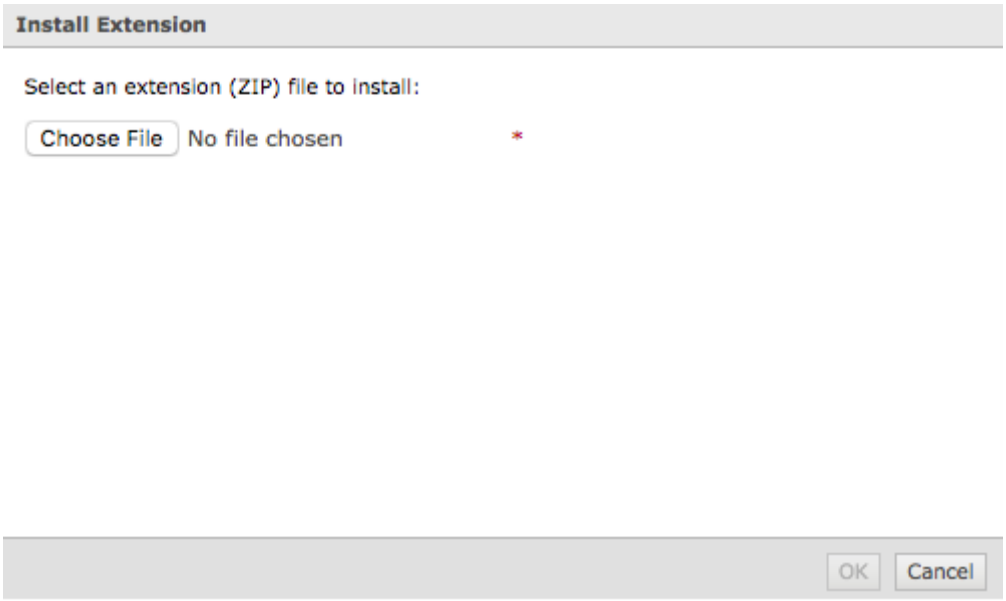
4. Na página Extensões exibida, clique em **Instalar extensão**.



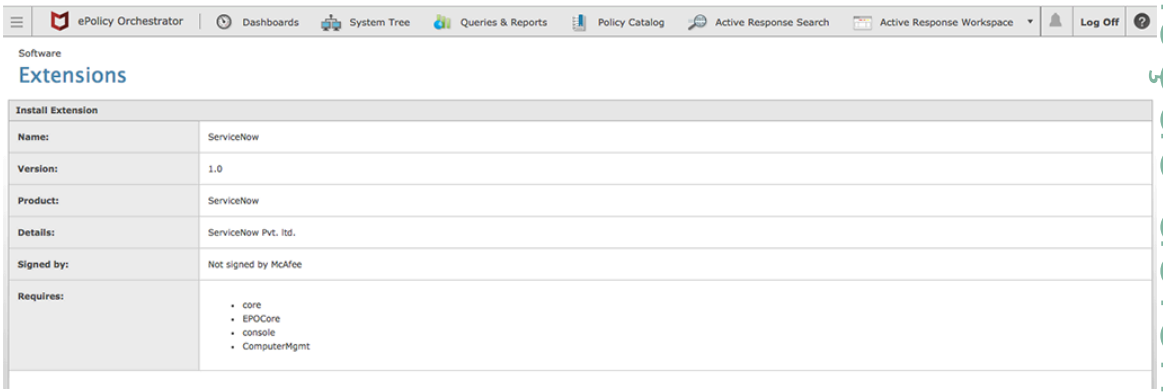
5. Na caixa de diálogo Instalar extensão, clique em **Escolher arquivo**, navegue até o arquivo `Servicenow.zip` em seu sistema e clique em **OK** para baixá-lo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que o download for concluído, a página Extensões de software será exibida com o plug-in Extensão ServiceNow listado.



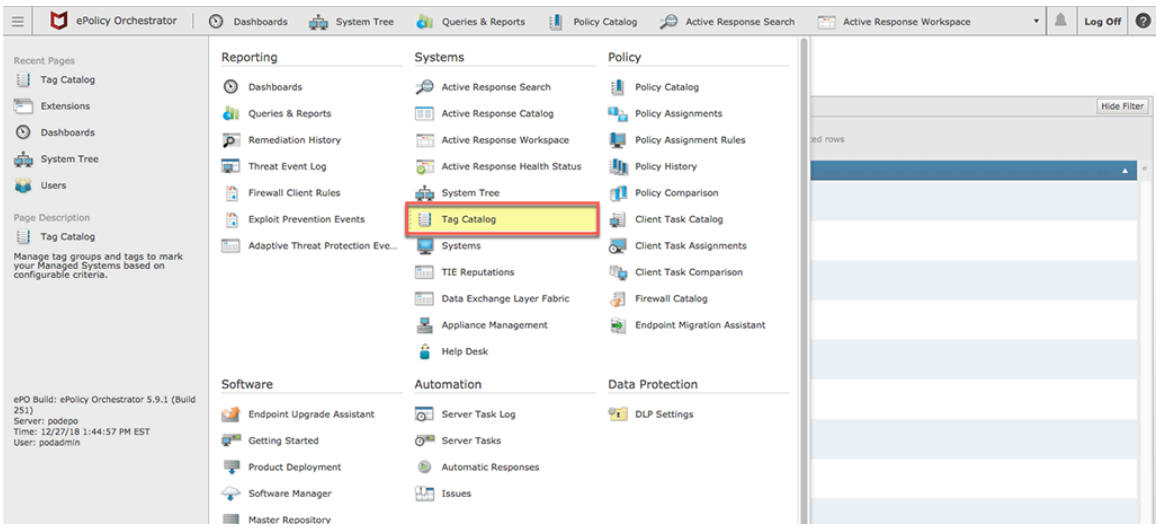
Você instalou com sucesso a extensão do plug-in ServiceNowMcAfee ePO no console [].

6. Se você não criou marcadores de segurança no console McAfee ePO para iniciar a verificação de malware e isolar as ações de host, siga estas etapas.

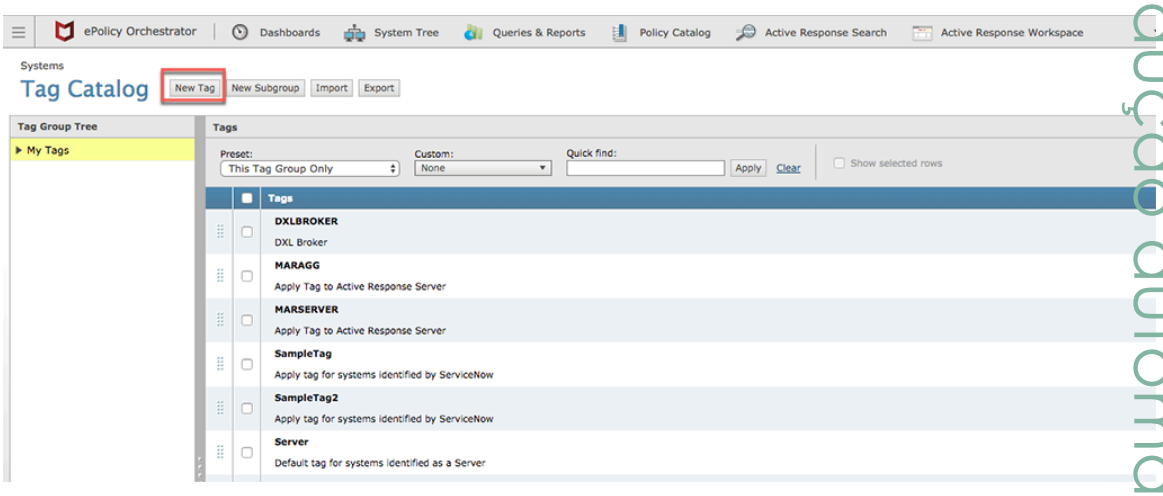
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até a página inicial e clique no link **Catálogo** de marcadores.

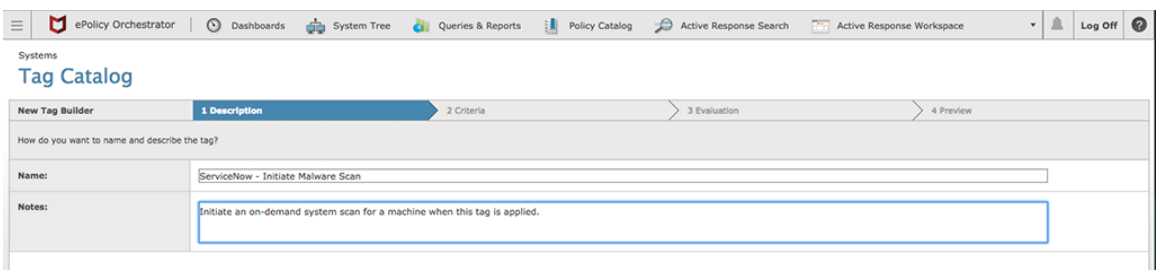


b. Na página Catálogo de marcadores exibida, clique em **Novo marcador**.



c. Com a etapa Descrição selecionada na barra de andamento exibida, insira um nome e uma descrição para o marcador.

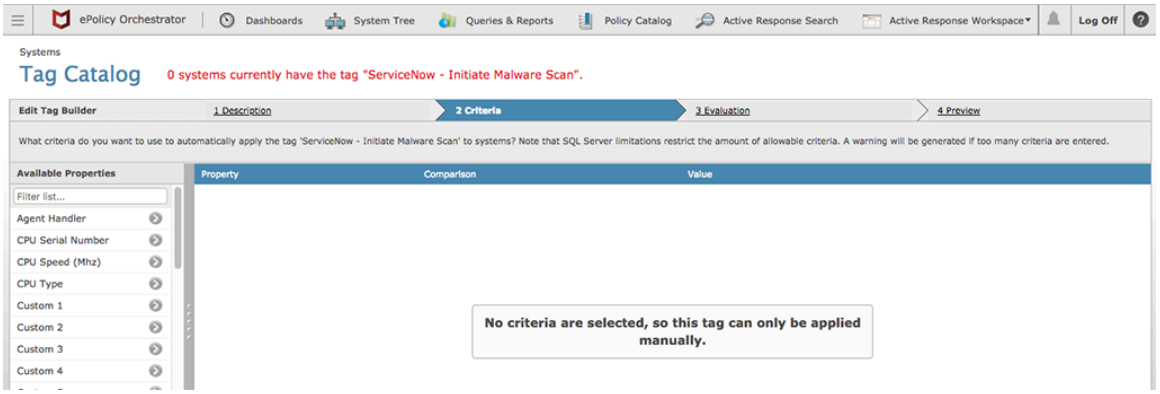
Para este exemplo, é exibido um marcador com um nome e uma descrição da capacidade Iniciar verificação de malware. Este nome de marcador é o que é correspondido e referenciado em sua instância Now Platform.



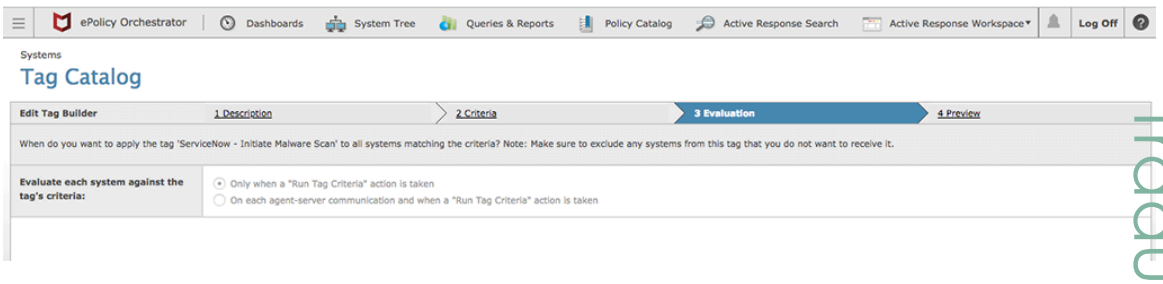
d. Para avançar para a etapa Critérios, clique em **Critérios** na barra de andamento.
As mensagens exibidas indicam que nenhuma ação está atribuída a este marcador no momento e que o marcador só pode ser aplicado manualmente.

Tradução automática

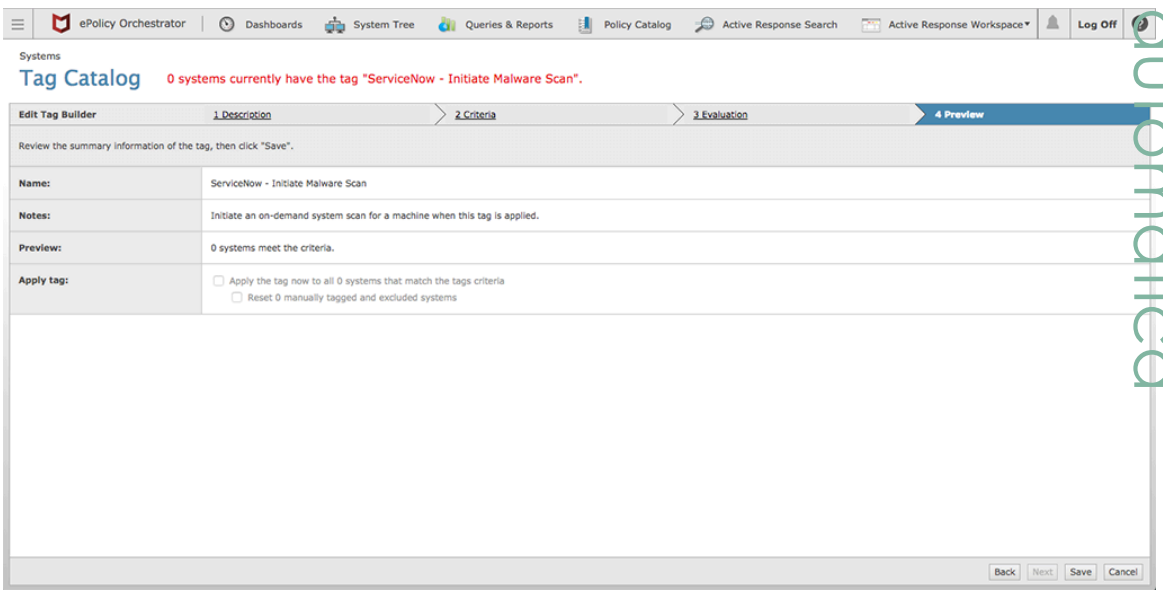
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Clique em **Avaliação** na barra de andamento para continuar.



f. Com a página Catálogo de marcadores da etapa Avaliação exibida, deixe as configurações nesta página em seus padrões e, na barra de andamento, clique em **Visualizar**.

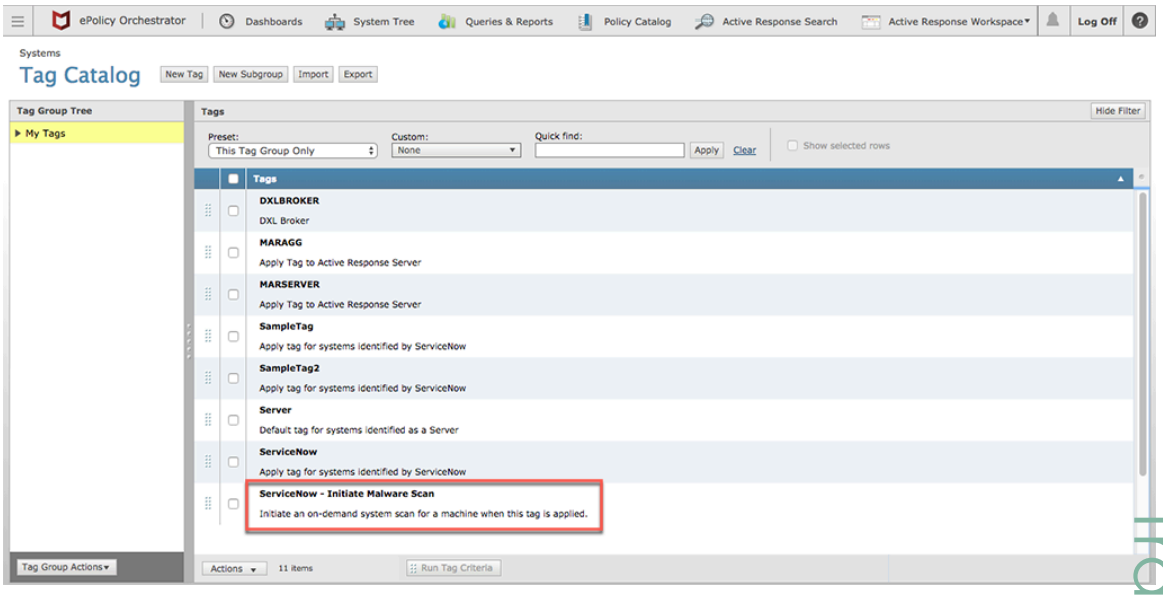


g. Com a página Visualização exibida, no canto inferior direito da página, clique em **Salvar** para salvar o registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O novo marcador é exibido no Catálogo de marcadores, conforme mostrado na figura a seguir.

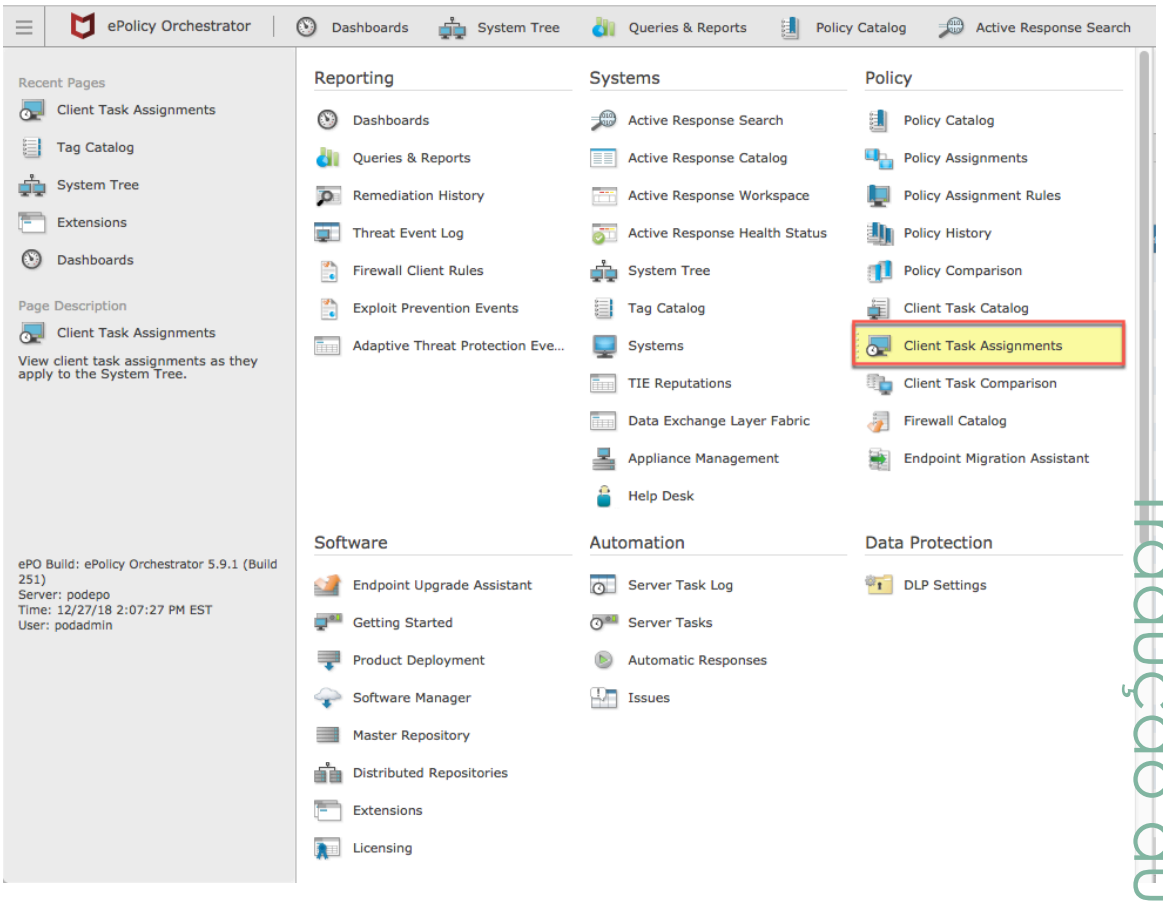


7. Crie um marcador de segurança para a ação de isolamento de host repetindo as etapas anteriores.
   Depois de criar os dois marcadores, você estará pronto para atribuir ações aos novos marcadores.
8. Para adicionar uma ação ao novo marcador, siga estas etapas.

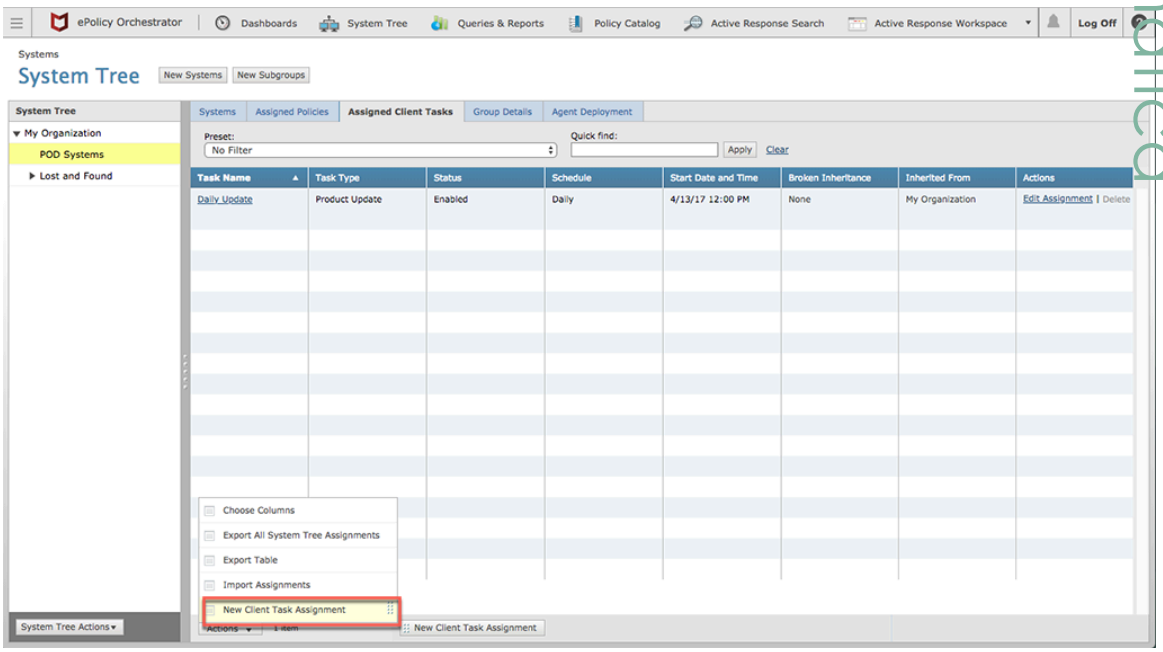
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até a página inicial e, na seção Política, clique no link **Atribuições de tarefa do cliente**.



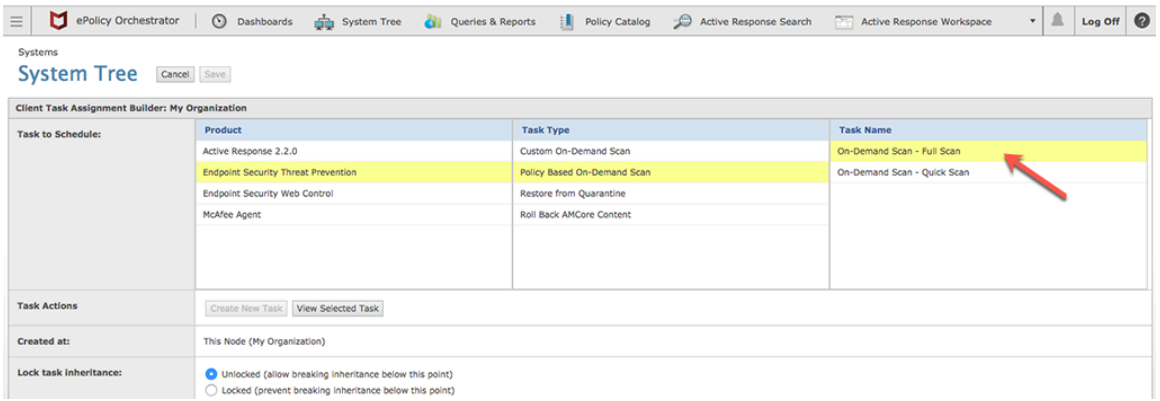
b. Na página Árvore do sistema exibida, na parte inferior da página, expanda o menu **Ações** e selecione **Nova atribuição de tarefa de cliente**.



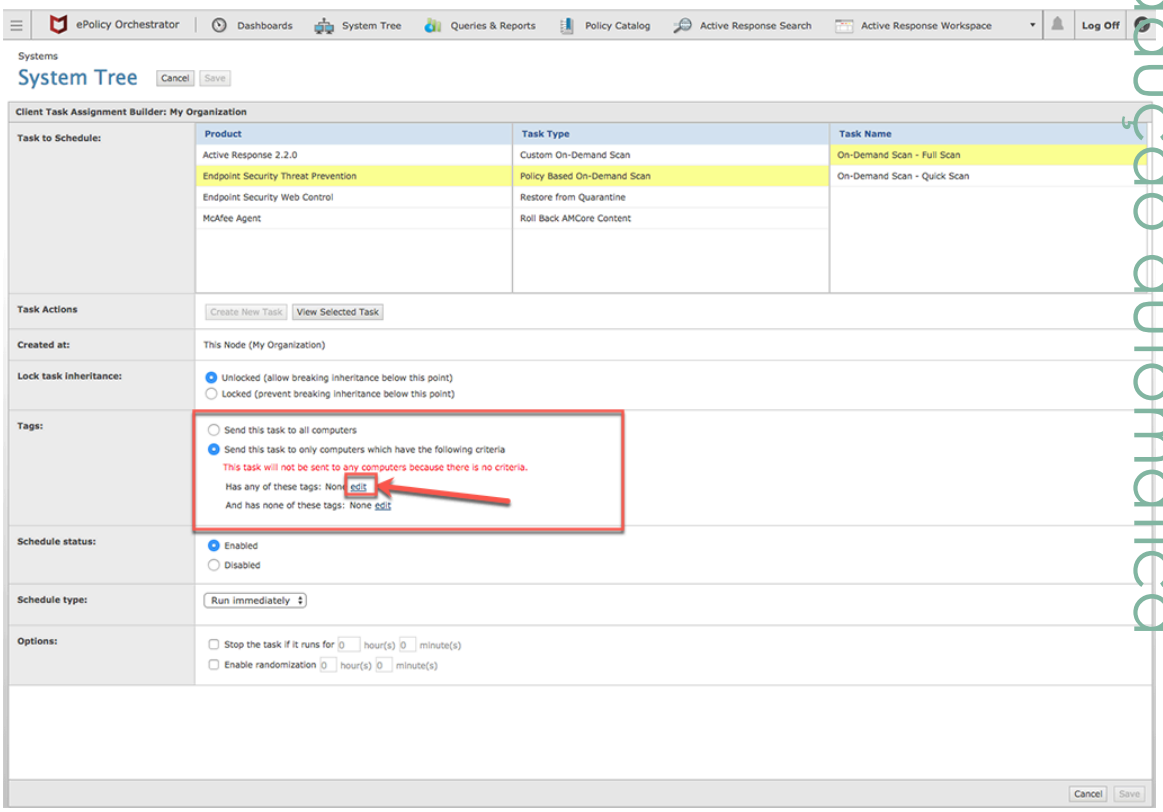
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na página exibida, navegue até **Prevenção de ameaças de segurança do endpoint** > **Verificação sob demanda baseada em política** > **Verificação sob demanda - Verificação completa** selecionando o caminho, conforme mostrado na figura a seguir.



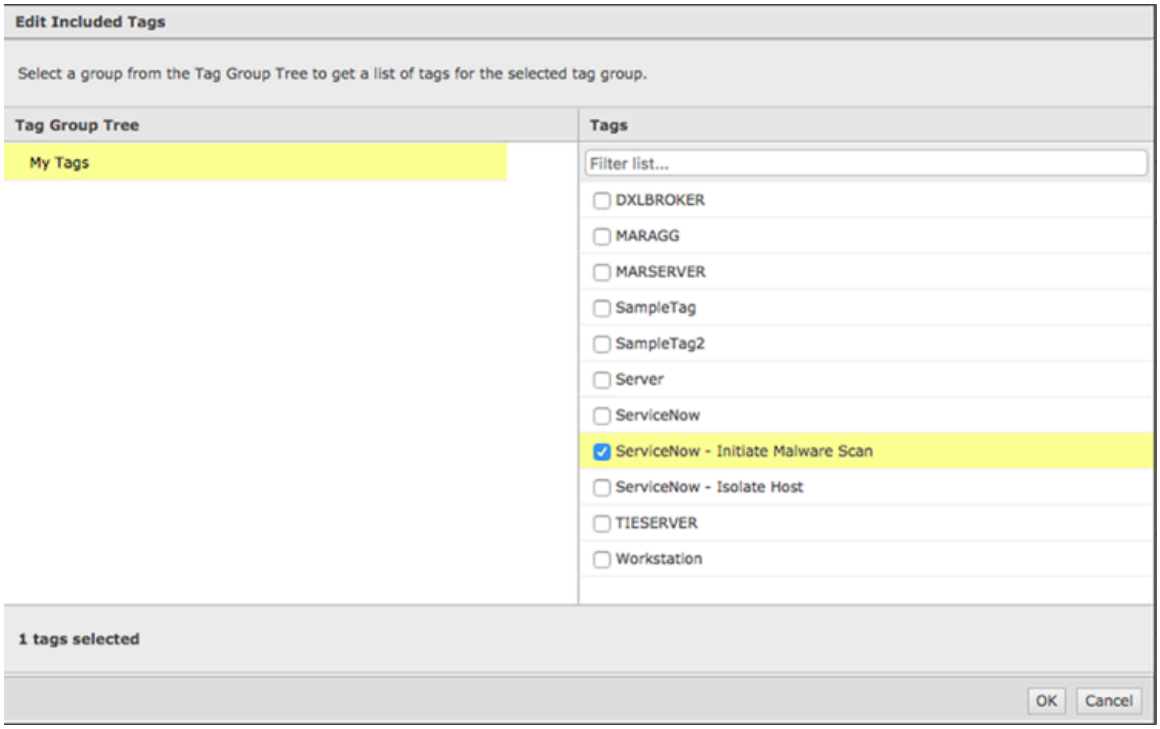
d. Na seção Marcadores, abaixo do botão de opção e ao lado de `Tem algum destes marcadores:`, clique no link de **edição** para editar os critérios do marcador.



e. Na caixa de diálogo exibida, selecione o marcador Iniciar verificação de malware ServiceNow que você criou nas etapas anteriores e clique em **OK**.

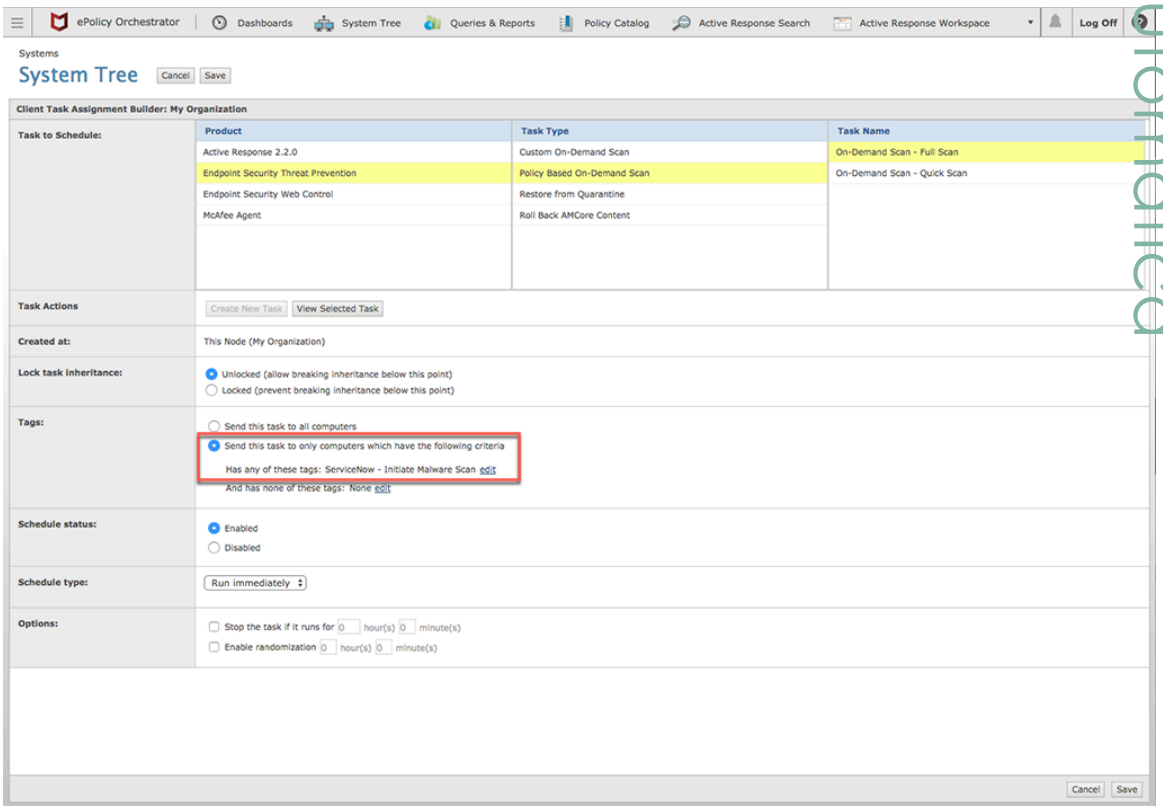
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O marcador de verificação de malware iniciada da ServiceNow que você criou é atribuído à ação de verificação sob demanda.

f. Clique em **OK**.
Na seção Marcadores, abaixo do botão de opção e ao lado de `Tem algum destes marcadores:`, o marcador Iniciar verificação de malware é exibido.

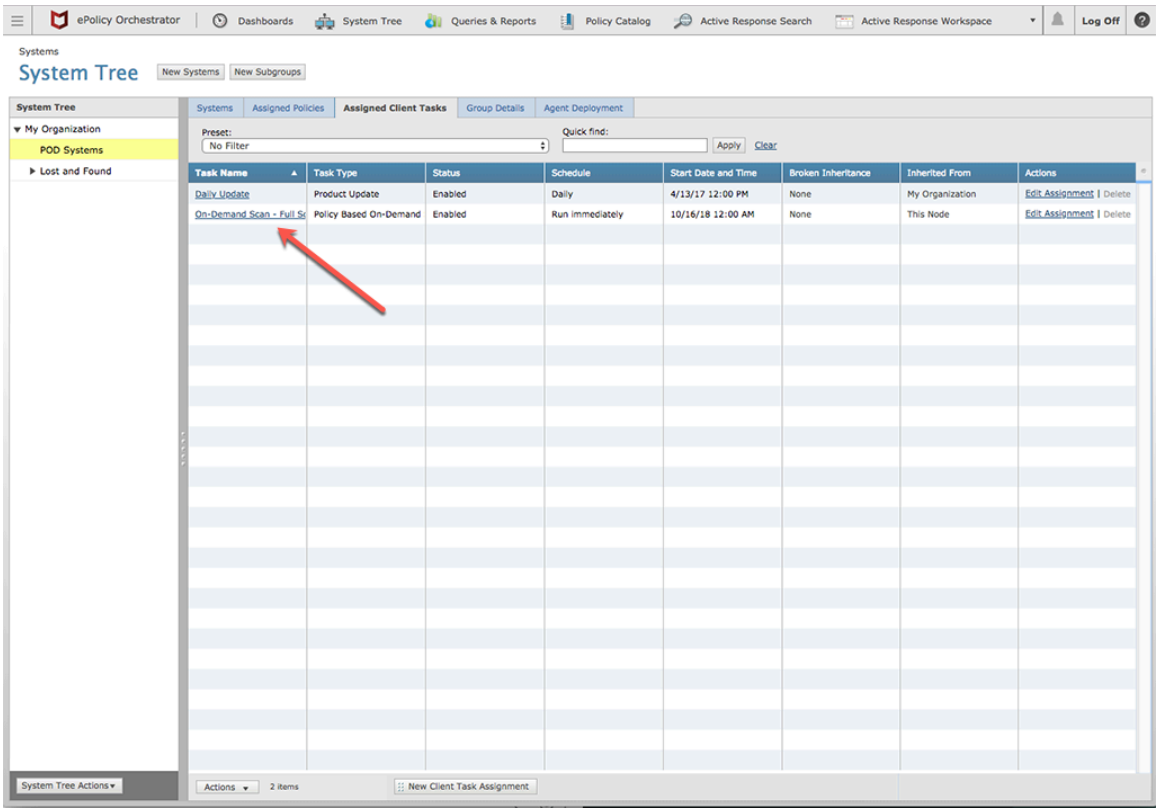


g. Clique em **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na página Árvore do sistema, a tarefa é exibida na lista Tarefas de cliente atribuídas (guia).



h. Se você não atribuiu uma ação à ação Isolar host, repita as etapas anteriores para atribuí-la.

Você instalou com sucesso o plug-in de extensão, criou marcadores de segurança e atribuiu tarefas aos seus marcadores. Você concluiu a configuração da integração no console McAfee ePO. A próxima etapa é configurar um servidor em sua instância Now Platform.

Instalar a aplicação e configurar um servidor para a integração McAfee ePO

Antes de invocar os fluxos de trabalho para a integração, instale e configure a aplicação McAfee ePO da ServiceNow Store em sua instância Now Platform. A configuração é necessária para se conectar ao console McAfee ePO.

Antes de Iniciar

Função necessária: Now Platform administrador (admin)

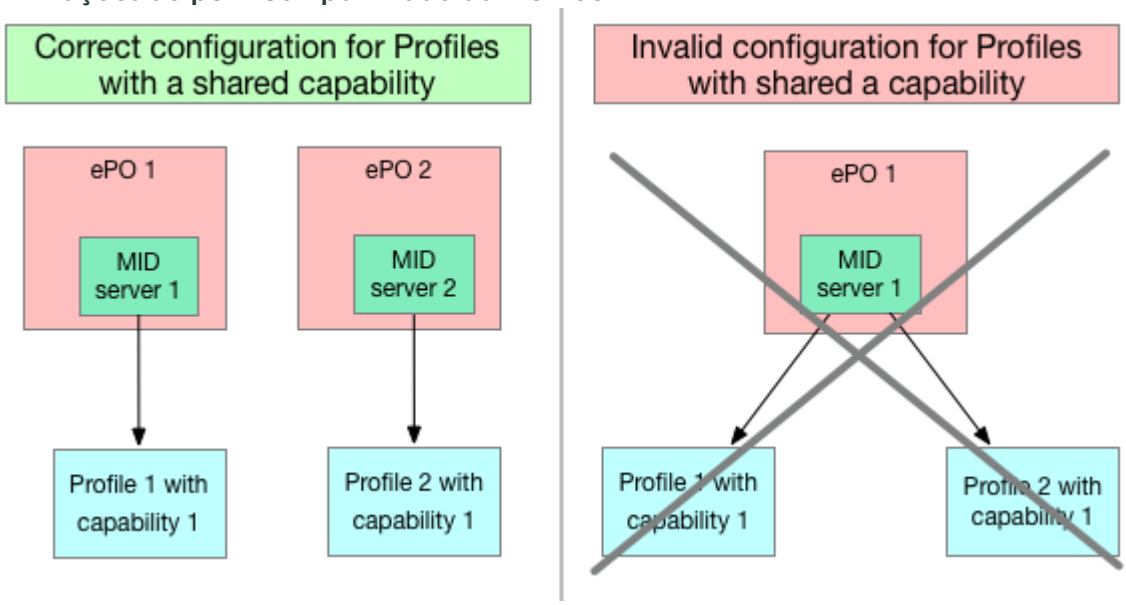
Por Que e Quando Desempenhar Esta Tarefa

A integração oferece suporte a vários servidores, no entanto, para evitar conflitos em perfis que compartilham as mesmas condições de acionamento, você não pode compartilhar uma capacidade McAfee ePO com vários perfis que usam o mesmo servidor McAfee ePO. Por exemplo, conforme mostrado na figura a seguir, você pode ter a capacidade 1 em mais de um perfil, desde que cada servidor McAfee ePO esteja mapeado para um perfil exclusivo que tenha a capacidade 1.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Limitações do perfil compartilhado da McAfee



Procedimento

1. Baixe o McAfee ePO para Operações de segurança do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco de integração McAfee ePO para Operações de segurança e clique em **Configurar**.

4. No formulário, preencha os campos.

Configuração de integração do McAfee ePO

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
Nome do Servidor do ePO	Nome do servidor McAfee ePO. Se você usar um servidor, um exemplo é, `McAfee HQ` (sede da McAfee). Este nome é como o servidor e as credenciais relacionadas são reconhecidos.

Tradução automática

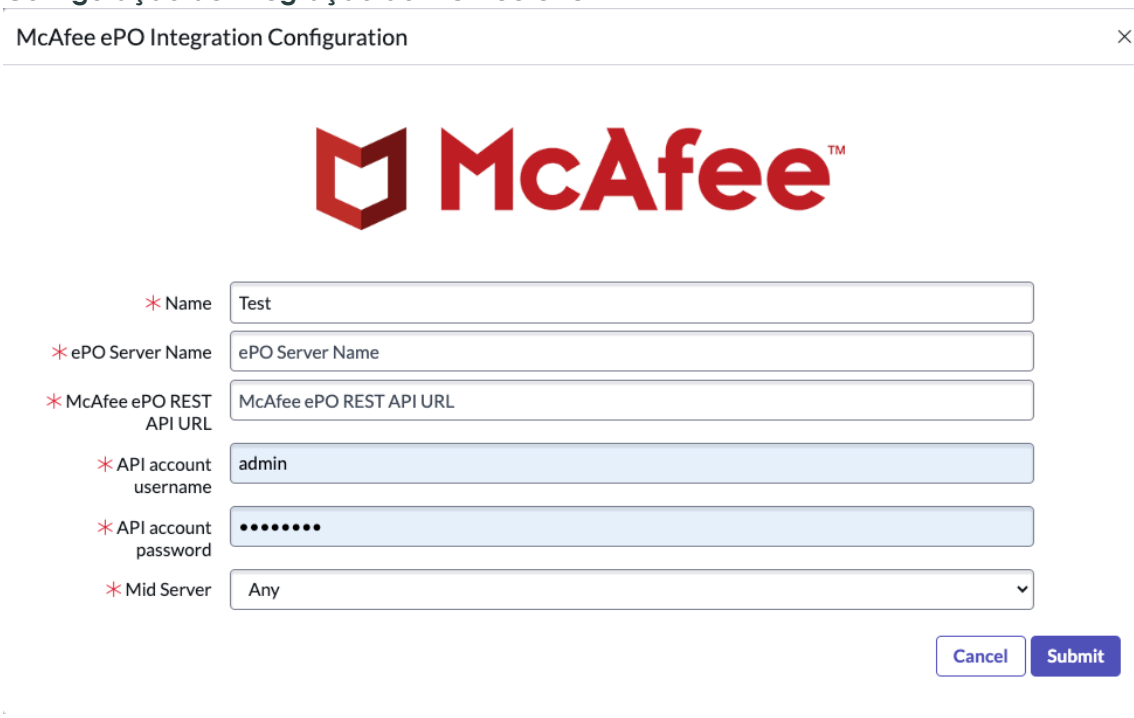
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se sua organização precisar de suporte para vários servidores, insira o nome de cada servidor e repita o processo.
URL da REST API do McAfee ePO	URL base que hospeda a McAfee ePO REST API. Insira o URL com o protocolo https://, por exemplo, `https://corp.epo_server:8443`.
Nome de usuário da conta da API	Nome de usuário exclusivo da conta, por exemplo, `ServiceNow API`.
Senha da conta da API	Senha exclusiva para a conta da API.
MID Server	Selecione o nome do MID Server que você configurou durante a configuração da sua instância Now Platform. Você pode selecionar um MID Server específico na lista ou selecionar **Qualquer** para habilitar uma seleção automática de um MID Server válido na lista para esta integração. **Nota:** ◦ O MID Server selecionado durante este tempo de configuração se aplica a toda esta integração. ◦ Somente os MID Servers ativos e validados são exibidos nesta lista. Por padrão, o valor é definido como **Qualquer**. Um nome de exemplo é `secops_local_midserver`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de integração do McAfee ePO



5. Clique em **Enviar**.
   A lista Configurações do McAfee ePO é exibida com o novo registro de configuração. Você concluiu com sucesso a configuração de um servidor McAfee ePO.

   Nota: Se sua organização precisar de suporte para vários servidores, repita as etapas.

Editar marcadores de segurança no Now Platform para a integração McAfee ePO

Como parte da configuração da integração, edite os nomes dos marcadores de segurança que você criou no console McAfee ePONow Platform da instância []. Edite os nomes dos marcadores na instância Now Platform para que correspondam aos nomes dos marcadores no console McAfee ePO.

Antes de Iniciar

Função necessária: Now Platform administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Os nomes dos marcadores de segurança no console McAfee ePO para iniciar a verificação de malware e isolar ações de host devem corresponder aos nomes dos marcadores de segurança nos registros desses recursos da instância Now Platform.

Antes de criar um perfil de capacidade para executar suas capacidades, exiba a lista de capacidades McAfee ePO disponíveis e edite os marcadores de segurança em sua instância Now Platform para que eles correspondam aos nomes de marcador de segurança no console McAfee ePO.

Para obter mais informações sobre como criar os nomes de marcador de segurança no console do McAfee ePO, consulte Configure o console McAfee ePO para integração com Security Incident Response (SIR).

Tradução automática

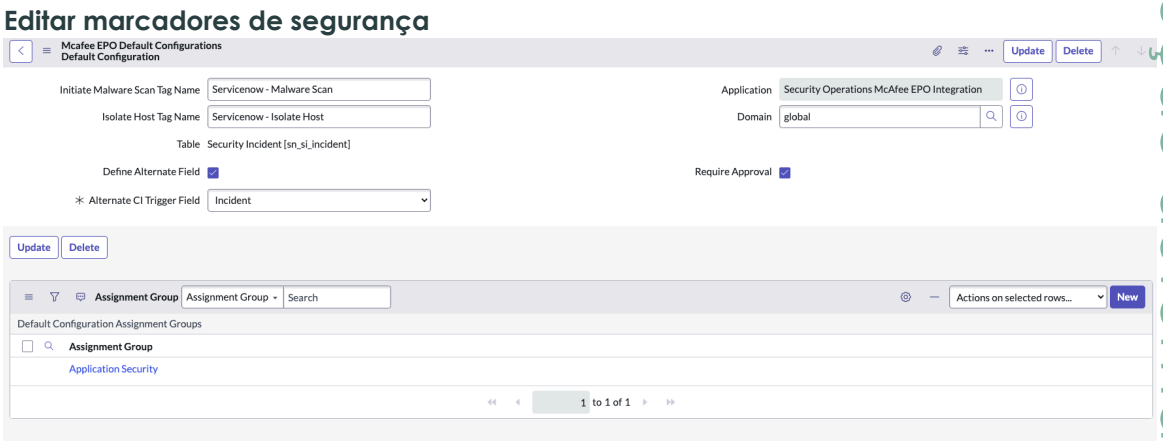
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração do McAfee ePO** > **Configurações Padrão**.
2. Para editar o nome do marcador de segurança da integração McAfee ePO, clique em **Configuração padrão**.

   Nota: Garante que você execute esta configuração depois de instalar a integração McAfee ePO.

3. No campo Iniciar nome do marcador de verificação de malware, insira o nome do marcador de segurança que você criou no console McAfee ePO para a ação de início da verificação.
   Por exemplo, ServiceNow - Malware Scan
4. No campo Isolar nome do marcador de host, insira o nome do marcador de segurança que você criou no console McAfee ePO para a ação de isolamento de host.
   Por exemplo, ServiceNow - Isolar host
5. Se você quiser não usar o campo de gatilho de IC após a criação do incidente, marque a caixa de seleção **Definir campo alternativo**.
   Quando esta opção está habilitada, a lista de seleção do campo de gatilho de IC alternativo é exibida.



6. Escolha um campo alternativo na lista de seleção para verificar seus critérios de pesquisa de IC.
   Para este exemplo, como um usuário com a função sn_si.admin, você acredita que o campo de IC não será preenchido no incidente de segurança após a criação do incidente. Como alternativa, você acha que as informações de IC para um FQDN, nome de host ou endereço IP serão preenchidas no campo `IC identificado` no incidente de segurança e seleciona o campo IC identificado como uma alternativa. O IC identificado é selecionado para este exemplo, mas você pode usar qualquer campo no incidente de segurança para o IC alternativo.
7. No campo Domínio, selecione um domínio ou grupo para esta configuração usando a opção de pesquisa.
   Por exemplo, global.
8. No campo Requer Aprovação, marque a caixa de seleção **Requer Aprovação** se você estiver usando as capacidades de isolamento Isolar Host e Remover.

   Nota: As capacidades Iniciar verificação de malware, Listar eventos de ameaça e Obter detalhes do sistema não precisam de aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Clique em **Atualizar**.
   O nome do marcador do EPO é atualizado e exibido na lista de configurações padrão do McAfee ePO. O nome do marcador de segurança para a ação de verificação de malware na instância Now Platform corresponde ao nome da verificação no console McAfee ePO.

   Você editou com sucesso os nomes de marcador do EPO para a verificação de malware e as capacidades de host isolado em sua instância Now Platform. A próxima etapa é criar um perfil para suas capacidades.

Informações relacionadas

Documentação de produto da McAfee

Criar um grupo de aprovação

Crie um grupo de aprovação para a integração McAfee ePO para Operações de segurança que pode aprovar solicitações para isolar máquinas host, restaurando-as na rede.

Antes de Iniciar

Você não pode reatribuir a autoridade de aprovação a um grupo, a menos que um grupo de aprovação esteja disponível em sua instância.

Nota: A opção de aprovações em Configurando perfis para a integração McAfee ePO aparece somente para as capacidades Isolar host e Remover isolamento de host.

Função necessária: Now Platform® Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

As solicitações de aprovação enviadas pelo analista de incidentes de segurança para isolar máquinas host e remover o isolamento são atribuídas ao usuário com a função sn_si.admin por padrão. Como um usuário com esta função, você pode reatribuir esta autoridade de aprovação durante a etapa de configuração de um perfil. Antes que você possa reatribuir autoridade a um grupo de aprovação, um grupo de aprovação deve estar disponível na lista `Grupos` em sua instância Now Platform.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na lista de grupos, clique em **Novo**.
3. No formulário, preencha os campos.

Formulário de grupo de aprovação

Campo	Descrição
Nome	Nome do grupo que é exibido quando uma solicitação de aprovação é enviada, por exemplo, `Aprovadores Isolamento de host da McAfee`.
E-mail do grupo	Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo, `McAfeeapproval@servicenow`.com

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Gerente	Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	(Opcional) Outro grupo do qual este grupo faz parte, se este grupo tiver um primário.
Descrição	Informações adicionais sobre este grupo.
Incluir membros	Opção para incluir membros neste grupo.
Atribuído padrão	Opção para escolher um usuário como atribuído padrão para este grupo. Use a opção Pesquisar para abrir a lista de usuários.
Funções	Opção para selecionar as funções para este grupo. Use a opção Adicionar e Remover para adicionar e remover funções.
Tipo	Opção para escolher uma categoria para este grupo. Use a opção Pesquisar para abrir a lista de tipos de grupo.
Fornecedores	Opção para escolher um fornecedor para este grupo. Use a opção Pesquisar para abrir a lista de fornecedores.

4. Clique em **Enviar**.
   O novo grupo é exibido na lista Grupos.

   Este grupo está disponível para processar solicitações quando você habilita a opção **Requer aprovação** durante a configuração deste perfil.

   Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação navega até a guia **Minhas aprovações** no Now Platform.

McAfee ePO perfis de capacidade de integração

Como um usuário com a função de administrador de incidentes de segurança (sn_si.admin), você cria perfis para as capacidades McAfee ePO em sua instância Now Platform®. Você agrupa consultas ou ações em perfis e determina quais McAfee ePO capacidades deseja executar quando um novo incidente de segurança for criado.

Perfis de capacidade

Você cria perfis™ para poder agrupar McAfee ePO capacidades e definir as configurações dessas capacidades a partir da sua instância Now Platform®. Você tem a flexibilidade de criar vários perfis para essas capacidades, o que permite determinar quais ações ou consultas são invocadas quando um incidente Security Incident Response (SIR) é criado. Para atender às necessidades da sua organização, você pode criar um único perfil que executa consultas para obter detalhes do sistema, iniciar verificações de malware e isolar máquinas host, por exemplo, ou criar vários perfis, cada um com sua própria capacidade McAfee ePO.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de perfil e capacidades McAfee ePO necessárias

Finalidade primária do seu perfil	Configurar requisitos	Recursos do McAfee ePO necessários para este tipo de perfil
Reunir detalhes do sistema	Nenhum(a)	**Obter detalhes do host**
Isolar um host	Verifique com o administrador McAfee ePO se você criou os marcadores de segurança para a ação isolar host no console McAfee ePO. Para obter mais informações, consulte Configure o console McAfee ePO para integração com Security Incident Response (SIR).	**Isolar host**
Verificar e pesquisar ameaças em seu host	Verifique com o administrador McAfee ePO se você criou os marcadores de segurança para a ação iniciar verificação de malware no console McAfee ePO. Para obter mais informações, consulte Configure o console McAfee ePO para integração com Security Incident Response (SIR).	**Iniciar verificação de malware** **Nota:** Como parte da verificação de malware McAfee ePO, a capacidade Listar eventos de ameaça é invocada automaticamente. No entanto, você não é obrigado a adicionar a capacidade Listar eventos de ameaça ao perfil com a capacidade de verificação de malware. Os resultados da verificação de malware são exibidos na guia Detalhes do evento de ameaça no incidente de segurança.
Remover isolamento de um host	Verifique com o administrador McAfee ePO se você criou os marcadores de segurança para a ação isolar host no console McAfee ePO. Para obter mais informações, consulte Configure o console McAfee ePO para integração com	**Remover isolamento**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de perfil e capacidades McAfee ePO necessárias

Finalidade primária do seu perfil	Configurar requisitos	Recursos do McAfee ePO necessários para este tipo de perfil
	Security Incident Response (SIR).	
Reúna dados de enriquecimento de ameaças.	Nenhum(a)	**Listar eventos de ameaça**

Criar um perfil de capacidade para a integração McAfee ePO

Crie um perfil e selecione os McAfee ePO recursos que você deseja que o perfil execute.

Antes de Iniciar

Função necessária: Now Platform® Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Para esta etapa da configuração, você cria um perfil para as capacidades McAfee ePO. Ao criar perfis, considere a intenção do perfil antes de adicionar McAfee ePO capacidades a ele. Consulte a tabela a seguir ao criar perfis.

A tabela a seguir lista os recursos que você precisa adicionar a um perfil se quiser que o perfil execute determinadas consultas ou ações. Crie um único perfil que execute consultas para obter detalhes do host, inicie verificações de malware, remova o isolamento e isole as máquinas host ou crie vários perfis, cada um com sua própria capacidade única.

Procedimento

1. Navegar até **Integração do McAfee ePO** > **Perfis de capacidade do McAfee ePO**.
   A lista McAfee ePO Perfis de capacidade é exibida.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do perfil de capacidade McAfee ePO. Este nome ajuda a identificar o tipo de perfil e descrevê-lo. Um exemplo de um perfil que executa consultas é Detalhes do host e da ameaça. Este nome também é o nome do marcador de segurança deste perfil por padrão.
Descrição	Informações adicionais sobre o perfil que descrevem melhor as atividades do perfil. Um exemplo de descrição de um perfil que executa consultas é Aprimoramento de ameaças para detalhes do sistema e uma lista de eventos de ameaça. Um exemplo de descrição de um perfil que executa ações é Isolar máquina host.

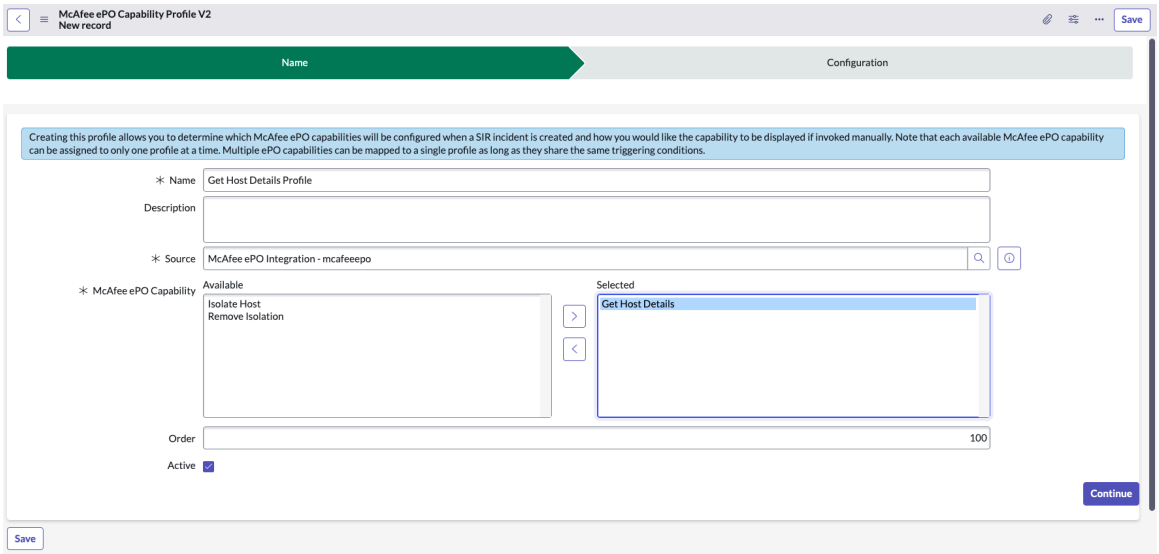
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Origem	Nome do servidor McAfee ePO. Somente servidores configurados estão disponíveis na lista de seleção.
Capacidade do McAfee ePO	Capacidades do perfil McAfee ePO. O McAfee ePO é compatível com os seguintes recursos: ◦ Obter detalhes do host ◦ Isolar perfil de host ◦ Iniciar verificação de malware ◦ Remover isolamento ◦ Listar eventos de ameaça Selecione os recursos desejados para este perfil na coluna **Disponível** e mova-os para a coluna **Selecionado**. Você não pode adicionar Obter detalhes do host, Iniciar verificação de malware e Listar eventos de ameaça no mesmo perfil e não pode adicionar Remover isolamento e Isolar host no mesmo perfil.
Ordem	Prioridade de fluxo de trabalho. O padrão é 100. O valor deste campo indica a ordem em que os fluxos de trabalho são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo de trabalho com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	A caixa de seleção é marcada por padrão para indicar que o perfil está ativo. Quando selecionado, o perfil está ativo e é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem especificadas durante a etapa de configuração. Quando inativo, o perfil não será executado e não estará disponível para ser invocado em uma lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para salvar e validar o perfil, clique em **Continuar**.
   Se a validação for bem-sucedida, a página será recarregada e o formulário de **configuração** será exibido.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, talvez você prefira revisar os conceitos de configuração de perfis e condições de acionamento. Para obter mais informações, consulte Configure o console McAfee ePO para integração com Security Incident Response (SIR) e Definição de condições de acionamento com um campo de item de configuração (IC) para um perfil McAfee ePO.

Definição de condições de acionamento com um campo de item de configuração (IC) para um perfil McAfee ePO

Depois de criar um perfil e selecionar os McAfee ePO recursos que deseja que o perfil execute, defina as configurações do perfil para que ele seja executado somente quando um conjunto de condições específicas for atendido.

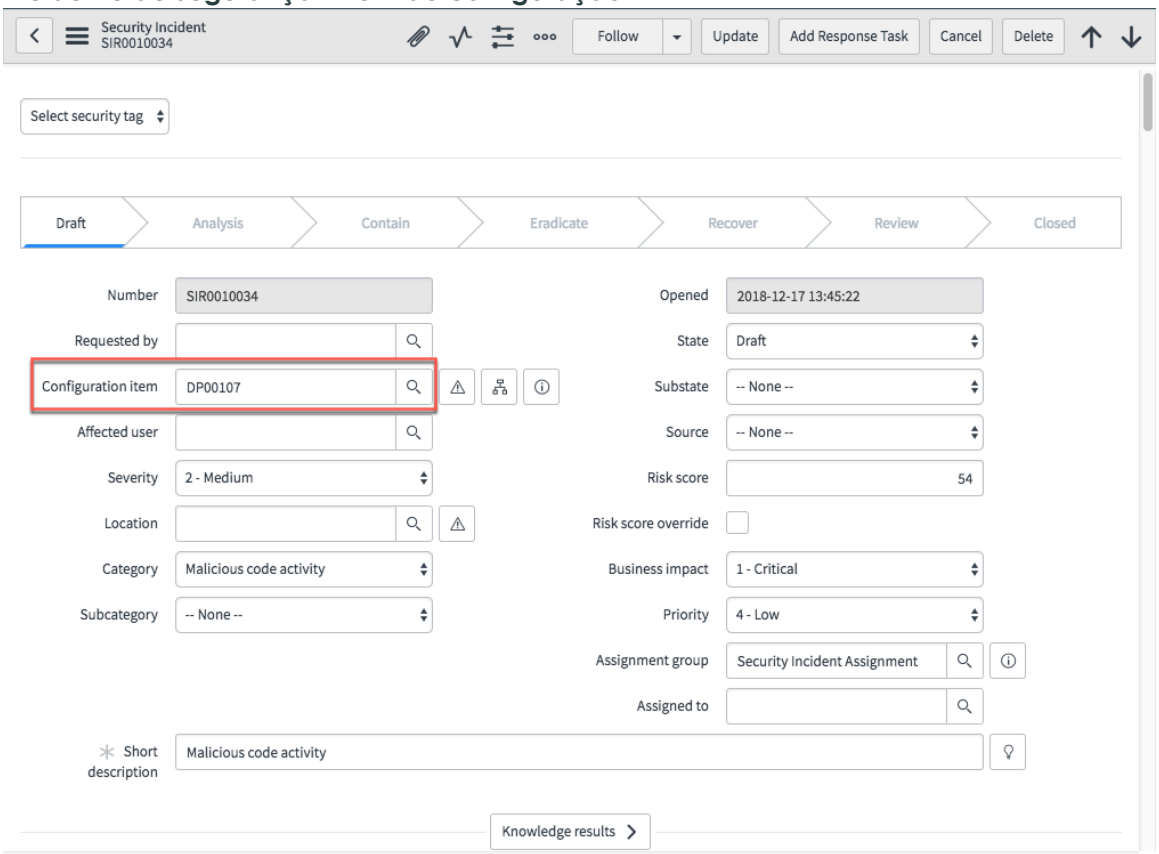
Você tem a flexibilidade de definir essas condições de acionamento para que o perfil seja executado automaticamente com base nos valores de campo padrão que são correspondidos em um incidente de segurança Now Platform® Security Incident Response. Como alternativa, você pode configurar um perfil para que ele pesquise correspondências nos valores de campos que você identifica especificamente no incidente de segurança.

Uma das chaves para a funcionalidade da integração e como um perfil funciona é o campo Item de configuração (IC) no incidente de segurança Now Platform® Security Incident Response (SIR). O valor deste campo é o valor principal em um incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos com as informações armazenadas no banco de dados Now Platform®. Quando um SIR incidente de segurança é criado por um evento de segurança e um perfil é ativado, seus ativos são verificados quanto a um valor correspondente para um nome de domínio totalmente qualificado (FQDN), um nome de host ou um endereço IP com base no valor de o campo Item de configuração.

Em um caso ideal, um valor correspondente é encontrado no banco de dados e os dados podem ser coletados do console McAfee ePO para o ativo correspondente, extraídos para sua instância Now Platform® e exibidos nas listas relacionadas de um incidente de segurança. A figura a seguir mostra um exemplo do campo Item de configuração preenchido com um nome de host em um incidente de segurança SIR.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança - Item de configuração



Nos casos em que o campo Item de configuração (IC) não estiver preenchido no incidente de segurança ou não for possível encontrar uma correspondência para um FQDN, um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no campo de segurança incidente para exibir todos os dados de aprimoramento de IC correspondentes encontrados durante a verificação de seus ativos.

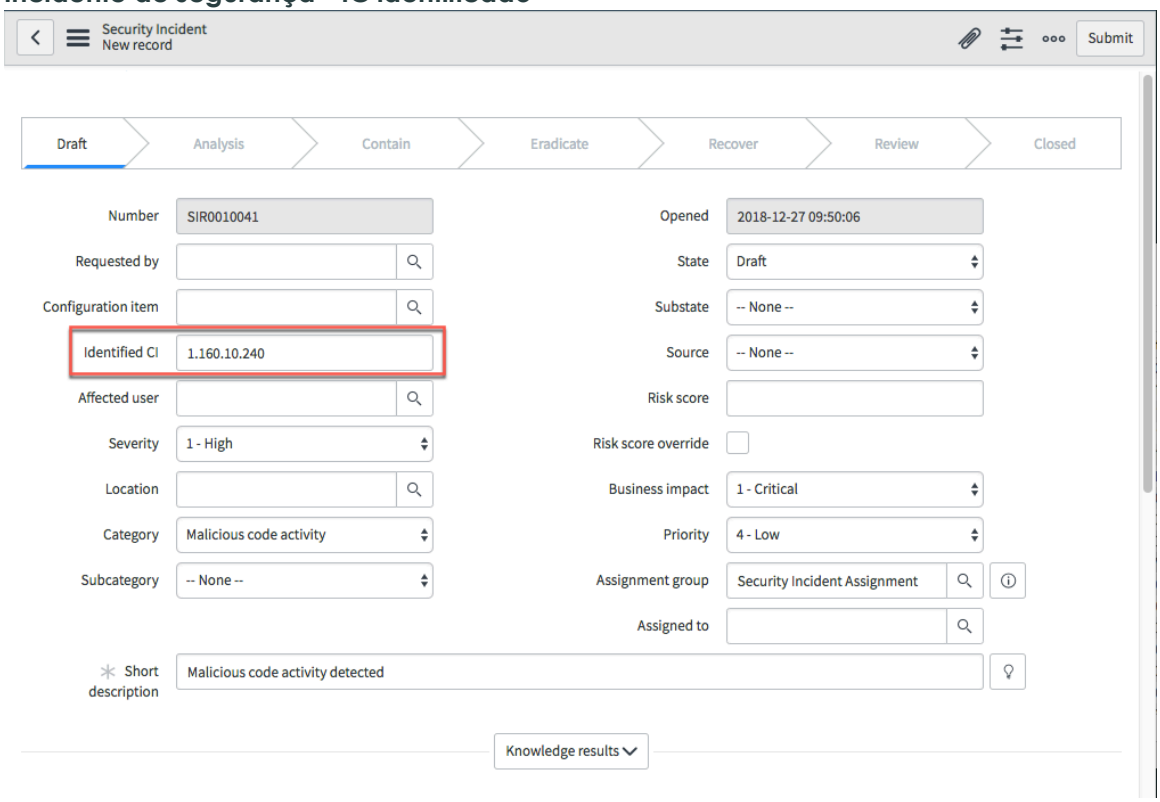
Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de gatilho de IC alternativo para identificação de endpoint para garantir que os dados de aprimoramento de IC da pesquisa McAfee ePO sejam preenchidos no incidente de segurança associado. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como um backup, você garante que seus perfis sejam executados mesmo que o campo de IC não esteja preenchido no incidente de segurança associado após a criação do incidente.

Por exemplo, como analista do centro de operações de segurança (SOC), você cria um campo personalizado para um incidente de segurança chamado Endereço IP no meu incidente de segurança. Se você não achar que o valor deste campo personalizado será exibido no campo Item de configuração no incidente de segurança após a criação do incidente, você pode configurar o perfil para que ele verifique este endereço IP. Se corresponder, o endereço IP será exibido no incidente de segurança no campo de sua escolha. Na figura a seguir, o campo `IC identificado` é selecionado como o campo alternativo para o endereço IP deste exemplo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança - IC identificado

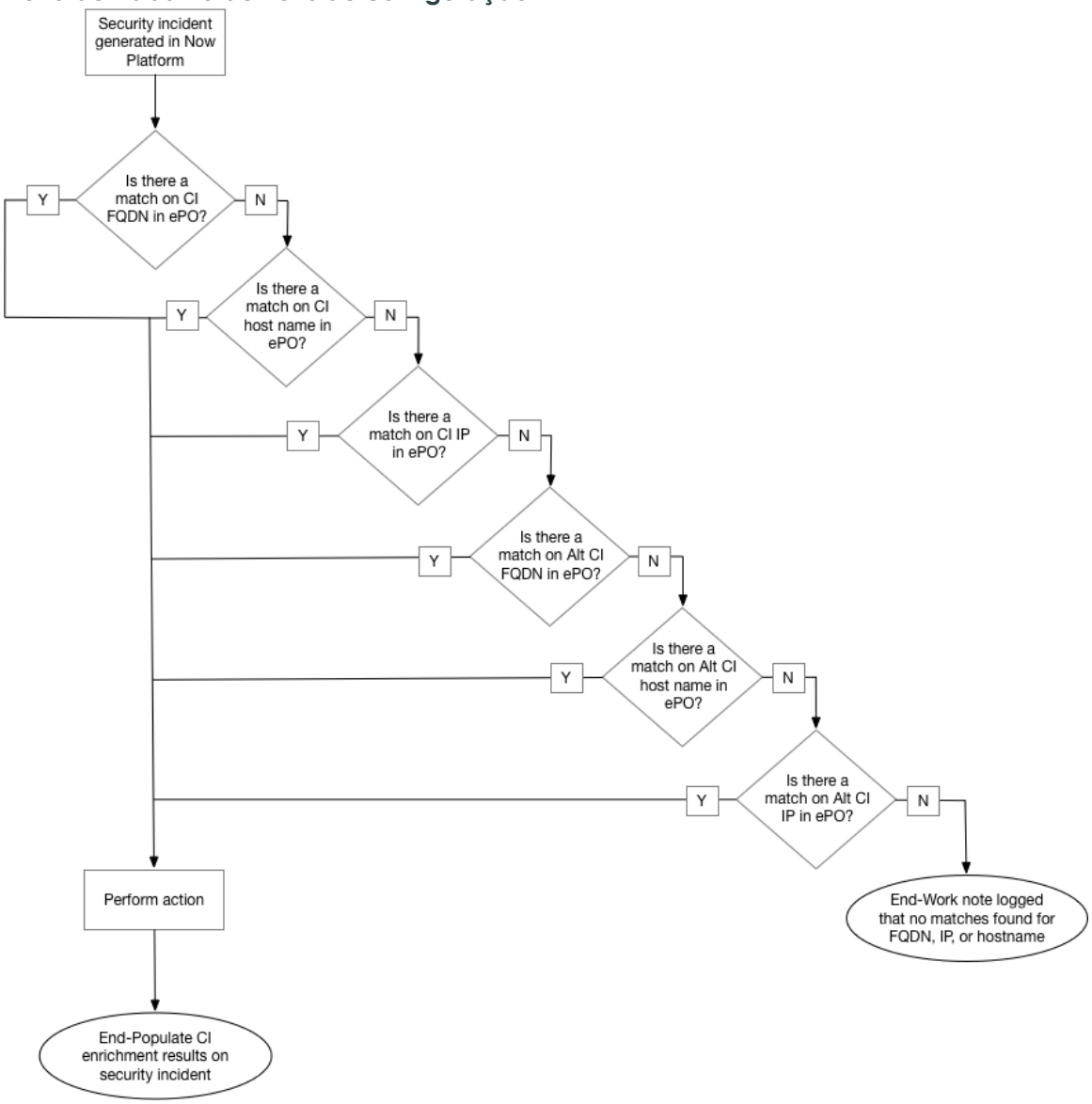


A figura a seguir ilustra como a primeira pesquisa do fluxo de trabalho verifica correspondências para Itens de configuração. Se o campo de gatilho de IC alternativo estiver habilitado, a segunda pesquisa verificará correspondências para valores alternativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de itens de configuração



Se não forem encontrados IDs correspondentes para o campo de IC ou o campo de IC alternativo, uma anotação de trabalho será registrada e uma mensagem será exibida no incidente de segurança. Quando nenhuma correspondência é encontrada, nenhum dado de aprimoramento é preenchido nos incidentes de segurança relacionados ao evento.

Você habilita o campo de gatilho de IC alternativo e seleciona o campo em que deseja exibir o ID correspondente durante a etapa de configuração de um perfil. Esta etapa para habilitar o campo de IC alternativo é descrita junto com os outros requisitos de configuração de perfil em Configurando perfis para a integração McAfee ePO.

Configurando perfis para a integração McAfee ePO

Depois de criar um perfil e selecionar os McAfee ePO recursos que você deseja que o perfil execute, defina as configurações para que o perfil seja invocado somente sob as condições específicas definidas por você.

Configurando um perfil

Nesta etapa, você configura um perfil de capacidade para que ele seja executado somente quando as condições especificadas forem atendidas. Você define quais condições em incidentes de segurança acionam automaticamente as capacidades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

McAfee ePO que você selecionou para o perfil. Você também tem a opção de selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento iniciem automaticamente o perfil. A etapa de configuração inclui as seguintes configurações no formulário de configuração do perfil.

Campo de gatilho de item de configuração (IC) alternativo

Nos casos em que o campo Item de configuração (IC) no incidente de segurança Now Platform® Security Incident Response (SIR) não estiver preenchido com um valor ou uma correspondência não puder ser encontrada no banco de dados, você poderá selecionar um campo alternativo no incidente de segurança para exibir qualquer dados de aprimoramento de IC correspondentes encontrados durante a verificação de seus ativos. Para obter mais informações sobre o item de configuração e os campos de item de configuração alternativo em um incidente de segurança, consulte Definição de condições de acionamento com um campo de item de configuração (IC) para um perfil McAfee ePO.

Marcadores de segurança

Para ajudá-lo a rastrear o status de máquinas host isoladas e quando as verificações de malware são iniciadas, um recurso de marcação opcional está disponível. Por padrão, esta opção está desabilitada no formulário de configuração de perfis. Se esta opção for habilitada durante a etapa de configuração, os nomes dos marcadores de segurança serão exibidos no formulário de configuração. Estes são os nomes dos marcadores exibidos em incidentes de segurança relacionados. Esses marcadores informam quando uma ação de isolamento de host é iniciada com sucesso e quando é aprovada. Depois que um host é retornado à rede com sucesso, o marcador de segurança é removido automaticamente do incidente de segurança. Para verificações de malware, um marcador é exibido no incidente de segurança relacionado quando uma verificação é programada. Depois que a verificação é concluída, o marcador programado é substituído automaticamente por um marcador que indica que a verificação foi concluída com sucesso.

Acionamento automático com base no incidente

Quando a opção Acionamento automático com base no incidente está habilitada, o construtor de condições de filtro está disponível e você deve definir as condições de filtragem que especificam quando o perfil é executado automaticamente. Um filtro comum é Categoria - atividade de código mal-intencionado™ e Impacto nos negócios é 1 - Crítico™. Com esses filtros, somente os incidentes de segurança relacionados a código mal-intencionado e que têm um impacto crítico nos negócios iniciam o perfil. Usar a opção de gatilho automático pode reduzir o número de incidentes de segurança que invocam automaticamente o perfil.

Aprovações

Se sua organização quiser um nível extra de controle sobre ações como isolar máquinas host e iniciar verificações de malware, você poderá habilitar a opção Exigir aprovação durante a etapa de configuração de um perfil.

Por exemplo, se os recursos de aprovação e marcação estiverem habilitados para um perfil, depois que uma solicitação para isolar uma máquina host ou devolvê-la à rede for enviada para aprovação, o incidente de segurança associado será marcado automaticamente para que a ação seja iniciada. As solicitações são enviadas para aprovação a um usuário com a função sn_si.admin por padrão, mas essa aprovação pode ser reatribuída a outro indivíduo ou a um grupo de aprovação para atender às necessidades da sua organização. Os aprovadores processam solicitações em **Minhas aprovações** em suas Now Platform® instâncias. Os marcadores de segurança são exibidos em incidentes de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

segurança relacionados. Todas as atividades de fluxo de trabalho também são registradas em anotações de trabalho para criar uma trilha de auditoria.

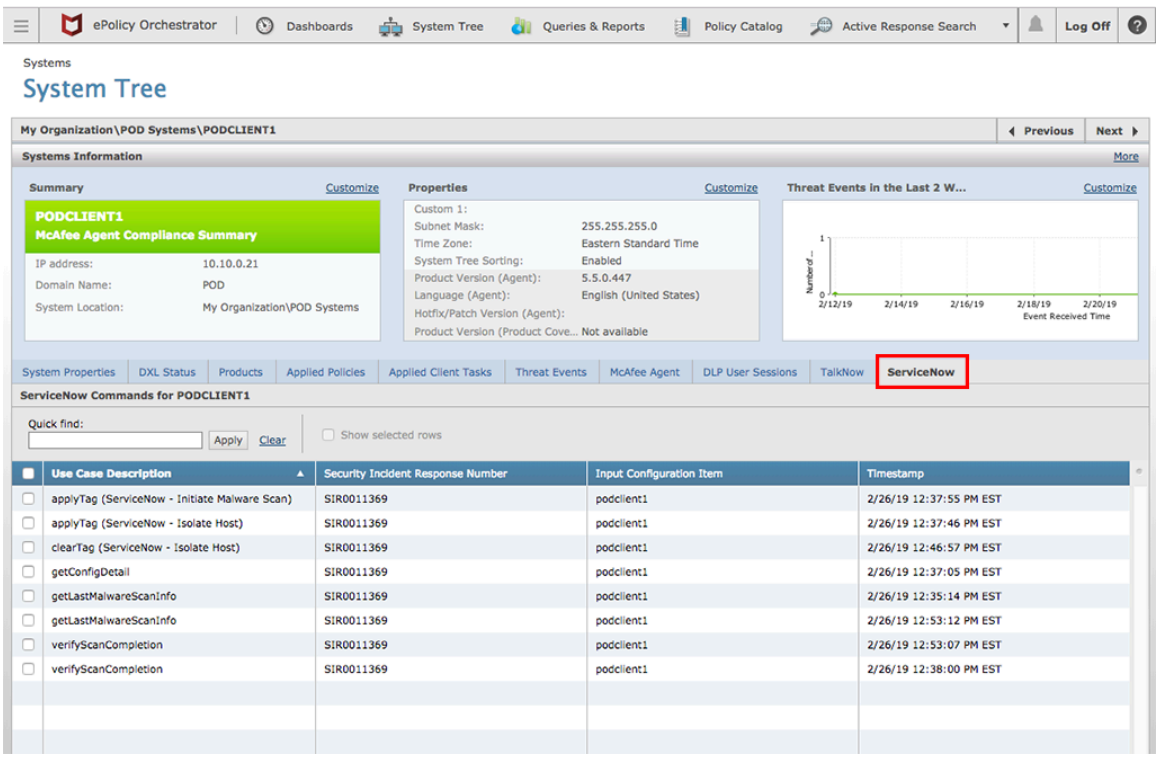
ServiceNow log de auditoria no console McAfee ePO

Na versão 5.10.0 de McAfee ePO, uma guia ServiceNow é exibida com um log de comandos que são iniciados a partir da sua instância Now Platform®. Depois que uma ação ou consulta é invocada de um perfil em sua instância Now Platform® em uma máquina host (endpoint) no console McAfee ePO, um log de auditoria de comandos ServiceNow é criado no console McAfee ePO. Este log é exibido na árvore do sistema no console do McAfee ePO e ajuda a auditar os horários dos comandos que são enviados para endpoints específicos. Para exibir eventos ServiceNow registrados em máquinas específicas em um console McAfee ePO, siga estas etapas.

1. Navegue até a Árvore do sistema no console do McAfee ePO e localize a guia ServiceNow.
2. Clique na guia para abrir uma lista de máquinas host.
3. Na coluna Nome, clique em um nome de host para abrir o log de auditoria.

Na imagem a seguir, é exibido um exemplo de log de um host (`PODCLIENT1`).

Cliente PODC



Os eventos iniciados a partir dos perfis em sua instância Now Platform® são registrados e exibidos no log. Verifique o status da máquina host se os eventos listados no log foram concluídos com sucesso no host.

Perfis de exemplo

Os tópicos a seguir incluem exemplos de como configurar perfis e testar incidentes de segurança. Esses exemplos incluem perfis para todos os recursos McAfee ePO que estão disponíveis para esta integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar perfis e incidentes de segurança para consultas de enriquecimento do sistema para a integração McAfee ePO

Defina as configurações de perfil para que o perfil seja acionado somente nas condições definidas por você.

Antes de Iniciar

Função necessária: Now Platform® administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Defina as condições que acionam automaticamente as capacidades McAfee ePO que você selecionou para o perfil. Você também pode selecionar um campo de entrada alternativo para o campo Item de configuração (IC). Neste campo alternativo, você pode definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento acionem automaticamente o perfil.

Procedimento

1. Se a página Configuração não for exibida, clique em **Configuração** na barra de andamento.
2. No formulário, preencha os campos

Opção	Descrição
Habilitar campo de gatilho de IC alternativo	Campo de gatilho de item de configuração (IC) alternativo. O padrão é limpo. Quando esta caixa de seleção está desmarcada e a opção de campo de gatilho de IC alternativo está desabilitada, uma alternativa para o campo de IC não é identificada. Se desabilitado, um valor para o campo de IC deverá ser preenchido em um incidente de segurança SIR, e o valor no campo deverá ser reconhecido pelo console McAfee ePO antes que o perfil reúna dados de aprimoramento. Marque esta caixa de seleção se você acredita que o campo de IC não será preenchido na criação do incidente, mas as informações de IC serão preenchidas em outro campo no incidente de segurança. Quando esta opção está habilitada, a lista de seleção do campo de gatilho de IC alternativo é exibida. Escolha um campo alternativo na lista de seleção para verificar seus critérios de pesquisa de IC. Para obter mais informações sobre o campo de gatilho de IC alternativo, consulte Definição de condições de acionamento com um campo de item de configuração (IC) para um perfil McAfee ePO.
Marcadores de exibição	Os marcadores de segurança são exibidos em incidentes de segurança. O padrão é limpo.

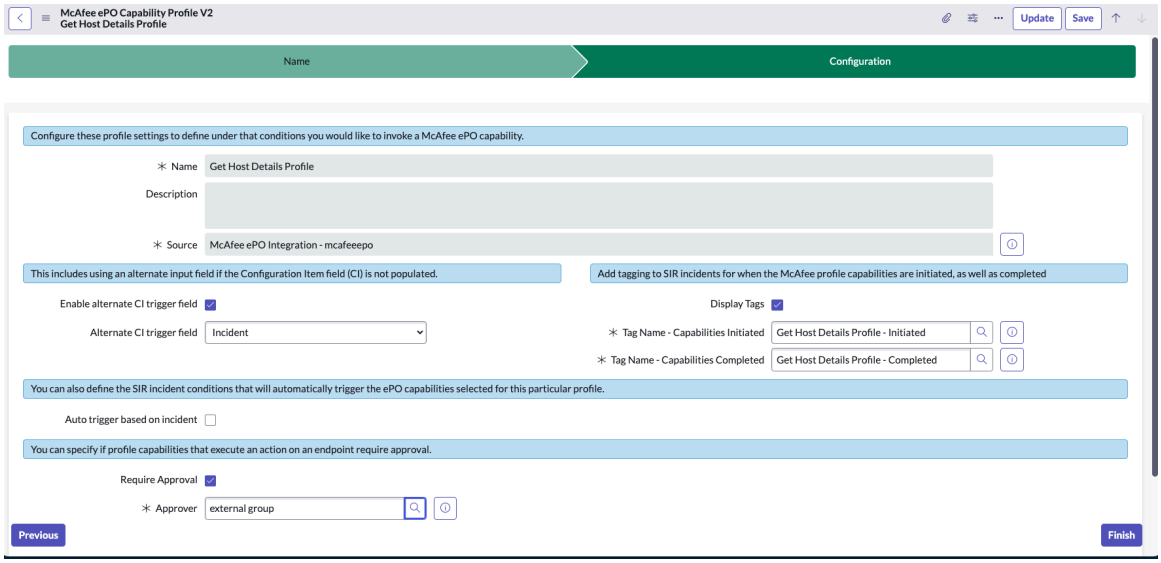
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Quando esta caixa de seleção está desmarcada e a opção de marcação está desabilitada, nenhum nome de marcador de segurança é exibido no formulário de configuração e os marcadores não são exibidos em incidentes de segurança relacionados. Para este exemplo, a opção de marcadores de segurança está desabilitada.
Gatilho automático com base no incidente	Condições do filtro. O padrão é limpo. Quando a caixa de seleção está desmarcada e a opção está desabilitada, o perfil deve ser invocado manualmente a partir de um incidente de segurança. Quando esta opção está habilitada, o Construtor de condições de filtro é exibido. É necessário definir as condições de filtragem para especificar quando o perfil é executado automaticamente após a criação do incidente. Um exemplo comum de um filtro para um perfil que executa consultas de aprimoramento é `Categoria - Atividade de código mal-intencionado` e `Impacto nos negócios é 1-Crítico`. Essas condições de filtro ajudam a localizar os incidentes relacionados a tipos específicos de eventos de segurança e ajudam a limitar o número de incidentes de segurança que você precisa revisar. Essas configurações de filtro permanecem salvas até que você as altere e estão disponíveis para edição durante a etapa de visualização e incidente de teste da configuração.
Requer aprovação	Opção de aprovação da solicitação. O padrão é limpo. Esta opção de aprovação está disponível para qualquer perfil. Normalmente, as aprovações são usadas para capacidades que invocam ações como isolamento de host e verificações de malware. Quando a caixa de seleção está desmarcada e esta opção está desabilitada, nenhuma solicitação de aprovação é enviada. Para este exemplo, nenhuma permissão anterior é necessária para consultas de aprimoramento do sistema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para habilitar a opção de campo de IC alternativo e definir as condições de filtragem que invocam automaticamente este perfil, siga estas etapas.

a. Marque a caixa de seleção **Habilitar campo de gatilho de IC alternativo**.
O campo Gatilho de IC alternativo é exibido. Para este exemplo, como um usuário com a função sn_si.admin, você acredita que o campo de IC não será preenchido no incidente de segurança após a criação do incidente. Como alternativa, você acha que as informações de IC para um FQDN, nome de host ou endereço IP serão preenchidas no campo `IC identificado` no incidente de segurança e seleciona o campo IC identificado como uma alternativa. O IC identificado é selecionado para este exemplo, mas você pode usar qualquer campo no incidente de segurança para o IC alternativo.

b. Na lista de seleção de campo de **gatilho de IC alternativo** exibida, selecione o campo **IC identificado**.

Todos os campos disponíveis no incidente de segurança são exibidos na lista, incluindo todos os campos personalizados. No campo Gatilho de IC alternativo, `IC identificado` é exibido.

Quando este perfil é invocado e o campo de IC não é preenchido no incidente de segurança associado após o gatilho do evento inicial, o perfil usa alternativamente o valor do campo de IC identificado na pesquisa.

c. Marque a caixa de seleção **Gatilho automático com base no incidente**.
O construtor de condições de filtro é exibido. Com esta opção, defina as condições de filtragem e especifique quando o perfil é invocado automaticamente após a criação de um incidente de segurança.

d. Defina as condições de incidente SIR que acionarão automaticamente os recursos do ePO selecionados para este perfil específico.

e. Se as capacidades de perfil que executam uma ação em um endpoint precisarem de aprovação, marque a caixa de seleção **Requer Aprovação**.

f. Selecione uma aprovação usando o ícone de pesquisa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Concluir**.
   Você configurou o perfil com sucesso para que ele seja acionado automaticamente após a criação do incidente e um campo alternativo seja usado para preencher os resultados de IC correspondentes.

Acionar o perfil McAfee ePO manualmente a partir de um incidente de segurança

Acione um perfil de capacidade manualmente a partir de um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar

Função necessária: sn_si.admin

Nota: A opção de aprovações em Configurando perfis para a integração McAfee ePO aparece somente para as capacidades Isolar host e Remover isolamento de host.

Por Que e Quando Desempenhar Esta Tarefa

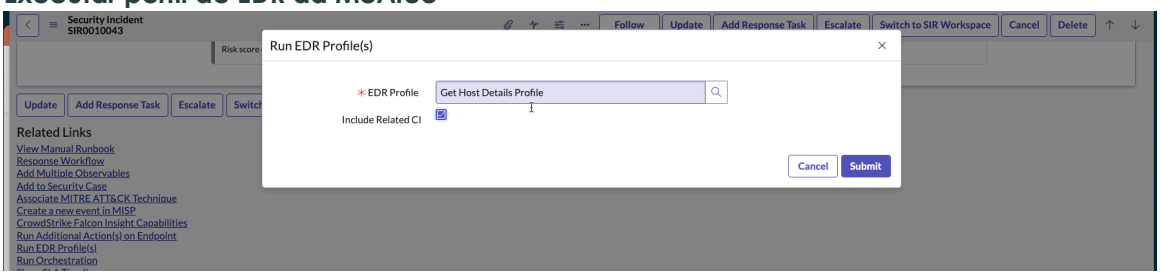
Você pode invocar uma solicitação para obter detalhes do host, isolar a máquina do host ou remover o isolamento de uma máquina automaticamente se as condições de acionamento especificadas no perfil corresponderem às condições nos incidentes de segurança. Como alternativa, se você quiser enviar uma solicitação manualmente, envie-a diretamente de um incidente de segurança.

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos Now Platform incidentes de segurança. McAfee ePO integrações também permitem que você execute capacidades individuais em itens de configuração (ICs) sem usar um perfil.

Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações McAfee ePO.
3. Na seção de listas relacionadas, selecione **Executar perfil(is) de EDR**.

Executar perfil de EDR da McAfee



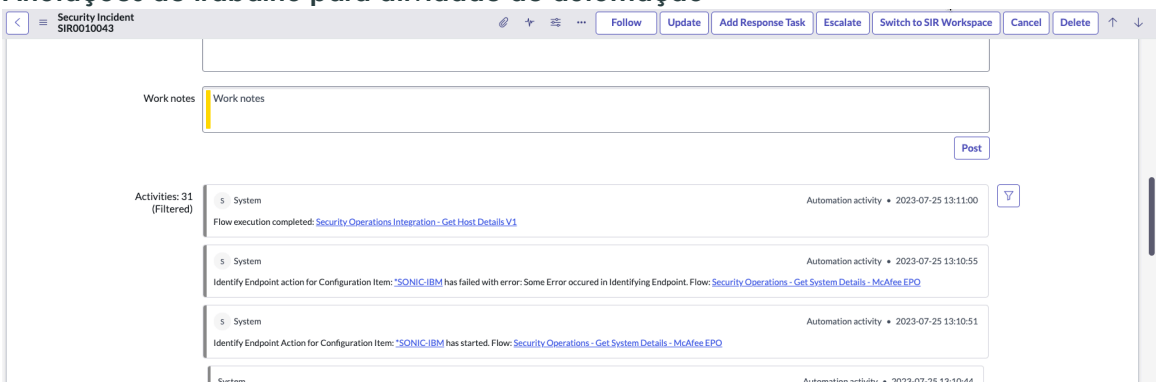
4. Navegue e selecione um perfil na lista de perfis disponíveis.
   A lista de perfis disponíveis é Obter detalhes do host, Isolar máquina host e Remover isolamento. Por exemplo, vamos selecionar Obter detalhes do host.
5. Selecione **Incluir IC relacionado** para executar este perfil em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O perfil selecionado é acionado manualmente. Você pode revisar a seção de anotações de trabalho e atividades e os marcadores iniciados e concluídos pelo perfil na seção de anotações de trabalho.

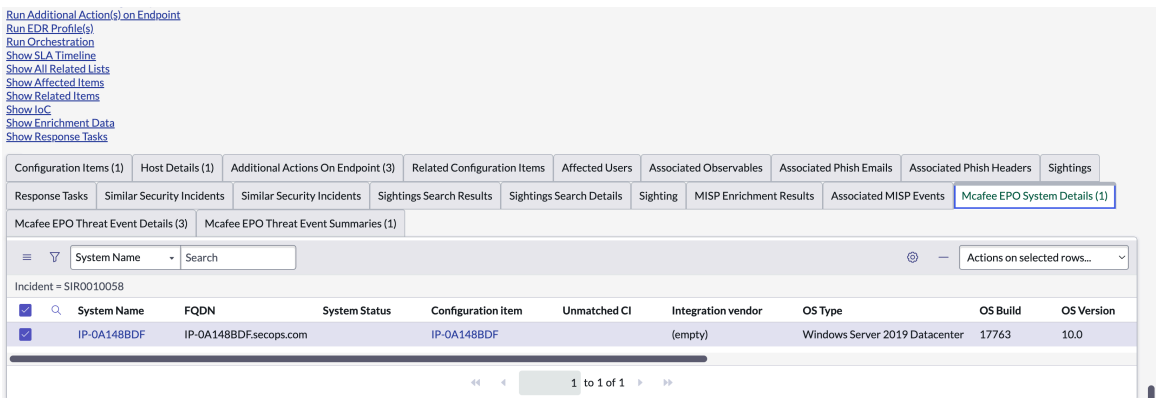
Anotações de trabalho para atividade de automação



Os resultados aparecem na forma de listas relacionadas, como Obter detalhes do host, Isolar máquina host ou Remover isolamento.

Nota: Todas as tabelas de lista relacionada estendem as tabelas base. Neste exemplo, os Detalhes do sistema EPO da McAfee são uma tabela estendida da tabela base de Detalhes do host.

Listas relacionadas da McAfee



7. Para executar capacidades individuais em um item de configuração (IC), execute as seguintes etapas:

   a. Na lista relacionada Itens de configuração, selecione o IC necessário.

   b. Clique na lista suspensa **Ações em linhas selecionadas...** e selecione a capacidade necessária que você deseja executar para o IC selecionado.
   Por exemplo, Isolar host.

   c. Clique em **Isolar host** para executá-lo no IC selecionado.
   O IC selecionado é isolado da rede.

Acionar ações adicionais na integração McAfee ePO

As capacidades Listar eventos de ameaça e Iniciar verificação de malware podem ser acionadas em Executar ações adicionais.

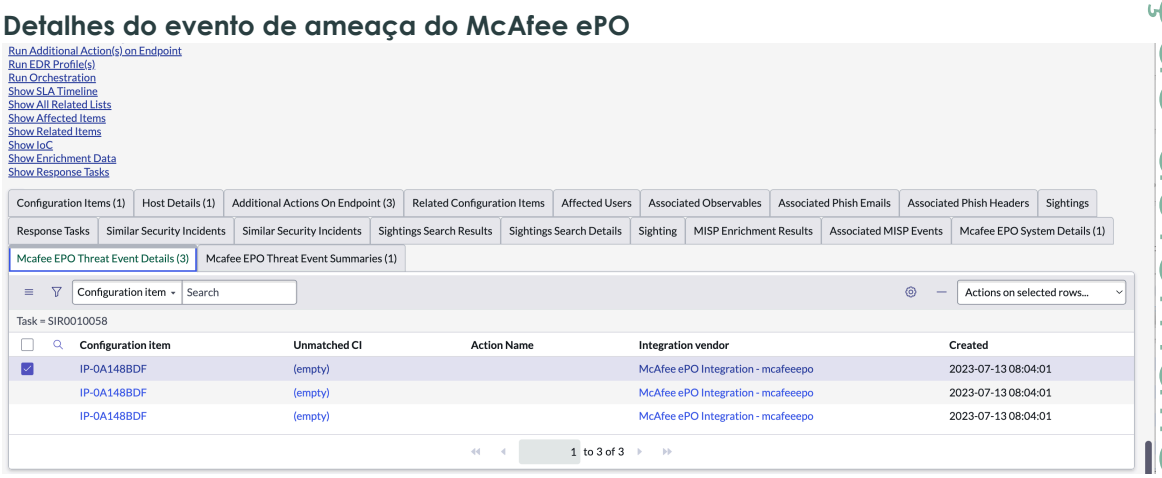
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode configurar e acionar ações adicionais na integração McAfee ePO usando **Executar ações adicionais no endpoint**, que incluem as capacidades McAfee ePO Listar eventos de ameaça e McAfee ePO Iniciar verificação de malware.

Procedimento
1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar as ações adicionais.
3. Na seção Links relacionados, clique em **Executar ação(ões) adicional(is) no endpoint**.
4. Pesquise e selecione a implementação da capacidade que você deseja acionar na lista de ações adicionais.
   Por exemplo, McAfee ePO Listar eventos de ameaça.
5. Selecione **Incluir IC relacionado** para executar esta ação adicional em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique **em Executar ações adicionais**.



Nota: Todas as tabelas de lista relacionada estendem as tabelas base. Neste exemplo, a tabela Detalhes do evento de ameaça do McAfee EPO é uma tabela estendida da tabela base Ações adicionais no endpoint.

7. Exiba e valide os detalhes do evento de ameaça do McAfee ePO nas listas relacionadas.

Usando a integração McAfee ePO no Espaço do analista

Use a integração McAfee ePO para aproveitar os recursos McAfee ePO no espaço do analista SIR.

Antes de Iniciar
Função necessária: sn_si.admin

Antes de usar a integração McAfee ePO no espaço do Security Incident Response, você deve baixá-la do ServiceNow Store e configurá-la. Para obter mais informações, consulte Configure sua instância Now Platform para a integração McAfee ePO.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

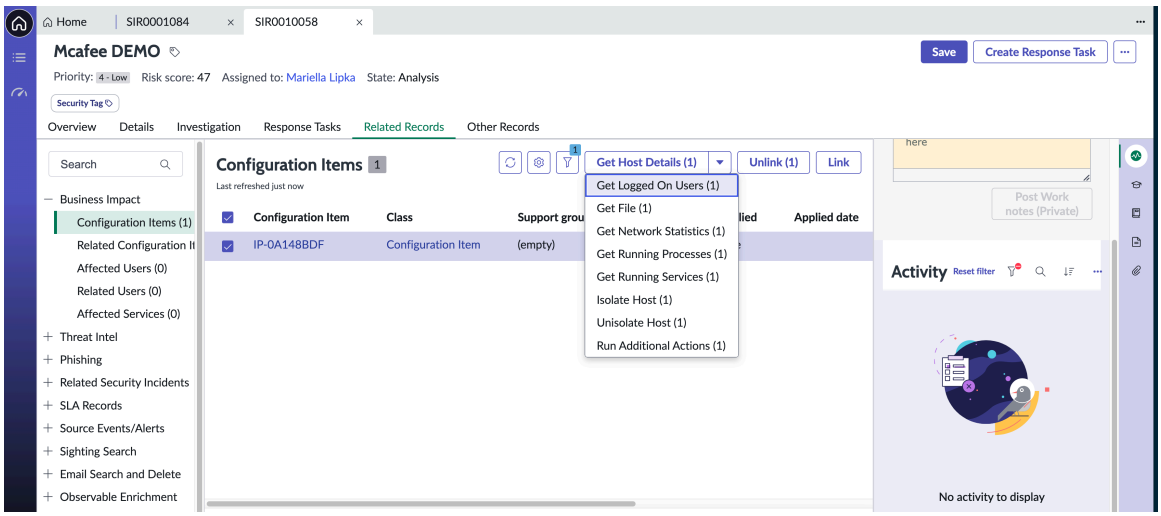
Você pode usar a integração McAfee ePO para realizar ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o espaço Security Incident Response.

A integração McAfee ePO permite que os analistas usem os seguintes recursos [McAfee ePO no espaço do analista Security Incident Response :

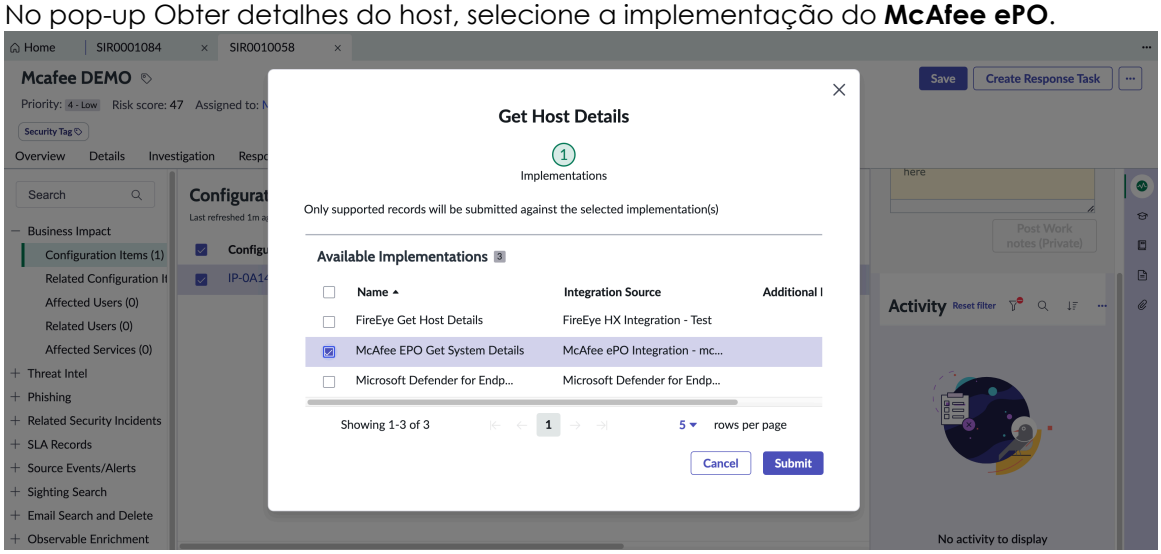
- **Obter detalhes do host**
- **Isolar host**
- **Remover isolamento**
- **Executar ações adicionais no endpoint**

Procedimento

1. Para abrir o incidente de segurança no espaço SIR, clique em **Alternar para o espaço SIR** no incidente de segurança.
2. No espaço SIR, selecione a guia **Registros relacionados**.
3. Selecione qualquer **item de configuração**e escolha uma capacidade do McAfee ePO para acionar na ação suspensa da lista relacionada.
   Por exemplo, Obter detalhes do host.



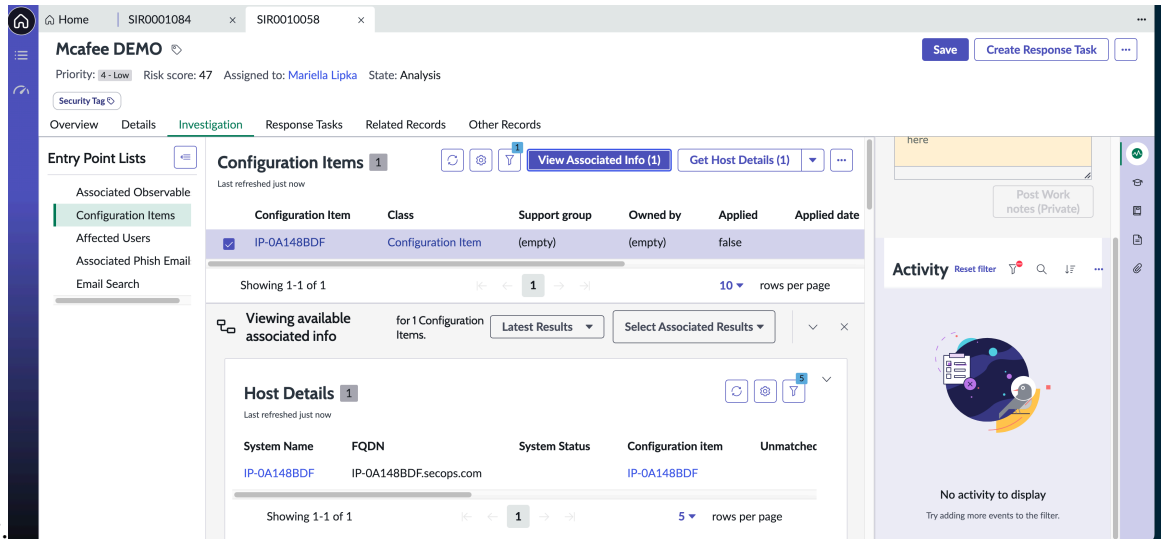
4. No pop-up Obter detalhes do host, selecione a implementação do **McAfee ePO**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.
   A capacidade Obter detalhes do host é invocada no IC. Você pode exibir as anotações de trabalho dos resultados e descobertas.
6. Para exibir os dados da capacidade acionada, selecione a guia **Investigação**.
7. Selecione o **item de configuraçãoe** clique na ação **Exibir informações associadas**.
   As informações associadas do item de configuração são exibidas. Por exemplo, Detalhes do host.



8. Clique no **item de configuração** para exibir os detalhes do host.
   Da mesma forma, você pode tentar usar a outra capacidade do McAfee ePO para seus incidentes de segurança no SIR Analyst Workspace.
9. Você pode usar os recursos do McAfee ePO na lista relacionada de **Detecção e resposta de endpoint (EDR)** para análise.
10. Navegue e selecione um perfil na lista de perfis disponíveis.
    A lista de perfis disponíveis é Obter detalhes do host, Isolar máquina host e Remover isolamento. Por exemplo, vamos selecionar Obter detalhes do host.
11. Selecione a implementação do **McAfee ePO** e clique em **Enviar**.

McAfee ESM - Integração do analisador de e-mail

A integração ESM – Analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do ESM para criar incidentes de segurança.

Configurar integração do McAfee ESM - Analisador de e-mail

A integração do McAfee ESM - Analisador de e-mail usa notificações por e-mail do ESM para gerar fluxos de trabalho de enriquecimento e de resposta.

Antes de Iniciar

Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa

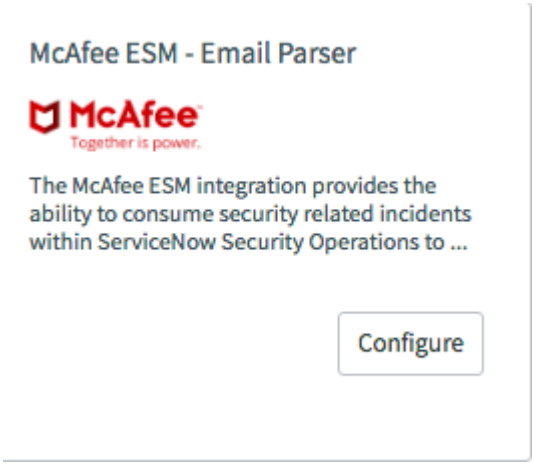
Um modelo de analisador de e-mail do McAfee ESM é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. A atualização do analisador o ativa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão McAfee ESM - Analisador de e-mail, clique em **Configurar**.
3. Na caixa de diálogo **McAfee ESM - Configuração do analisador de e-mail**, clique no link **Configurar analisador de e-mail**.
4. Clique no link do **McAfee ESM** para editar as configurações no analisador de e-mail de modelo fornecido.
   No mínimo, preencha o campo O `e-mail é de`. Para criar seu próprio analisador de e-mail, consulte Criar analisadores de e-mail em Operações de segurança.
5. Marque a caixa **Ativo**.
6. Clique em **Atualizar** no formulário **Analisador de e-mail**.
   O analisador de e-mail está ativo. Você não precisa retornar às **Configurações de integração**.

McAfee ESM - Incident Enrichment Integration

McAfee ESM - A integração de aprimoramento de incidentes pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	**Configurar** • Introdução ao McAfee ESM - Incident Enrichment integration • Criar registros de configuração de pesquisa de detecções
Usar • Executar uma pesquisa de detecções • Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções	**Desenvolver** • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

• Operações de segurança - Fluxo de trabalho Pesquisa de detecções do McAfee ESM • Exibir detalhes da pesquisa de detecções • Exibir resultados da pesquisa de detecções	
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução ao McAfee ESM - Incident Enrichment integration

McAfee ESM protege endpoints contra vírus, Spyware, Cavalos de Tróia e outras ameaças de malware e se integra facilmente com Operações de segurança. Antes de poder usar a integração McAfee ESM - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL base da API e as credenciais de login apropriadas.

Antes de Iniciar

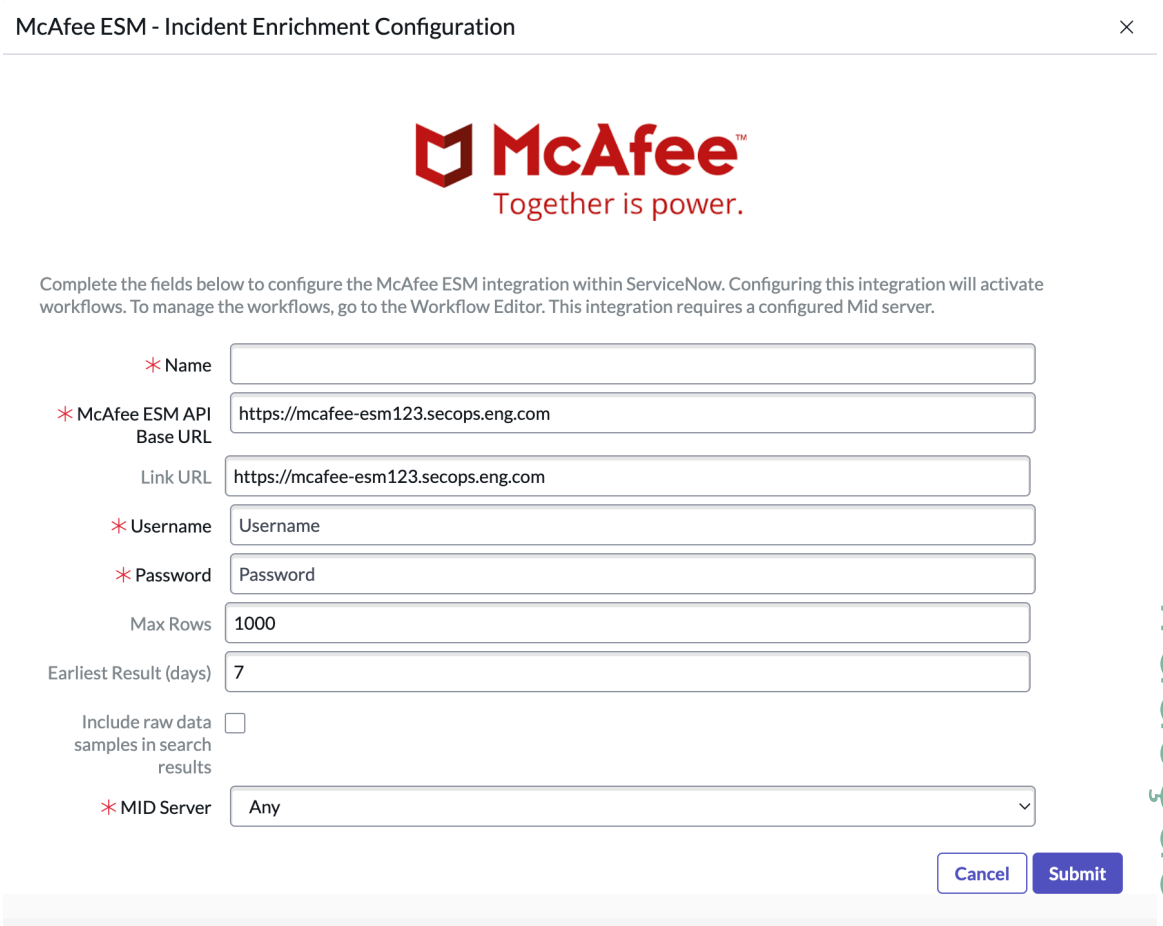
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão McAfee ESM - Aprimoramento de incidentes, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL Base da API McAfee ESM	A URL base que você adquiriu no site do McAfee ESM.
URL do Link	[Opcional] A URL do link que vincula a uma instância do McAfee ESM, quando disponível. **Nota:** Se você estiver recebendo um erro, use a URL Base da API do McAfee ESM.
Nome de usuário	Seu nome de usuário do McAfee ESM.
Senha	Sua senha do McAfee ESM.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
dados brutos nos resultados da pesquisa	retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração de Microsoft Azure Sentinel

Microsoft Azure Sentinel é uma solução baseada em nuvem de Gestão de eventos de informações de segurança (SIEM) e Resposta automatizada de orquestração de segurança (SOAR). Você pode usar a integração Microsoft Azure Sentinel para ingerir incidentes do Azure Sentinel e criar automaticamente incidentes de segurança em Security Incident Response.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

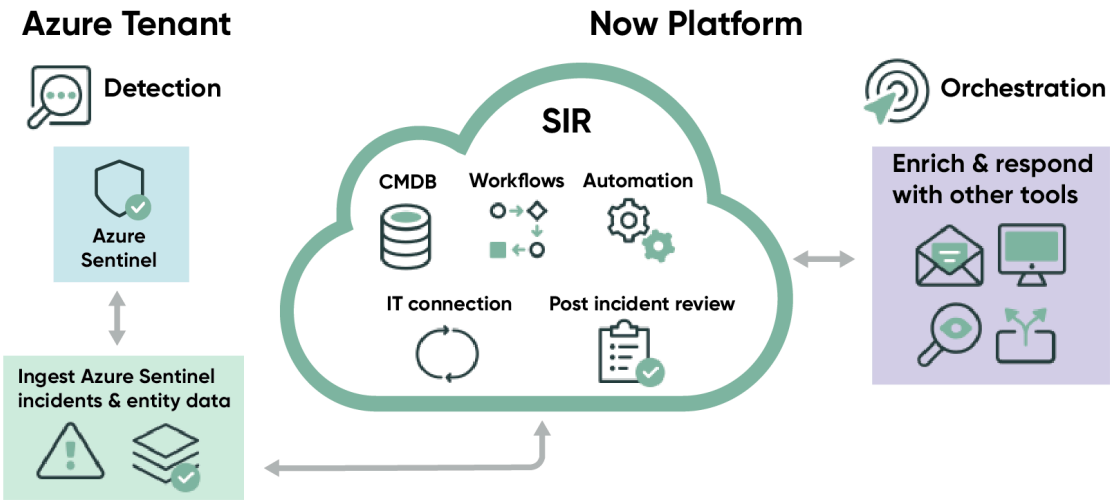
Visão geral

Consulte o diagrama a seguir para saber como Microsoft Azure Sentinel se integra às aplicações Now Platform Operações de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Now Platform - Azure Sentinel integration overview



Principais recursos

Use os principais recursos desta integração para realizar as seguintes ações:

- Descubra Microsoft Azure Sentinel incidentes que são candidatos a incidentes de segurança e automatize a criação desses incidentes de segurança.
- Mapeie Microsoft Azure Sentinel campos de incidente e entidade para SIR campos de incidente de segurança.
- Filtrar Microsoft Azure Sentinel incidentes.
- Agregue incidentes a incidentes de segurança abertos existentes para que você não precise criar incidentes de segurança duplicados.
- Automatize Microsoft Azure Sentinel atualizações de status de incidentes do Security Incident Response para que você possa criar e fechar incidentes de segurança.

  Nota: ServiceNow atualiza o status de Microsoft Azure Sentinel incidentes com base na criação ou fechamento do incidente de segurança. Esta atualização também inclui comentários de incidentes agregados e novos incidentes.

- Programe a ingestão de incidentes para criar incidentes de segurança periodicamente.
- Sincronize Microsoft Azure Sentinel comentários de incidentes com SIR Anotações de trabalho.

Conheça esta integração

Identificador do documento	Título do documento
Microsoft site de documentação do produto	Site de documentação de produtos da Microsoft
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução à integração Microsoft Azure Sentinel

Ative e configure o plug-in Microsoft Azure Sentinel – Ingestão de incidentes for Security Operation para interagir com sua instância [Now Platform e produto Security Incident Response.

Antes de Iniciar

Função necessária: Microsoft Azure desenvolvedor de aplicações, Microsoft Azure administrador de locatário

Antes de poder usar a integração Microsoft Azure Sentinel, você deve baixá-la do ServiceNow Store.

Por Que e Quando Desempenhar Esta Tarefa

Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração sem problemas.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria perfis de incidentes. ◦ Mapeia os campos de dados de incidentes Microsoft Azure Sentinel para os campos de incidentes de segurança. ◦ Programa a ingestão de incidentes contínuos. ◦ Habilita atualizações de incidentes quando um Security Incident Response incidente é criado ou encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst).
Atribua as Microsoft Azure funções necessárias.	As funções a seguir são necessárias em Microsoft Azure para registrar e configurar sua aplicação: • Desenvolvedor de aplicações para registrar a aplicação. • Administrador de locatário para conceder permissões à aplicação chamando o endpoint de consentimento do administrador.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.	O plug-in ServiceNow Integration Hub Starter Pack Installer [com.glide.hub.integrations] é necessário. O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Operações de segurança que são necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação, uma de cada vez, na seguinte ordem para garantir uma instalação sem problemas: **1.** Security Incident Response **2.** IU Security Incident Response **3.** Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) **4.** Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest)
Registre e configure sua aplicação no Microsoft Azure portal.	Registre sua aplicação no portal Microsoft Azure e conceda aos usuários acesso de leitura e gravação à aplicação.

Registrar e configurar o portal Microsoft Azure

Registre sua aplicação no portal Microsoft Azure e conceda aos usuários acesso de leitura e gravação à aplicação.

Antes de Iniciar

Função necessária: Microsoft Azure desenvolvedor de aplicações, Microsoft Azure administrador de locatário

Procedimento

1. Entre no portal Microsoft Azure.

2. Pesquise e selecione **Registros de aplicações**.

3. Clique **em Novo registro**.

Tradução automática

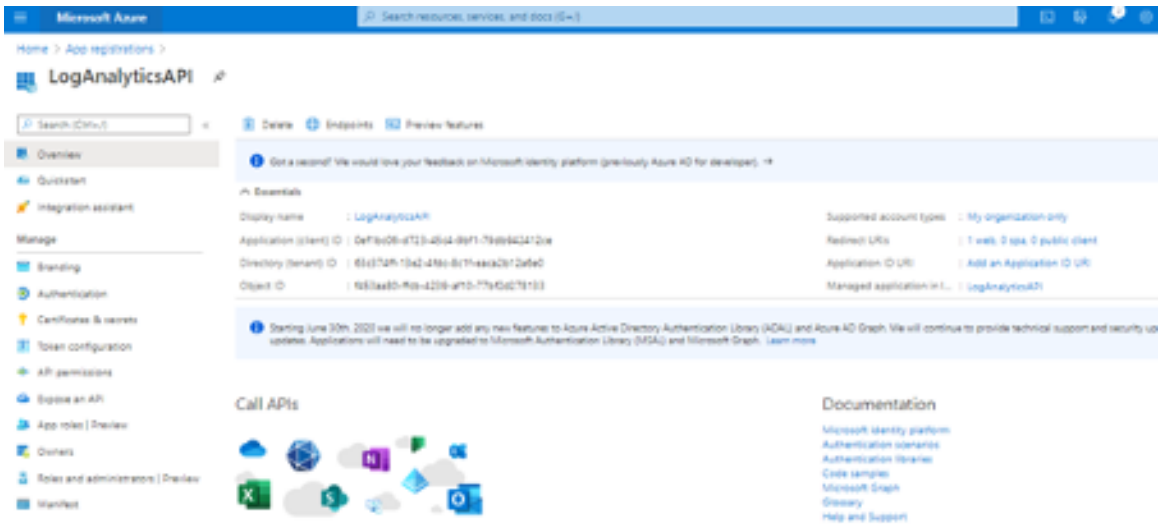
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

Registrar um formulário de aplicação

Campo	Descrição
Nome	Nome de exibição da aplicação para o usuário. Por exemplo, LogAnalyticsAPI.
Tipos de conta compatíveis	Tipo de conta que pode usar esta aplicação ou acessar a API.
Redirecionar URI	Redirecionar URI. A resposta de autenticação é direcionada para este URI após a autenticação bem-sucedida de um usuário.

5. Clique em **Registrar**.
   Depois de registrar a aplicação com sucesso, você verá a página Visão geral.



6. Navegar até **Gerenciar** > **Certificados e segredos**.
7. Na seção Segredos do cliente, clique em **Novo segredo do cliente**.
   Você não pode exibir o segredo do cliente posteriormente, portanto, certifique-se de copiar e salvar o segredo do cliente agora nesta etapa. Se você esquecer o segredo do cliente, poderá gerar um novo seguindo as instruções nas etapas 4 e 5.
8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique **em Adicionar uma permissão**.
10. Na janela Solicitar permissões de API, clique na guia **APIs que minha organização usa**.
11. Pesquise e selecione o nome da aplicação **da API de análise de logs**.
12. Nas permissões da API Análise de logs, selecione **Permissões da aplicação**.
    Habilitar essa permissão garante que a aplicação seja executada como um serviço ou daemon em segundo plano sem um usuário conectado.
13. Na seção Dados, selecione **Data.Read**
14. Clique **em Adicionar permissões**.
    As permissões foram atualizadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

15. Habilite a opção **Conceder consentimento do administrador para diretório padrão** para a permissão da API Data.Read que você habilitou na etapa 13.
16. Pesquise e selecione **espaços de Análise de logs**.
17. Selecione o espaço de Análise de logs do Sentinel.
    Agora você vê a página Visão geral do espaço de Análise de logs do Sentinel.
18. Navegar até **Controle de acesso (IAM)** > **Atribuições de função**.
19. Clique em **Adicionar**e selecione **Adicionar atribuição de função**.
20. No formulário, preencha os campos.

Adicionar formulário de atribuição de função

Campo	Descrição
Função	Tipo de conta que pode usar esta aplicação. Selecione **Respondente do Azure Sentinel**.
Atribuir acesso a	Escopo de permissões definido por você. Selecione **Usuário**, **grupo**ou **entidade de serviço**.
Selecionar	Aplicação que você criou anteriormente na etapa 4. Por exemplo, LogAnalyticsAPI.

21. Clique em **Salvar**.

Instalar e configurar a integração Microsoft Azure Sentinel

Instale e configure a integração Microsoft Azure Sentinel da ServiceNow Store na sua instância Now Platform para começar a ingerir incidentes do Azure Sentinel.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe a integração Microsoft Azure Sentinel do ServiceNow Store e instale-a.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco Microsoft Azure Sentinel e clique em **Configurar**.
4. No formulário, preencha os campos.

Microsoft Azure Sentinel - Formulário de configuração de ingestão de incidentes

Campo	Descrição
Nome	Nome da configuração da instância Microsoft Azure Cloud.
URL de identidade	URL de identidade para o locatário Microsoft Azure Cloud. Por exemplo, `login.microsoftonline.com`. Para obter informações adicionais, consulte a documentação do Microsoft Azure .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Azure Resource Manager	Endpoint do Azure Resource Manager para locatário Microsoft Azure Cloud. Por exemplo, `management.azure.com`. Para obter informações adicionais, consulte a documentação do Microsoft Azure .
ID de locatário	Microsoft Azure Sentinel ID do locatário. Esta é a instância da qual todos os incidentes no portal Microsoft Azure são recuperados.
ID de cliente	ID de cliente da aplicação que você registrou no portal Microsoft Azure.
Segredo do cliente	Segredo do cliente da aplicação registrada.
ID de Assinatura	ID de assinatura da sua aplicação registrada.
Nome do grupo de recurso	Nome do grupo de recursos da aplicação registrada.
Nome do espaço	Nome do espaço da sua aplicação registrada.

5. Clique em **Enviar**.

Resultados
Depois de validar e enviar a configuração com sucesso, cada configuração do servidor de ingestão de incidentes será salva na página Integrações de segurança como um bloco.

Criar um perfil para Microsoft Azure Sentinel

Crie um perfil de incidente em sua instância Now Platform e determine os incidentes Microsoft Azure Sentinel que são adequados para criar incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A integração permite criar diferentes tipos de incidentes, como tentativas de acesso não autorizadas e malware. Esses incidentes são criados com base nos perfis que você configura na instância Now Platform. Todos os incidentes são criados inicialmente para um tipo de incidente configurado em um perfil. Os incidentes criados podem ser filtrados para especificar quais incidentes criam incidentes de segurança.

Todos os incidentes que atendem aos critérios de seleção em seu locatário Microsoft Azure e estão disponíveis na API Microsoft Azure Sentinel, são ingeridos inicialmente em sua instância Now Platform.

Procedimento

1. Navegar até **Todos** > **Integração do Microsoft Azure Sentinel** > **Perfil de incidentes do Azure Sentinel**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Azure Sentinel - Formulário de configuração de ingestão de incidentes

Campo	Descrição
Nome	Nome do perfil. Este nome ajuda a identificar o tipo de perfil e também é o nome padrão para o marcador de segurança associado a este perfil.
Ativo	Indicador de que o perfil está ativo. Quando o perfil está ativo, isso indica que o Now Platform está pesquisando ativamente os incidentes do Azure Sentinel e que os incidentes de segurança correspondentes são criados em SIR quando as condições de filtragem são correspondidas.
Origem	Microsoft Azure locatário que você configurou para ingerir incidentes. Se você tiver vários locatários configurados, selecione o locatário apropriado para os tipos de incidentes que você planeja ingerir para o perfil.
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Descrição	Texto extra para ajudá-lo a distinguir este perfil de outros perfis.

4. Para passar para a seção Mapeamento, clique em **Continuar**.

O que Fazer Depois
Mapeie campos de incidentes Microsoft Azure Sentinel individuais para os campos no incidente de segurança Now Platform SIR.

Mapear os Microsoft Azure Sentinel campos de incidentes

Mapeie os campos de incidente Microsoft Azure Sentinel individuais para os campos no incidente de segurança SIR para que você possa criar incidentes com os dados mapeados.

Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na página de mapeamento, na seção Mapeamento de campo do Azure Sentinel, selecione um dos Métodos de ingestão de amostra.

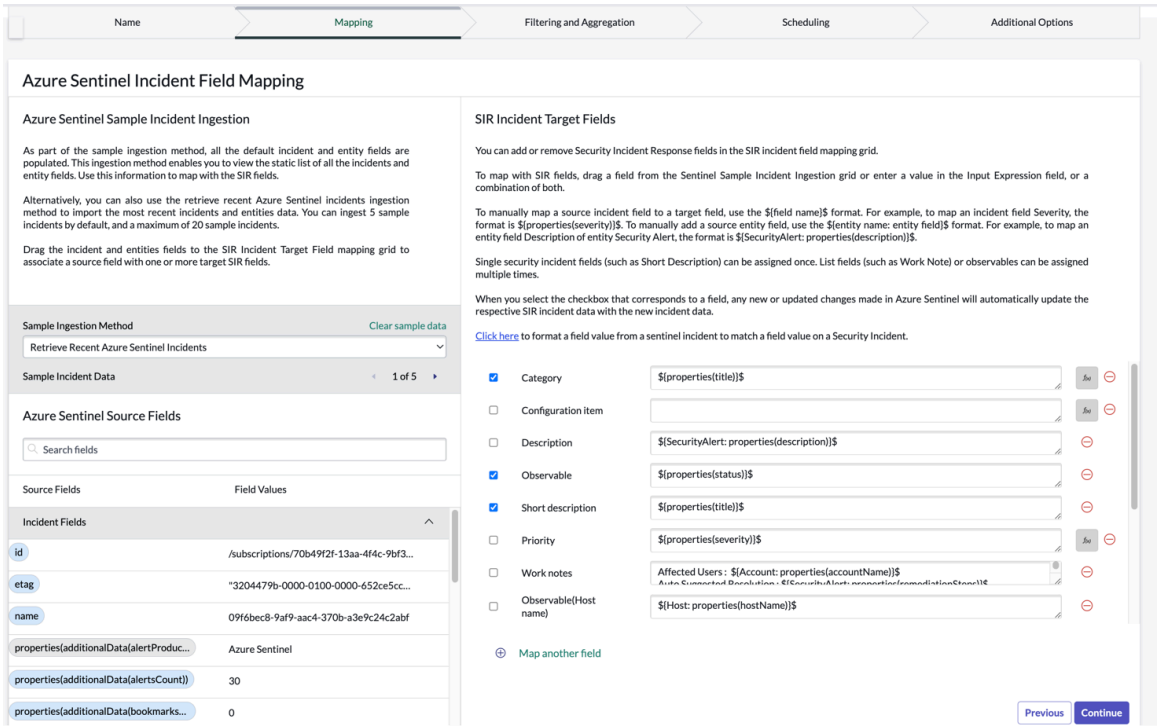
Métodos de ingestão de amostra

Campo	Descrição
Todos os campos padrão de Incidente e entidade	Use este método de ingestão para exibir a lista estática de todos os incidentes e campos de entidade. Este método contém somente nomes de campo padrão sem valores. Você pode usar essas informações para mapear com os campos SIR.
Recuperar incidentes recentes do Azure Sentinel	Use este método de ingestão para importar os dados de entidades e incidentes mais recentes. Se o incidente do Azure Sentinel contiver os dados da entidade, os dados da entidade serão recuperados e estarão disponíveis para mapeamento na seção Campos de origem do Azure Sentinel. Às vezes, o incidente do Azure Sentinel pode não conter os dados da entidade e, portanto, os campos da entidade não estão disponíveis para mapeamento nesse cenário. Se o incidente do Azure Sentinel contiver vários alertas, o alerta mais antigo que fizer parte do incidente será mostrado na seção de mapeamento. Durante a ingestão, os valores mais antigos do campo de alerta de segurança serão usados. Você pode ingerir 5 incidentes de amostra por padrão e um máximo de 20 incidentes de amostra. Os valores do campo de incidente de amostra são preenchidos quando o perfil ingere os incidentes de amostra. Você pode mapear esses incidentes para os **Campos de destino do incidente SIR**. Os campos e valores de incidente aparecem como guias individuais.
Importar dados de amostra	Clique em **Importar dados de amostra** para importar incidentes de amostra do Azure Sentinel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este botão aparece quando você seleciona o método de ingestão Recuperar incidentes recentes do Azure Sentinel. A recuperação de incidentes de amostra do servidor Microsoft Azure Sentinel pode demorar um pouco. Mapeie esses incidentes recuperados para os **campos de destino do incidente SIR**. Os campos e valores de incidente aparecem como guias individuais.



2. Para adicionar campos aos campos padrão que são exibidos no incidente de segurança, execute as seguintes ações:

a. Na seção Campos de destino do incidente SIR, clique no botão

Botão Mapear outro campo.
Ele mostra uma lista de SIR campos, na qual você pode selecionar um campo para um novo campo a ser exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Vários observáveis podem ser exibidos no mesmo incidente de segurança. Por exemplo, o campo **Observável** pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos **Item de configuração** e **Anotações de trabalho** oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não é compatível com vários valores, verá uma mensagem de erro informando que este campo não é compatível com vários valores. Da mesma forma, se um campo em um incidente de segurança tiver uma lista na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista, o campo não será preenchido no incidente de segurança.

c. Na seção Campos de origem do Azure Sentinel, arraste e solte seu campo para mapeá-lo para o novo campo.

d. Quando você marca a caixa de seleção que corresponde a um campo, todas as mudanças novas ou atualizadas feitas no Azure Sentinel atualizam automaticamente os respectivos dados de incidente SIR com os novos dados de incidente.

Nota: No sistema base, a propriedade do sistema sn_sec_sentinel.incident_updates é definida por padrão como Verdadeira para receber as Microsoft Azure Sentinel atualizações relacionadas a novos alertas vinculados ao SIR.

- Por padrão, os campos Usuários afetados, Itens de configuração e Observáveis são verificados. Isso significa que sempre que houver novos observáveis ou itens de configuração associados, ou usuários afetados que sejam adicionados ao incidente, essas informações serão extraídas automaticamente e preenchidas nas respectivas listas relacionadas no Security Incident Response (SIR) durante esse intervalo de pesquisa.
- Para todos os outros campos, você deve marcar a caixa de seleção que corresponde a um campo para todas as mudanças novas ou atualizadas feitas no registro de incidente do Azure Sentinel no Azure Sentinel. Isso atualizará automaticamente os respectivos dados de incidente SIR com os novos dados de incidente.

Importante: É necessário fazer a diligência prévia antes de selecionar esta funcionalidade, pois a substituição dos dados existentes pode resultar em dados instáveis para o analista trabalhar e qualquer outra automação definida até mesmo pelos valores de campo do incidente de segurança também pode ser afetada. Portanto, é muito importante fazer a devida diligência antes de selecionar qualquer funcionalidade de substituição.

3. Para remover um campo, use o botão Remover Remover item ao lado do campo de expressão de entrada na seção Campos de destino do incidente SIR.

4. Para mapear um valor de campo da seção Campos de origem do Azure Sentinel para um campo na seção Campos de destino do incidente SIR, use uma das seguintes ações:

a. Arraste o nome do campo (por exemplo, id) e solte-o ao lado de um nome de campo na coluna Campos de destino do incidente SIR.

Você pode corresponder qualquer valor da seção Campos de origem do Azure Sentinel a um campo na seção Campos de destino do incidente SIR. Os campos são codificados por cores para que você não ignore ou duplique os campos de incidente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no processo de mapeamento. Os campos em azul claro indicam que um campo de incidente ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de incidente de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Dessa forma, você pode visualizar quais valores de campo foram adicionados ao incidente de segurança e se alguma informação importante do incidente restante permanece não mapeada.

b. Você pode adicionar uma combinação de texto e campo.
Por exemplo, `o nome do incidente é ${name}$`. Aqui, o `nome do incidente` pode ser inserido manualmente enquanto `${name}$` é mapeado na seção Campos de origem do Azure Sentinel.

c. Você pode inserir e mapear manualmente um incidente de origem ou campo de entidade para um campo de destino.

- Para mapear manualmente um campo de incidente de origem, use o formato ${field name}$. Por exemplo, para mapear um campo de incidente Gravidade, o formato é`${properties(severity)}$`.
- Para adicionar manualmente um campo de entidade de origem, use o `formato ${entity name: entity field}$`. Por exemplo, para mapear um campo de entidade Descrição do alerta de segurança da entidade, o formato é `${SecurityAlert: properties(description)}$`.

Esta integração classifica determinados subtipos de observável. Quando você mapeia um campo do Azure Sentinel com o campo do observável SIR, o Now Platform classifica automaticamente o observável. Se você quiser mapear genericamente o observável do Azure Sentinel de entrada para o tipo de observável em SIR, arraste e solte o campo do Azure Sentinel no campo Observável. No entanto, se você estiver ciente do tipo de observável para o observável do Azure Sentinel de entrada em SIR, mapeie especificamente para o campo de tipo de observável SIR. Alguns exemplos de tipos de observável específicos em SIR incluem Observável (nome do domínio), Observável (endereço de e-mail), Observável (endereço IP (V4)) e Observável (nome do host).

Se os campos de entrada do Azure Sentinel contiverem MITRE-ATT&CK informações, mapeie-as para o campo MITRE-ATT&CK Técnica. Certifique-se de que o campo de entrada do Azure Sentinel contenha o ID da técnica MITRE-ATT&CK ou o nome da técnica.

Às vezes, os valores do campo de incidente em Microsoft Azure Sentinel podem não ser convertidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos.

5. Para formatar uma tradução de campo para um novo campo de um incidente do Azure Sentinel para corresponder a um valor de campo em um incidente de segurança, clique no link **Clique aqui** no cabeçalho **Campos de destino do incidente SIR**.

6. Para modificar os campos que oferecem suporte à tradução de campos, clique no Formato de campo ícone de tradução de campo de formato de script.
Os campos que oferecem suporte à tradução de campos são **Categoria**, **Item de configuração**e **Prioridade**. Por exemplo, clique no ícone do ao lado da Categoria.
O editor de script Tradução de campo do Azure Sentinel é aberto.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças e retornar à página Mapeamento.
   Por exemplo, para Categoria, defina o seguinte no editor de script:

   ```
   "<Incoming Sentinel Incident Field Value>" : "<Category to assign to
    the Security Incident>".
   ```

   Este mapeamento garante que um perfil use somente categorias configuradas.
8. Continue o mapeamento adicionando ou removendo valores de campos.
   Você pode usar os mesmos valores de campos no construtor Condições de geração de incidentes para definir critérios adicionais que um incidente de entrada deve satisfazer para criar um incidente de segurança.
9. Para mover para a seção Filtragem e Agregação, clique em **Continuar**.

O que Fazer Depois

Defina e defina as condições do filtro para que você possa especificar quais incidentes devem criar incidentes de segurança. Você pode usar os mesmos valores de campo (definidos na seção Mapeamento) no construtor Condições de geração de incidente (na seção Filtragem e agregação) para definir critérios adicionais que um incidente de entrada deve satisfazer para criar um incidente de segurança.

Definição de critérios de filtro e agregação

Você pode definir e definir condições de filtro para que possa especificar quais Microsoft Azure Sentinel incidentes de entrada devem criar incidentes de segurança. Você também pode definir critérios de campo de incidente adicionais que permitem que um incidente de entrada seja anexado a um incidente de segurança aberto em vez de criar um incidente.

Definir as condições de filtragem para incidentes de segurança

Defina as condições de filtragem para que os incidentes de segurança sejam criados somente quando as condições de filtragem corresponderem.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda a isolar incidentes de segurança e limita o número de incidentes de segurança que você cria. Se você definir critérios de filtragem adicionais, somente os incidentes necessários serão ingeridos sem a necessidade de alterar a consulta ou a configuração do incidente acionado.

Procedimento

1. Para definir os critérios que um incidente Microsoft Azure Sentinel de entrada deve satisfazer para que um incidente de segurança seja criado, selecione **Filtrar com base nas condições**.

   As opções no primeiro campo nas Condições do filtro correspondem aos campos exibidos na seção Ingestão de incidente de amostra do Azure Sentinel para o incidente que você ingeriu. Esses campos são dinâmicos e mudam dependendo do incidente que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.

   Use a condição de filtro *contida* para os seguintes campos com vários valores:

   - properties(labels)
   - properties(additionalData(alertProductNames))

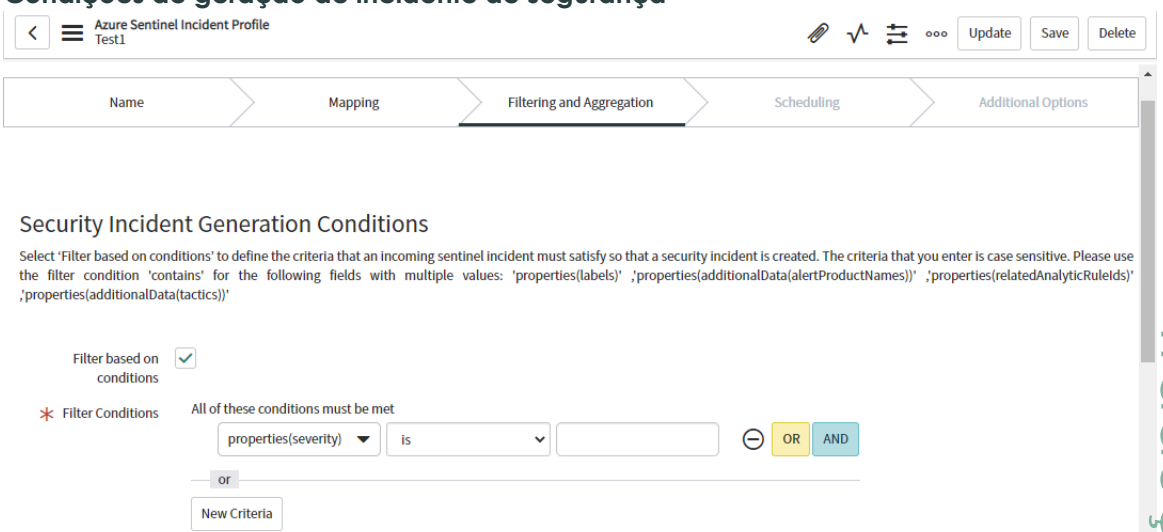
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- properties(relatedAnalyticRuleIds)
- properties(additionalData(tactics))

Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar a condição de filtro "*contém*" nos campos acima para garantir que os dados sejam filtrados corretamente.

Condições de geração de incidente de segurança



2. Usando as listas e os campos do construtor de condições, defina os filtros para a primeira linha.
3. Para adicionar mais condições, clique em **E** ou **OU**.
   - Se **E** for selecionado, todas as condições deverão ser atendidas.
   - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.
4. Para definir uma segunda condição de filtro, clique em **Novos critérios**.

Definir condições de agregação

Defina critérios de agregação de incidentes adicionais que agregam um incidente de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Quando você usa critérios de valor de correspondência de campo para cada perfil, essa agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de incidentes relacionados em um único incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Se um novo incidente corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o incidente será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os incidentes agregados adicionados em uma lista relacionada em um incidente de segurança.
Todos os incidentes agregados em um incidente de segurança são exibidos na lista relacionada de incidentes agregados do Azure Sentinel. Esta lista detalha os carimbos de

Tradução automática

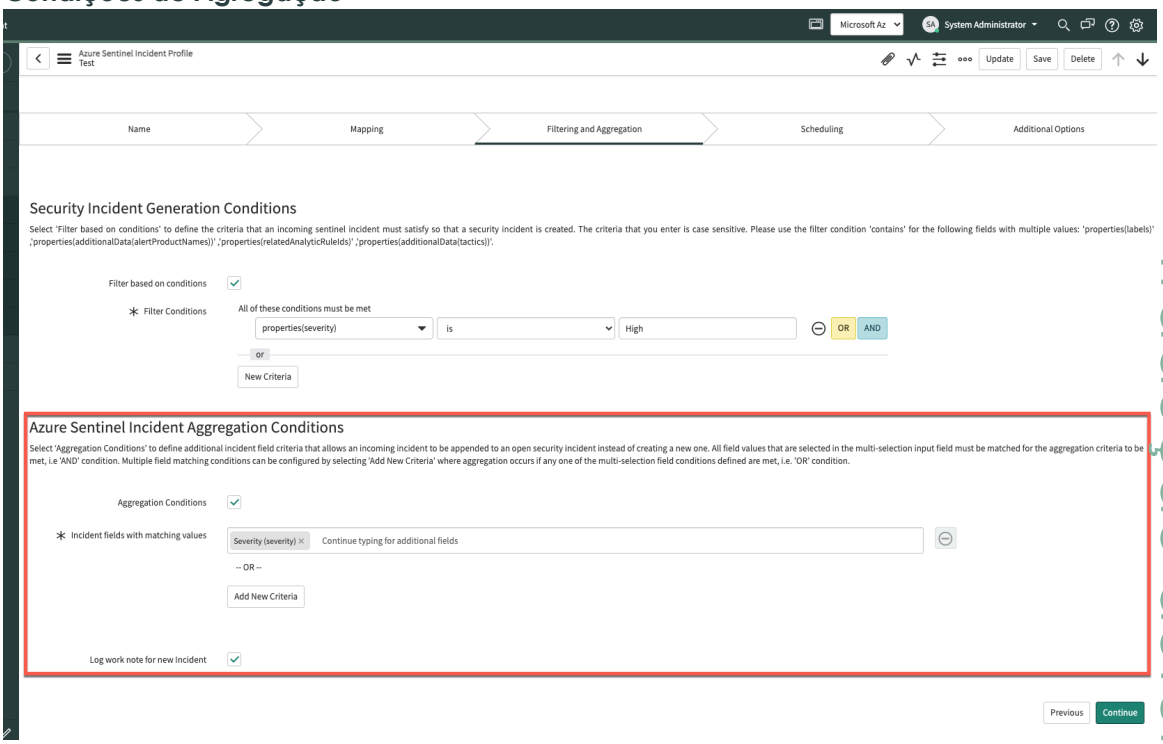
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que os incidentes são adicionados aos incidentes de segurança existentes.

Procedimento

1. Para definir critérios de campo de incidente adicionais que permitam que um incidente Microsoft Azure Sentinel de entrada seja anexado a um incidente de segurança aberto em vez de criar um novo incidente, selecione a opção **Condições de Agregação** conforme mostrado na figura a seguir.

Condições de Agregação



2. No campo **Campos de incidente com valores correspondentes**, insira os valores de campo que você deseja corresponder em incidentes de segurança existentes em sua instância Now Platform.
   Todos os valores de campo selecionados no campo de entrada de seleção múltipla devem corresponder para que os critérios de agregação sejam atendidos e para que este incidente de entrada possa ser anexado a um incidente de segurança existente. Esta seleção implica que é uma condição *AND* em que campos, como Observáveis e Itens de configuração que podem ter vários valores de campo, são mapeados para eles. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de incidente do Azure Sentinel não serão atendidas e um novo incidente de segurança será criado.
3. Para adicionar várias condições de correspondência de campo, clique em **Adicionar novos critérios**
   A agregação ocorrerá se qualquer uma das condições do campo de seleção múltipla que você definir for atendida. Esta seleção implica a condição *OU*.
4. Para atualizar a anotação de trabalho de um novo incidente quando ele for adicionado a um incidente de segurança, selecione **Registrar anotação de trabalho no novo incidente**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A anotação de trabalho registra que um novo incidente foi adicionado e inclui um link para os detalhes do incidente. A anotação de trabalho de log também atualiza mais detalhes adicionados ao campo de anotação de trabalho na seção de mapeamento.

5. Para configurar a programação, clique em **Continuar**.

O que Fazer Depois
Defina uma programação para recuperar os dados do incidente e os incidentes ingeridos que correspondam aos critérios no perfil.

Programar a Microsoft Azure Sentinel recuperação de incidentes

Defina uma programação para recuperar os dados do incidente e ingerir os Microsoft Azure Sentinel incidentes que correspondem aos critérios no perfil.

Antes de Iniciar
Função necessária: sn_sni.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode planejar com que frequência deseja pesquisar futuros Microsoft Azure Sentinel incidentes que correspondam à configuração do perfil de incidente.

Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. Para definir uma data e hora específicas para a ingestão inicial, habilite **definir tempo de ingestão do incidente**. A ingestão subsequente é baseada no período de intervalo de pesquisa.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da integração de incidentes Microsoft Azure Sentinel. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente. Um valor padrão de um minuto é definido para todos os perfis. Você pode modificar esta configuração com base na urgência do incidente e na carga prevista no seu sistema.

Todos os alertas adicionados ao incidente em um intervalo de pesquisa específico terão um processo executado e, em seguida, anexados às listas relacionadas a alertas do Azure Sentinel e a anotação de trabalho também será publicada.

Procedimento
1. No formulário de programação, preencha os campos.

   Configure a programação para definir como e quando você extrai incidentes do locatário Microsoft Azure.

Formulário de programação

Campo	Descrição
Ingestão de incidentes em andamento	Ingestão contínua de incidentes que a instância Now Platform extrai do locatário Microsoft Azure para novos incidentes. Os incidentes de segurança serão criados se forem encontrados incidentes acionados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Definir tempo de ingestão do incidente	Ingestão de incidentes que se baseia na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Tempo de adição do incidente de entrada	Data e hora que você especifica para a ingestão de incidentes.
Recuperação Única	Marque esta caixa de seleção para permitir a recuperação única de incidentes históricos do Azure Sentinel e, em seguida, fazer a reconciliação dos dados. Quando você seleciona este checkox, a aplicação extrai todos os incidentes abertos e encerrados do Azure Sentinel pelo período de até 6 meses aproximadamente. Ao processar os dados, tanto os incidentes em andamento quanto os dados históricos são extraídos, mas o processamento dos incidentes em andamento tem precedência sobre a extração histórica. Caso contrário, a extração histórica poderá levar algum tempo com base na duração e no número de incidentes que você está ingerindo . **Nota:** Os incidentes históricos do Azure Sentinel recuperados passam por verificações de desduplicação para evitar duplicações na aplicação Security Incident Response.
Desde a data	A data desde quando os incidentes históricos foram ingeridos do Azure Sentinel. **Nota:** Os dados de incidentes são extraídos aproximadamente dos últimos 6 meses.

A página de programação permite que você defina como e quando os incidentes são extraídos do locatário Microsoft Azure.

2. Para navegar até a página Opções adicionais, clique em **Continuar**.

Automatizar as atualizações e fechamentos de incidentes pelo status de incidente SIR

Automatize as atualizações e fechamentos de incidentes pelo status de incidente SIR. A integração Microsoft Azure Sentinel tem uma interface bidirecional que permite que ambos os incidentes criem incidentes de segurança e atualizem os incidentes depois que o incidente de segurança é criado ou encerrado.

Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No formulário, preencha os detalhes.
   Siga as instruções para concluir a configuração de atualização de incidentes ao criar ou fechar um incidente de segurança em SIR.

Formulário de atualizações de incidentes de automação

Categoria	Campo	Descrição
Atualizações de criação de incidente	Atualizar status de incidentes do Azure Sentinel após a criação do incidente SIR	Opção que permite que você use a funcionalidade de atualização automatizada de incidentes. O status do incidente Microsoft Azure Sentinel é atualizado no incidente Microsoft Azure com os comentários depois que o incidente SIR é criado no Now Platform.
	Atualização de status de incidente inicial	Status do incidente inicial que é atualizado no ambiente Microsoft Azure Sentinel. Você pode selecionar **Novo** ou **Ativo** como o status.
	Comentários iniciais retornados para o incidente	Comentários iniciais que são publicados no incidente no ambiente Microsoft Azure Sentinel. Edite o texto padrão que é exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente SIR.
Atualizações de fechamento de incidentes	Fechar incidentes do Azure Sentinel após o fechamento do incidente SIR	Opção que permite que você use a funcionalidade de atualização automatizada de status de incidente. Microsoft Azure Sentinel incidentes são encerrados no incidente Microsoft Azure com os comentários fornecidos depois que o incidente SIR é encerrado no Now Platform.
	Atualização de status de incidente de fechamento	Atualização de status no incidente Microsoft Azure Sentinel quando o incidente é encerrado em SIR.
	Comentários de fechamento retornados para o incidente	Comentários que são publicados no incidente no incidente Microsoft Azure Sentinel quando o incidente é encerrado em SIR. Edite o texto padrão que é exibido na seção de comentários

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

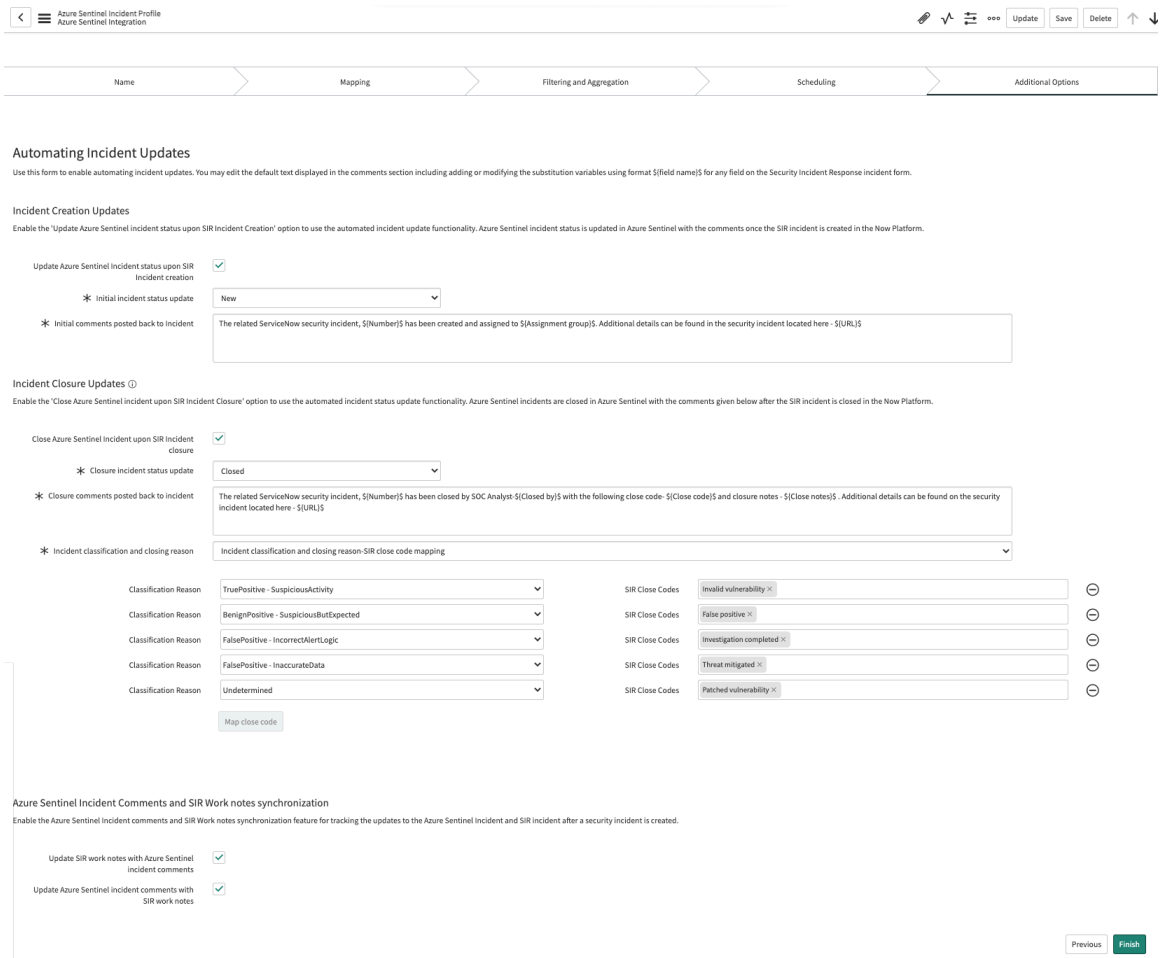
Categoria	Campo	Descrição
		adicionando ou modificando as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente SIR.
	Classificação de incidente e motivo do fechamento	Método para a classificação de incidente e motivo de fechamento que é usado para fechar o incidente no ambiente Microsoft Azure Sentinel. Selecione a **classificação de incidente padrão e o método de motivo de fechamento** para fechar o incidente no ambiente Microsoft Azure Sentinel. Ao selecionar este método, você deve definir a **classificação de incidente padrão e o motivo de fechamento**. Quando você fecha um incidente no SIR, o status do incidente no Azure Sentinel também é fechado com a **classificação de incidente padrão e o motivo de fechamento**especificados. Selecione o método de **mapeamento de código de fechamento SIR para classificação de incidente e motivo de fechamento** para fechar os incidentes e mapear os motivos de classificação com os códigos de fechamento SIR. Você pode mapear vários códigos de fechamento SIR para um único motivo de classificação. Depois de fechar um incidente em SIR usando o código de fechamento, o status do incidente no Azure Sentinel também será fechado com a classificação de incidente mapeada e o motivo de fechamento. Se o motivo da classificação e os códigos de encerramento SIR não estiverem mapeados ou uma correspondência não for encontrada, o incidente será encerrado usando o motivo de classificação padrão como "Indeterminado" no ambiente Microsoft Azure Sentinel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Campo	Descrição
Sincronização de Anotações de trabalho de SIR e comentários de incidente do Azure Sentinel	Atualizar anotações de trabalho SIR com comentários de incidentes do Azure Sentinel	Opção que você pode selecionar para atualizar seus comentários [Microsoft Azure Sentinel nas anotações de trabalho SIR. O comentário nas anotações de trabalho SIR aparece com o prefixo *Comentário do Sentinel*. O comentário também contém o ID do Sentinel, os detalhes do analista e o carimbo de data/hora.
	Atualizar comentários de incidentes do Azure Sentinel com anotações de trabalho SIR	Opção que você pode selecionar para atualizar suas SIR anotações de trabalho nos Microsoft Azure Sentinel comentários do incidente. O comentário em Microsoft Azure Sentinel aparece com o prefixo *Comentário da ServiceNow*.

O exemplo a seguir mostra as opções de configuração que estão disponíveis para automatizar atualizações de incidentes.



2. Clique em **Concluir**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois
O perfil passa para o estado Aguardando. Quando a mensagem de confirmação mostrar que a instalação e a configuração estão concluídas, você poderá ativar o perfil.

Copiar um perfil Microsoft Azure Sentinel

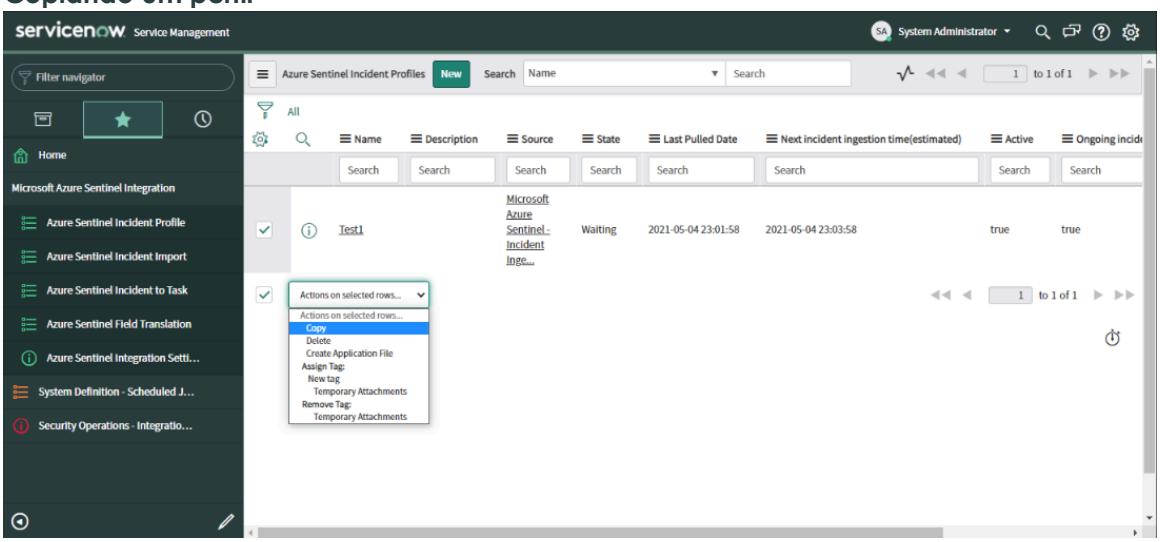
Copie um perfil existente e suas configurações associadas em vez de criar um perfil. Ao criar vários perfis, você pode reutilizar as configurações de um perfil existente copiando esses perfis.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Quando você copia um perfil, o nome do perfil é modificado inicialmente para evitar a criação de perfis duplicados. O perfil copiado também é desativado (definido como falso) para garantir que você não o ative acidentalmente antes de concluir a configuração. Você pode copiar os perfis e usar mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento
1. Navegar até **Todos** > **Integração do Microsoft Azure Sentinel** > **Perfil do Azure Sentinel**.
2. Na lista Perfis do Azure Sentinel, selecione um perfil que você deseja copiar e, em seguida, na lista Ações nas linhas selecionadas, clique em **Copiar** conforme mostrado no exemplo a seguir.

Copiando um perfil

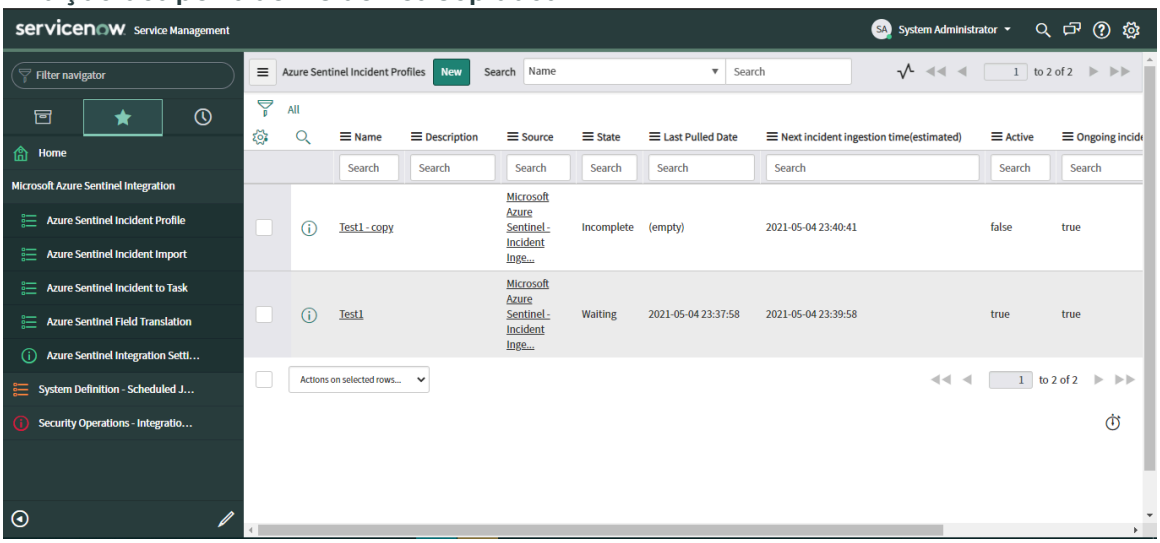


O perfil é copiado e exibido na lista, conforme mostrado no exemplo a seguir. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém a palavra "cópia". Embora o perfil original esteja habilitado (verdadeiro), a cópia está desativada neste ponto (falso). Você pode preferir editar valores do perfil copiado e renomeá-los para que as definições de configuração se apliquem ao novo perfil conforme necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição dos perfis de incidentes copiados



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. O status da coluna Ativa está definido como falso, o que significa que o perfil deve ser ativado.

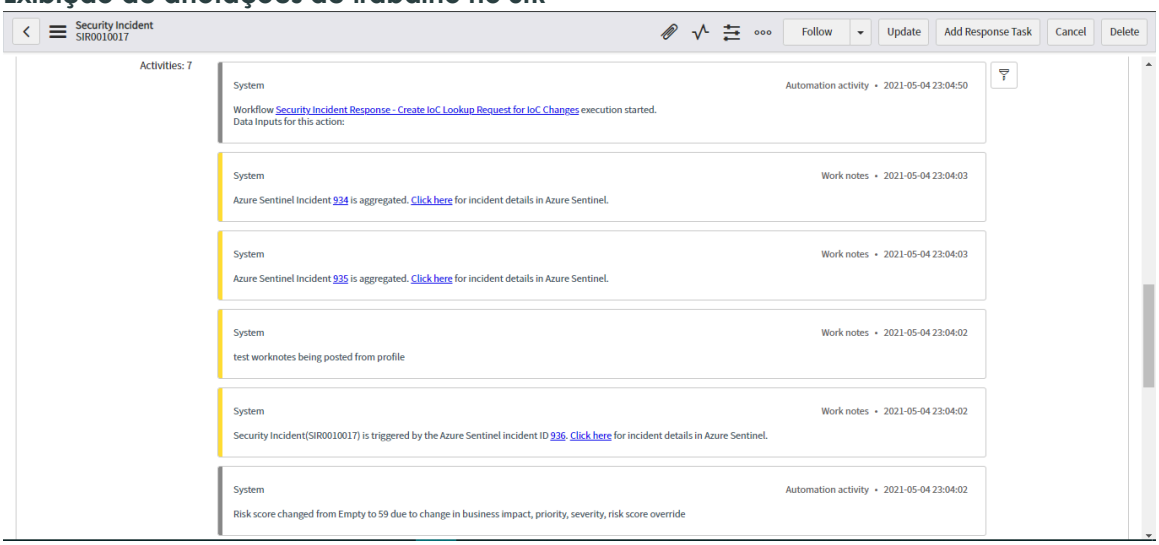
SIR formulário após ingestão de um incidente

Depois que o Now Platform ingere o incidente Microsoft Azure Sentinel, um incidente de segurança é criado e as atualizações são feitas nesse registro de incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada quando um incidente é agregado e se você tiver configurado a opção **Registrar anotação de trabalho para novo incidente** nos Critérios de agregaçãode incidentes. O exemplo a seguir mostra as anotações de trabalho em SIR.

Exibição de anotações de trabalho no SIR



Ao clicar no número do incidente, você pode exibir o registro de importação do incidente interno que contém os dados brutos do incidente. O exemplo a seguir mostra os dados brutos do incidente em SIR.

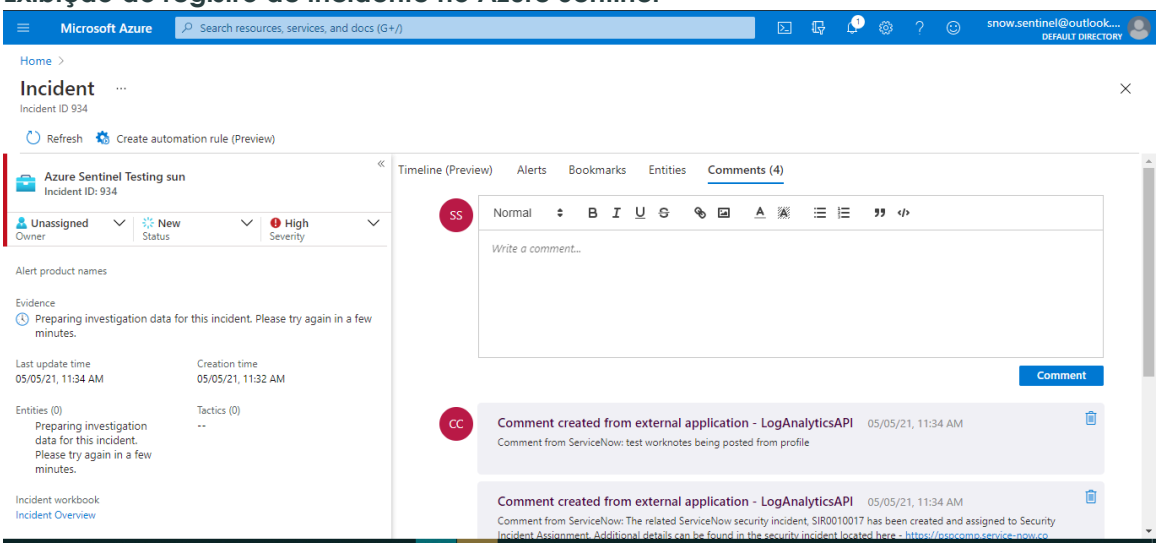
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição dos dados brutos do incidente em SIR

Ao clicar no link **Clique aqui**, você pode exibir o registro no ambiente Microsoft Azure Sentinel. O exemplo a seguir mostra o registro no ambiente Microsoft Azure Sentinel.

Exibição do registro de incidente no Azure Sentinel

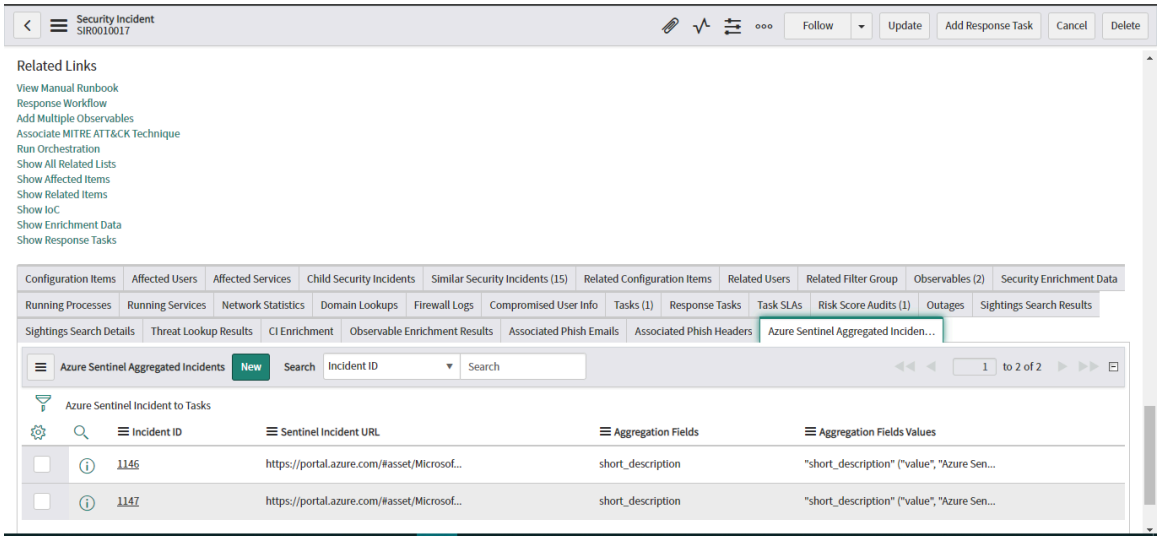


Incidentes agregados do Sentinel

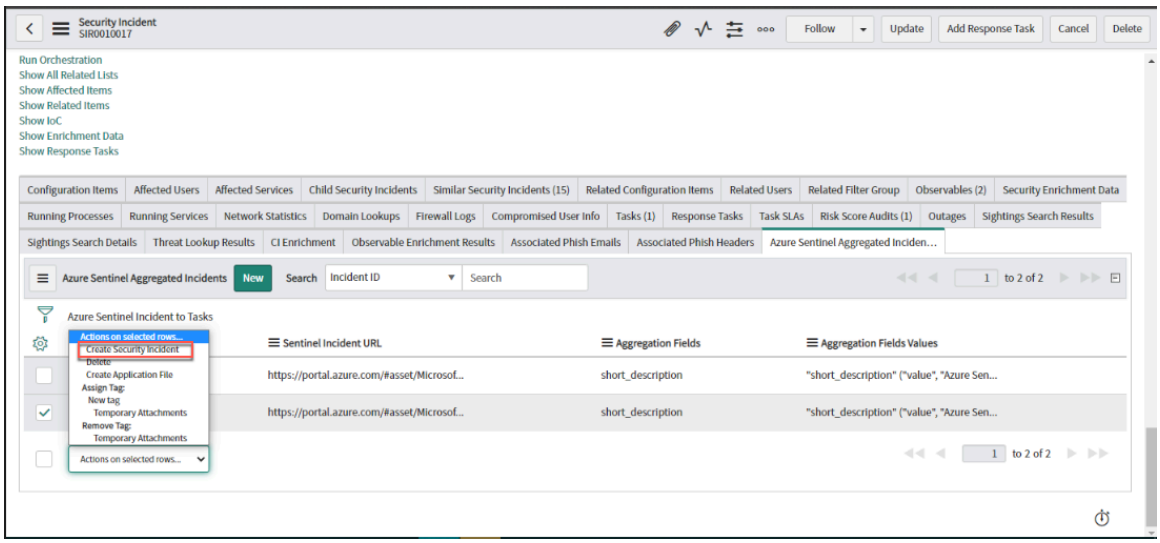
Exibir incidentes agregados do Sentinel: exibe os incidentes que estão agregados ao incidente de segurança. Navegar até **Mostrar todas as listas relacionadas** > **Incidentes agregados do Microsoft Azure Sentinel**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar incidente de segurança: selecione um incidente na lista, clique no menu **Ações** e, em seguida, clique em **Criar incidente de segurança**. Esta opção cria um novo incidente de segurança para o incidente e este incidente é desagregado do incidente de segurança primário.



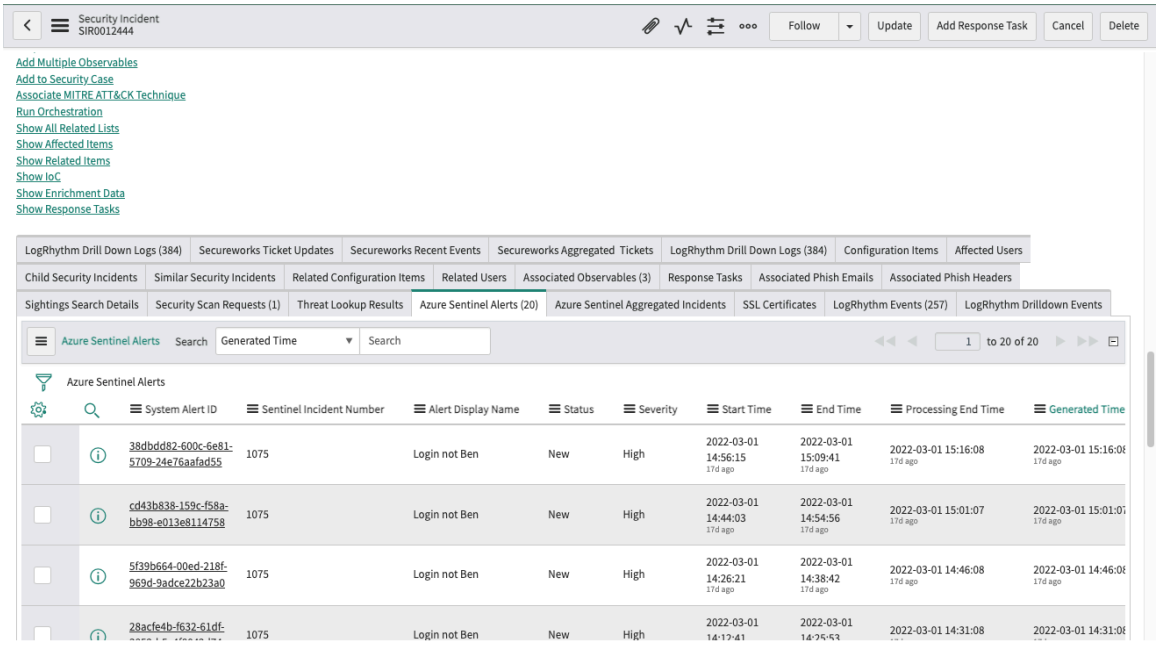
Alertas do Azure Sentinel

Para exibir os alertas associados ao incidente do Sentinel que acionou o incidente de segurança, navegue até **Mostrar todas as listas relacionadas** > **Alertas do Azure Sentinel**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alertas do Azure Sentinel



Revisar as configurações de integração Microsoft Azure Sentinel

Revise as configurações de integração Microsoft Azure Sentinel para que você possa modificar as propriedades do sistema para adequá-las ao seu ambiente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Integração do Microsoft Azure Sentinel** > **Configurações de integração do Azure Sentinel**.
2. Modifique as seguintes configurações conforme necessário.

Microsoft Azure Sentinel Configurações de integração

Nome da Propriedade	Descrição
Impor um limite ao número de dias para os quais os dados de amostra podem ser obtidos. sn_sec_sentinel.max_num_of_days_for_sample_data	Número máximo de dias para os quais você pode buscar dados de amostra do ambiente Microsoft Azure Sentinel. Tipo: inteiro Valor padrão: 7
Receba atualizações relacionadas a novos alertas vinculados ao SIR. sn_sec_sentinel.incident_updates	Ative a opção para receber atualizações de incidentes. Tipo: booleano Valor padrão: Verdadeiro
O caractere delimitador para dividir os valores em mapeamentos de campo Microsoft Azure Sentinel.	O caractere delimitador para dividir os valores em mapeamentos de campo Microsoft Azure Sentinel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
sn_sec_sentinel.delimiter	Tipo: cadeia de caracteres Valor padrão: ', ' (vírgula com espaço)
Impor um limite ao número de incidentes de amostra que podem ser obtidos. sn_sec_sentinel.max_num_of_sample_incidents_per_sentinel	Número máximo de incidentes de amostra que você busca do ambiente Microsoft Azure Sentinel para ingestão. Tipo: inteiro Valor padrão: 5 Valor máximo de amostra: 20
Impor um limite ao número de incidentes do Sentinel que podem ser agregados a um único incidente. sn_sec_sentinel.max_aggregations_per_si	Limite de agregação de incidentes de segurança. Por exemplo, se houver 102 incidentes, os primeiros 100 serão agregados ao incidente de segurança_1 e os 2 restantes ao incidente de segurança_2. Tipo: inteiro Valor padrão: 100
Impor um limite ao número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_sentinel.max_si_per_day	Número máximo de incidentes de segurança que podem ser criados em um período de 24 horas no Now Platform. Tipo: inteiro Valor padrão: 1000
Limite máximo de paginação para buscar os dados do incidente em uma chamada REST. sn_sec_sentinel.max_page_size	Limite de paginação para buscar os dados do incidente em uma chamada REST do ambiente Microsoft Azure Sentinel. Tipo: inteiro Valor padrão: 100
Valor da versão da API para incidentes. sn_sec_sentinel.sentinel_security_incident_api_version	A versão da API da Microsoft para recuperar incidentes do Sentinel. Valor padrão: 2021-10-01
Valor da versão da API para alertas. sn_sec_sentinel.sentinel_security_alert_api_version	A versão da API da Microsoft para recuperar alertas do Sentinel. Valor padrão: 2021-10-01
Valor da versão da API para entidades. sn_sec_sentinel.sentinel_security_entities_api_version	A versão da API da Microsoft para recuperar entidades do Sentinel. Valor padrão: 2021-10-01

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
sn_sec_sentinel.logging.verbosity	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ◦ **error** ◦ **aviso** ◦ **informações** ◦ **depurar** Valor padrão: **informações**.

3. Clique em **Salvar**.
   Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Domain Separation e a integração Microsoft Azure Sentinel

A separação de domínios é compatível com esta aplicação. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, emissão de relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona na integração Microsoft Azure Sentinel

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com a função sn_si.admin no respectivo domínio.

> **Nota:** Ao criar o perfil, use o seletor de domínio para selecionar um domínio. Não crie o usuário no domínio primário e altere posteriormente o domínio do perfil. Você deve ter um usuário para cada domínio do seu perfil com a função sn_si.admin. Use este usuário para criar ou modificar configurações no perfil.

Tradução automática

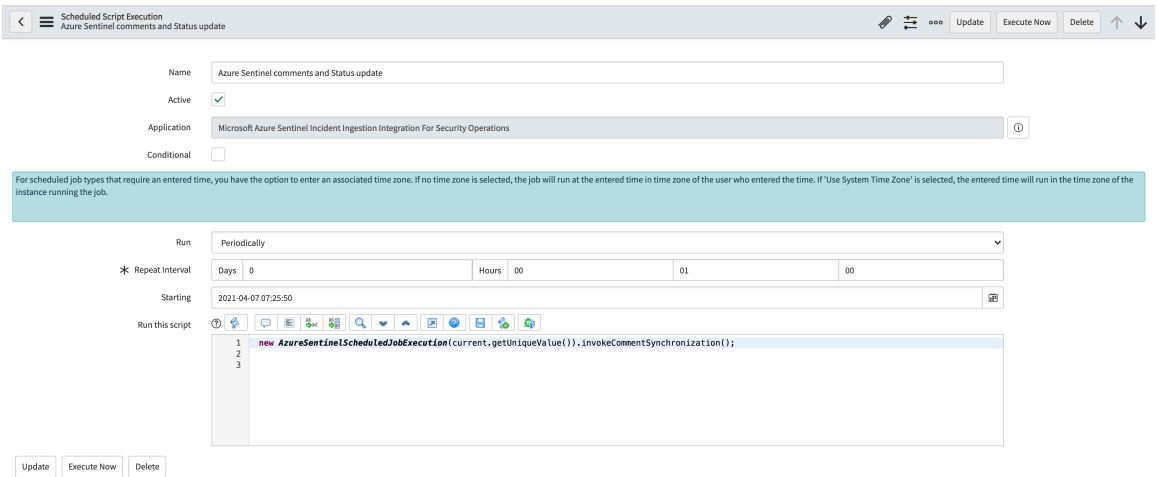
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desabilite os trabalhos agendados existentes.
- Replique os seguintes trabalhos agendados para cada domínio:
  - Entidades e alertas de busca do Azure Sentinel
  - Sincronização de comentários do Azure Sentinel
  - Atualização de status do Azure Sentinel
  - Processo de perfil do Azure Sentinel
  - Dados brutos do processo do Azure Sentinel
  - Limpeza de dados do Azure Sentinel
  - Extração de comentário histórico do Azure Sentinel

  Nota: Depois de replicar os trabalhos agendados, use o navegador e pesquise o módulo Políticas de acesso ao módulo para exibir os registros criados recentemente cujo **script de destino** mostra os trabalhos agendados recém-criados. Modifique o valor do campo **Resultado** para **Rastrear**.

- Altere **Executar como** do usuário do sistema para o usuário com a função sn_si.admin no respectivo domínio e execute o trabalho agendado.

O exemplo a seguir mostra como replicar os comentários do Azure Sentinel e o trabalho de atualização de status e executar o trabalho como um usuário do sistema.



Informações relacionadas

Domain Separation para provedores de serviço

Comparando integrações Microsoft Azure Sentinel e API de Segurança do Microsoft Graph com SIR

Você pode exibir as diferenças entre as integrações Microsoft Azure Sentinel e API de Segurança do Microsoft Graph e escolher a integração certa com sua instância Now Platform.

Visão geral Microsoft Azure Sentinel – Ingestão de incidentes

Microsoft Azure Sentinel é uma solução baseada em nuvem de gestão de eventos de informações de segurança (SIEM) e resposta automatizada de orquestração de segurança (SOAR). Microsoft Azure Sentinel oferece análise de segurança inteligente e inteligência

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

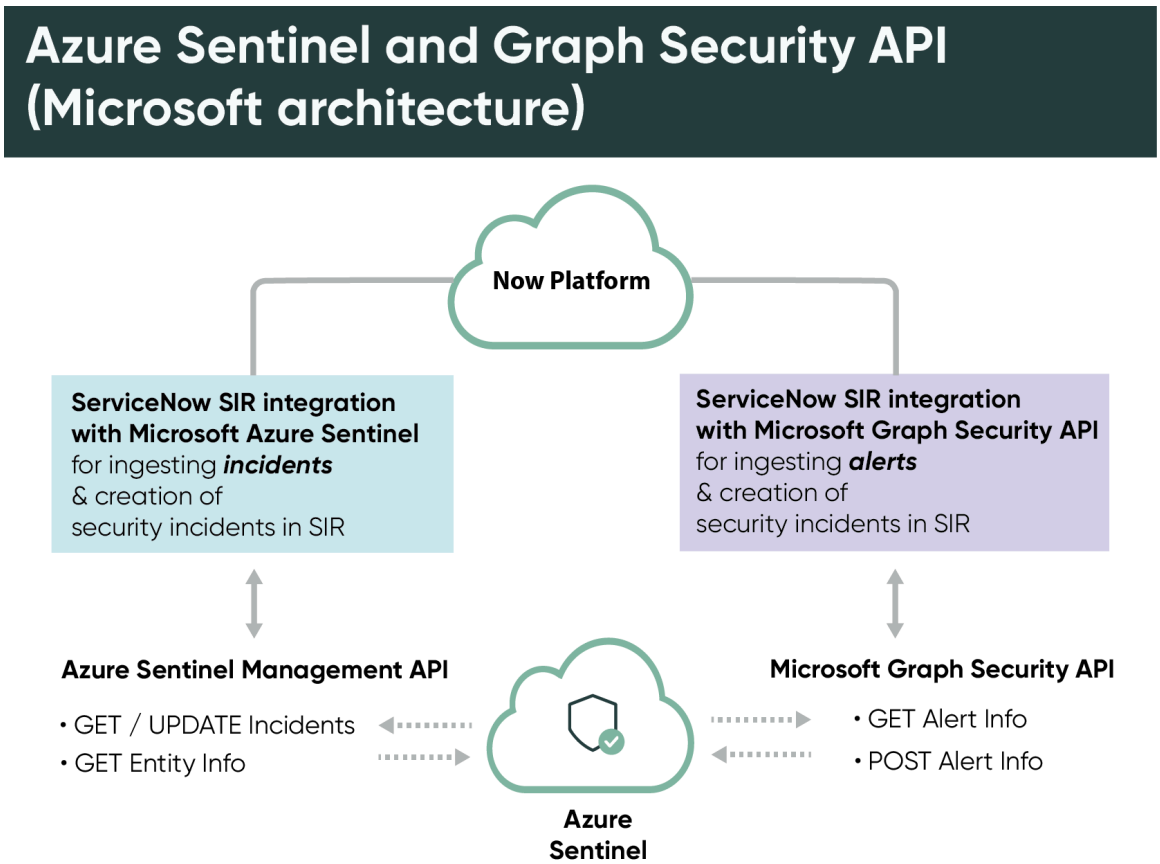
contra ameaças em toda a empresa. Ele fornece uma solução única para detecção de alertas, visibilidade de ameaças, caça proativa e resposta a ameaças.

Visão geral API de Segurança do Microsoft Graph

O API de Segurança do Microsoft Graph é um serviço intermediário (ou agente) que fornece uma única interface programática para conectar vários provedores de segurança (Native to Microsoft, bem como ServiceNow Parceiros).

A integração API de Segurança do Microsoft Graph resolve esses problemas usando o API de Segurança do Microsoft Graph para se conectar a diferentes tecnologias de segurança da Microsoft, como Azure Sentinel, Proteção Avançada contra Ameaças do Microsoft Defender e Proteção Avançada contra Ameaças do Azure. Os alertas dos provedores de segurança da Microsoft são ingeridos e os incidentes de segurança são criados automaticamente em Security Incident Response.

Resumo das diferenças de recursos



Microsoft Azure Sentinel versus API de Segurança do Microsoft Graph

Microsoft Azure Sentinel	API de Segurança do Microsoft Graph
Ingere Microsoft Azure Sentinel incidentes junto com as informações da entidade (quando disponíveis) e automatiza a criação de incidentes de segurança em SIR.	Ingere alertas de vários provedores de segurança (incluindo o Azure Sentinel) em um esquema padrão e automatiza a criação de incidentes de segurança em SIR.
Automatiza Microsoft Azure Sentinel atualizações de status de incidente para o Security Incident Response para que	Oferece suporte a atualizações de alerta (mudança de status de alerta e

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Azure Sentinel versus API de Segurança do Microsoft Graph

Microsoft Azure Sentinel	API de Segurança do Microsoft Graph
você possa criar e fechar incidentes de segurança. **Nota:** ServiceNow atualiza o status de Microsoft Azure Sentinel incidentes com base na criação ou fechamento do incidente de segurança.	fechamento de alerta) para provedores de segurança selecionados. **Nota:** Para obter mais informações sobre os API de Segurança do Microsoft Graph provedores de segurança compatíveis, consulte a documentação da Microsoft .
Use esta integração se o seu cenário incluir as seguintes condições: • A investigação de incidentes preliminares está em Microsoft Azure Sentinel e a investigação subsequente está em SIR • Ingerir Microsoft Azure Sentinel incidentes para SIR	Use esta integração se o seu cenário incluir as seguintes condições: • Execute a investigação de incidentes em SIR. • Ingerir Microsoft Azure Sentinel alertas em SIR. • Incidentes não são criados em Microsoft Azure Sentinel.
O alerta é uma entidade em Microsoft Azure Sentinel. Você não pode recuperar alertas autônomos ou específicos usando a API de gestão Microsoft Azure Sentinel. Você só pode recuperar os dados de alerta associados a um incidente. Os dados de alerta disponíveis usando esta integração são mais avançados do que os dados de alerta disponíveis usando o API de Segurança do Microsoft Graph.	Os dados de alerta normalizados Microsoft Azure Sentinel estão disponíveis. Os Microsoft Azure Sentinel campos de alerta que são mapeados internamente em API de Segurança do Microsoft Graphe estão disponíveis em API de Segurança do Microsoft Graph, estão disponíveis para uso nesta integração.
	Você não pode atualizar alertas em Microsoft Azure Sentinel usando esta integração.

Integração de Microsoft Defender for Endpoint

O Microsoft Defender for Endpoint permite que você inspecione, analise e contenha proativamente ameaças conhecidas e desconhecidas em qualquer endpoint.

A integração Microsoft Defender for Endpoint ajuda os analistas de segurança a investigar e corrigir incidentes de segurança com eficiência sem precisar navegar entre as ferramentas.

Você pode usar esta integração para criar configurações para recuperar os detalhes do host, detalhes de usuários conectados, detalhes de máquinas relacionadas e outros recursos de enriquecimento. Você pode solicitar para isolar qualquer máquina do acesso às redes ou remover as máquinas do isolamento. As solicitações podem ser aceitas ou rejeitadas pelos aprovadores.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Microsoft Defender for Endpoint tem os seguintes recursos principais:

- Execute a Pesquisa de segurança empresarial para detectar possíveis observáveis mal-intencionados nos endpoints e tomar medidas de correção.
- Execute ações de resposta como Isolar host, Remover isolamento, Restringir execução de app, Executar verificação antivírus, Remover restrição de app e Parar e colocar arquivo em quarentena.
- Crie ou atualize indicadores.
- Execute o aprimoramento de observável e recupere dados relacionados a indicadores.

Microsoft Defender for Endpoint

Explorar Introdução ao Microsoft Defender para endpoint	**Instalar** Instalar a aplicação e configurar uma origem para a integração	**Configurar** Configurar perfis e incidentes de segurança para o Microsoft Defender para endpoint
Perfil de capacidade Crie um perfil de capacidade para a integração do Microsoft Defender for Endpoint.	**Configurações adicionais** Configurações adicionais que você pode executar no Microsoft Defender for Endpoint	**Diversos** Crie e configure um perfil para pesquisa de detecções e indicadores com o Microsoft Defender para endpoint.

Registrar e configurar o Microsoft Defender for Endpoint no portal Microsoft Azure

Registre a aplicação Microsoft Defender for Endpoint no portal do Microsoft Azure e conceda acesso de leitura e gravação à aplicação.

Antes de Iniciar

Função necessária: desenvolvedor de aplicações, administrador de locatário.

Procedimento

1. Faça login no portal do Microsoft Azure.
2. Insira `Registros de app` na caixa Pesquisar e clique em **Clique em Novo registro**.
3. Insira um nome para sua aplicação e o URI de redirecionamento e clique em **Registrar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um nome de exemplo é `Microsoft Defender for Endpoint`. O URI de redirecionamento é usado ao fornecer o consentimento do administrador para a aplicação.

4. Na página **Registros de aplicações**, selecione a aplicação que você registrou na Etapa 3.
5. Em Gerenciar, selecione **Certificados e segredos**.
6. Para criar um segredo do cliente, selecione **Novo segredo do cliente**.
7. Copie o segredo do cliente e salve-o.

   Caso tenha esquecido o segredo do cliente, você pode gerar um novo segredo do cliente.

8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique **em Adicionar uma permissão**.
10. Na janela Solicitar permissões de API, clique na guia **APIs que minha organização usa**.
11. Pesquise e selecione **WindowsDefenderATP**.
12. Nas permissões do WindowsDefenderATP, selecione **Permissões da aplicação**. Habilitar essa permissão garante que a aplicação seja executada como um serviço ou daemon em segundo plano sem um usuário conectado.
13. Adicione as seguintes permissões de nível de aplicação e conceda consentimento de administrador para as permissões de API recém-adicionadas.

Permissão	Nome de exibição da permissão
Máquina.Leitura.Todos	Ler todos os perfis de máquina
User.Read.All	Ler perfis de usuário
Isolar.Máquina	Isolar máquina
Execução.RestriçãoDeMáquina	Restringir execução de código
Varredura.Máquina	Verificar máquina
Máquina.ParaREmQuarentena	Parar e colocar em quarentena
URL.Ler.Todos	URLs de Leitura
Arquivo.Lido.Todos	Perfis de arquivo de leitura
Ip.Leitura.Todos	Ler perfis de endereço IP
Ti.LeituraGravação.Todos	Indicadores de leitura e gravação

Tradução automática

Comece com a integração Microsoft Defender for Endpoint

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação Microsoft Defender for Endpoint da ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções necessárias do Now Platform e do Security Incident Response (SIR).	As seguintes funções são necessárias: **1.** Você deve ter a função de administrador do sistema (admin) para instalar a aplicação para a integração. **2.** Você deve ter a função de administrador de incidentes de segurança (sn_si.admin) para configurar a integração, criar, ativar e remover perfis. **3.** Você deve ter a função de analista de incidentes de segurança (sn_si.analyst) para trabalhar com incidentes de segurança. Um usuário com esta função pode iniciar qualquer uma das capacidades disponíveis na integração.
Verifique se as aplicações principais da ServiceNow necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação, uma de cada vez, na seguinte ordem para garantir uma instalação sem problemas: **1.** Security Incident Response **2.** Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) **3.** Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest)
Antes de habilitar a opção de aprovação para perfis, verifique se você criou um grupo de aprovação.	Um fluxo de trabalho de aprovação opcional está disponível para isolar máquinas host, restaurá-las na rede e executar ações adicionais no endpoint. Se sua organização quiser um nível extra de controle sobre essas ações, habilite a opção Requer aprovação durante a configuração dos perfis. Em um cenário em que o perfil está disponível, a configuração do perfil para aprovação tem precedência. Em um cenário em que o perfil não está disponível, as aprovações são tratadas com base nas configurações padrão. Como administrador de segurança, você pode configurar a aprovação ao configurar os perfis e as configurações padrão. Um

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	grupo de aprovação deve estar disponível na lista Grupos em sua instância. Para monitorar e processar solicitações enviadas pelos usuários com a função sn_si.analyst, cada membro do grupo de aprovação deve navegar até Minhas aprovações no Now Platform®. Como alternativa, os aprovadores podem encontrar as solicitações enviadas exclusivamente para integração Microsoft Defender for Endpoint no módulo Aprovações. Para obter mais informações sobre como criar um grupo de usuários, consulte Criação de um grupo de usuários .

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração Microsoft Defender for Endpoint. A próxima etapa é instalar a aplicação Microsoft Defender for Endpoint da ServiceNow Store para a integração.

Instalar a aplicação e configurar uma origem para a integração

Instale e configure a integração Microsoft Defender for Endpoint do ServiceNow Store em sua instância Now Platform. Comece a criar perfis de capacidade usando as configurações.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe a integração do Microsoft Defender for Endpoint em ServiceNow Store e instale-a.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco do Microsoft Defender para endpoint e clique em **Configurar**.
4. No formulário, preencha os campos a seguir.

Configurar o Microsoft Defender para endpoint

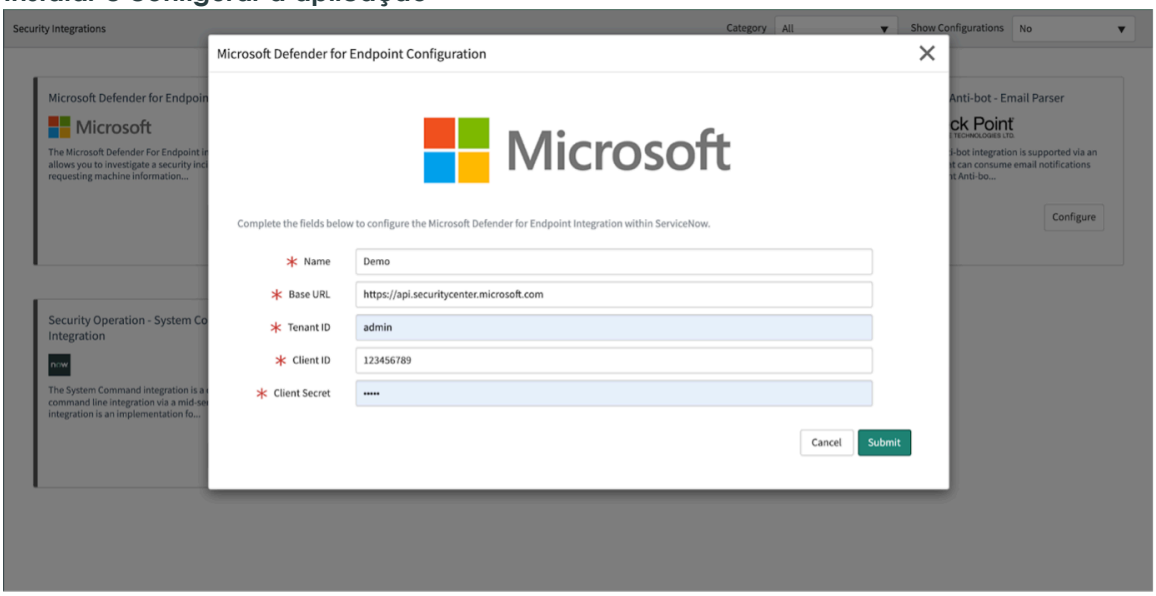
Nome	Nome da configuração da instância Microsoft Defender for Endpoint.
URL base	A URL base de serviço para Microsoft Defender for Endpoint
ID de locatário	O Microsoft Defender for Endpoint ID do locatário. Todas as ações seriam executadas nesta instância.
ID de cliente	ID de cliente da aplicação que você registrou no portal do Microsoft Azure.
Segredo do cliente	Segredo do cliente da aplicação registrada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.

Instalar e configurar a aplicação



Resultados
A lista de configurações Microsoft Defender for Endpoint é exibida com o novo registro de configuração. Você concluiu a configuração do Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint Configurações padrão

Há definições de configuração adicionais que você deve executar após concluir a instalação.

Depois de concluir a instalação, você pode encontrar o módulo Configurações padrão na aplicação Microsoft Defender for Endpoint no painel de navegação à esquerda. Ele contém as configurações padrão para diferentes Microsoft Defender for Endpoint funcionalidades.

Funções necessárias: sn_si.admin, sn_si.analyst (somente leitura).

Configurações adicionais

A seguir estão as definições de configuração adicionais:

- **Aprovação**: esta aprovação é especificamente para a ação Isolar host, Remover isolamento de host e ações adicionais, como Restringir execução de app, Remover restrição de app e Executar verificação antivírus. Você pode usar esta aprovação somente quando as ações são acionadas diretamente da Lista relacionada e se não houver perfis existentes. Se houver perfis para essas capacidades, a configuração de aprovação no perfil terá precedência.
  - **Exigir aprovação**: quando você habilita **Requer aprovação**, o campo Aprovadores fica disponível no formulário.
  - **Aprovadores**: lista de grupos de aprovadores. Depois de enviar uma solicitação, é necessária a aprovação do grupo para concluir a solicitação.
- **IC alternativo**: habilitar esta caixa de seleção fornece a lista de campos disponíveis para passar um IC alternativo para a capacidade. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Esta configuração é aplicável somente para a capacidade Executar ações adicionais no endpoint. Use esta configuração para definir um campo de entrada de IC alternativo somente para a capacidade Executar

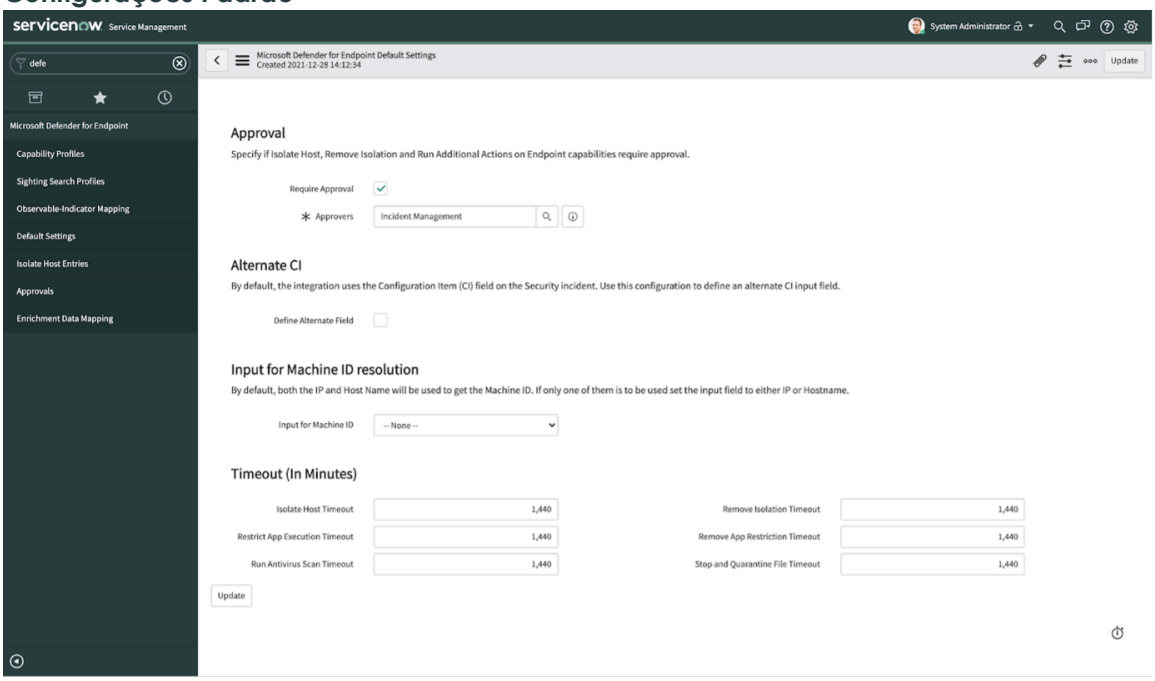
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ações adicionais no endpoint. Para os outros recursos, use a configuração na seção de perfil. Se os perfis não definirem um IC alternativo, as capacidades usarão o campo de IC do formulário de Incidente de segurança.

- **Entrada para resolução do ID do agente**: por padrão, o IP e o nome do host são usados para obter o ID do agente. Se você for usar apenas um deles, defina o campo de entrada como IP ou Nome do host.
- **Tempo limite**:
  - **Tempo limite de isolamento de host (em minutos):** indica o limite de execução das capacidades de isolamento de host.
  - **Remover tempo limite de isolamento (em minutos):** indica o limite de execução da capacidade de remover tempo limite de isolamento.
  - **Tempo limite de execução de app de restrição (em minutos):** indica o limite de execução da capacidade de execução de app de restrição.
  - **Tempo limite de restrição de remoção de app (em minutos):** indica o limite de execução da capacidade de remoção de restrição de app.
  - **Tempo limite de execução da verificação antivírus (em minutos):** indica o limite de execução da capacidade de execução da verificação antivírus.
  - **Tempo limite de parar e colocar arquivo em quarentena (em minutos):** indica o limite de execução da capacidade de parar e colocar arquivos em quarentena.

Configurações Padrão



Mapear os tipos de indicador Microsoft Defender for Endpoint

Mapeie o tipo de observável da ServiceNow com o tipo de indicador Microsoft Defender for Endpoint. Este mapeamento seria usado em ações de Aprimoramento de observável e Criar indicador no Microsoft Defender.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst (somente leitura)

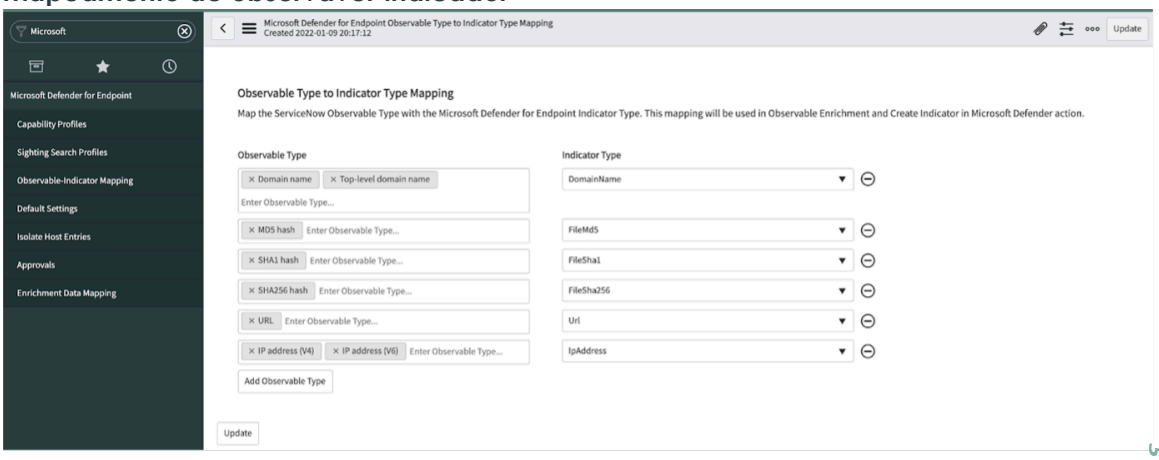
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
Em um cenário em que o tipo de observável não está mapeado para um tipo de indicador, esses observáveis não são qualificados para enriquecimento de observável e criação de indicador no Microsoft Defender para endpoint.

Procedimento
1. Navegar até **Microsoft Defender para Ponto de Extremidade** > **Mapeamento de observável-indicador**.

Mapeamento de observável-indicador



2. Adicione ou atualize um tipo de observável de uma das seguintes maneiras:
   - Para adicionar um novo mapeamento, clique em **Adicionar tipo de observável**.
   - Para atualizar o observável para o mapeamento do tipo de indicador, clique em qualquer linha existente.
3. Para salvar o mapeamento, clique em **Atualizar**.

Criar um perfil de capacidade para a integração Microsoft Defender for Endpoint

Crie um perfil e selecione os Microsoft Defender for Endpoint recursos que você deseja que o perfil execute.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Os perfis são criados para agrupar ou agrupar as capacidades, o que ajudaria os analistas a executar a investigação ou correção com facilidade. Você pode adicionar os seguintes recursos ao perfil:

- Obter detalhes do host
- Obter usuários conectados
- Isolar host
- Remover isolamento

Você não pode agrupar as capacidades Isolar host e Remover isolamento de host com outras capacidades ao criar um perfil. Os perfis para essas capacidades devem ser criados individualmente. Por outro lado, as capacidades Obter detalhes do host e Obter usuários conectados podem ser combinadas. Você pode criar perfis individualmente ou agrupando-os no todo ou em partes de acordo com seus requisitos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

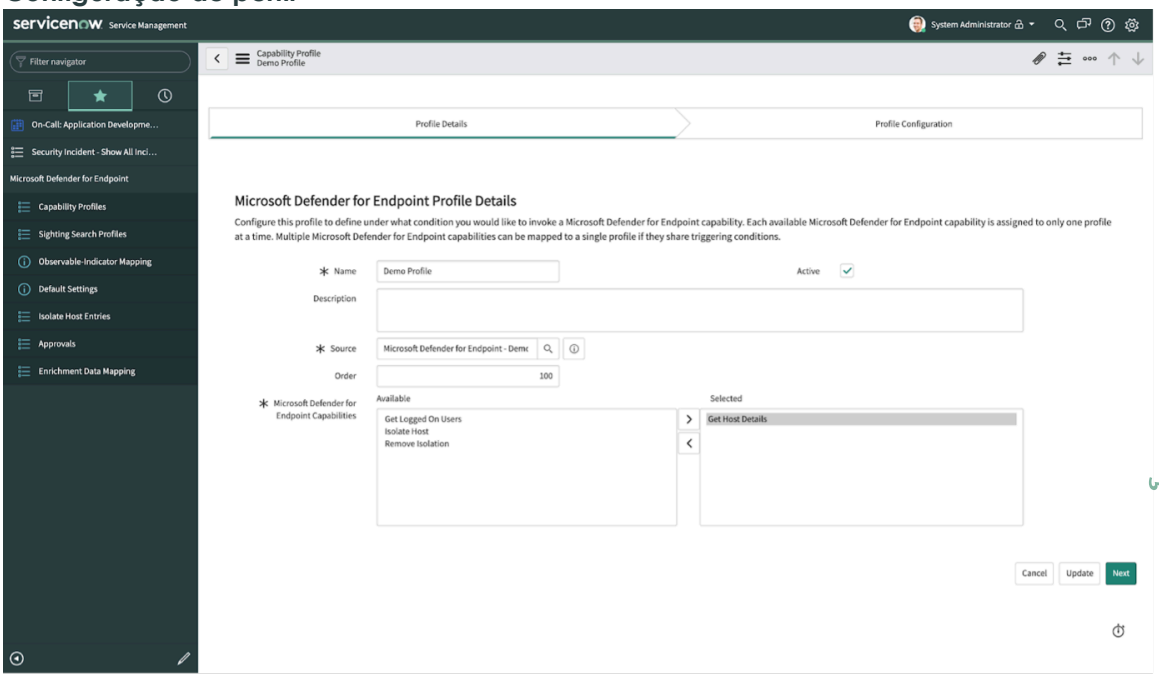
Nota: Depois que uma capacidade é incluída em um perfil, ela não pode ser incluída em nenhum outro perfil da mesma origem.

Procedimento

1. Navegar até **Microsoft Defender para Ponto de Extremidade** > **Perfis de capacidade**.

   A lista de perfis de capacidade do Microsoft Defender for Endpoint é exibida.

Configuração de perfil



2. Clicar **Novo**.
3. No formulário, preencha os campos.

Formulário Perfil de capacidade

Campo	Descrição
Nome	Nome do perfil de capacidade Microsoft Defender for Endpoint. Este nome ajuda a identificar o tipo de perfil e descrevê-lo.
Descrição	Informações adicionais sobre o perfil que descrevem melhor o perfil.
Origem	Nome da origem Microsoft Defender for Endpoint. Somente origens configuradas estão disponíveis na lista.
Capacidades do Microsoft Defender para endpoint	Capacidades do perfil Microsoft Defender for Endpoint. Selecione os recursos desejados para este perfil na coluna Disponível e mova-os para a coluna Selecionado.
Ordem	Prioridade de fluxo. O padrão é 100. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	Opção para indicar que o perfil está ativo. Depois que o perfil estiver ativo, o perfil será acionado automaticamente quando um incidente de segurança for criado e corresponder às condições de filtragem que você especificou na configuração.

4. Para continuar na Configuração de perfil, clique em **Avançar**.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, talvez você prefira revisar como os perfis e as condições configuradas e de acionamento. Para obter mais informações, consulte Condições do gatilho em um item de configuração.

Condições do gatilho em um item de configuração

Depois de criar um perfil e selecionar os Microsoft Defender for Endpoint recursos que você deseja que o perfil execute, defina as configurações do perfil para que o perfil seja executado somente quando um conjunto de condições específicas for atendido.

Como acionar condições em um item de configuração

Você pode definir condições do gatilho para que o perfil seja executado automaticamente sempre que um incidente de segurança for criado que corresponda à condição do gatilho. Se a condição do gatilho não estiver definida, esses perfis poderão ser executados manualmente clicando no formulário Executar perfis de EDR no incidente de segurança e selecionando o perfil.

Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos com as informações armazenadas no Now Platform Configuration Management Database (CMDB). Quando um incidente de segurança é criado e um perfil é executado automática ou manualmente, o CMDB é pesquisado para recuperar o nome do host ou o endereço IP com base no valor do campo de IC. O nome do host ou IP é usado para resolver o ID do agente em Microsoft Defender for Endpoint para identificar o endpoint.

Em um cenário ideal, um valor correspondente é encontrado no banco de dados e os dados são coletados do console Microsoft Defender for Endpoint para o ativo correspondente. Os dados de várias capacidades são extraídos para sua instância Now Platform Configuration Management Database (CMDB) e exibidos nas listas relacionadas de um incidente de segurança. Quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host com ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança que contenha o nome do host ou o IP para executar a resolução do ID do agente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de IC alternativo para identificação de endpoint para garantir que você possa identificar o endpoint em Microsoft Defender for Endpoint. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como um backup, você garante que seus perfis sejam executados mesmo que o campo de IC não esteja preenchido no incidente de segurança associado na criação do incidente.

Nota: Os campos de IC alternativo são considerados somente para capacidades que podem ser adicionadas a um perfil. Esses recursos incluem Obter detalhes do host, Obter usuários conectados, Isolar host e Remover isolamento. Para todas as ações adicionais, o IC alternativo deve ser configurado no módulo Configurações padrão.

Configurar perfis e incidentes de segurança para a integração Microsoft Defender for Endpoint

Crie um perfil e selecione os Microsoft Defender for Endpoint recursos que você deseja que o perfil execute. Você precisa definir as configurações para que o perfil possa ser acionado somente nas condições definidas.

Antes de Iniciar
Função necessária: sn_si.admin, sn_si.analyst (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa
Configure o perfil para que ele seja executado somente quando as condições especificadas forem atendidas. Se necessário, você pode selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem para que o perfil possa ser acionado automaticamente quando um incidente de segurança que atenda às condições do gatilho for criado.

Nota: Você pode navegar até a página Configuração do perfil somente depois de ter inserido a página Detalhes do perfil.

Procedimento

1. Navegar até **Microsoft Defender para Ponto de Extremidade** > **Perfis de capacidade**.
2. Depois de concluir a seção Detalhes do perfil, clique em **Avançar**.
   Revise e configure as seções.
3. Na seção Definir critérios de incidente (Automação), selecione a opção **Definir critérios de incidente** para acionar automaticamente as capacidades Microsoft Defender for Endpoint no perfil.
   Definir critérios de incidente (automação): defina as condições de incidente de segurança que acionariam automaticamente as capacidades do Microsoft Defender for Endpoint para o perfil. Se você não selecionar a opção **Definir critérios de incidente**, o perfil e as capacidades subjacentes poderão ser invocados manualmente a partir do incidente de segurança.

   Nota: As capacidades de isolamento Isolar host e Remover host não podem ser acionadas automaticamente.

   a. Em **Condições do filtro**, selecione o campo obrigatório.
   b. Adicione **novos critérios** e defina também a condição **OU** ou **E.**
4. Na seção Aprovações, marque a caixa de seleção **Requer aprovação** para fornecer um nível extra de controle.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você selecionar esta opção, terá mais controle ao usar os recursos do Microsoft Defender for Endpoint para isolar máquinas host, restaurá-las na rede e obter arquivos.

A opção Aprovações na configuração do perfil aparece somente para as capacidades Isolar host e Remover isolamento de host, respectivamente.

5. Na seção Configuração adicional, selecione a opção **Definir campo** alternativo para definir um campo de entrada alternativo.
Configuração adicional: quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança para consultar o Microsoft Defender para APIs de endpoint .

   Nota: Para obter mais informações, consulte Condições do gatilho em um item de configuração.

   a. Selecione a opção **Definir campo** alternativo.

   b. Selecione o campo de entrada em **Campo de gatilho de IC alternativo**.

6. Na seção Marcadores, marque a caixa de seleção **Exibir** marcador para habilitar a marcação de incidentes de segurança. O nome do perfil é prefixado na habilitação do marcador.

   Opcionalmente, você pode marcar incidentes de segurança com marcadores para perfis iniciados, perfis concluídos e perfis com falha. Por padrão, esta opção está desativada para todos os perfis.

7. Clicar **Concluído**.

Verificar os filtros de condição do gatilho

Valide o perfil e verifique se os filtros de condição do gatilho que você configurou estão funcionando conforme o esperado.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos Now Platform® incidentes de segurança.

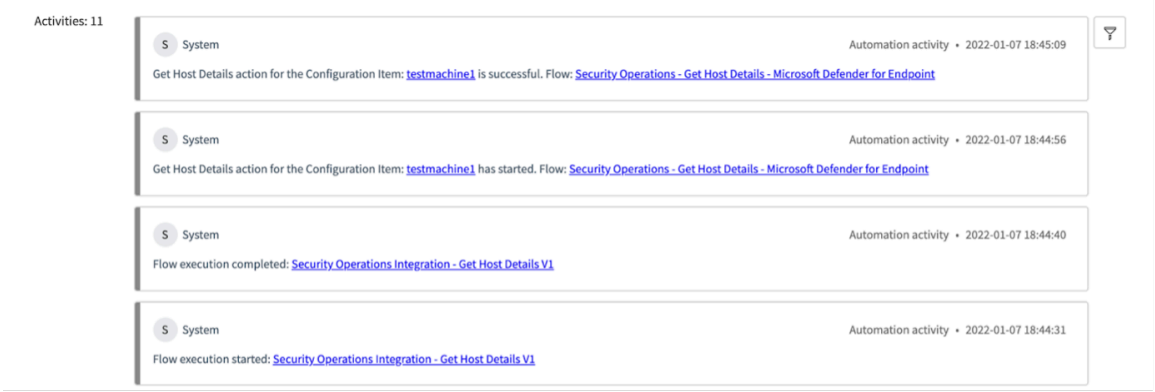
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Para criar um novo incidente de segurança, selecione **Novo**.
3. Para acionar o respectivo perfil, forneça as condições de filtro conforme fornecido no perfil de capacidade.
4. Clicar **Salvar**.
5. Para validar as anotações de trabalho e a seção de atividades, exiba e verifique os registros marcados com os marcadores de perfil iniciado, perfil concluído ou perfil com falha.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anotações de trabalho e atividades



6. Para validar todos os dados nas listas relacionadas, clique em **Mostrar todas as listas relacionadas**.
7. Clique em qualquer guia da **Lista relacionada** para validar os detalhes.
   Por exemplo, Detalhes do host.

Acionar as capacidades Microsoft Defender for Endpoint de Links Relacionados

Acione um perfil de capacidade manualmente após revisar um incidente de segurança de links relacionados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Além de executar o perfil para o IC ou o IC alternativo do incidente de segurança, você também pode executar o perfil para valores de IC presentes na lista relacionada Item de configuração selecionando **Incluir IC relacionado** na caixa de diálogo. Isso recupera os dados dos valores de IC presentes na lista relacionada. Como alternativa, você pode executar o perfil apenas para os valores de IC presentes na lista relacionada.

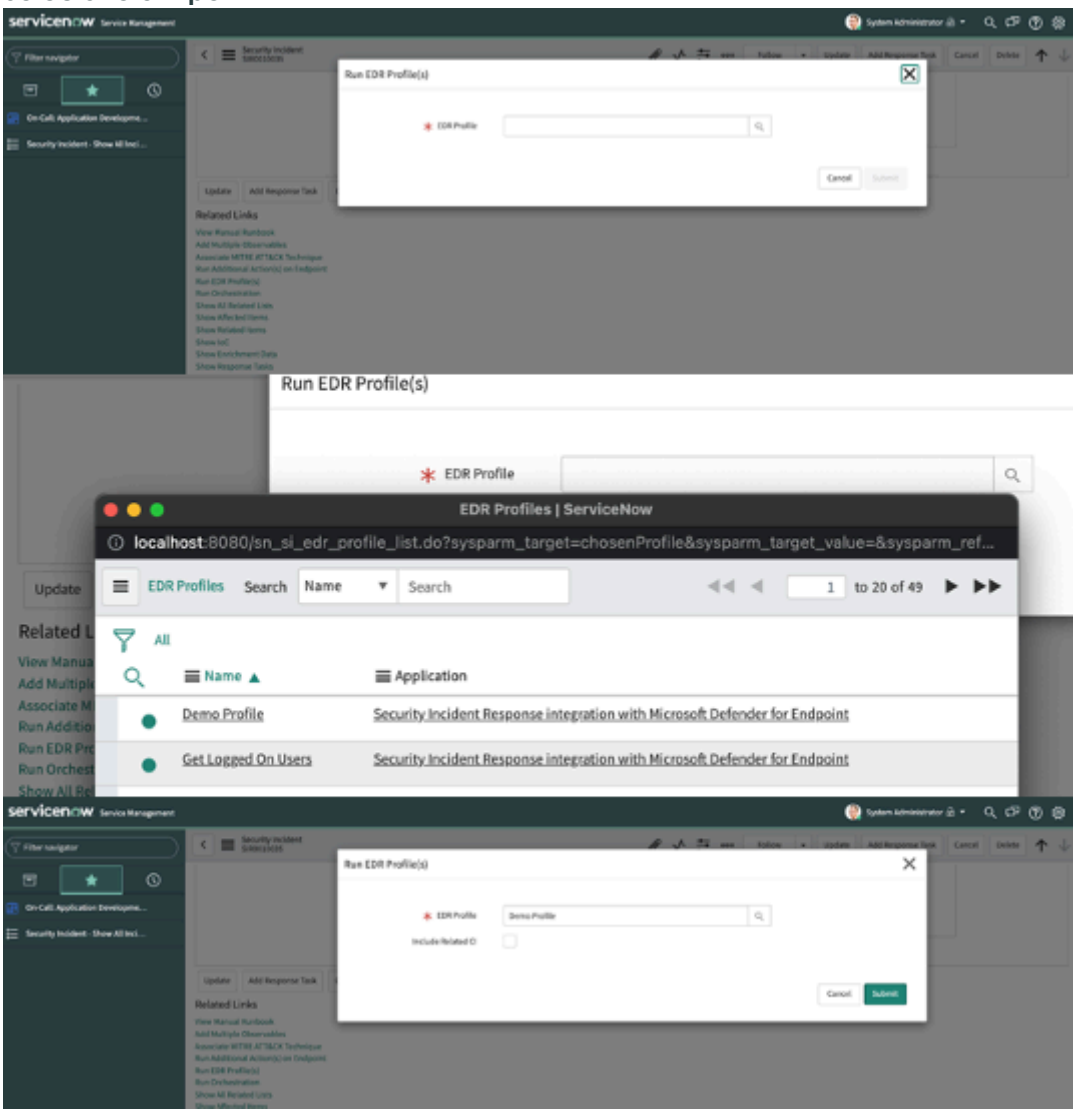
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações Microsoft Defender for Endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(is) de EDR**.
4. Navegue e selecione um perfil na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione um perfil



O perfil selecionado é acionado manualmente.

5. Valide as anotações de trabalho e a seção de atividades.
6. Exiba os marcadores e valide os dados nas listas relacionadas.

Acionar o Microsoft Defender for Endpoint da lista relacionada de item de configuração

Acione um perfil de capacidade manualmente na lista relacionada de itens de configuração.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações Microsoft Defender for Endpoint.
3. Clicar **Mostrar todas as listas relacionadas**.
4. Clique na lista relacionada Item de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os itens de configuração adicionados.
6. Nas linhas **Ações** nas linhas selecionadas, selecione uma capacidade.
   A capacidade selecionada é acionada manualmente.
7. Valide as anotações de trabalho e a seção de atividades.
8. Exiba os marcadores e valide os dados nas listas relacionadas.

Configurações adicionais em Microsoft Defender for Endpoint

A integração Microsoft Defender for Endpoint oferece suporte à execução de ações adicionais além das ações padrão.

O Microsoft Defender for Endpoint é compatível com as seguintes configurações adicionais:

Configurar a capacidade Isolar host no Microsoft Defender for Endpoint

Isole o host de acessar a rede em Microsoft Defender for Endpoint com base na gravidade do ataque. Isolar o host da rede permite que você evite outras atividades mal-intencionadas ou possíveis ataques a outros hosts.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para a capacidade Isolar host

Capacidade	Obrigatório	Descrição
Isolar host	Tipo de isolamento	(Obrigatório) Tipo de isolamento (completo ou seletivo).
	Comentário	(Obrigatório) Comentário a ser associado à ação.

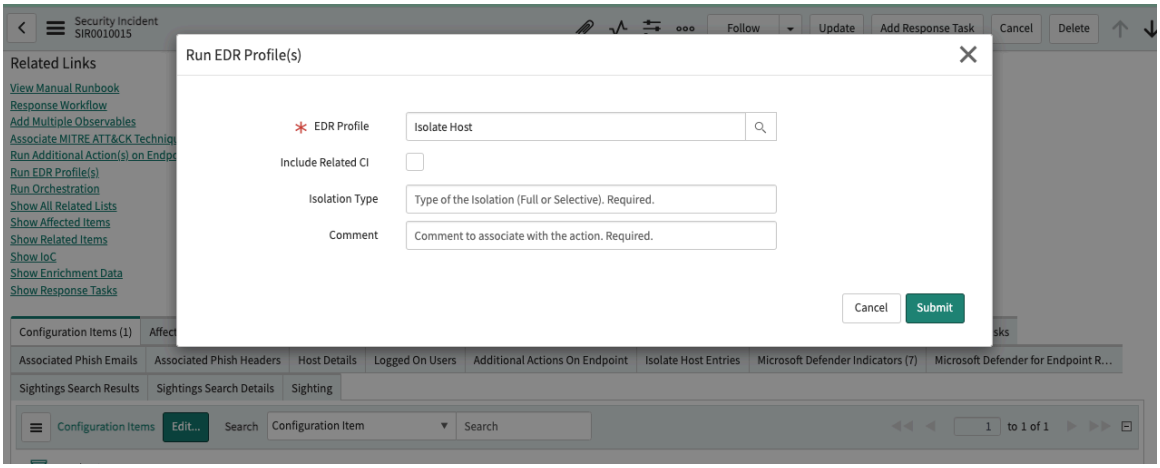
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(is) de EDR**.
4. Pesquise e selecione um perfil com a **capacidade Isolar host** selecionado na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isolar host



Como alternativa, você pode executar as seguintes etapas:

a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.

b. Clique na lista relacionada **Item de configuração**.

c. Selecione **Isolar host** e selecione os recursos correspondentes.

5. Valide a atividade de automação e a seção de atividades e verifique se os dados estão conforme o esperado.

6. Exiba os dados e valide os detalhes do host isolado nas listas relacionadas.

Configurar a capacidade Remover isolamento de host no Microsoft Defender for Endpoint

Se necessário, remova o isolamento de um host que foi isolado anteriormente da rede em Microsoft Defender for Endpoint. Você pode impedir outras atividades mal-intencionadas ou possíveis ataques em outros hosts.

Antes de Iniciar

Requisitos para a capacidade Remover isolamento

Capacidade	Entrada necessária	Descrição
Remover isolamento	Comentário	(Obrigatório) Comentário a ser associado à ação.

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.

2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.

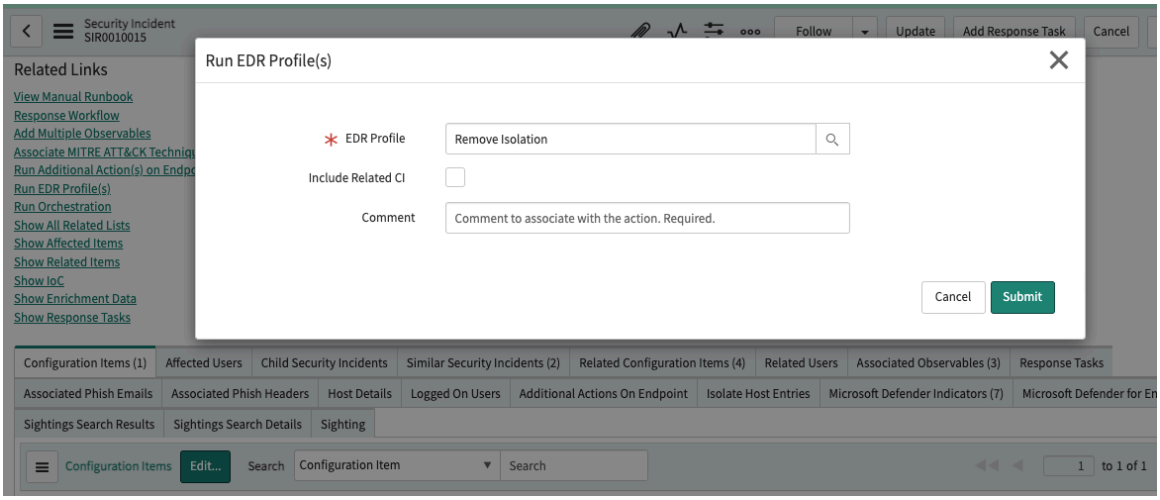
3. Na seção Links relacionados, clique em **Executar perfil(is) de EDR**.

4. Pesquise e selecione um perfil com a **capacidade Remover isolamento** selecionado na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Remover isolamento



Como alternativa, você pode executar as seguintes etapas:

a. Clique em **Mostrar todas** as listas relacionadas na seção de listas relacionadas.

b. Clique na lista relacionada **Item de configuração**.

c. Selecione **Remover isolamento** e selecione as capacidades correspondentes.

5. Valide a atividade de automação e a seção de atividades.

6. Exiba os dados e valide os detalhes do host isolado nas listas relacionadas.

7. Valide as atividades de automação da execução.

Configurar a capacidade Executar verificação antivírus no Microsoft Defender for Endpoint

Inicie remotamente uma verificação antivírus para ajudar a identificar e corrigir malwares que podem estar presentes em um dispositivo comprometido. Execute a verificação como parte do processo de investigação ou resposta.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para a capacidade Executar verificação antivírus

Entrada	Descrição
Tipo de Verificação	(Obrigatório) Tipo de verificação (completa ou rápida).
Comentário	(Obrigatório) Comentário a ser associado à ação.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.

2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.

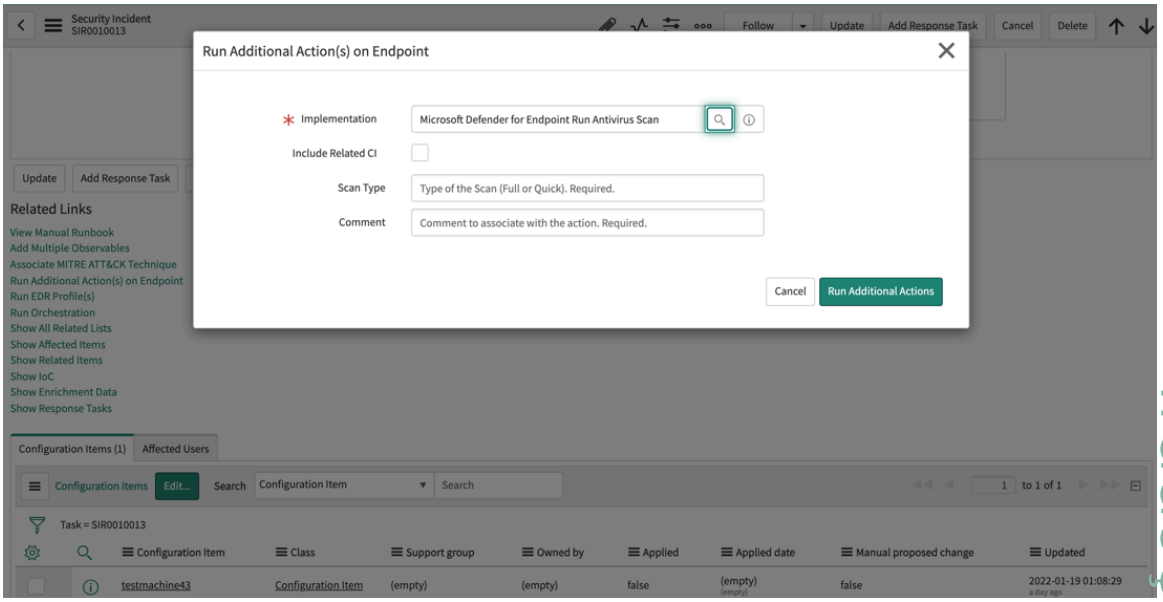
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.

b. Navegue e selecione a capacidade necessária.
Por exemplo, clique na capacidade **Executar verificação antivírus**.

Executar varredura antivírus



Como alternativa, você pode executar as seguintes etapas:

a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.

b. Clique na lista relacionada **Item de configuração**.

c. Selecione os itens de configuração adicionados e, em Ações nas linhas selecionadas, selecione **Executar ações adicionais no endpoint**.
Depois de selecionar a implementação da capacidade **Executar verificação antivírus**, os campos de entrada **Tipo de verificação adicional** e **Comentário** são exibidos.

3. Selecione o **tipo de verificação** que você deseja executar (rápida ou completa) e adicione um comentário antes de executar a verificação.
4. Para iniciar a verificação do antivírus, clique em **Executar ação adicional**.
5. Exibir as atividades de automação da execução e validá-las.
6. Valide o status da ação nas listas relacionadas Ações adicionais nas listas relacionadas ao endpoint.

Configurar a capacidade de execução de app restrita em Microsoft Defender for Endpoint

Para conter um ataque, restrinja ou bloqueie um dispositivo e evite que tentativas subsequentes de execução de programas potencialmente mal-intencionados.

Antes de Iniciar

Requisitos para a capacidade de execução de app restrita

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Tradução automática

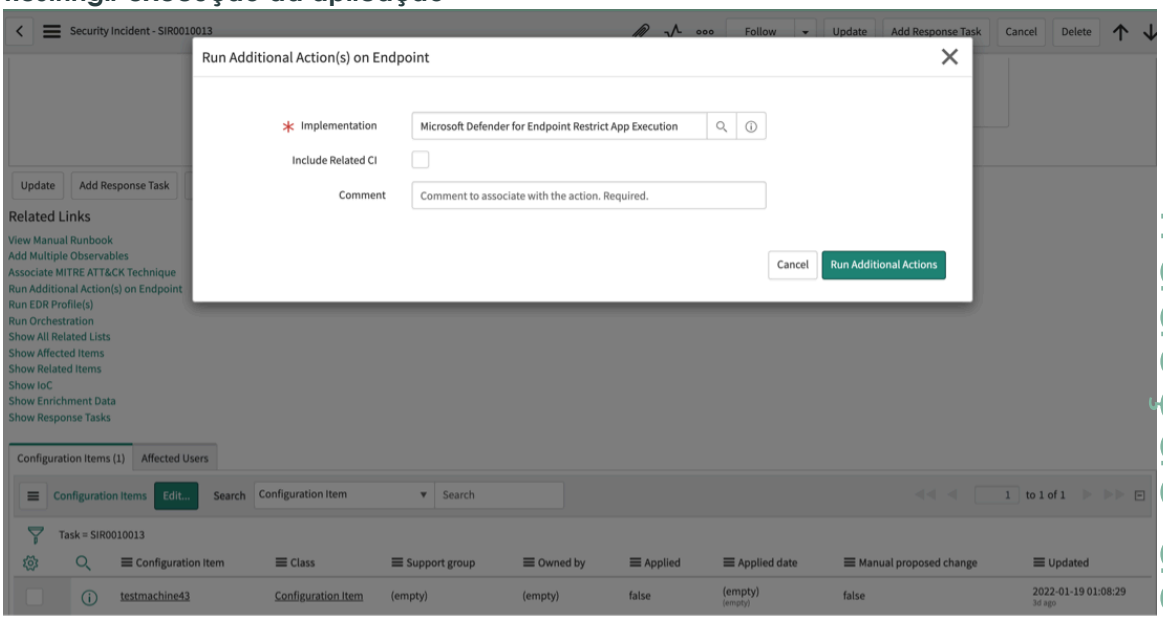
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.
   a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Navegue e selecione a capacidade **Restringir execução de app**.

Restringir execução da aplicação



Como alternativa, você pode executar as seguintes etapas:

   a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.
   b. Clique na lista relacionada **Item de configuração**.
   c. Selecione os itens de configuração adicionados.
   d. Em Ações em linhas selecionadas, selecione **Executar ações adicionais no endpoint**.
3. Para habilitar Restringir execução de app na máquina, clique em **Executar ação adicional**.
4. Exibir as atividades de automação da execução e validá-las.
5. Valide o status da ação nas listas relacionadas Ações adicionais nas listas relacionadas ao endpoint.

Configurar a capacidade Remover restrição de app em Microsoft Defender for Endpoint

Se necessário, remova as restrições de qualquer aplicação no dispositivo.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

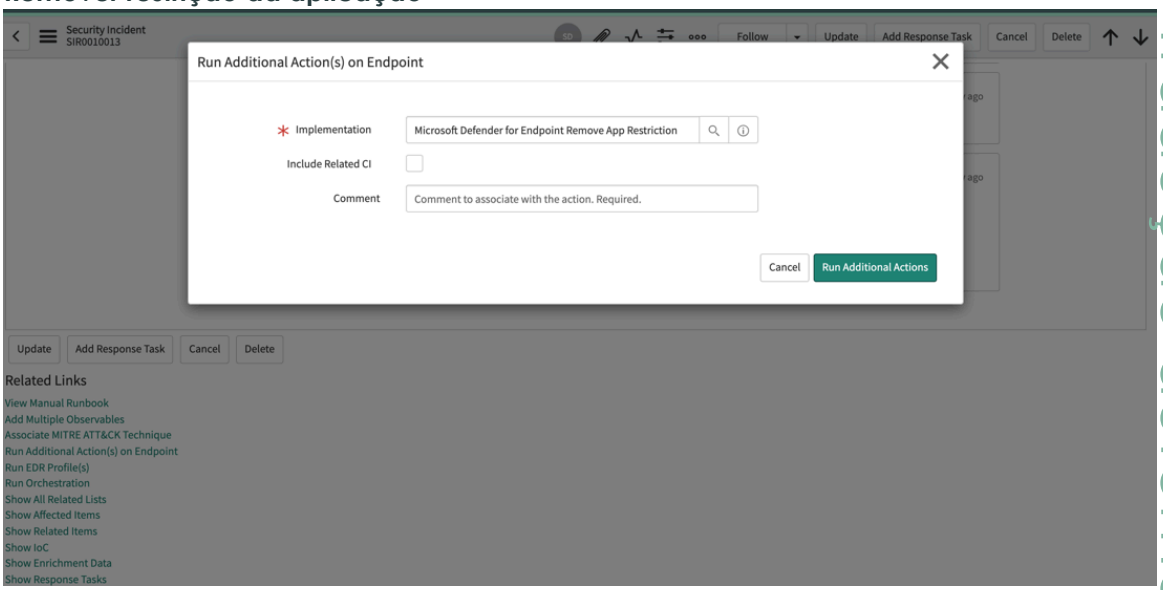
Requisitos para a capacidade de remover restrição de app

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.
   a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Navegue e selecione a capacidade **Remover restrição da aplicação**.

Remover restrição da aplicação



Como alternativa, você pode executar as seguintes etapas:

   a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.
   b. Clique na lista relacionada **Item de configuração**.
   c. Selecione os itens de configuração adicionados.
   d. Selecione **Executar ações adicionais no endpoint**.
   O campo de entrada Comentário adicional é exibido.
3. Para remover a restrição do app, clique em **Executar ação adicional**.
4. Exibir as atividades de automação da execução e validá-las.
5. Valide o status da ação nas listas relacionadas Ações adicionais nas listas relacionadas ao endpoint.

Configurar Obter máquinas relacionadas da capacidade do Defender no Microsoft Defender for Endpoint

Obtenha a lista de máquinas relacionadas de observáveis específicos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Nota: Os tipos de observável compatíveis são Nome de domínio, hash SHA1 e Nome de usuário.

Função necessária: sn_si.admin ou sn_si.analyst

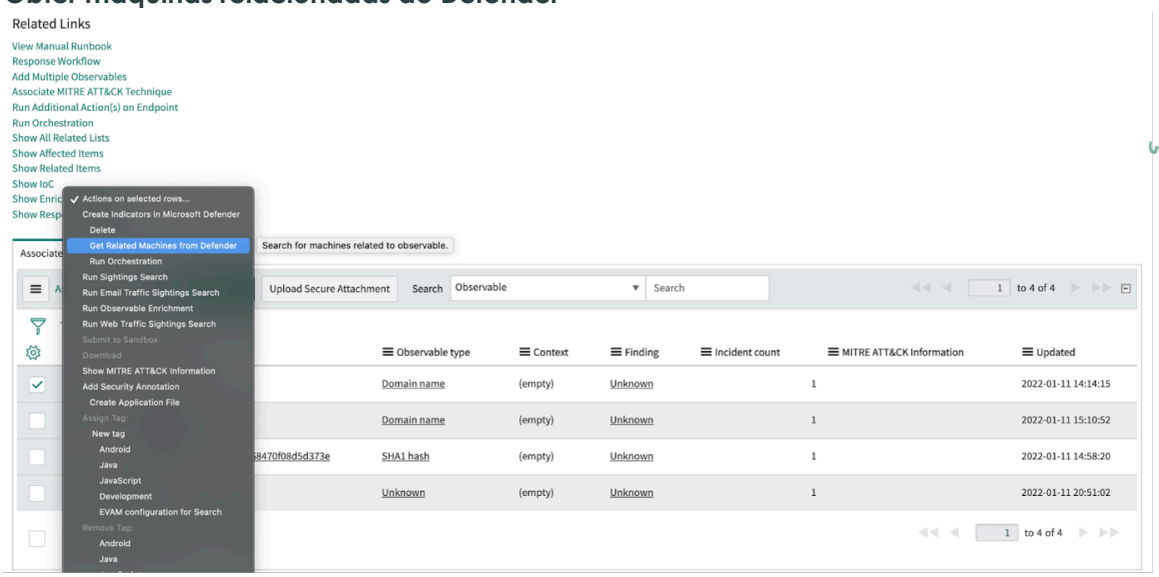
Por Que e Quando Desempenhar Esta Tarefa

Você pode recuperar a lista de máquinas que acessaram os observáveis específicos. Você pode armazenar a lista na tabela Detalhes do Microsoft Defender for Endpoint Related Machines. Você pode acionar a capacidade Obter máquinas relacionadas do Defender na lista relacionada Observáveis associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.

Obter máquinas relacionadas do Defender



3. Na seção Links relacionados, clique em **Mostrar IoC**.
4. Clique na lista relacionada Observáveis associados.
5. Selecione os observáveis associados.
6. Na lista Ações, selecione a capacidade **Obter máquinas relacionadas do Defender**.
7. Valide a atividade de automação e a seção de atividades.
8. Exiba os dados e valide os detalhes do Microsoft Defender para máquinas relacionadas ao endpoint nas listas relacionadas.
9. Exibir as atividades de automação da execução e validá-las.

Configurar a capacidade de parar e colocar arquivo em quarentena no Microsoft Defender for Endpoint

Interrompa e coloque em quarentena arquivos da plataforma Microsoft Defender.

Antes de Iniciar

Tipos de observável compatíveis: hash SHA1.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Requisitos para a capacidade de parar e colocar arquivo em quarentena

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode executar a ação Interromper e colocar arquivo em quarentena somente nos observáveis específicos do tipo SHA1. Armazene os detalhes na tabela Ações adicionais no endpoint. Você pode acionar a capacidade Interromper e colocar arquivo em quarentena na lista relacionada de detalhes do Microsoft Defender para máquinas relacionadas ao endpoint.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.
3. Na seção de links relacionados, clique em **Mostrar todas as listas relacionadas**.
4. Clique na lista relacionada Detalhes do Microsoft Defender para Endpoint Related Machines.
5. Selecione um ou mais registros.
6. Em **Ações** em linhas selecionadas, selecione a capacidade **Parar e colocar arquivo em quarentena**.
7. Valide a atividade de automação e a seção de atividades.
8. Exiba os dados e valide os dados nas listas relacionadas.
9. Exibir as atividades de automação da execução e validá-las.

Crie e configure um perfil para pesquisa de detecções com a integração Microsoft Defender for Endpoint

Crie e configure o perfil de pesquisa de detecções automaticamente usando o Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar o fluxo de trabalho Pesquisa de detecções para executar as pesquisas de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra capacidades de implementação, cria as consultas baseadas nas configurações de pesquisa de detecções e executa as pesquisas baseadas no fluxo de trabalho configurado.

O Microsoft Defender for Endpoint fornece um perfil de pesquisa de detecções do sistema de base que permite configurar as pesquisas de detecções automáticas. Com este perfil, você pode acessar as informações de detecções de observáveis relacionadas de uma organização e também ver as detecções de outras organizações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Integrações** > **Configuração de pesquisa de detecções**.
2. Clique em **Nova**.
3. No formulário, preencha os campos a seguir.

Formulário Configuração de pesquisa de detecções

Campo	Descrição
Nome	Nome do perfil de pesquisa de detecções.
Pesquisa salva	Opção para salvar a configuração de pesquisa. As consultas de configuração de pesquisa salvas são consultas de exemplo. Você pode substituí-los pelos parâmetros do seu ambiente e criar configurações de pesquisa salvas adicionais conforme necessário.
Origem da pesquisa de detecções	A origem configurada para a pesquisa de detecções na integração Microsoft Defender for Endpoint.
Pesquisar	Cadeia de caracteres de pesquisa nativa que forma uma consulta.
Ativo	Opção para habilitar a configuração de pesquisa salva. Somente configurações de pesquisa ativas podem executar uma pesquisa de detecções.
Tipo de observável	Tipo de categoria de observável. Por exemplo, endereço IP, valor de hash, URL e nome de domínio.
Máximo de observável por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa. Defina este valor como 1 para esta integração.
Parâmetros de pesquisa de detecções	Parâmetros para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado.

4. Clique em **Enviar**.

Executar uma pesquisa de detecções manual no Microsoft Defender for Endpoint

Selecione observáveis individuais ou múltiplos e execute uma pesquisa de detecções manual em Microsoft Defender for Endpoint para determinar a predominância de uma ameaça ao longo do tempo.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os tipos de observável compatíveis são os seguintes:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Nome do domínio
- Endereço IP (V4)
- Endereço IP (V6)
- Hash MD5
- Hash SHA1
- Hash SHA256

Procedimento

1. Navegue até **Incidentes de segurança**.
2. Abra um SIR existente ou crie um novo SIR.
3. Nos links relacionados, clique em **Mostrar IoC**.
4. Clique nas listas relacionadas a Observáveis associados.
5. Selecione os observáveis.
6. Na lista Ações, clique em **Executar aprimoramento de observável**.
7. Selecione os observáveis em **Ação** nas linhas selecionadase clique em **Executar Pesquisa de detecções**.

   Nota: A pesquisa de detecções é compatível com os tipos de observáveis nome de domínio, endereço IP (V4), endereço IP (V6), hash MD5, hash SHA1 e hash SHA256, respectivamente.

8. Especifique o intervalo de tempo para a pesquisa e clique em **Pesquisar**.

   Nota: O Microsoft Defender para endpoint oferece suporte à pesquisa de detecções somente nos últimos 30 dias. Se a consulta de intervalo for anterior aos últimos 30 dias, a pesquisa de detecções não recuperará nenhum dado. Se a consulta de intervalo se sobrepuser aos últimos 30 dias, as vistas somente dos últimos 30 dias serão recuperadas e, se a consulta de intervalo estiver nos últimos 30 dias, as vistas da hora de início definida até a hora atual serão recuperadas.

9. Ao concluir a pesquisa, valide os resultados e os detalhes nas listas relacionadas.
10. Clique em **Detalhes da pesquisa** de detecções para exibir os detalhes da pesquisa de detecções.
11. Clique na guia **Detecção** para obter detalhes e na guia **Resultados** da pesquisa de detecções para obter os resultados da pesquisa.

    Você pode exibir informações adicionais relacionadas à detecção específica no campo **Resumo**.

Executar um aprimoramento automático de observável em Microsoft Defender for Endpoint

Execute um aprimoramento automático de observável em Microsoft Defender for Endpoint para aprimorar observáveis com informações adicionais de várias fontes.

Antes de Iniciar

Verifique se você habilitou a propriedade do sistema do **Security Incident Response**. Esta opção aciona a capacidade de enriquecimento do observável no SIR, sempre que um observável está associado a um incidente de segurança.

Função necessária: sn_si.admin, sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar essa capacidade durante as investigações de resposta do incidente para conter uma ameaça identificada. Quando novos observáveis são associados ao incidente de segurança, você pode habilitar o enriquecimento de observáveis na capacidade do Microsoft Defender para Endpoint para ser executado automaticamente.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.
3. Valide a atividade de automação depois que os novos observáveis tiverem sido associados ao incidente de segurança.
4. Exiba os resultados do aprimoramento na lista relacionada de Indicadores do incidente de segurança.
   Você pode usar a tabela a seguir para obter mais informações sobre o enriquecimento observável.

Indicador do Microsoft Defender

Campo	Descrição
ID do indicador	Identidade da entidade do indicador. Clique em **Abrir** para exibir o registro em detalhes na instância Now Platform
Observável	O observável associado ao resultado.
Título	Título do indicador.
Tipo de Indicador	Tipo do indicador.
Ação	Ação realizada pelo indicador.
Ação recomendada	Ações recomendadas para o indicador.
Fornecedor de integração	Integração de origem do Defender da qual os dados são recuperados.
Data de Vencimento	Tempo de expiração do indicador.
Data de recuperação	Data em que o registro de aprimoramento foi criado.

Tradução automática

Executar um aprimoramento de observável manual em Microsoft Defender for Endpoint

Selecione observáveis individuais ou múltiplos e execute um aprimoramento de observável manual para aprimorar observáveis com informações adicionais de Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

A integração Microsoft Defender for Endpoint permite o aprimoramento de observável para todos os tipos de observável que são mapeados no módulo Mapeamento de observável-indicador.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender para endpoint.
3. Clique **em Mostrar todas as listas relacionadas**.
4. Clique na guia **Observáveis associados**.
5. Selecione os observáveis.
6. Na lista Ações, clique em **Executar aprimoramento de observável**.
7. Selecione um Microsoft Defender para **origem** do endpoint e mova-o para a coluna **Selecionado** para especificar qual implementação você deseja usar para aprimorar os observáveis selecionados.
8. Clique em **Enviar**.
9. Para validar o status da execução, exiba as anotações de trabalho.
10. Para exibir os resultados, clique na guia **Indicador do Microsoft Defender**.
    Você pode usar a tabela a seguir para obter mais informações sobre o enriquecimento observável.

Indicador do Microsoft Defender

Campo	Descrição
ID do indicador	Identidade da entidade do indicador. Clique em **Abrir** para exibir o registro em detalhes na instância Now Platform
Observável	O observável associado ao resultado.
Título	Título do indicador.
Tipo de Indicador	Tipo do indicador.
Ação	Ação realizada pelo indicador.
Ação recomendada	Ações recomendadas para o indicador.
Fornecedor de integração	Integração de origem do Defender da qual os dados são recuperados.
Data de Vencimento	Tempo de expiração do indicador.
Data de recuperação	Data em que o registro de aprimoramento foi criado.

Tradução automática

Como criar Indicadores em Microsoft Defender for Endpoint

Crie indicadores de observáveis associados do incidente de segurança usando o Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

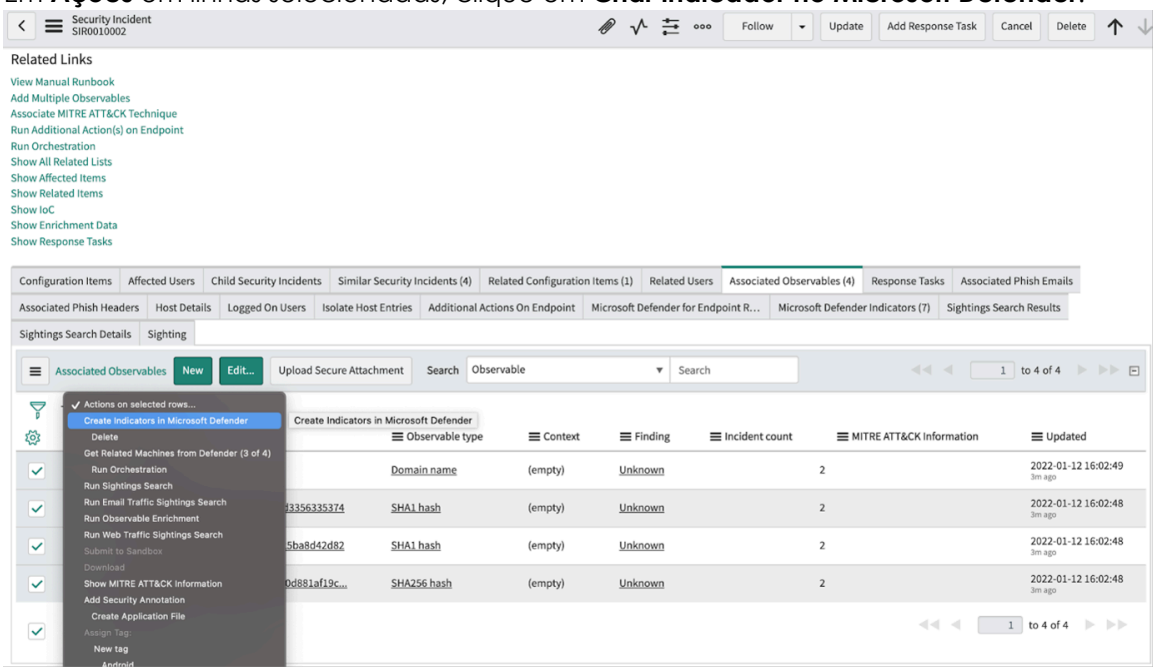
A integração Microsoft Defender for Endpoint permite o aprimoramento de observável para todos os tipos de observável que são mapeados no módulo de mapeamento Observable-Indicator.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar indicadores fornece a capacidade de definir uma lista de indicadores para detecção e para bloqueio de prevenção e respostas. Você pode criar os indicadores do observável associado do incidente de segurança.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja criar indicadores no Microsoft Defender para Endpoint.
3. Clique nas listas relacionadas a Observáveis associados.
4. Adicione observáveis existentes ou crie novos observáveis.
5. Selecione os observáveis.
6. Em **Ações** em linhas selecionadas, clique em **Criar indicador no Microsoft Defender**.



7. No formulário, preencha os campos.

Campo	Descrição
Observáveis selecionados	Observáveis afetados. Esta ação pode ser usada para criar indicadores para vários observáveis. Se você quiser desmarcar um observável, poderá fazer isso desmarcando os observáveis da lista. **Nota:** Se os tipos de observável compatíveis não forem mapeados, os indicadores não serão criados no Microsoft Defender para esses observáveis.
Título	Título do indicador.
Descrição	Descrição do indicador.
Tempo de expiração	Tempo de expiração do indicador.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ações recomendadas	Ações recomendadas que devem ser realizadas para o indicador.
Origem	Configuração de integração para criar o indicador.
Ação	Ações que serão executadas se o indicador for descoberto na organização. Os valores possíveis são os seguintes: ◦ **Aviso** ◦ **Bloquear** ◦ **Auditoria** ◦ **'BloquearERemediar** ◦ **Permitido**
Aplicação	A aplicação Microsoft Defender for Endpoint associada ao indicador. Este campo é aplicável somente para um novo indicador e não pode ser usado para um indicador existente.
Gravidade	Gravidade do indicador. Os valores possíveis são os seguintes: ◦ **Baixo(a)** ◦ **Média** ◦ **Alto**
Nomes dos grupos do RBAC	Nomes dos grupos RBAC aos quais o indicador será aplicado. Os nomes estão em uma lista separada por vírgulas.

8. Clique **em Criar indicador**
9. Valide a atividade e as mensagens de IU.
10. Clique na guia **Indicador do Microsoft Defender** para exibir os resultados.

Atualizar indicadores no Microsoft Defender for Endpoint

Atualize os indicadores existentes em Microsoft Defender for Endpoint no menu de contexto da lista ou na exibição de formulário do indicador do Microsoft Defender, respectivamente.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Clique em **Mostrar todas as listas relacionadas** e, em seguida, clique na guia **Indicadores do Microsoft Defender**.

Tradução automática

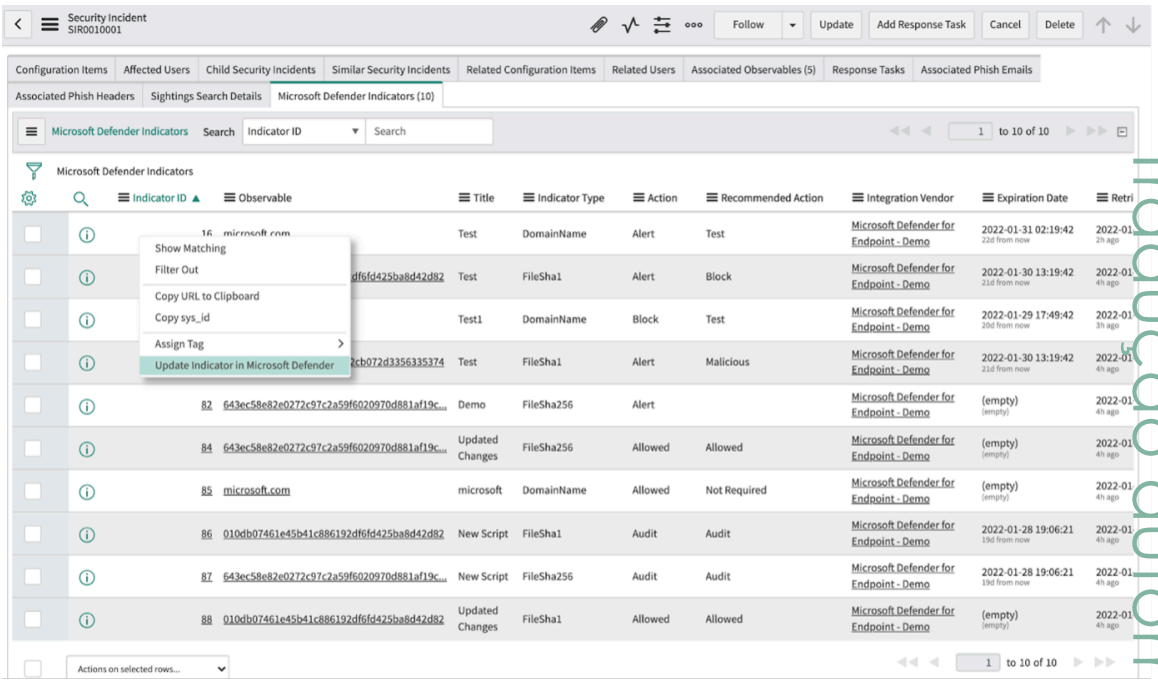
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Você deve configurar a lista relacionada aos Indicadores do Microsoft Defender, que aparecem nas listas relacionadas a Incidentes de segurança. Para obter mais informações, consulte Ações de IU de formulário.

3. Atualize os indicadores do Microsoft Defender for Endpoint de uma das seguintes maneiras:
   - Para atualizar os indicadores no menu de contexto da lista, selecione a linha do indicador que você deseja atualizar e clique em **Atualizar indicador na opção Microsoft Defender**.

Atualizar indicadores usando o menu de contexto da lista

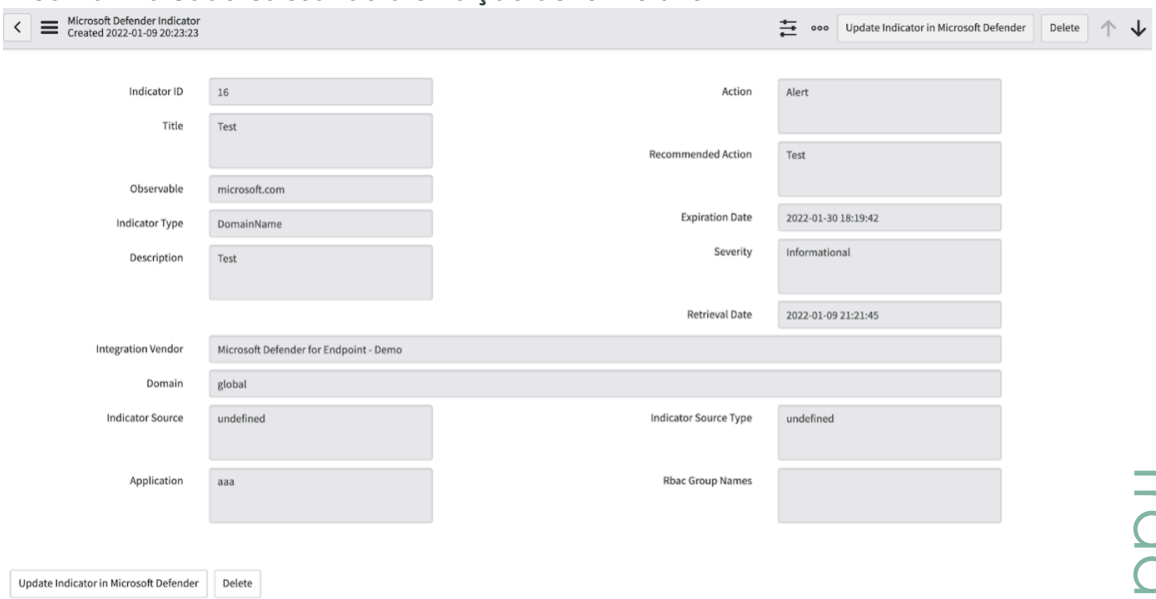


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para atualizar os indicadores na exibição de formulário, clique em **Atualizar indicador no Microsoft Defender** na exibição de formulário.

Atualizar indicadores usando a exibição de formulário



4. No formulário, preencha os campos.

Formulário do indicador do Microsoft Defender

Campo	Descrição
Título	Título do indicador.
Descrição	Descrição do indicador.
Tempo de expiração	Tempo de expiração do indicador.
Ações recomendadas	Ações recomendadas a serem executadas para o indicador.
Origem	Configuração de integração para criar o indicador.
Ação	Ações que são executadas se o indicador for descoberto na organização. Os valores possíveis são os seguintes: ◦ **Aviso** ◦ **Bloquear** ◦ **Auditoria** ◦ **Bloquear e corrigir** ◦ **Permitido**
Aplicação	A aplicação Microsoft Defender for Endpoint associada ao indicador. Este campo é aplicável somente para um novo indicador e não pode ser usado para um indicador existente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Gravidade	Gravidade do indicador. Os valores possíveis são os seguintes: ◦ **Baixo(a)** ◦ **Média** ◦ **Alto**
Nomes dos grupos do RBAC	Nomes dos grupos RBAC aos quais o indicador é aplicado. Os nomes estão em uma lista separada por vírgulas.

5. Clique **em Atualizar indicador**.
6. Valide a atividade e as mensagens de IU.

Separação de domínios na integração Microsoft Defender for Endpoint

O Domain Separation é compatível com a integração Microsoft Defender for Endpoint. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico

Use as seguintes etapas para Domain Separation:

1. Crie um usuário com a função sn_si.admin no respectivo domínio.
2. Execute os procedimentos de integração Microsoft Defender for Endpoint no domínio apropriado.

Configuração de limite de taxa na integração Microsoft Defender for Endpoint

Configure o limite de taxa da API e o tempo limite para o limite de taxa para integração Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst (somente leitura)

Procedimento

1. No filtro de navegação, insira `sys.properties.list`.
   A lista inteira de propriedades na tabela Propriedades do sistema [sys_properties] é exibida.
2. Pesquise e modifique as seguintes propriedades de acordo com seus requisitos.

Nome da Propriedade	Descrição
sn_sec_defender_ep.rate_limit_timeout_in_minutes	Se uma solicitação não for executada dentro do intervalo de tempo especificado, a execução será interrompida e uma mensagem de erro apropriada será exibida. Valor padrão: 75.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
sn_sec_defender_ep.request_per_hour_limit	Se a chamada de API configurada for feita no mesmo endpoint dentro de uma hora, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 1500.
sn_sec_defender_ep.request_per_minute_limit	Se a chamada de API configurada for feita no mesmo endpoint em um minuto, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	Se a chamada de API configurada for feita no endpoint em um minuto, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 30.

Integração de Microsoft Exchange Online

Para a aplicação de integração [Microsoft Exchange Online da ServiceNow, o produto Now Platform® Security Incident Response (SIR) é integrado ao serviço Microsoft Exchange Online, um dos serviços baseados em nuvem no pacote de produtos Microsoft Office 365. O analista do Security Operation Center (SOC) pode pesquisar ameaças relacionadas à segurança no ambiente de e-mail corporativo e remover e corrigir e-mails de phishing com recursos de pesquisa e exclusão de e-mail.

Visão geral

Como analista de incidentes de segurança, você executa a integração na interface do analista de segurança e o fluxo de trabalho retorna detalhes da mensagem de e-mail que correspondem aos critérios de pesquisa. As pesquisas de e-mail são baseadas em critérios que incluem linhas de assunto e endereços de e-mail do remetente e do destinatário. Depois que a pesquisa de e-mail for concluída, você poderá excluir e-mails suspeitos do serviço Microsoft Exchange Online e um processo de aprovação opcional pode ser configurado para solicitar aprovação antes de excluir e-mails.

Esta integração de pesquisa e exclusão de e-mail pode ser usada com um runbook ou fluxo de trabalho de incidente de resposta de phishing mais amplo. Depois que um usuário ou funcionário corporativo recebe um e-mail suspeito e o relata à equipe de resposta a phishing ou à caixa de entrada da empresa, o e-mail relatado é encaminhado para Now Platform e categorizado como um incidente de segurança. Depois de verificar que um e-mail é um ataque de phishing, como analista responsável pela investigação de incidentes de phishing, você pode iniciar uma pesquisa de e-mail para determinar se outros usuários corporativos receberam esse e-mail de phishing. A pesquisa permite localizar e-mails relacionados da mesma campanha de phishing e identificar outras possíveis vítimas que podem ter recebido o e-mail, lido e também clicado em uma URL mal-intencionada ou aberto um anexo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

A integração inclui os seguintes recursos principais:

- Configure os critérios de pesquisa para ameaças de phishing no Security Incident Response com base nas combinações dos campos remetente, destinatário e assunto nas mensagens de e-mail.
- Para pesquisas de e-mail grandes e demoradas, o analista de incidentes de segurança é notificado por e-mail quando a pesquisa é concluída com sucesso, junto com o número de mensagens correspondentes.
- O status de mensagens individuais informa se os destinatários leram ou excluíram e-mails suspeitos.
- Se configurados, os processos de aprovação opcionais garantem que e-mails suspeitos não sejam excluídos sem aprovação prévia.
- Uma trilha de auditoria completa para solicitações de exclusão que inclui o número de e-mails excluídos é registrada nas anotações de trabalho dos incidentes de segurança.
- Se a marcação estiver configurada, os marcadores de segurança serão registrados quando os fluxos de trabalho de pesquisa e exclusão de e-mail forem iniciados e concluídos com sucesso em incidentes de segurança.

Versões da Microsoft Exchange Online compatíveis

Esta integração oferece suporte a Microsoft Exchange Online serviços, que fazem parte do pacote Microsoft do Office 365. A integração não é compatível com ambientes hospedados Microsoft do Exchange. Microsoft executa Microsoft Exchange Online serviços na versão do Exchange 2016.

Pré-requisitos

O plug-in com.snc.si_dep é necessário para qualquer versão Now Platform. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações.

As Operações de segurança aplicações a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Estrutura de integração de segurança
2. Security Support Common
3. Orquestração de suporte de segurança
4. Resposta a incidentes de segurança

Arquitetura de integração e conexão de sistemas

Para obter mais informações sobre a arquitetura da integração, incluindo termos-chave e detalhes da conexão de sistemas externos, consulte Arquitetura de integração e conexão de sistemas externos para a integração Microsoft Exchange Online.

Check-list

Os tópicos a seguir estão numerados. Siga os tópicos listados abaixo na ordem em que são apresentados para uma instalação e configuração tranquilas da aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter uma check-list imprimível dessas etapas, consulte Check-list para a integração Microsoft Exchange Online. Você pode usar essa lista para monitorar o andamento enquanto trabalha nas tarefas de ponta a ponta da configuração de integração, configuração e verificação de resultados.

Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online

Conclua as seguintes tarefas de configuração no portal do Azure Microsoft antes de instalar a aplicação ServiceNow para esta integração. Esta conta permite o acesso ao locatário Microsoft Exchange Online para obter detalhes da mensagem de e-mail.

Antes de Iniciar

Função necessária: Microsoft administrador do portal do Azure

Esta conta é necessária para acessar o locatário Microsoft Exchange Online para coletar detalhes adicionais da mensagem de e-mail e para excluir mensagens de e-mail. Esta conta está configurada no Microsoft portal do Azure.

As imagens nas tarefas a seguir são privilegiadas e proprietárias e são usadas com permissão de Microsoft. Este conteúdo está sujeito a atualizações até Microsoft. Para verificar se você tem acesso ao conteúdo mais atual, consulte o site de documentação da Microsoft .

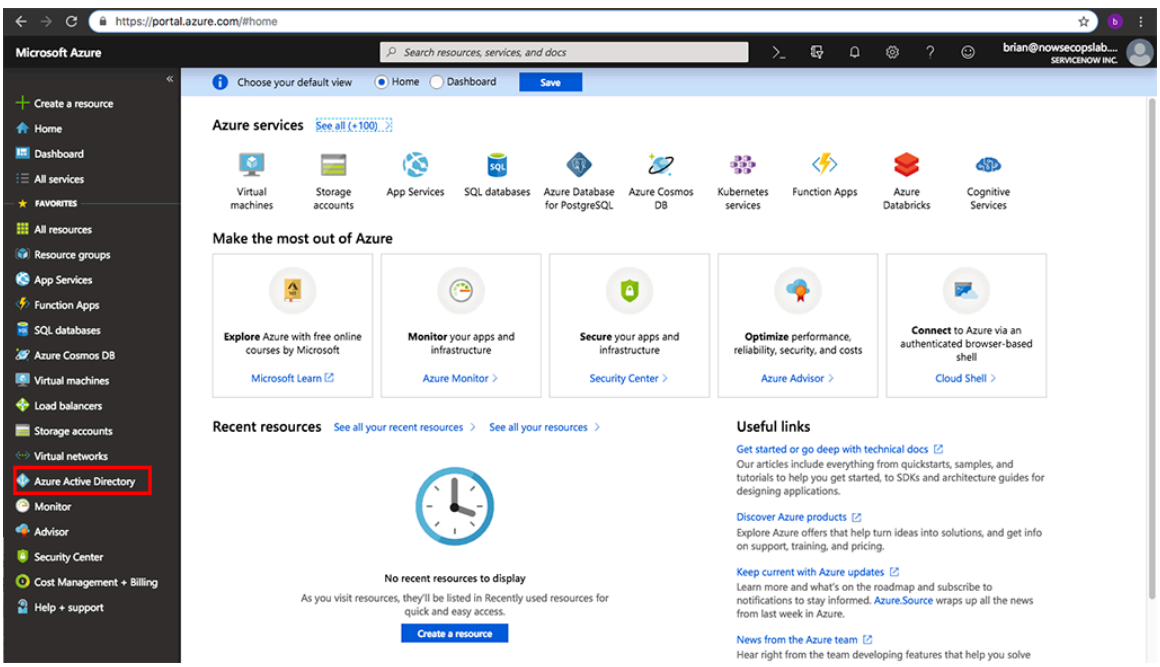
Nas imagens a seguir, `ServiceNow Inc.` é exibido para o nome da conta nos exemplos do portal do Azure. Na sua conta do portal do Azure, o nome da empresa da sua conta no portal do Azure é exibido.

Procedimento

Se você não criou uma ID de aplicação para autenticação OAUTH no Microsoft portal do Azure, siga estas etapas.

a. Faça login no Microsoft portal do Azure usando suas credenciais de administrador do portal do Azure.

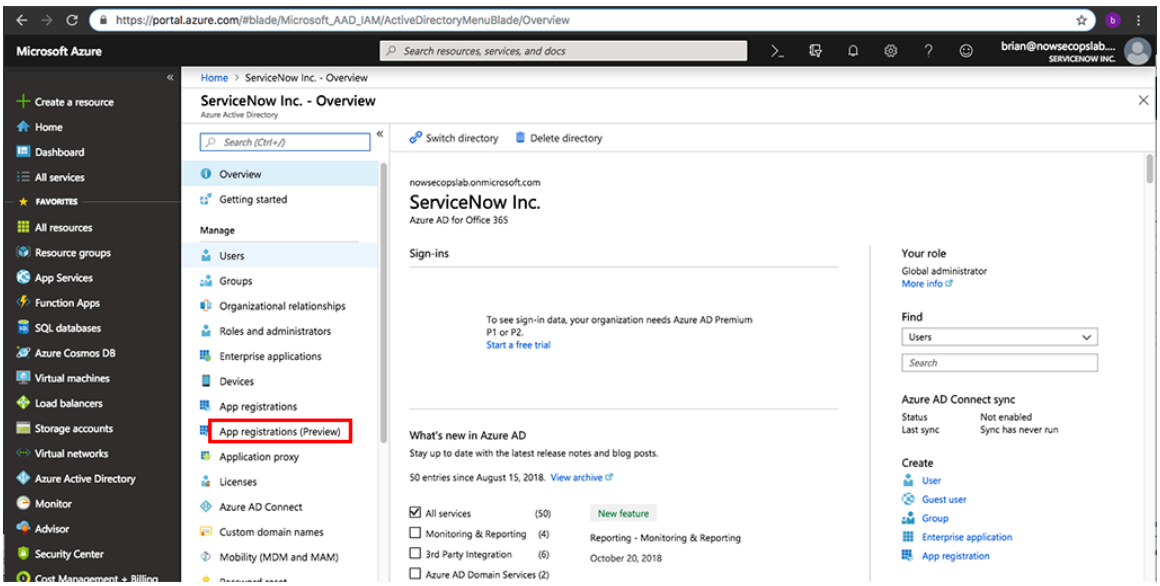
b. No painel de navegação esquerdo do painel inicial, clique em **Azure Active Directory**.



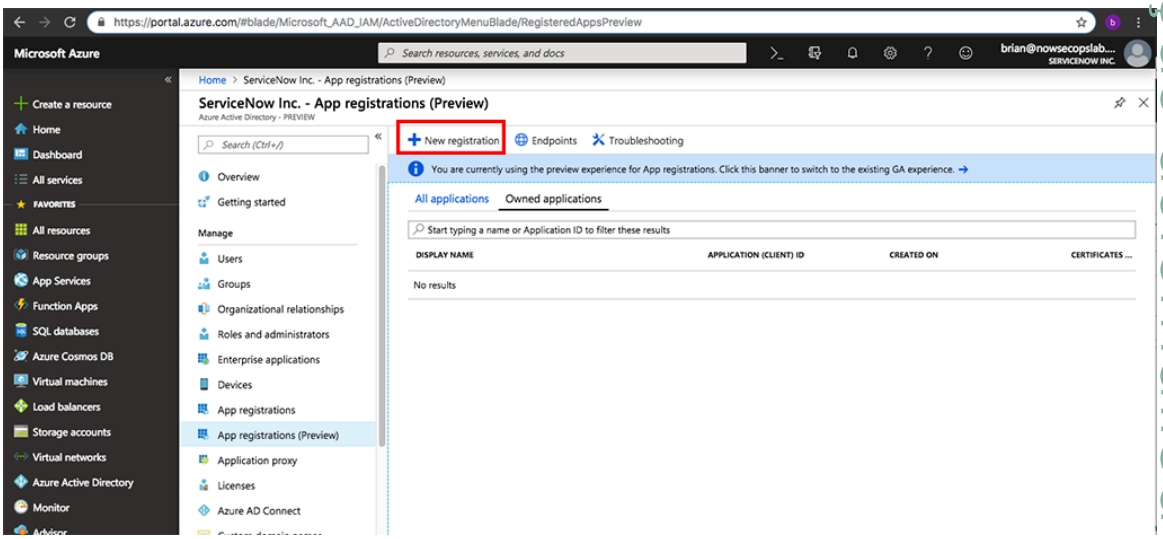
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. No painel Visão geral exibido, clique em **Registros de apps (Visualização)**.



d. No painel Registros de aplicações (Visualização) que será exibido, clique em **Novo registro**.



e. Preencha o formulário Registrar uma aplicação que é exibido.

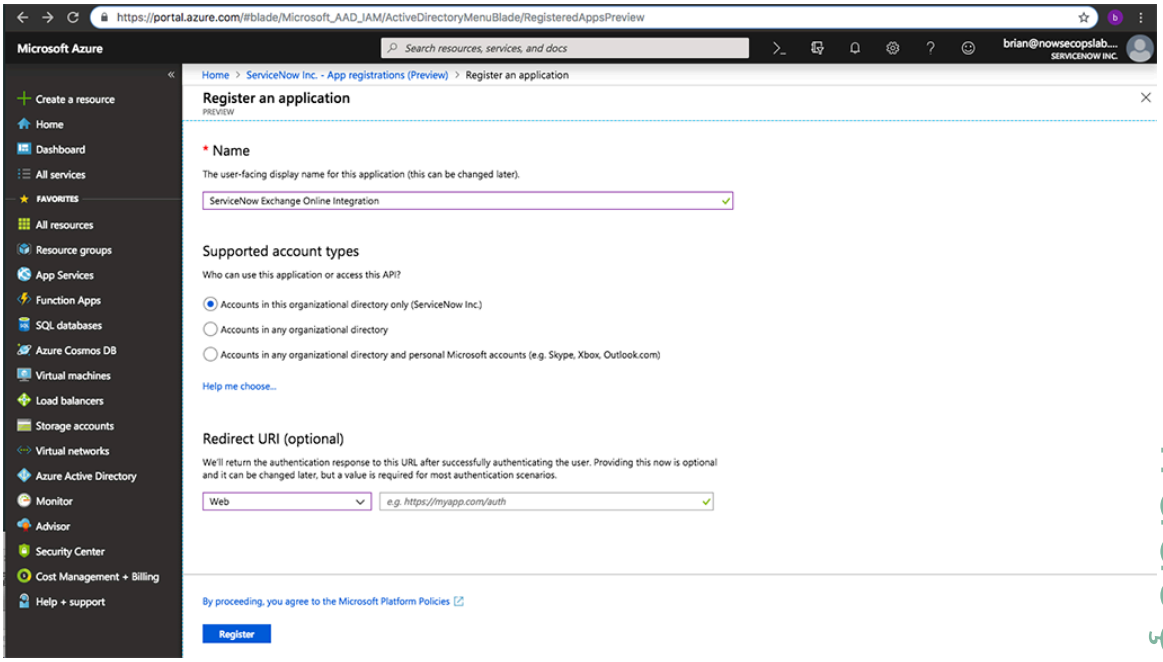
Um exemplo de um formulário preenchido é mostrado após a tabela.

Campo	Descrição
Nome	Nome da aplicação. Neste exemplo, `a Integração do Exchange Online da ServiceNow` foi inserida.
Tipos de conta compatíveis	Para esta conta, em Tipos de conta compatíveis, clique **em Contas neste diretório organizacional somente ServiceNow Inc.)**. Este domínio é usado para as pesquisas de e-mail.

Tradução automática

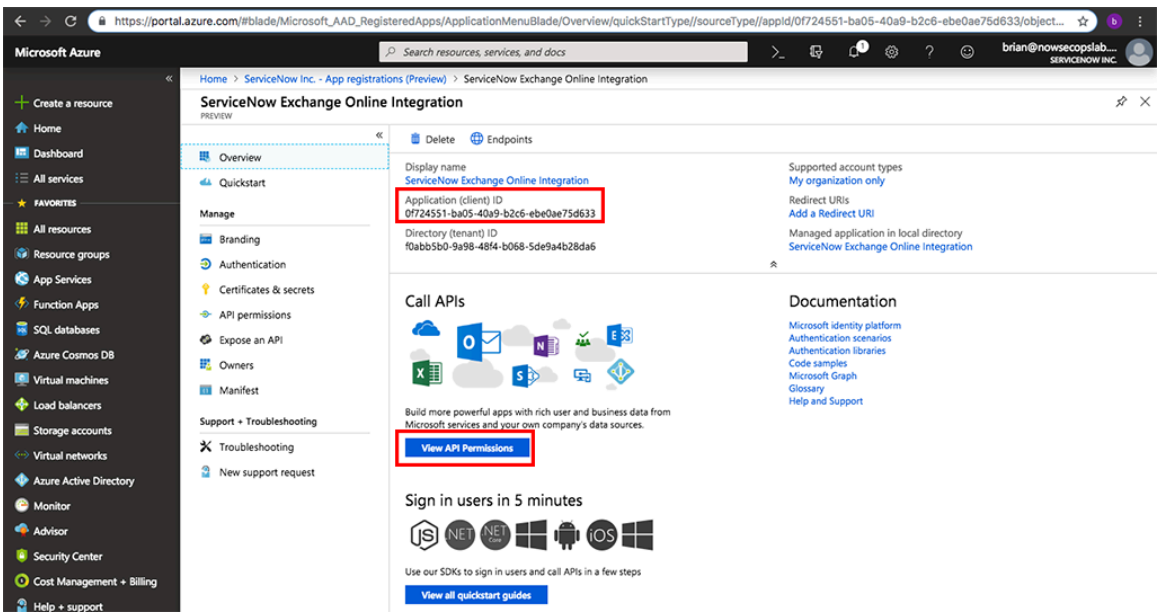
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Redirecionar URL (opcional)	Se você inserir um valor para este campo, ele não será usado pela integração.



f. Clique em **Registrar**.
Um ID de aplicação é criado. Este ID é semelhante a um nome de usuário. Você insere este valor na página de configuração no campo **ID da aplicação OAUTH** durante a etapa de configuração em sua instância Now Platform, que é descrita em Configure a integração Microsoft Exchange Online com sua instância Now Platform.

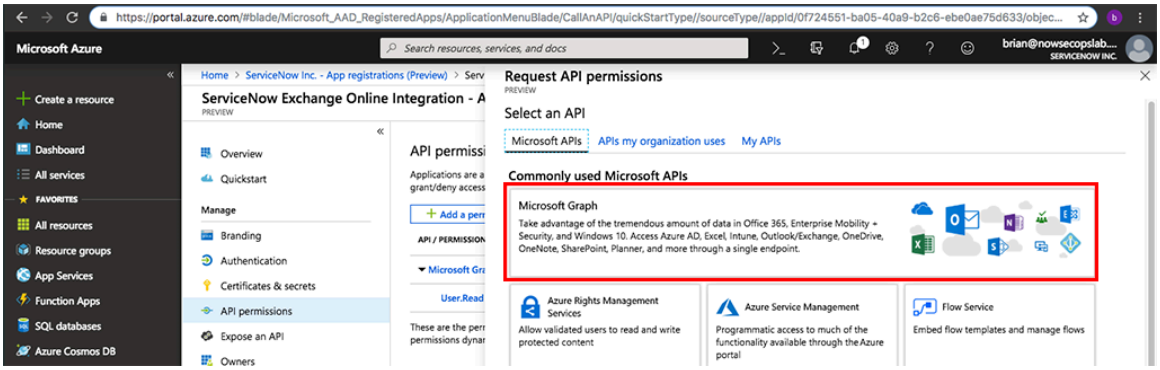
g. Com o ID da aplicação (cliente) exibido no painel Integração do Exchange Online da ServiceNow, clique em **Exibir permissões de API**.



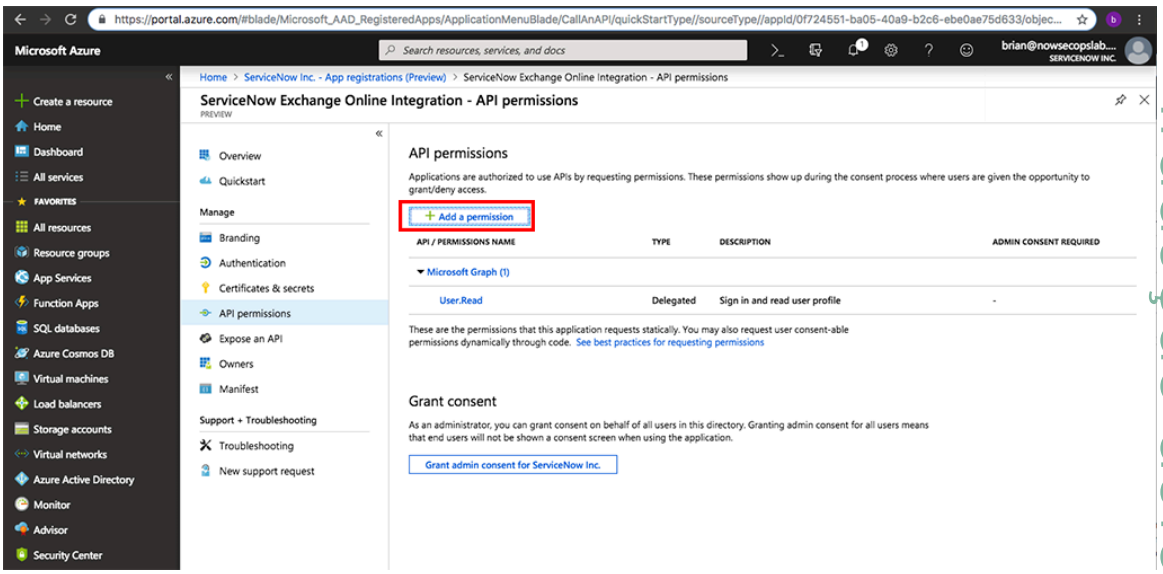
h. No painel de permissões da API de solicitação exibido, clique em **Microsoft Graph**.

Tradução automática

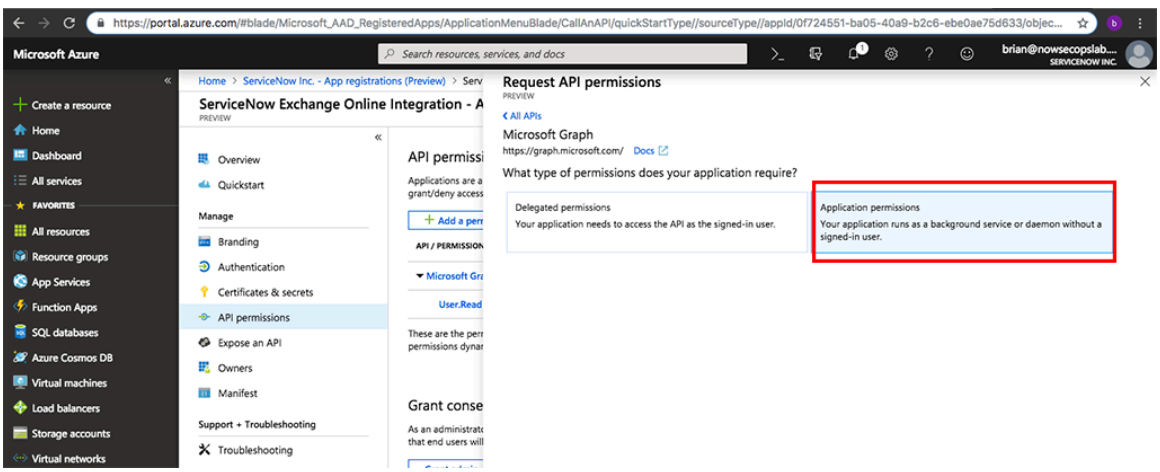
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



i. No painel Integração do Exchange Online da ServiceNow - Permissões de API exibido, clique em **Adicionar uma permissão**.



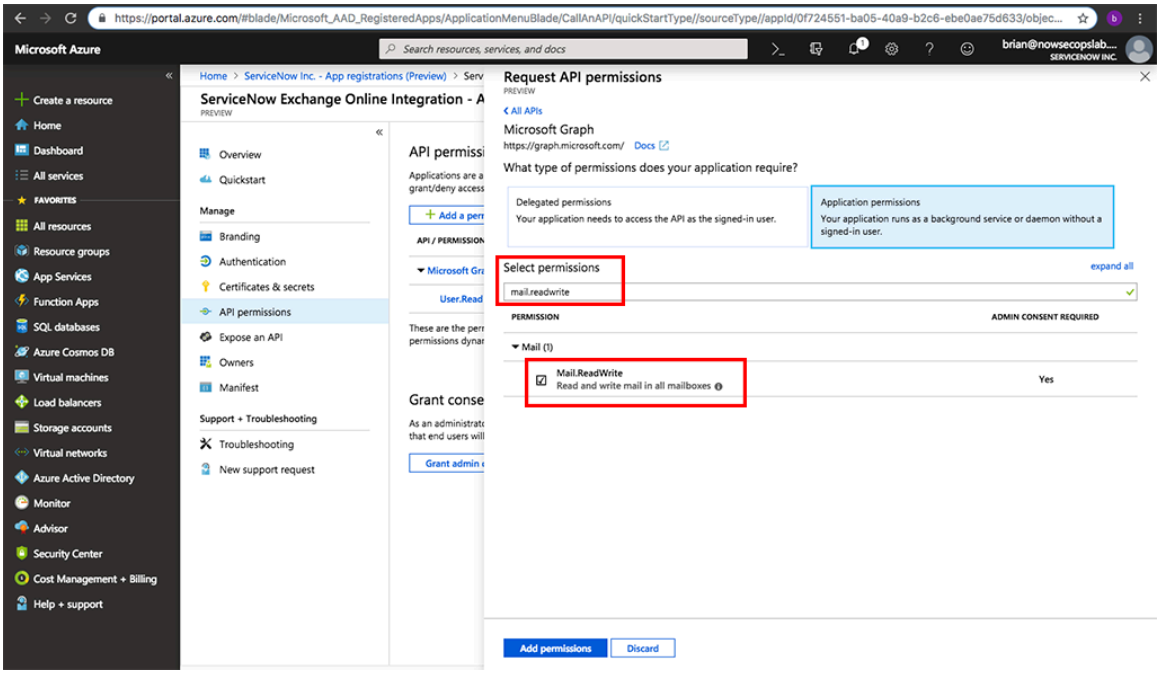
j. No painel de permissões da API de solicitação exibido, clique em **Permissões da aplicação**.



k. No campo Selecionar permissões exibido, insira **Mail.ReadWrite** e marque a caixa de seleção **Mail.ReadWrite**.

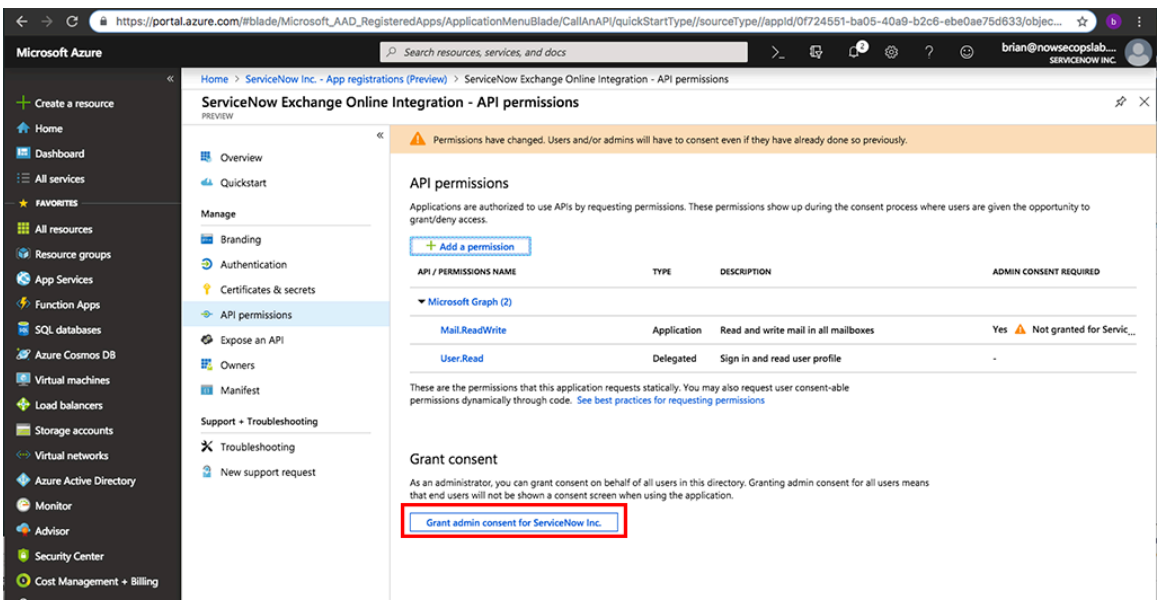
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



l. Clique **em Adicionar permissões**.

m. No painel Integração do Exchange Online da ServiceNow - Permissões de API exibido, clique em **Conceder consentimento de administrador para**<your organization name> .

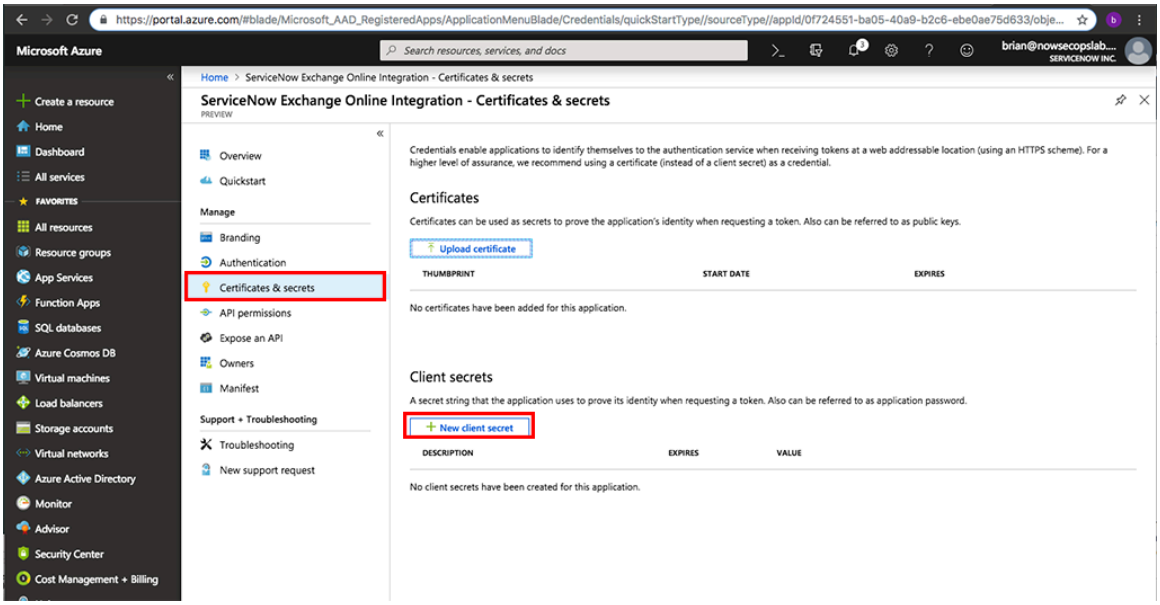


n. Para confirmar a seleção de API anterior (Microsoft Graph API) que você inseriu, clique em **Confirmar**.

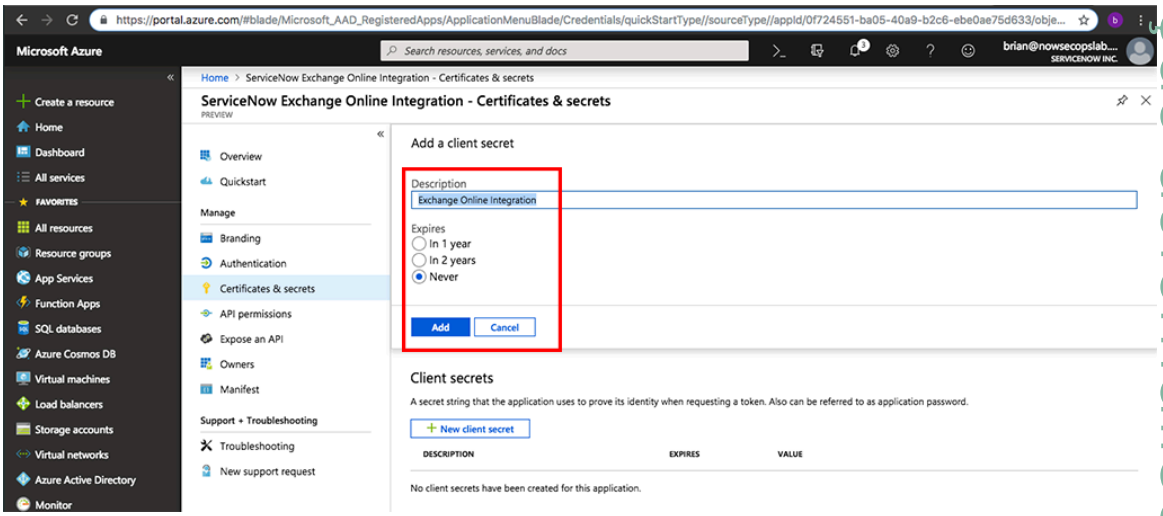
o. No painel Integração do Exchange Online da ServiceNow - Certificados e segredos, clique em **Certificados e segredos** seguidos por **Novo segredo do cliente** (senha).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



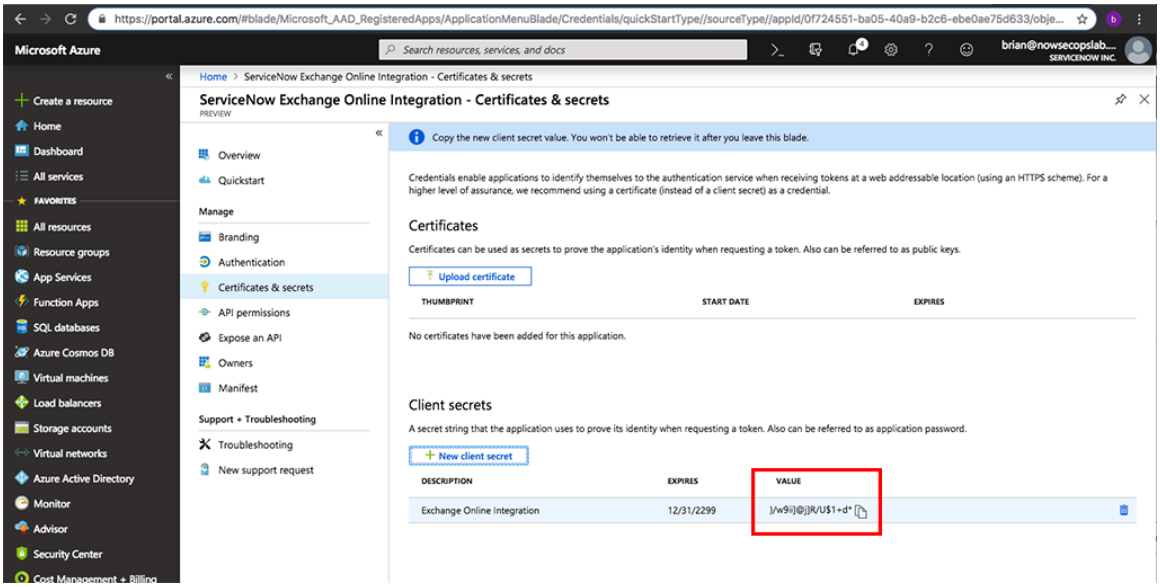
p. No formulário exibido no painel Integração do Exchange Online da ServiceNow - Certificados e segredos, insira o nome da aplicação no campo `Descrição`, clique em uma opção de expiração e clique em **Adicionar**.



No painel Certificados e segredos exibido, na seção **Segredos do cliente**, em `Valor`, a linha é preenchida com o novo segredo do cliente (senha). Salve esta senha em um local seguro. Depois de sair desta página, este valor de senha não estará mais visível. Você insere essa senha no campo **Segredo do cliente OAUTH** na página de configuração durante a etapa de configuração da integração em sua instância Now Platform.
As etapas de configuração da integração são descritas em Configure a integração Microsoft Exchange Online com sua instância Now Platform.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você criou com sucesso uma ID de aplicação para autenticação OAuth no Microsoft portal do Azure.

O que Fazer Depois

Você está pronto para configurar sua instância Now Platform® para a integração.

Configurar autenticação baseada em certificados ou autenticação somente de app

Uma integração inicial é necessária para autenticação usando objetos de aplicação. A aplicação e a entidade de serviço são usadas de forma intercambiável, mas uma aplicação é como um objeto de classe, enquanto uma entidade de serviço é como uma instância da classe.

Para obter mais informações sobre objetos principais de serviço e aplicação no Azure Active Directory, consulte Objetos principais de serviço e aplicativo no Azure Active Directory . Para obter um fluxo visual detalhado sobre como criar aplicações no Azure AD, consulte Criar uma aplicação e entidade de serviço do Azure Active Directory que possa acessar recursos do .

Para configurar a autenticação baseada em certificados ou a autenticação somente de app, execute as seguintes etapas:

1. Registre a aplicação no Azure AD.
2. Atribua permissões de API à aplicação.

   Para que o objeto de aplicação acesse recursos, ele precisa ter a permissão de aplicação `Exchange.ManageAsApp` e `Mail.ReadWrite`.

3. Gere um certificado autoassinado e conceda acesso à chave privada.

   Crie e configure um certificado X.509 autoassinado, que é usado para autenticar sua aplicação em relação ao Azure AD, ao solicitar o token de acesso somente da aplicação. Os certificados de próxima geração (CNG) não são compatíveis com a autenticação somente de aplicativo com o Exchange. Os certificados CNG são criados por padrão nas versões modernas do Windows. Você deve usar um certificado de um provedor de chaves CSP. `(-Provider = 'Provedor de criptografia forte da Microsoft')`.

4. Anexe o certificado à aplicação do Azure AD.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Atribua funções do Azure AD à aplicação.

   A aplicação precisa ter a função `Administrador de conformidade do` Azure AD atribuída.

6. Crie uma nova entidade de serviço.

Etapa 1: registrar a aplicação no Azure AD

1. Abra o portal do Azure AD .
2. Na caixa **Pesquisar** na parte superior da página, digite **Registros de app**.
3. Selecione **Registros de app** nos resultados na seção Serviços.

   Como alternativa, você pode navegar até a página **Registros de aplicações** usando https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade .

4. Na página **Registros de aplicações**, selecione **Novo registro**.
5. Na página**Registrar uma aplicação**, defina as seguintes configurações:

Campo	Descrição
Nome	Insira algo descritivo. Por exemplo, ExO PowerShell CBA.
Tipos de conta compatíveis	Verifique se **Contas somente neste diretório organizacional (** <YourOrganizationName> somente - locatário único) está selecionado. Para tornar a aplicação multilocatária para cenários delegados do Exchange Online, selecione o valor Contas em qualquer diretório organizacional (Qualquer diretório do Azure AD - Multilocatário).

6. Depois de concluir o registro do aplicativo, selecione **Registrar** e feche a página do aplicativo.

Etapa 2: atribuir permissões de API à aplicação

Os procedimentos nesta seção substituem todas as permissões padrão que foram configuradas automaticamente para o novo app. O app não precisa das permissões padrão que foram substituídas.

1. Na página do aplicativo, selecione **Manifesto** em Gestão.
2. Na página Manifesto, localize a entrada `requiredResourceAccess` (na linha 47 ou próximo a ela).
3. Modifique os valores de `resourceAppId`, `resourceAccess id`e `tipo de resourceAccess` conforme mostrado no seguinte snippet de código:

```
"requiredResourceAccess": [
  {
   "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
   "resourceAccess": [
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    {
     "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
     "type": "Role"
    }
   ]
  },
  {
   "resourceAppId": "00000003-0000-0000-c000-000000000000",
   "resourceAccess": [
    {
     "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
     "type": "Role"
    }
   ]
  }
 ],
```

4. Selecione **Salvar**.
5. Na página **Manifesto**, selecione **Permissões de API** em Gestão.
6. Na página **Permissões de API**, preencha os campos.

Campo	Descrição
Nome da API/permissões	Verifique se o valor `Exchange.ManageAsApp` e `Mail.ReadWrite` é mostrado.
Status	O valor incorreto atual é **Não concedido para**<Organization> , e este valor precisa ser alterado. Selecione **Conceder consentimento ao administrador para**<Organization> , leia a caixa de diálogo de confirmação que é aberta e selecione **Sim**. O valor de Status agora deve ser **Concedido para**<Organization> .

7. Feche a página de permissões de API atual (não a guia do navegador) para retornar à página de registros da aplicação.

Etapa 3: gerar um certificado autoassinado e conceder acesso à chave privada

Crie um certificado x.509 autoassinado executando o seguinte:

- Use os cmdlets New-SelfSignedCertificate , Export-Certificate e Export-PfxCertificate em uma sessão elevada (executar como administrador) do Windows PowerShell para solicitar um certificado autoassinado e exportá-lo para `.cer` e `.pfx` (SHA1 por padrão). Por exemplo:

```
# Create certificate
$mycert = New-SelfSignedCertificate -DnsName
 "snowsecops.onmicrosoft.com" -CertStoreLocation
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
 "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(2) -KeySpec
 KeyExchange -Provider "Microsoft Strong Cryptographic Provider"

# Generate password fro private key
$mypwd = ConvertTo-SecureString -String '<password>' -Force
 -AsPlainText

# Export certificate to .pfx file
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $mypwd

# Export certificate to .cer file
$mycert | Export-Certificate -FilePath mycert.cer
```

- Forneça acesso de chave privada ao usuário do serviço MID usando as seguintes etapas:
  1. Abra **o MMC (Microsoft Management Console)**.
  2. No Console de gestão Microsoft (MMC), navegue até **Certificados (computador local)** > **Pessoal** > **Certificados**.

     (Se o MMC não tiver nenhum item de menu, adicione-o navegando até **Arquivo** > **Adicionar/remover snap-in**.
  3. Clique com o botão direito do mouse no certificado que você gerou.
  4. Expandir **Todas as tarefas** > **Gerenciar chaves privadas**
  5. Adicione o **usuário do serviço MID** à lista de acessadores.

Etapa 4: anexar o certificado à aplicação do Azure AD

Depois de registrar o certificado com sua aplicação, você pode usar a impressão digital para autenticação.

1. Na guia **Aplicações de propriedade** na página **Registro** de aplicações no final da Etapa 2, selecione sua aplicação.

   Se você precisar voltar para a página **Registro de aplicações**, use https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/%7E/RegisteredApps , verifique se a guia **Aplicações** próprias está selecionada e selecione sua aplicação.
2. Selecione **Certificados e segredos** em Gerenciar.
3. Na página **Certificados e segredos** que é aberta, selecione **Carregar certificado**.
4. Navegue até o certificado autoassinado (arquivo `.cer`) que você criou na Etapa 3.
5. Depois de concluir, selecione **Adicionar**.

   O certificado agora é mostrado na seção Certificados.
6. Anote `CertificateThumbprint` e feche a página atual de **certificados e segredos**.

Etapa 5: atribuir funções do Azure AD à aplicação

1. Abra o portal do Azure AD .
2. No campo **Pesquisar** na parte superior da página, procure **Funções e Administradores**.
3. Selecione **Funções e administradores do Azure AD** nos resultados na seção Serviços.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como alternativa, você pode navegar até a página de **funções e administradores do Azure AD** usando https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade .

4. Na página **Funções e administradores do Azure AD**, localize e selecione uma das funções compatíveis clicando no nome da função (não na caixa de seleção) nos resultados.

   Encontre e selecione a função de **Administrador de Conformidade**.

5. Na página **Atribuições**, selecione **Adicionar atribuições**.
6. No pop-up **Adicionar atribuições**, localize e selecione o app que você criou na Etapa 1.
7. Depois de concluir, selecione **Adicionar**.
8. Volte para a página **Atribuições** e verifique se a função foi atribuída ao app.

Etapa 6: criar uma nova entidade de serviço

Importante: Certifique-se de estar conectado ao **PowerShell de Segurança e Conformidade** antes de concluir as etapas para criar uma nova entidade de serviço. Criar uma nova entidade de serviço sem se conectar ao PowerShell não funcionará (a ID do app do Azure e a ID do objeto são necessárias para criar a nova entidade de serviço).

1. Execute o seguinte comando para armazenar os detalhes da aplicação do Azure que você registrou na Etapa 1 (<AppName>) em uma variável:

```
Install-Module -Name AzureAD
Import-Module -Name AzureAD
Connect-AzureAD
$AADApp = Get-AzureADServicePrincipal -SearchString"<AppName>"
```

   Para obter informações detalhadas de sintaxe e parâmetro, consulte Get-AzureADServicePrincipal .

2. Na mesma janela do PowerShell, conecte-se ao PowerShell de Segurança e Conformidade :

```
Import-Module ExchangeOnlineManagement
Connect-IPPSSession -CertificateThumbPrint
 "<Your_Certificate_ThumbPrint>" -AppID $AADApp.AppId -Organization
 "<Your_organization>
```

   Execute os seguintes comandos para criar um objeto principal de serviço para a aplicação do Azure:

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.ObjectId
 -DisplayName "<Descriptive Name>"
```

   Para obter informações detalhadas de sintaxe e parâmetro, consulte New-ServicePrincipal .

Configure sua instância Now Platform® para a integração Microsoft Exchange Online

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação Microsoft Exchange Online. Revise a check-list e verifique se você concluiu essas tarefas antes de baixar e instalar a aplicação Microsoft

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exchange Online para a integração para garantir uma instalação e configuração sem problemas.

Antes de Iniciar

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR).	As seguintes funções ServiceNow são necessárias: • O administrador do sistema (admin) instala aplicações e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) configura a aplicação para a integração. Se necessário, a função de administrador de incidentes de segurança também atribui ao analista de incidentes de segurança (sn_si.analyst) as funções de leitura e gravação de e-mail (sn_sec_cmn.cap_email_write e sn_sec_cmn.cap_email_read). As funções (sn_sec_cmn.cap_email_read) e (com.snc.security_incident) são instaladas com o produto Security Incident Response. Eles são atribuídos ao administrador de incidentes de segurança por padrão e podem ser reatribuídos conforme necessário. • O analista de incidentes de segurança (sn_si.analyst) executa pesquisas de e-mail e exclui e-mails. Esta função também verifica se os e-mails foram excluídos e funciona com incidentes de segurança. ◦ A função de gravação permite que o sn_si.analyst edite, crie e execute pesquisas de e-mail e exclua mensagens. Não há função separada necessária para excluir mensagens. ◦ A função de leitura permite que o sn_si.analyst exiba resultados em listas relacionadas a incidentes de segurança. **Nota:** O sn_si.analyst deve ter as funções (sn_sec_cmn.cap_email_read) e (sn_sec_cmn.cap_email_write) para exibir os resultados da pesquisa de e-mail e criar e executar consultas de pesquisa de e-mail.

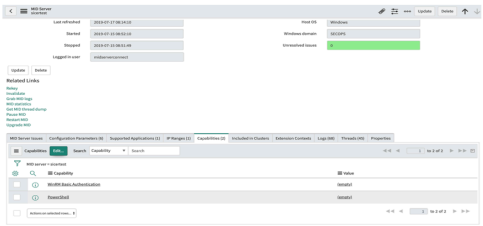
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Se não for atribuído, as etapas a seguir descrevem como atribuir as funções (sn_sec_cmn.cap_email_read) e (sn_sec_cmn.cap_email_write) ao analista de incidentes de segurança. Para obter mais informações sobre como atribuir funções em Security Incident Response, consulte Funções instaladas com SIR.
Verifique se você configurou um Windows MID Server em sua instância Now Platform.	O MID Server é necessário em seu ambiente Now Platform. Embora o produto Microsoft Exchange Online e o Now Platform sejam ofertas de nuvem, um MID Server é necessário para essa integração. O script do PowerShell é executado em um servidor Windows no ambiente do cliente para se conectar ao servidor Microsoft Exchange Online por meio de um MID Server. A partir da versão 10.5 da integração Microsoft Exchange Online para Operações de segurança, você precisa instalar o módulo PowerShell V2 do Exchange Online no MID Server. Para obter mais informações, consulte a documentação da Microsoft sobre o módulo PowerShell V2 do Exchange Online . Uma conexão HTTPS de saída do MID Server é necessária para que a integração recupere informações do locatário do serviço Microsoft Exchange Online. Para obter mais informações sobre o MID Server, consulte MID Server Você testa a conexão entre sua instância e o MID Server do Windows depois de instalar a aplicação durante a etapa de configuração da integração.
Configurar o Windows MID Server para lidar com Microsoft Exchange Online consultas	• Configure a autenticação baseada em certificados do Exchange Online no MID Serversdesignado. • Atribua capacidades do PowerShell e autenticação baseada em certificados do Exchange Online ao(s) MID Server(s) designado(s).

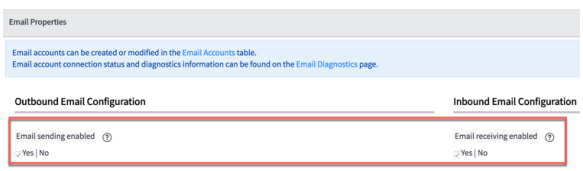
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Em seu ambiente atual do MID Server, se você tiver definido os recursos como **TODOS** para cada MID Server, a **autenticação baseada em certificados do Exchange Online** será adicionada automaticamente para todos os MID Servers. Nesse caso, qualquer um dos MID Servers em seu ambiente pode receber Microsoft Exchange Online solicitações de pesquisa de integração. Para garantir que as solicitações de pesquisa sejam enviadas somente para os MID Servers designados e para evitar o roteamento de pesquisa incorreto, clique em **Editar** e siga estas etapas: • Remova a capacidade **TODAS** de qualquer MID Server que não tenha a funcionalidade **de autenticação baseada em certificados do Exchange Online** necessária. • Selecione as capacidades necessárias conforme mostrado abaixo e clique em **Salvar**.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário e instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .
Se sua organização planeja usar Now Platform notificações por e-mail, verifique se	Siga estas etapas para verificar se a capacidade de envio e recebimento de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
a capacidade de envio/recebimento de e-mail está habilitada.	e-mail está habilitada em sua instância Now Platform®. Esta capacidade notifica os usuários por e-mail quando pesquisas e solicitações de exclusão são iniciadas e concluídas com sucesso. **1.** Navegar até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**. **2.** Em Configuração de e-mail de saída, verifique se `Envio de e-mail habilitado` e Recepção de e-`mail habilitado` estão selecionados. Esta capacidade de envio/recebimento de e-mail é necessária para que o analista de incidentes de segurança receba notificações por e-mail enviadas pelo Now Platform®. Se o recurso de aprovação de exclusão estiver habilitado, as solicitações para excluir e-mails também serão enviadas aos aprovadores por e-mail. Além de habilitar esta propriedade de e-mail, não há nenhuma outra configuração necessária para enviar e receber e-mails no Now Platform®.
	

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Como um administrador de incidentes de segurança Now Platform (sn_si.admin), as funções de leitura e gravação de e-mail (sn_sec_cmn.cap_email_read) e (sn_sec_cmn.cap_email_write) são atribuídas automaticamente a você quando você baixa o produto Security Incident Response (SIR). Como administrador de incidentes de segurança, você atribui essas funções ao analista de incidentes de segurança (sn_si.analyst) ou a outra função. Se você não atribuiu essas funções ao analista de incidentes de segurança ou a outra função, siga estas etapas para atribuí-las.

Procedimento

1. Navegar até **Organização** > **Usuários**.

2. Clique no módulo **Usuários**.

a. Na lista Usuários exibida, clique em **Novo**.

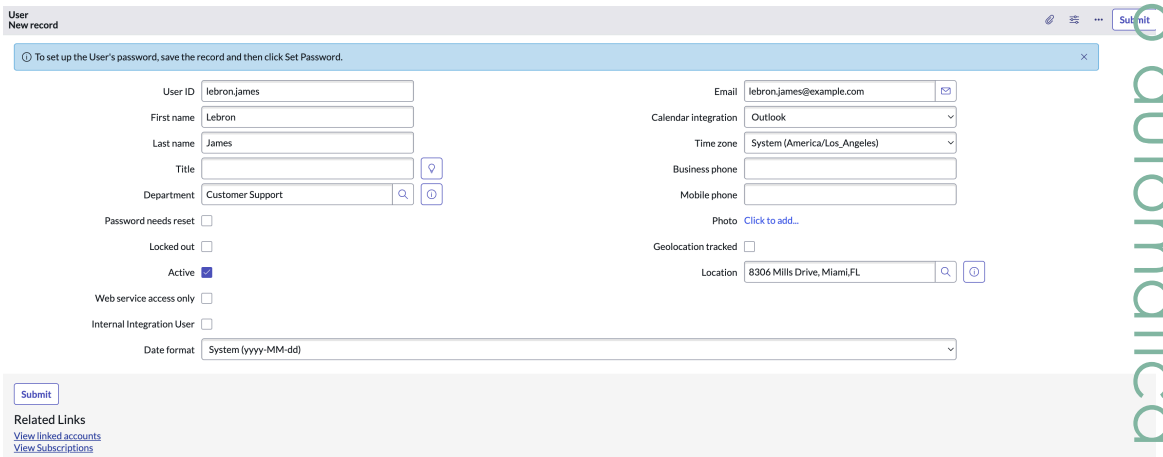
b. No novo formulário de usuário exibido, preencha o formulário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
UserID	ID do usuário para a função Now Platform de analista de incidentes de segurança, por exemplo, `jferguson`.
E-mail	Endereço de e-mail da empresa. As notificações de resultados de pesquisa de e-mail e confirmações de exclusão de e-mail são enviadas para este endereço de e-mail. Para este exemplo, `jferguson@servicenow.com` é usado, mas qualquer endereço de e-mail da empresa pode ser usado para receber essas notificações por e-mail conforme exigido pela sua organização.
Nome	Nome
Sobrenome	Sobrenome
Título	Analista de`incidentes`de segurança , `Analista de segurança`ou Analista `do Centro de operações de segurança (SOC)`, por exemplo.

Novo formulário de usuário

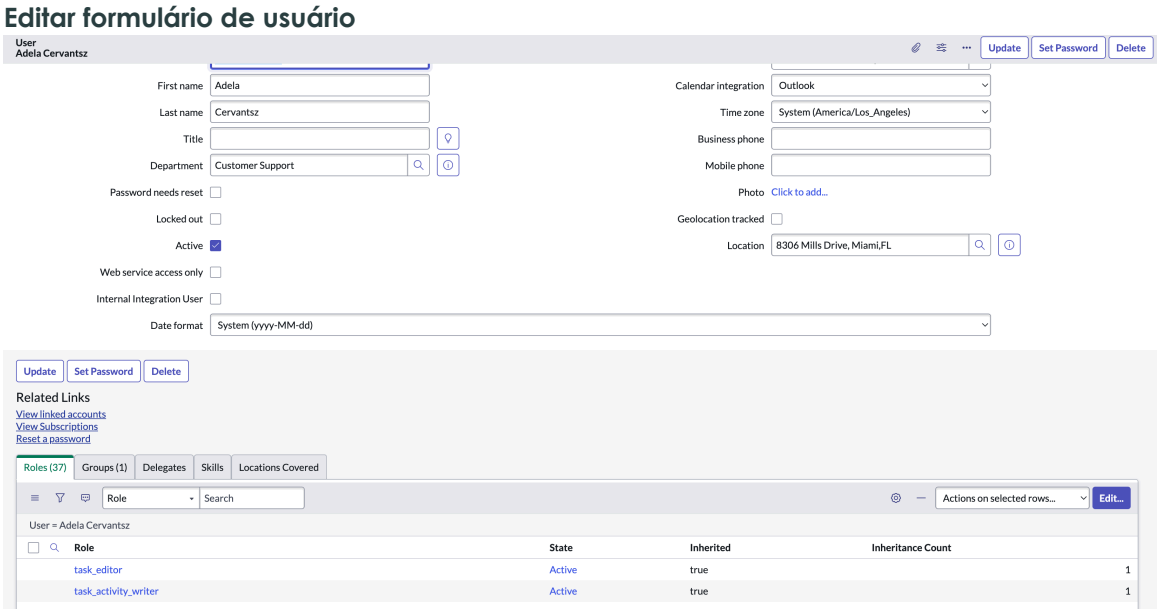


Tradução automática

c. Clique em **Enviar**.
   O novo usuário é exibido na lista Usuários.

3. Na lista Usuários na coluna ID do usuário, clique no nome do usuário ao qual você deseja atribuir as funções `sn_sec_cmn.cap_email_read` e `sn_sec_cmn.cap_email_read`.
4. No registro aberto na seção Links relacionados, clique em **Editar**.

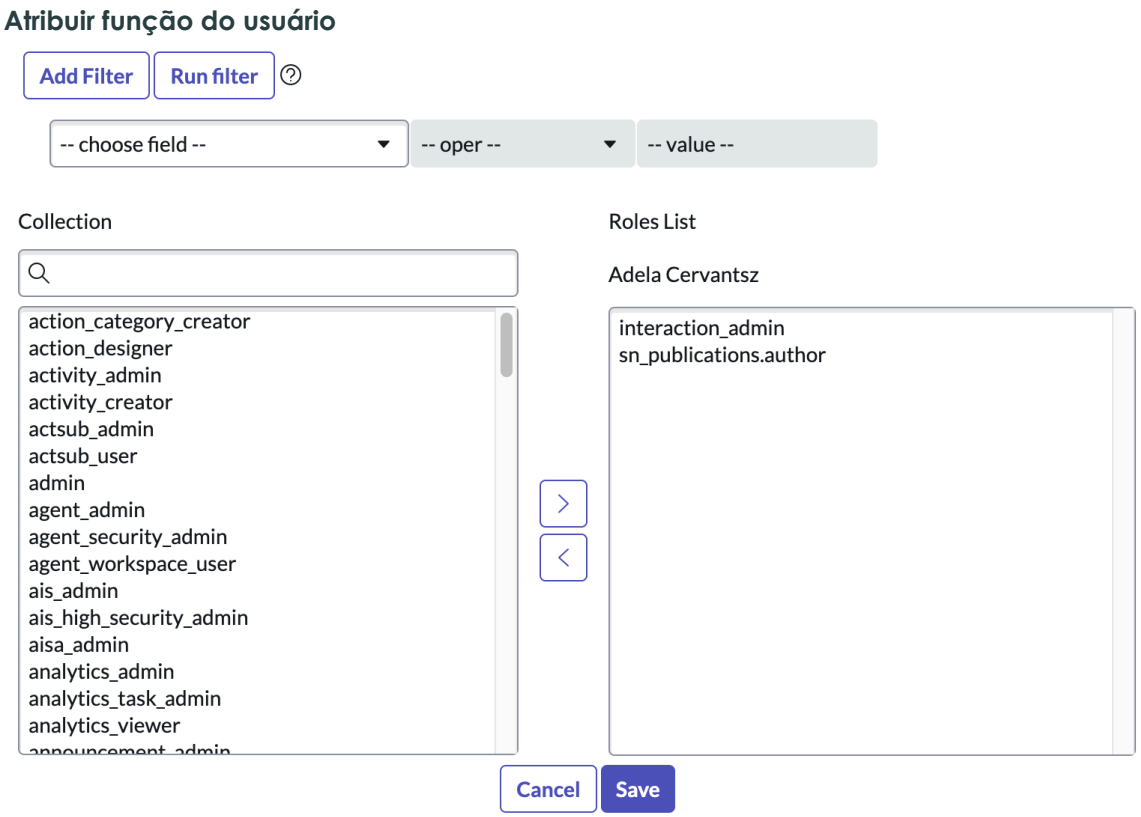
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. No formulário `Editar Membros` exibido, insira `sn_sec_cmn.cap_email_read` no campo de coleta.

   Nota: A coluna abaixo do campo é preenchida automaticamente. Se o usuário não tiver sido atribuído à função sn_si.analyst, insira `sn_si.analyst` no campo Coleção. Na figura a seguir, a função sn_si.analyst já foi atribuída a Joe Ferguson.

6. Na coluna Coleção, selecione e mova `sn_sec_cmn.cap_email_read` e `sn_sec_cmn.cap_email_read` e `sn_si.analyst` (se ainda não estiverem atribuídos) para a Lista de funções.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Salvar**.
   As funções `sn_sec_cmn.cap_email_read` e `sn_sec_cmn.cap_email_read` são atribuídas ao analista de segurança (jferguson).
8. Adicione usuários e atribua funções conforme necessário para sua organização.
9. Opcional: Se você quiser habilitar a capacidade de aprovação para solicitações de exclusão de e-mail, siga estas etapas para criar um grupo de aprovação.

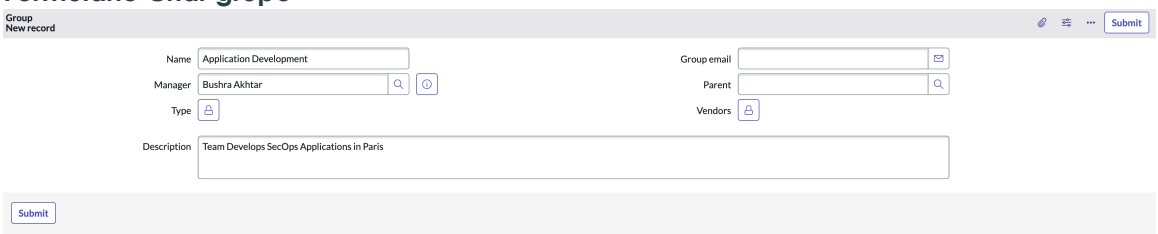
   a. Navegar até **Administração de usuários** > **Grupos**.

   b. Na lista Grupos exibida, clique em **Novo**.

   c. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do grupo que processa uma aprovação quando uma solicitação de exclusão de e-mail é enviada, `por exemplo, Aprovadores do Exchange Online`.
E-mail do grupo	Insira um endereço de e-mail se quiser uma lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo. (Optional) Deixe este campo em branco se quiser que as notificações por e-mail sejam enviadas para os endereços de e-mail individuais de cada usuário do grupo.
Gerente	(Opcional) Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	(Opcional) Se este grupo tiver um primário, o outro grupo do qual este grupo é membro.
Tipo	(Opcional) Defina categorias de grupos.
Fornecedores	(Opcional) Atribua a função vendor_manager a usuários que estão envolvidos com o processo de gestão de fornecedores da sua organização.
Descrição	(Opcional) Informações adicionais sobre o grupo.

Formulário Criar grupo



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como criar grupos e atribuir funções, consulte Criação de um grupo de usuários .

d. Clique em **Enviar**.
Na coluna `Nome`, o novo grupo é exibido na lista Grupos.

Você pode adicionar mais usuários a este grupo. Um usuário herda funções de todos os grupos aos quais o usuário pertence. Você também pode atribuir funções diretamente a um usuário. Para obter mais informações, consulte Gestão de funções . Cada usuário pode aprovar solicitações de exclusão de e-mail enviadas pelo analista de segurança. Somente um usuário é necessário para aprovar ou rejeitar a solicitação.

Se sua organização quiser um nível extra de controle sobre a exclusão de e-mails com esta integração, habilite a capacidade de aprovação opcional. Marque a caixa de seleção **Habilitar** na guia `Configurações adicionais` durante a etapa de configuração para habilitar as aprovações. No exemplo anterior, cada usuário do grupo de `Aprovadores do Exchange Online` está disponível para processar solicitações de exclusão por meio de notificação por e-mail.

Instalar a aplicação Microsoft Exchange Online para a integração ServiceNow Microsoft Exchange Online

Antes de executar a integração em sua instância, instale a aplicação Microsoft Exchange Online para a integração a partir do ServiceNow Store.

Antes de Iniciar

Antes de instalar a aplicação da ServiceNow Store na instância Now Platform, conclua todas as tarefas listadas nas check-lists de pré-requisito.

Função necessária: administrador

Importante:

- A autenticação baseada em certificados do Microsoft Exchange Online é compatível com o Microsoft Exchange Online for Security Operations versão 10.5.4 ou posterior.
- Se você instalar dados de demonstração, uma configuração de demonstração sem credenciais será criada automaticamente. Isso pode causar erros. Para obter detalhes, consulte KB0755880 .

Procedimento

1. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação da ServiceNow Store, configure-a para se conectar à sua instância Now Platform.

Informações relacionadas

Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online

Configurar autenticação baseada em certificados ou autenticação somente de app

Configure sua instância Now Platform para a integração Microsoft Exchange Online

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure a integração Microsoft Exchange Online com sua instância Now Platform

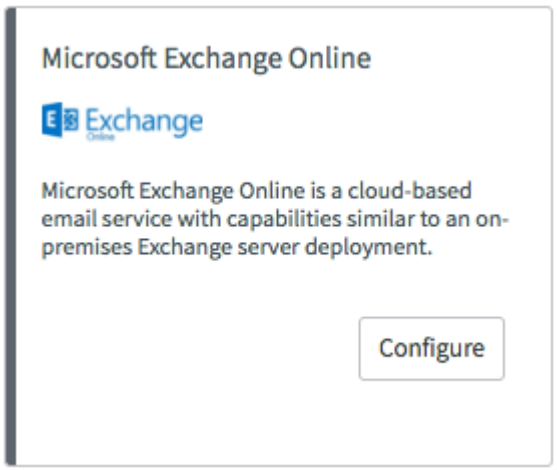
Depois de instalar a aplicação da ServiceNow Store, configure-a para se conectar à sua instância Now Platform. Esta ativação ativa os fluxos de trabalho de pesquisa e exclusão.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

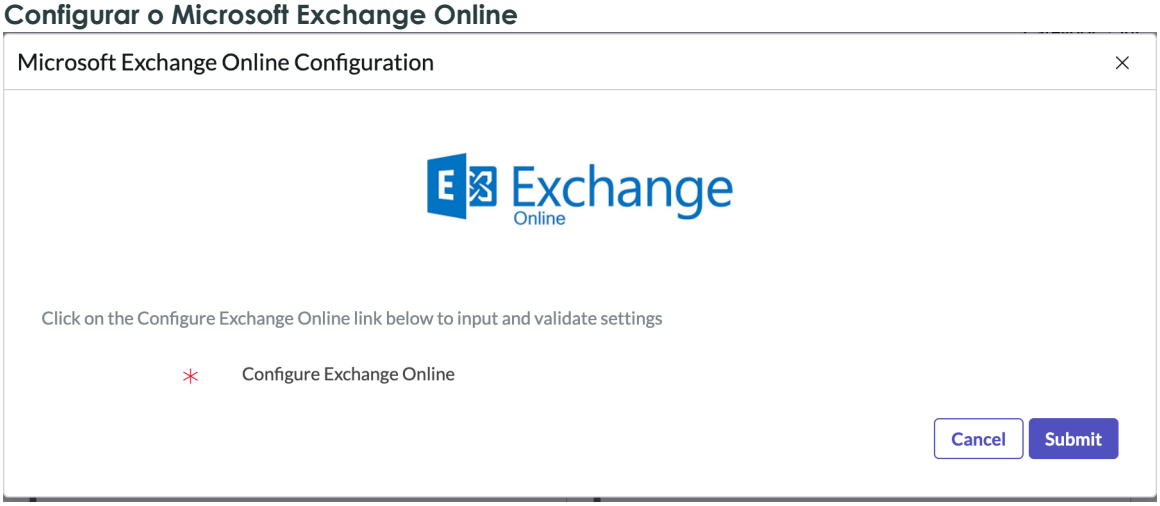
1. Em sua instância Now Platform, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
2. Localize o bloco Microsoft Exchange Online.
3. Clique em **Configurar**.



4. Na caixa de diálogo Microsoft Exchange Online Configuração exibida, clique em **Configurar Exchange Online**.

   Um exemplo de um formulário preenchido e validado segue a tabela.

Configurar o Microsoft Exchange Online



Opção	Descrição
Guia Configurações de conexão	
Locatário	O locatário Microsoft Exchange Online no qual você deseja executar pesquisas. Es-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	te texto é o nome exclusivo que aparece após @ para endereços de e-mail da sua organização. Para este exemplo, `snowse-cops.onmicrosoft.com` é o locatário (domínio).
Impressão Digital do Certificado	Uma impressão digital de certificado é um hash de um certificado, calculado sobre todos os dados do certificado e sua assinatura. Impressões digitais são usadas como identificadores exclusivos para certificados, em aplicações ao tomar decisões de confiança, em arquivos de configuração e exibidas em interfaces.
ID da aplicação OAuth	A ID da aplicação (cliente) que foi gerada para a conta que você criou no Microsoft portal do Azure. Para obter mais informações, consulte Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online.
Segredo do cliente OAuth	Senha (segredo do cliente) da conta que você criou no Microsoft portal do Azure. Para obter mais informações, consulte Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online.
Guia Configurações adicionais	
Janela de pesquisa de e-mail (dias)	O intervalo do histórico de pesquisa de e-mail em número de dias. A integração pesquisa mensagens de e-mail que foram enviadas ou recebidas no servidor Microsoft Exchange Online para o número de dias corridos que você inserir. Você deve inserir um valor entre 1 e 30. 30 dias é o padrão e o número máximo de dias que você pode inserir para uma pesquisa. Inserir um número baixo de dias no intervalo da janela de pesquisa melhora o tempo de resposta, mas talvez você não capture todas as mensagens correspondentes como resultado. Esta configuração global é para todas as pesquisas. Antes de executar a pesquisa de e-mail, não há parâmetros que permitam alterar este valor para pesquisas individuais.
Duração máxima da pesquisa	Use esta opção para definir o limite de tempo limite de pesquisa. Se o limite de tempo limite for atingido, a pesquisa será encerrada e nenhum resultado será exibido. Vo-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	cê pode especificar um valor padrão de 90 minutos e um valor máximo de 240 minutos. Ao definir este limite, você pode evitar loops de pesquisa infinitos que podem causar problemas de desempenho no locatário Microsoft Exchange Online e na instância ServiceNow.
Marcação	Marcador de segurança. O padrão é selecionado. Quando habilitados, os marcadores de segurança são aplicados automaticamente a incidentes de segurança relacionados quando os recursos de pesquisa e exclusão são iniciados e concluídos com sucesso. Os nomes de marcador padrão são exibidos, mas os nomes e cores de marcador podem ser editados. Para obter mais informações, consulte Editar marcadores de segurança na Now Platform para a integração Microsoft Exchange Online.
Recuperar e-mails excluídos	O padrão é selecionado. Este item se aplica somente a e-mails que você excluiu usando esta integração. Se você não quiser que os usuários em sua organização tenham acesso aos e-mails que você excluiu, verifique se esta caixa de seleção está desmarcada. Se a caixa de seleção estiver desmarcada, os e-mails excluídos usando o fluxo de trabalho desta integração serão excluídos permanentemente e colocados na pasta Limpezas. Esta pasta é uma subpasta dentro da pasta Itens recuperáveis em Microsoft Exchange Online que um usuário normalmente não pode acessar. Se você quiser que os usuários recuperem os e-mails excluídos, marque esta caixa de seleção. Se esta caixa de seleção estiver marcada, dependendo de como a conta do usuário estiver configurada em Microsoft Exchange Online, os e-mails excluídos usando o fluxo de trabalho desta integração serão colocados na pasta Itens excluídos na caixa de correio do usuário. Se uma conta estiver configurada para que o usuário possa exi-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

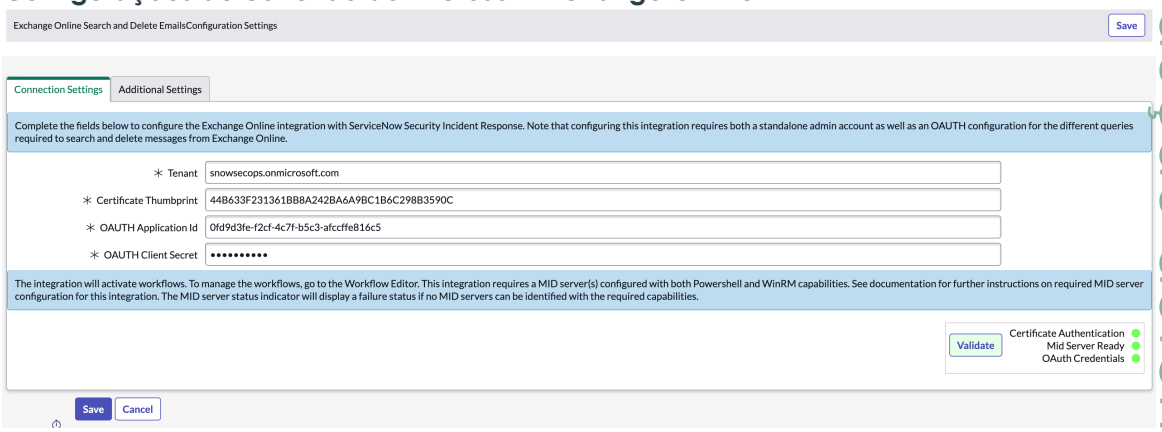
Opção	Descrição
	bir a pasta Itens excluídos em sua caixa de correio, o usuário poderá recuperar os e-mails excluídos de sua conta do Microsoft Exchange Online. Para obter mais informações, consulte Recuperação de itens ou e-mails excluídos no Outlook Web App .
Pesquisar notificações de conclusão	Selecione esta opção para habilitar notificações quando a pesquisa for concluída. Se a caixa de seleção **Habilitar** estiver marcada, você receberá notificações se algum e-mail correspondente for encontrado. Se a caixa de seleção estiver desmarcada, as notificações de conclusão de pesquisa não serão enviadas.
Aprovações	Solicite aprovação para excluir e-mails. O padrão é limpo. Quando a caixa de seleção está desmarcada, o processo de aprovação opcional para solicitar permissão anterior antes de excluir e-mails do serviço Microsoft Exchange Online é desabilitado. Verifique se esta caixa de seleção está desmarcada se você quiser conceder permissão ao analista de incidentes de segurança para excluir e-mails sem solicitar permissão prévia. Se habilitado, uma solicitação será enviada por e-mail para cada membro de um grupo de aprovação. Na lista, selecione um grupo de aprovação. Para obter mais informações sobre como criar um grupo de aprovação, consulte Configure sua instância Now Platform para a integração Microsoft Exchange Online. Depois que uma solicitação é enviada para um grupo de aprovação, somente uma aprovação é necessária do grupo para concluir a solicitação. Qualquer membro do grupo de aprovação tem autoridade de aprovação. Ter um grupo com mais de uma pessoa com permissão de aprovação garante que essas solicitações sejam processadas em tempo hábil.
Notificações de falha	Marque a caixa de seleção para habilitar as notificações de falha quando a ação de pesquisa ou exclusão falhar devido a credenciais OAuth inválidas. Se habilitado, as

Tradução automática

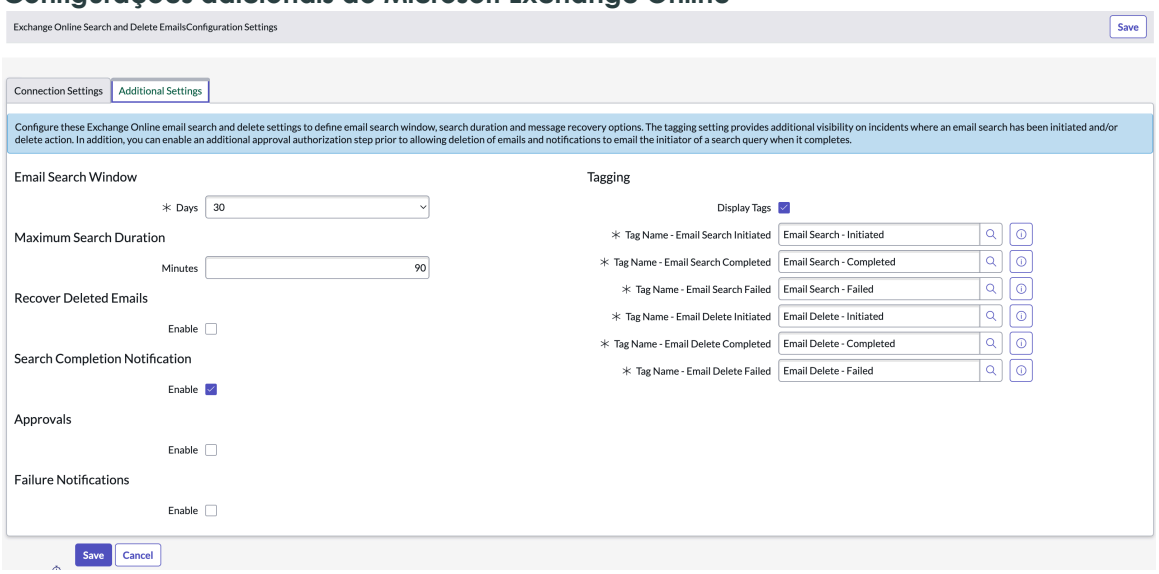
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	notificações de falha serão enviadas por e-mail para cada membro do grupo de notificações de falha quando as credenciais do OAuth forem inválidas. Se a caixa de seleção estiver desmarcada, nenhuma notificação de falha será enviada.
Limite de resultado de e-mail	Na versão 10.3 ou posterior, você pode especificar um limite de exclusão de e-mail para aprovações. Se o número de e-mails excluídos for maior ou igual ao valor especificado aqui, a solicitação de exclusão deverá ser aprovada antes que a ação Excluir seja invocada. Se o valor do limite estiver definido como 1, todas as solicitações de exclusão deverão ser aprovadas.

Configurações de conexão do Microsoft Exchange Online



Configurações adicionais do Microsoft Exchange Online



5. Escolha um para continuar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Salvar	Salve suas edições. Esta ação não verifica sua conexão.
Na guia Configurações de conexão, clique em Validar.	Esta ação valida a autenticação de certificado, a conexão do MID Server e as credenciais do OAuth. Se suas credenciais forem válidas, o botão **Validar** e ambos os indicadores ficarão verdes.

Trouble?
Se uma mensagem de erro for exibida ou um ou mais indicadores à direita do botão Validar estiverem vermelhos, verifique se as credenciais da conta de usuário inseridas são válidas. Insira suas credenciais e clique em **Salvar** novamente.

Validação malsucedida

Consulte a tabela a seguir para obter mais informações sobre o botão **Validar** e os ícones coloridos.

Estado do botão e indicadores de validação	Descrição
O botão Validar é verde e todos os pequenos indicadores coloridos são verdes.	Indica que a conexão do MID Server e as credenciais (autenticação de certificado e OAuth) são válidas.
O botão Validar é vermelho claro com uma borda azul e um ou todos os pequenos indicadores coloridos são laranja.	A validação está em andamento. A validação pode levar mais alguns minutos para ser concluída.
O botão Validar está vermelho claro e um ou todos os pequenos indicadores coloridos estão vermelhos.	• O botão da autenticação baseada em certificados do Exchange Online ou das credenciais do OAuth está vermelho: indica que a autenticação baseada em certificados do Exchange Online ou as credenciais do OAuth são inválidas. • Os botões Autenticação baseada em certificados do Exchange Online e MID Server Pronto estão vermelhos: indica que o MID Server não está acessível e, portanto, houve falha na autenticação baseada em certificados do Exchange Online por meio do MID Server. • O indicador de autenticação baseada em certificados do Exchange Online está vermelho, mas o botão Pronto do MID Server está verde: indica que o MID Server está ativo e configurado corretamente, mas a autenticação baseada em certificados do Exchange Online está incorreta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir critérios de pesquisa de e-mail e solicitar uma pesquisa no serviço Microsoft Exchange Online

Como um usuário com a função sn_si.analyst, defina os critérios de pesquisa e envie uma solicitação de pesquisa por e-mail com base nos detalhes do incidente em um registro de incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

As imagens neste procedimento são mostradas com **Formulários com guias** selecionados em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar formulários com guias, consulte a seção intitulada Exibir formulários com guias em Como configurar o layout do formulário no site de documentação de produtos da ServiceNow .

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O status de mensagens individuais que correspondem à consulta de pesquisa e os resultados da pesquisa são relatados no registro de incidente de segurança. Se as notificações por e-mail estiverem habilitadas, você poderá exibir os resultados da pesquisa de uma mensagem de e-mail.

Os critérios de pesquisa podem incluir endereços de remetentes de mensagens, endereços de destinatários ou nomes de assunto. As seguintes combinações de parâmetros de pesquisa Assunto, Remetente e Destinatário da mensagem geralmente são usadas para encontrar mensagens de e-mail relacionadas a phishing que podem fazer parte de uma única campanha de phishing:

- Encontrar todos os e-mails originais enviados por uma conta de phishing: pesquisar por remetente.
- Encontrar todos os e-mails originais de uma única campanha de phishing: pesquise por assunto e remetente.
- Encontrar todos os e-mails recebidos para uma única campanha de phishing (original e encaminhado, qualquer remetente): pesquise por assunto.
- Encontrar todos os e-mails encaminhados para um único e-mail de phishing de um único usuário: pesquisar por destinatário + assunto.
- Encontrar todos os e-mails relacionados a phishing enviados para um único usuário: pesquisar por remetente + destinatário.

Nota: As pesquisas são realizadas em e-mails enviados ou recebidos nos últimos 30 dias corridos, a menos que uma janela de pesquisa mais curta seja configurada durante a configuração inicial. Uma pesquisa de e-mail bem-sucedida é necessária antes que você possa excluir e-mails.

O exemplo a seguir mostra como iniciar uma pesquisa a partir de um Now Platform incidente de segurança. Um incidente de segurança é criado com base no e-mail original de um ataque de phishing suspeito no servidor Microsoft Exchange Online da sua organização. Para este exemplo, os critérios de pesquisa são Remetente (De) mais Assunto, em que De é `phisher@cbazyx.com`e o Assunto é `login na sua conta`.

Os resultados de pesquisas sobre assuntos são retornados quando a pesquisa encontra cadeias de caracteres de texto que contêm palavras-chave que correspondem aos critérios de pesquisa inseridos. Neste exemplo, o assunto é `faça login na sua conta`. Use o operador **E** para separar as condições de pesquisa De e Assunto para retornar resultados para todas as mensagens de e-mail que contêm esses critérios de pesquisa fornecidos. As

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

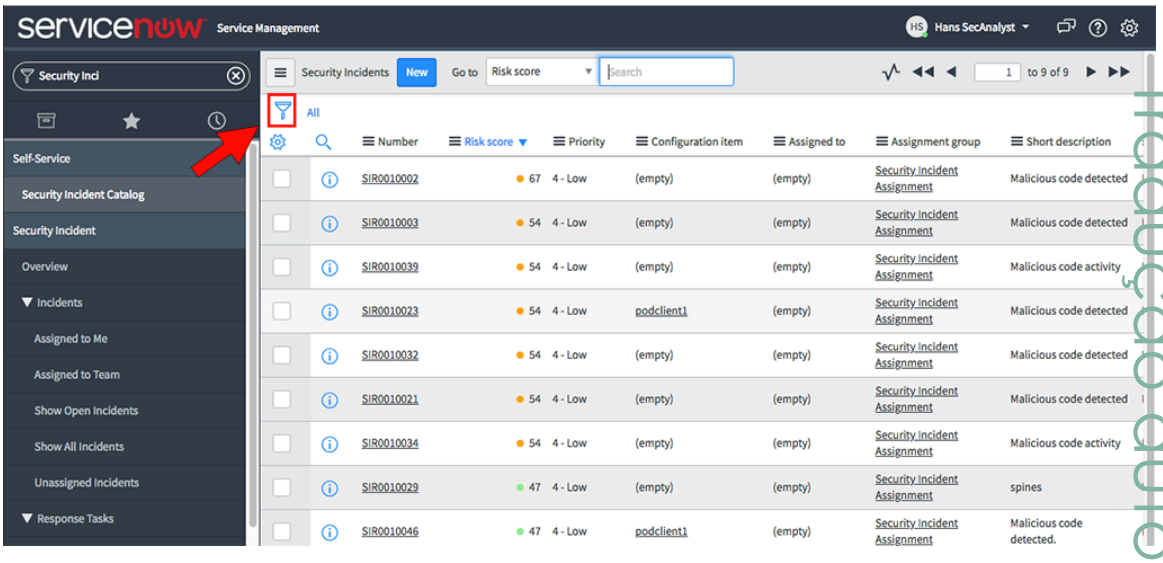
etapas a seguir descrevem como configurar uma pesquisa que encontra somente e-mails que contêm texto de linha de assunto enviado por uma conta de phishing específica.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes** e localize o incidente de segurança com o qual você está trabalhando.
2. Como alternativa, siga estas etapas para definir e executar um filtro para que somente os incidentes de segurança criados por eventos de phishing sejam exibidos.

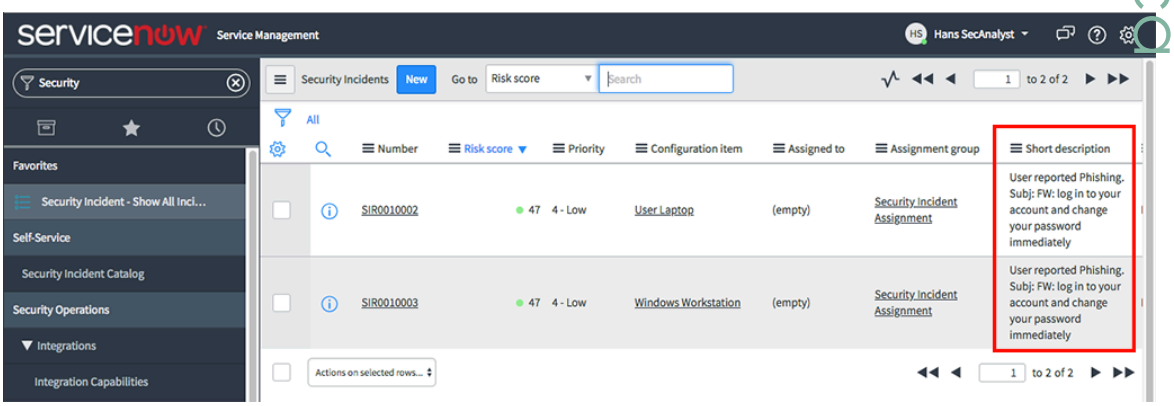
   a. Navegar até **Incidente de segurança** > **Mostrar todos os incidentes** para abrir a lista de Incidentes de segurança.

   b. No canto superior esquerdo da lista exibida, clique no ícone de filtro.



   c. Nos campos exibidos, selecione **Descrição resumida** > **contém** nas listas de seleção, insira **phishing relatado pelo usuário** e clique em **Executar**.

   Os incidentes de segurança relacionados ao phishing são exibidos.



   d. Use o texto na coluna Descrição resumida para ajudá-lo a localizar o incidente de segurança com o qual você está trabalhando.

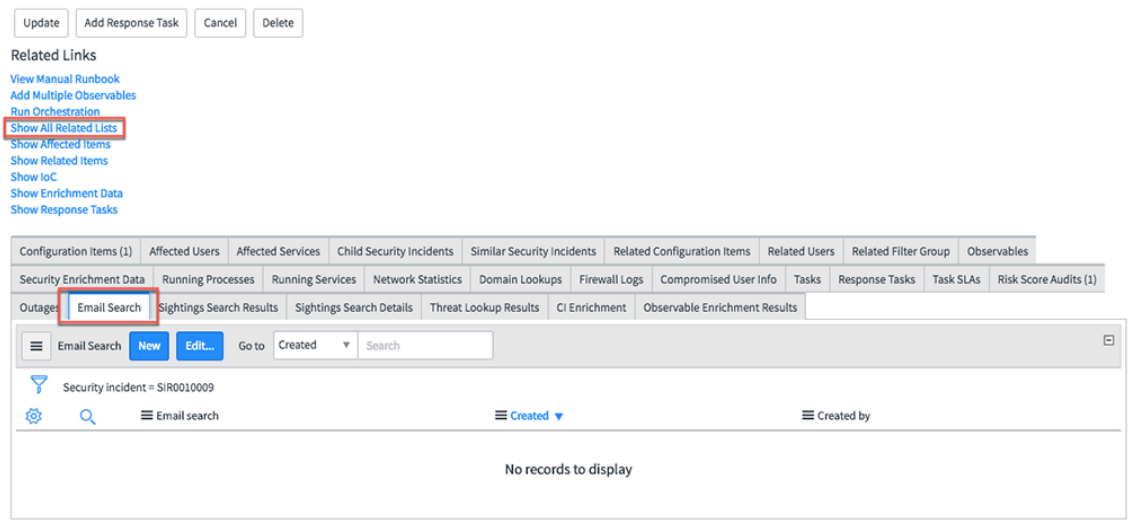
   e. Na coluna Número, clique em um incidente de segurança para abrir um registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Role até a parte inferior do registro de Incidente de segurança e clique na lista relacionada Pesquisa de e-mail.

   Se a lista relacionada Pesquisa de e-mail não for exibida, clique no link relacionado **Mostrar todas as listas** relacionadas para exibir essa lista relacionada.

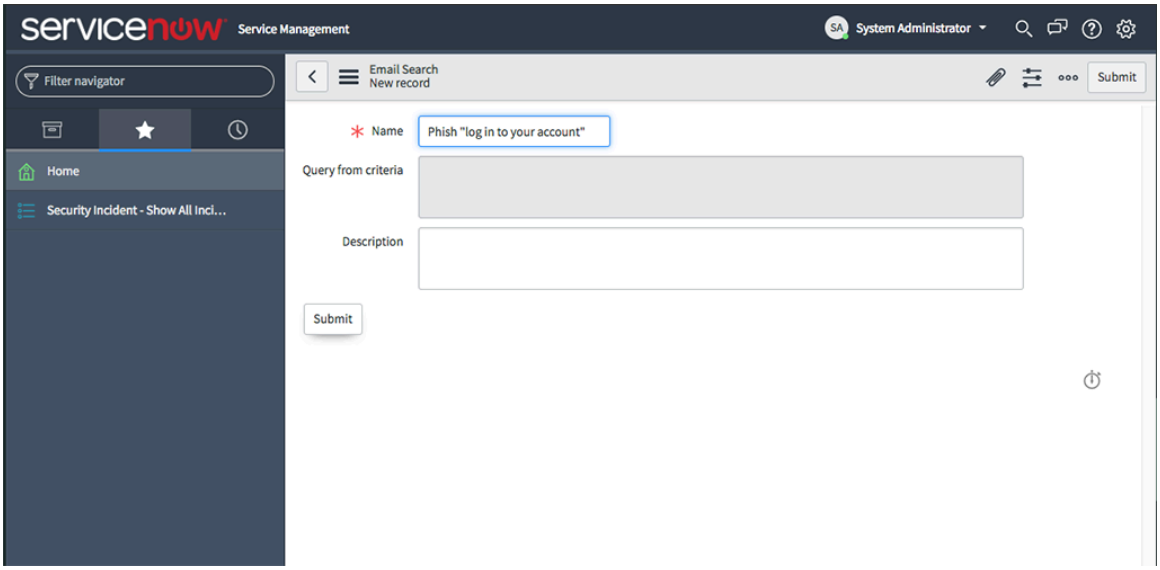


4. Na lista relacionada Pesquisa de e-mail, clique em **Novo** para criar um novo registro de pesquisa de e-mail.
   O formulário Pesquisa de e-mail é exibido. Se você determinar que deseja executar novamente esta consulta de pesquisa para o mesmo incidente relacionado a phishing com pequenas modificações, poderá usar este registro de consulta de pesquisa novamente. No entanto, é improvável que você use essa pesquisa para um incidente diferente relacionado a phishing, porque as campanhas de phishing são dinâmicas e os campos de remetente e mensagem mudam com frequência.
5. Opcional: Para editar um registro de consulta de pesquisa existente, clique em **Editar**.
6. No formulário Pesquisa de e-mail, preencha os campos.

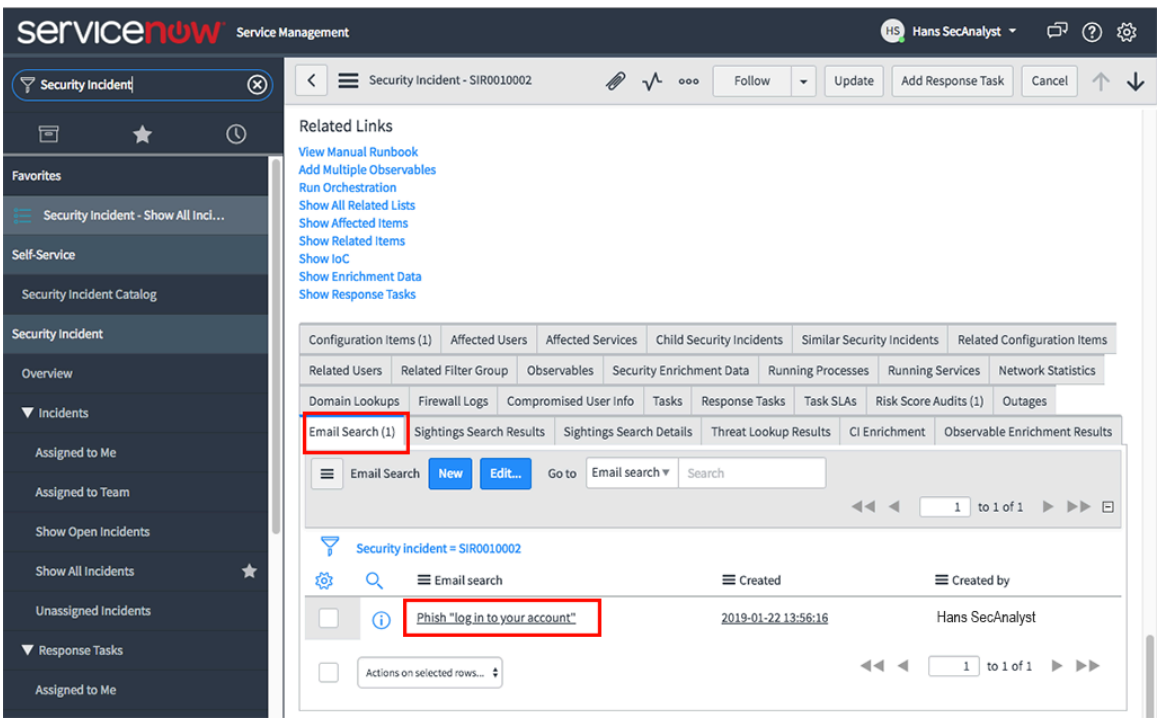
Campo	Descrição
Nome	Informações para descrever o tipo de pesquisa. Para este exemplo, um nome para uma pesquisa De + Assunto é `Phish "faça login na sua conta"`.
Descrição	Informações sobre a pesquisa no servidor de e-mail. Um exemplo dessa pesquisa é `From=phisher@cbazyx.com + Subject=log in to your account`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



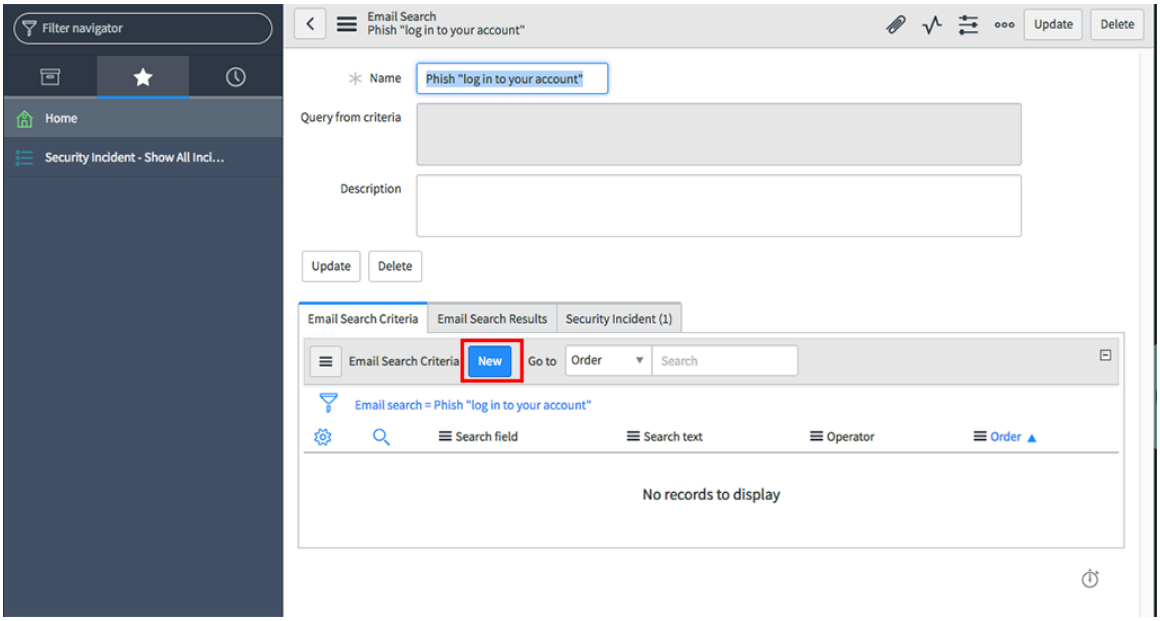
7. Clique em **Enviar**.
   O incidente de segurança é exibido e o nome da pesquisa de e-mail é exibido na coluna Pesquisa de e-mail na lista relacionada Pesquisa de e-mail. Antes que você possa usar esta nova consulta de pesquisa, os critérios de pesquisa devem ser definidos para o registro de pesquisa.
8. Para definir critérios de pesquisa, com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique em **Phish "fazer login na sua conta"**.



9. No registro de pesquisa de e-mail exibido, clique na lista relacionada Critérios de pesquisa de e-mail e clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. No formulário Critérios de pesquisa de e-mail, preencha os campos.

Um exemplo de um formulário preenchido segue a tabela.

Campo	Descrição
Pesquisa de e-mail	O campo é preenchido automaticamente com o nome que você inseriu para o registro de pesquisa de e-mail.
Ícone de pesquisa	Pesquisa usando lista. Uma lista de pesquisas salvas. Clique no ícone para abrir uma lista de pesquisas de e-mail salvas. Clique em um item nesta lista para remover a pesquisa atual e selecionar uma pesquisa de e-mail salva anteriormente.
Ícone de informações	Ícone usado para exibir o registro de pesquisa de e-mail. Clique no ícone para exibir o registro de pesquisa de e-mail.
Campo de pesquisa	Critério de pesquisa (**Assunto**, **De**ou **Destinatário**). Selecione o critério de pesquisa na lista de seleção e defina um valor que você deseja pesquisar no campo de texto. Para este exemplo, comece com From `phisher@cbazyx.com` (o endereço de e-mail do remetente do e-mail de phishing).
Ativo	Opção para ativar a pesquisa. A pesquisa é ativada por padrão. Se você desmarcar esta opção, este registro não será incluído em uma pesquisa.

Tradução automática

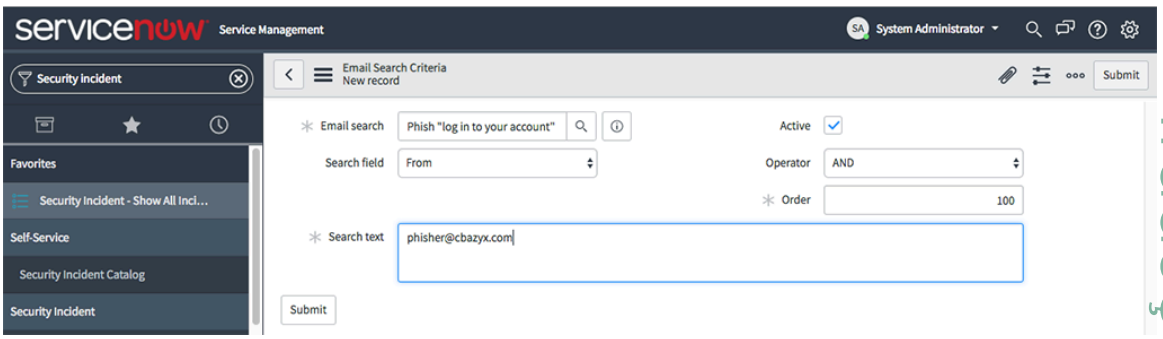
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Operador	Operadores (**AND**, **OR**) para definir ainda mais sua pesquisa. **AND**: o sistema pesquisará as condições separadas por **AND** e retornará resultados somente se todas as condições forem atendidas. Para a pesquisa de remetente mais assunto, use o operador **E** para que ambas as condições de pesquisa sejam atendidas durante a pesquisa de e-mail. Para este exemplo, use o operador **E** para que a consulta seja De (remetente) = `phisher@cbazyx.com` **E** Assunto = `faça login na sua conta`. **OU**: o sistema pesquisará e retornará resultados se qualquer uma das condições separadas por **OU** for atendida. Um exemplo é De (Remetente) = `phisher@cbazyx.com` **OU** De (Remetente) = `phisher-2@cbazyx.com`.
Ordem	Se você inserir mais de duas condições de pesquisa, use Ordem para priorizar as condições. 100 é o padrão. Insira um valor entre 1 e 100 para cada condição, por exemplo, 100, 95, 90, 80. A condição com o número mais baixo atribuído tem a prioridade de pesquisa mais alta em um grupo de condições.
Pesquisar texto	Os valores de texto (palavras-chave) para a pesquisa (endereços de e-mail ou linhas de assunto). O campo de pesquisa contém o texto usado na pesquisa, por exemplo, `phisher@cbazyx.com`. Para que a pesquisa retorne resultados precisos para pesquisas de Remetente (De) e destinatário, as cadeias de caracteres de pesquisa devem corresponder exatamente. Para pesquisas de assunto, a cadeia de caracteres de pesquisa pode conter palavras-chave que fazem parte de uma cadeia de caracteres maior. Por exemplo, um assunto pode conter a cadeia de caracteres de pesquisa exata que é correspondida em um cabeçalho de mensagem encaminhada ou de resposta, como `FW: faça login na sua conta e mude sua senha imediatamente`.

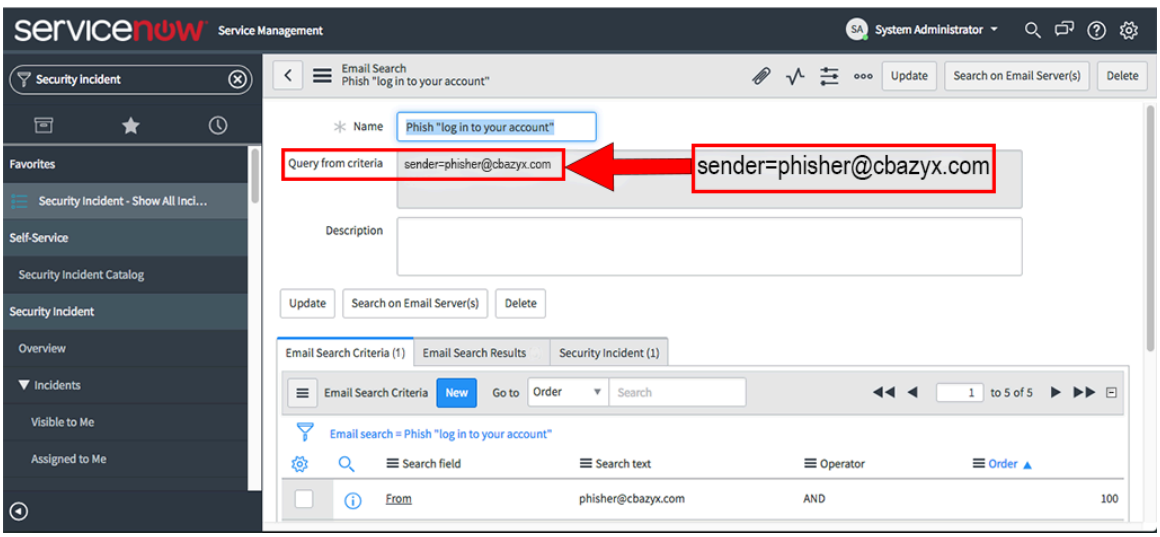
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por exemplo, `Faça login na sua conta` são palavras-chave exatas na cadeia de caracteres `faça login na sua conta e mude sua senha imediatamente`. Nenhuma designação de curinga (*) é necessária para oferecer suporte a um tipo de pesquisa " contém ". Atualmente, não existe nenhum método de filtragem para corresponder a uma cadeia de caracteres de pesquisa exata que não faça parte de uma cadeia de caracteres de texto maior.



11. Clique em **Enviar**.
O registro de pesquisa de e-mail é exibido. No campo **Consulta de critérios**, os critérios de pesquisa que você adicionou para o Remetente (De) são exibidos.

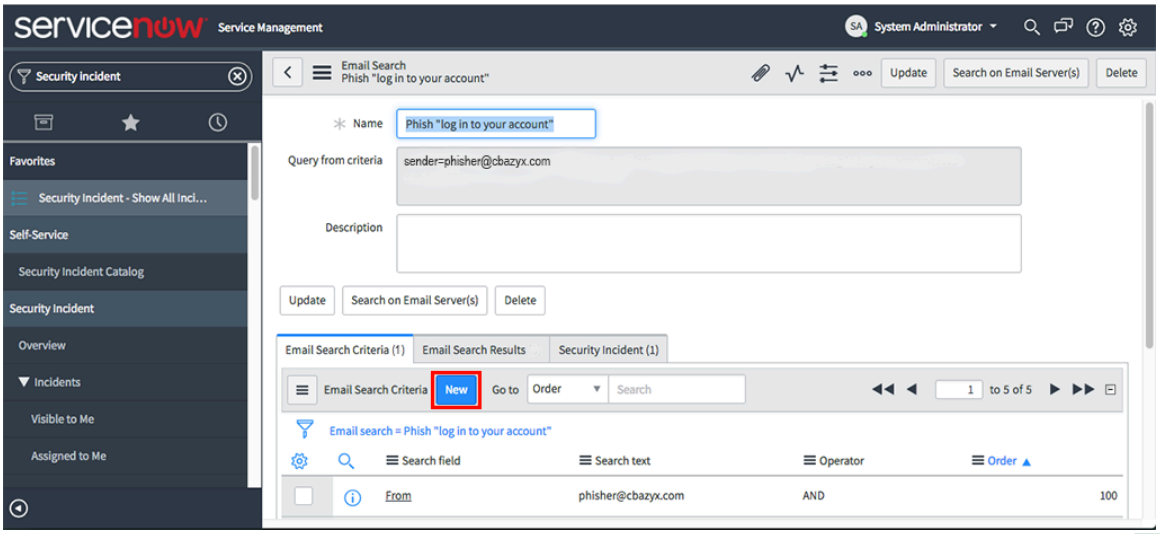


12. Para atualizar esses critérios de pesquisa de e-mail com mais informações para que a consulta inclua a condição de assunto mais remetente desejada, siga as etapas para adicionar outra condição de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

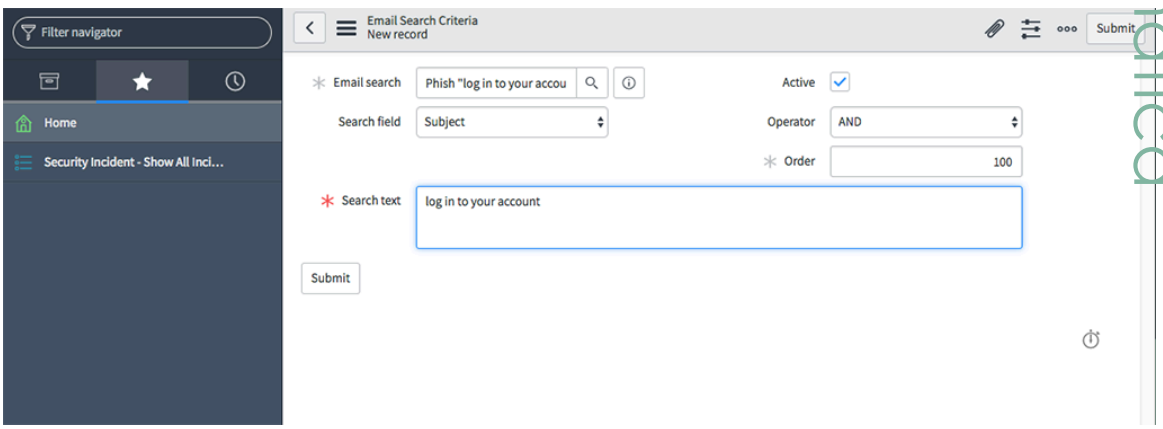
a. Na lista relacionada Critérios de pesquisa de e-mail, clique em **Novo**.



b. Na lista **Campo de pesquisa**no registro Critérios de pesquisa de e-mail exibido, selecione **Assunto**.

c. Na lista Operador, selecione**E** ou **OU**.
Se você selecionar **OU**, a pesquisa retornará resultados se as palavras-chave na cadeia de caracteres de texto da linha de assunto corresponderem ou se a condição do endereço de e-mail for correspondida. **E** está selecionado para este exemplo para que a pesquisa retorne resultados somente para e-mails que contenham as palavras-chave da cadeia de caracteres de texto do assunto e que correspondam ao endereço de e-mail do remetente.

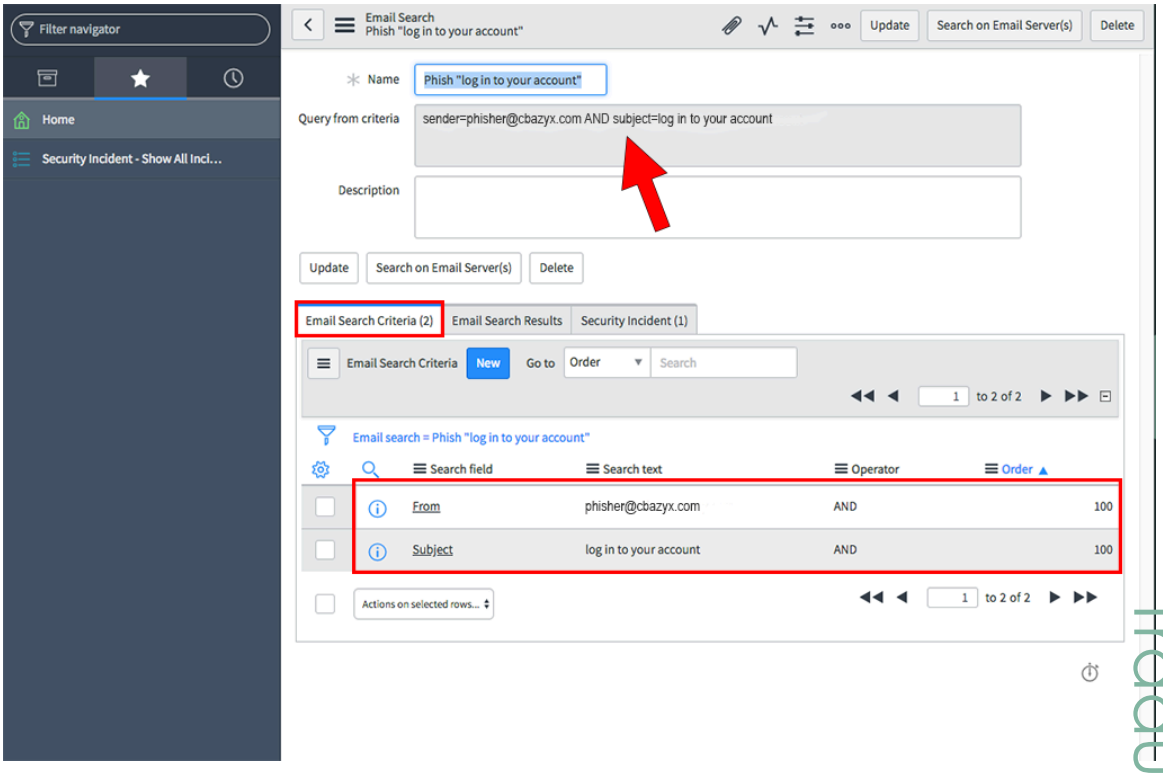
d. No campo **Texto de pesquisa**, insira o valor do texto da linha de assunto, `faça login na sua conta`.



e. Clique em **Enviar**.
A nova condição é exibida na lista relacionada Critérios de pesquisa de e-mail **e** ambas as condições são exibidas no campo **Consulta de critérios** separados pelo operador E.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Opcional: Se você tiver mais de duas condições de pesquisa e selecionar **E** para separar cada condição, defina o valor da ordem para priorizá-las.

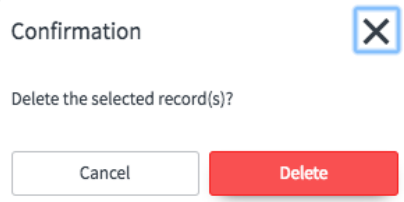
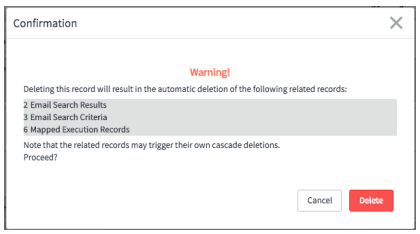
g. Continue a adicionar, modificar ou remover critérios de pesquisa conforme desejado e clique em **Atualizar** para salvar suas mudanças no registro.

13. Escolha uma opção para continuar.

Opção	Descrição
Atualizar	Atualize e salve suas mudanças no registro.
Pesquisar em Servidor(es) de E-mail	Inicie uma pesquisa nos servidores com os critérios que você salvou no registro Critérios de pesquisa de e-mail.
Excluir	Exclua este registro de pesquisa de e-mail da sua instância Now Platform. Esta ação não exclui as mensagens de e-mail reais. Exclui somente o registro de pesquisa usado para localizar mensagens. Uma caixa de diálogo é exibida. Se você clicar em **Excluir**, os resultados da pesquisa de e-mail e os critérios de pesquisa de e-mail para este registro de pesquisa serão excluídos.

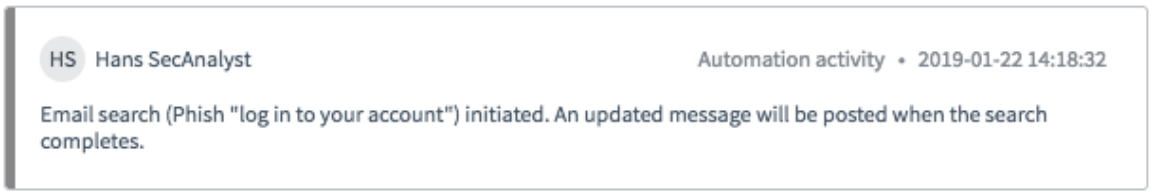
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	 Se um registro tiver resultados de pesquisa, o aviso a seguir será exibido. 

14. Para iniciar uma pesquisa de e-mail, no registro de pesquisa de e-mail, clique **em Pesquisar em servidores de e-mail**.
    Uma mensagem é exibida indicando que a solicitação de pesquisa foi enviada.

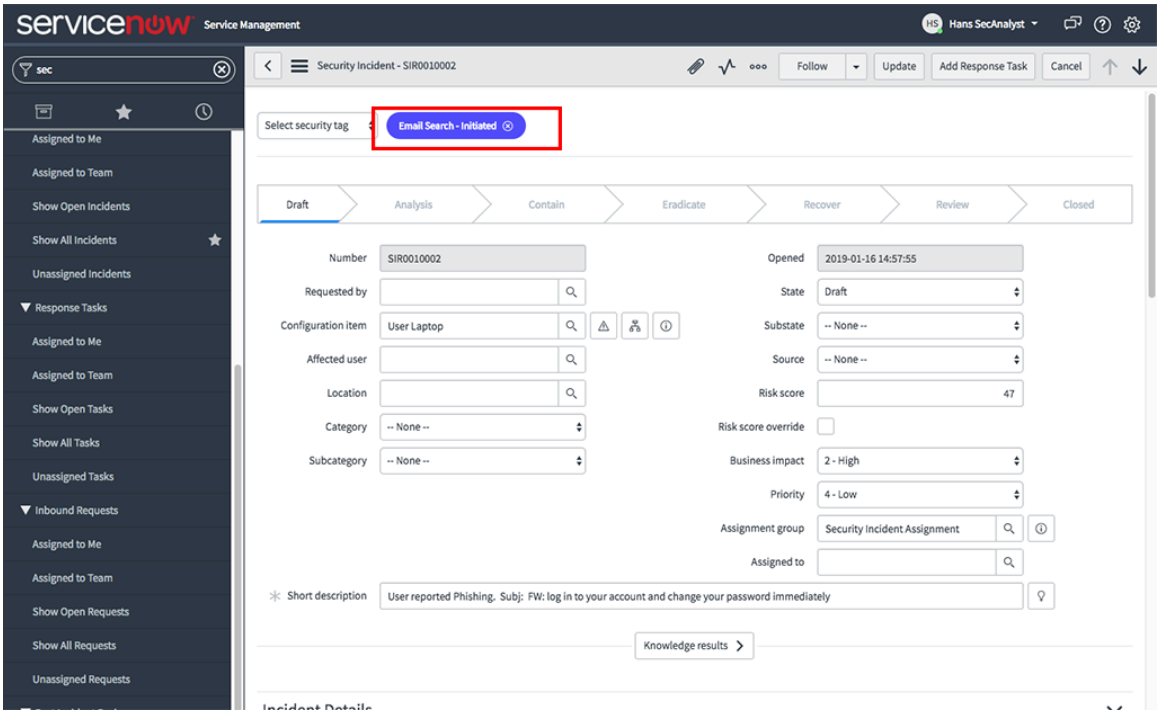
    No registro de Incidente de segurança, uma anotação de trabalho é exibida indicando que uma pesquisa foi iniciada.

    Se a marcação estiver habilitada, na parte superior do registro de Incidente de segurança, o marcador de segurança `Pesquisa de e-mail - Iniciado` será exibido.

Tradução automática

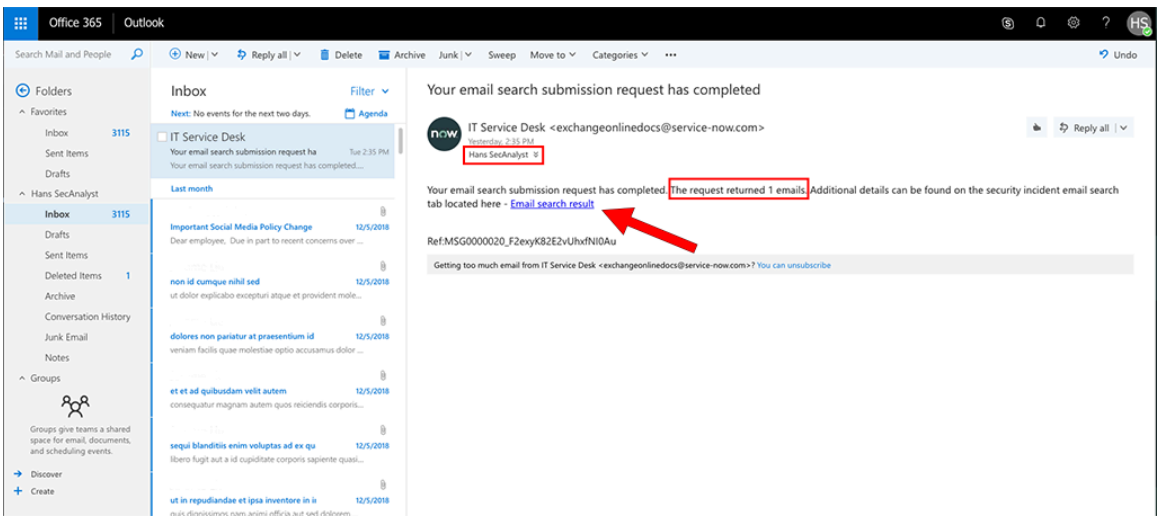
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que a pesquisa for concluída com sucesso, se as notificações por e-mail estiverem habilitadas, um e-mail será enviado para o endereço de e-mail do indivíduo que iniciou a pesquisa.

Neste exemplo, o usuário com a função sn_si.analyst, `Hans SecAnalyst`, enviou esta pesquisa. A imagem a seguir mostra que esta notificação é enviada para uma conta em Microsoft Exchange Online. No entanto, essas notificações podem ser enviadas para um serviço de e-mail diferente, conforme necessário.

Esta notificação permite que você exiba todos os resultados correspondentes que exigem acompanhamento e exclusão. O exemplo a seguir mostra que há um e-mail que correspondeu aos critérios de pesquisa. Um link de resultado de pesquisa de e-mail para o registro de resultado de pesquisa de e-mail em sua instância Now Platform também é fornecido. Se você quiser exibir o registro de pesquisa, clique neste link.



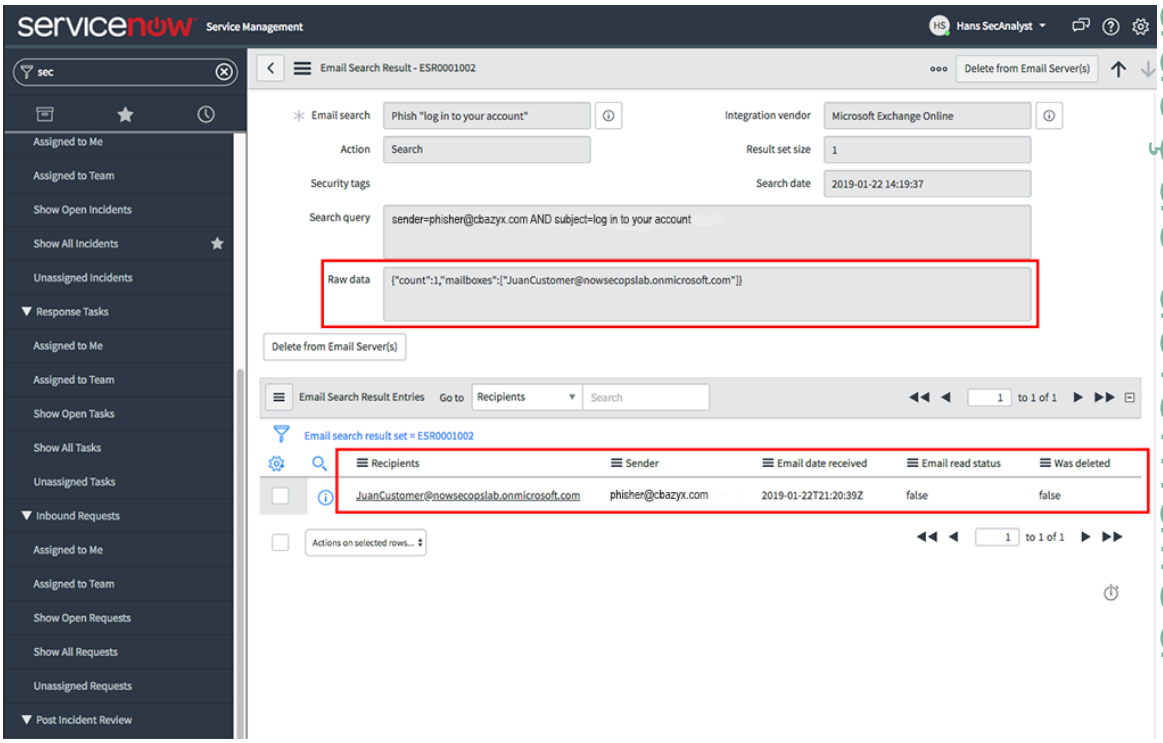
15. A partir deste e-mail, para exibir os resultados da pesquisa, clique no link Resultado da pesquisa por e- **mail**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro do resultado da pesquisa de e-mail é exibido. Neste registro, você pode verificar e revisar os dados a seguir.

- No campo **Dados brutos**, a contagem de e-mail para o número de e-mails que corresponderam aos critérios de pesquisa `{"count":1}` e os endereços de caixa de correio onde os e-mails foram encontrados são exibidos `["JuanCustomer@nowsecopslab.onmicrosoft.com"]`.
- Na coluna Destinatários, o destinatário é (`JuanCustomer@nowsecopslab.onmicrosoft.com`).
- Na coluna `Remetente`, a origem do e-mail é exibida.
- Na coluna Data de `recebimento` do e-mail, a data e a hora em que o e-mail foi recebido são exibidas para ajudar você a rastrear os cronogramas da campanha de phishing.
- Na coluna `Status de leitura` de e-mail, o e-mail neste exemplo não foi lido (`falso`). Se um e-mail tiver sido lido, `verdadeiro` será exibido.
- Na coluna `Foi excluído`, o e-mail neste exemplo não foi excluído. Se um e-mail tiver sido excluído, `verdadeiro` será exibido.

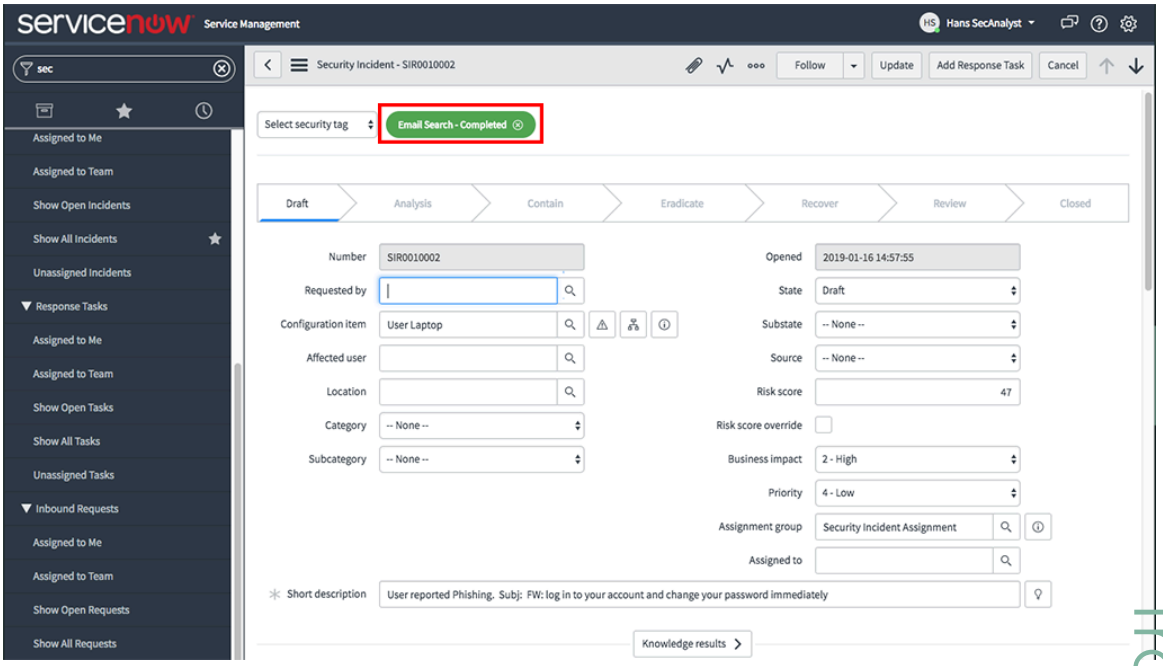


16. Como alternativa, para exibir os resultados da pesquisa do incidente de segurança, siga estas etapas.

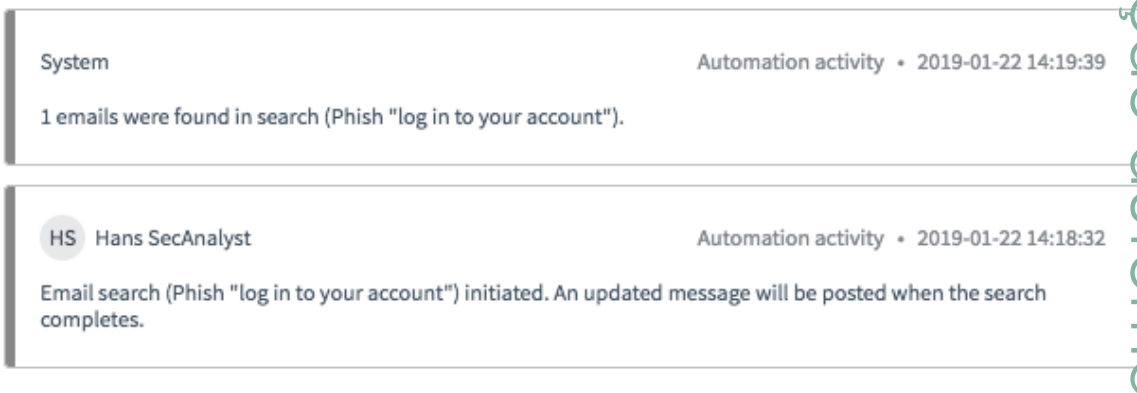
a. Navegar até **Incidente de segurança** > **Incidentes** e abra o incidente de segurança com o qual você está trabalhando.
Na parte superior do registro, quando a pesquisa é concluída com sucesso, o marcador de segurança `Pesquisa de e-mail - Concluído` substitui o marcador de segurança `Pesquisa de e-mail - Iniciada`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As anotações de trabalho são exibidas informando que a pesquisa foi concluída com sucesso e que um e-mail correspondente foi encontrado.

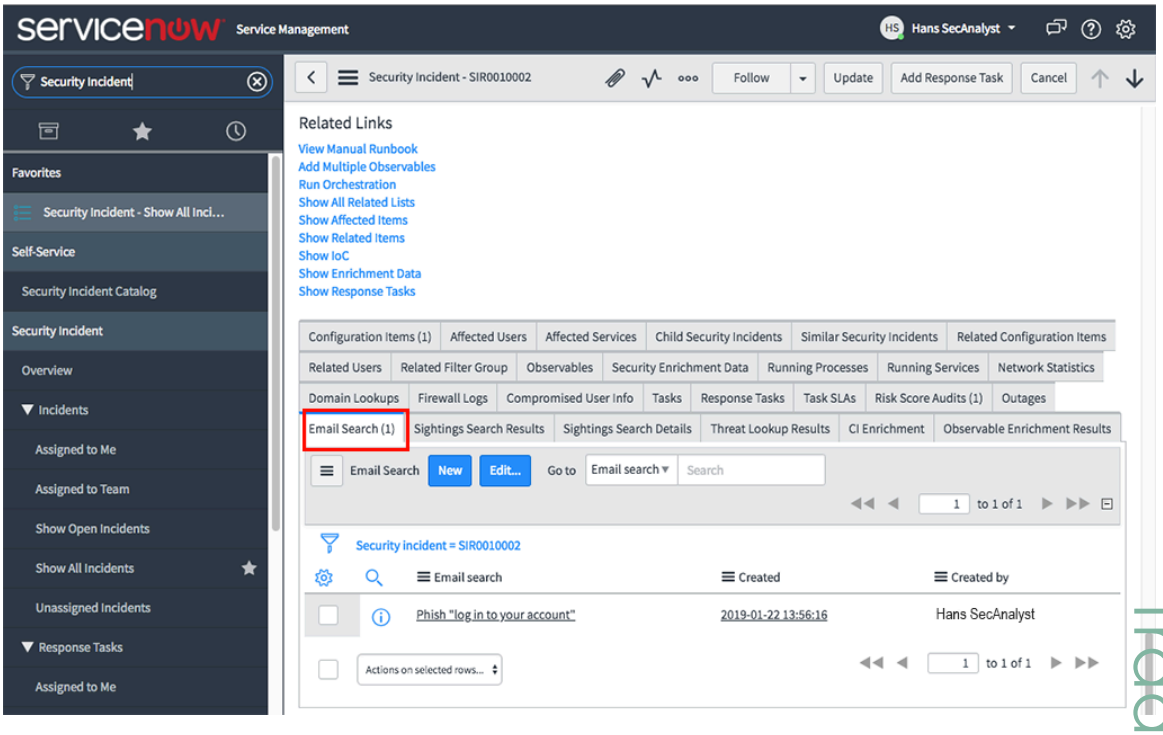


b. Role até a parte inferior do registro de Incidente de segurança e clique na lista relacionada Pesquisa de e-mail.

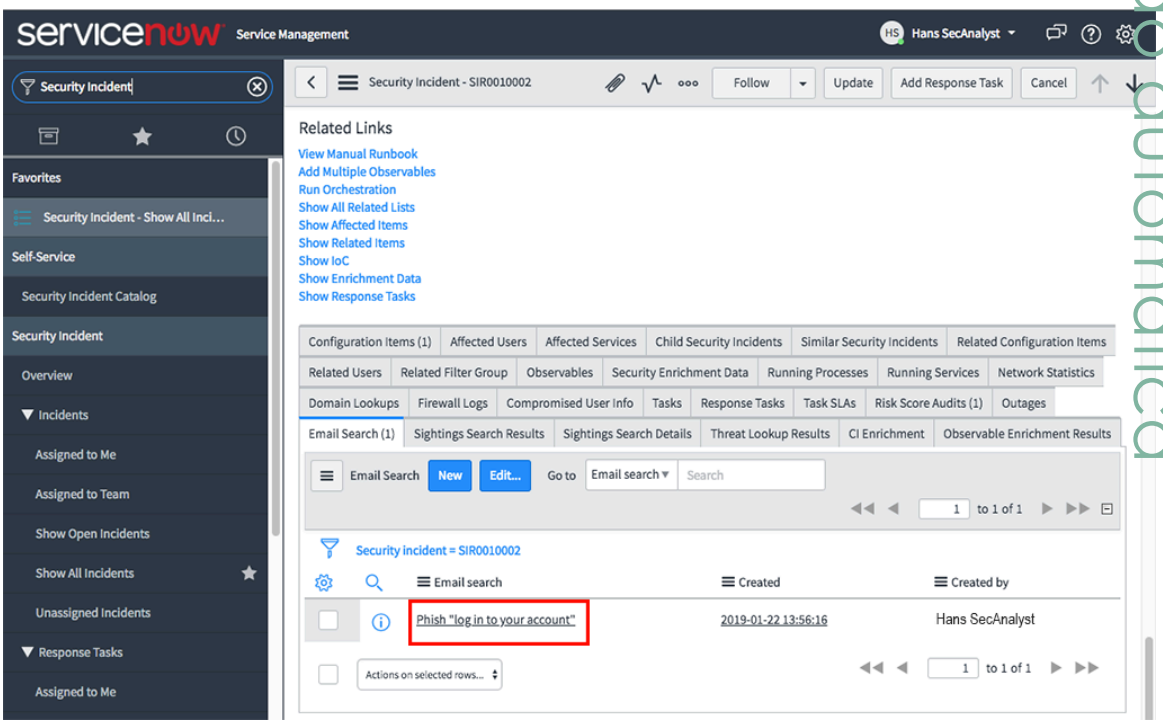
Se a lista relacionada Pesquisa de e-mail não for exibida, clique no link relacionado**Mostrar todas as listas** relacionadas para exibir essa lista relacionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique no nome da sua pesquisa.



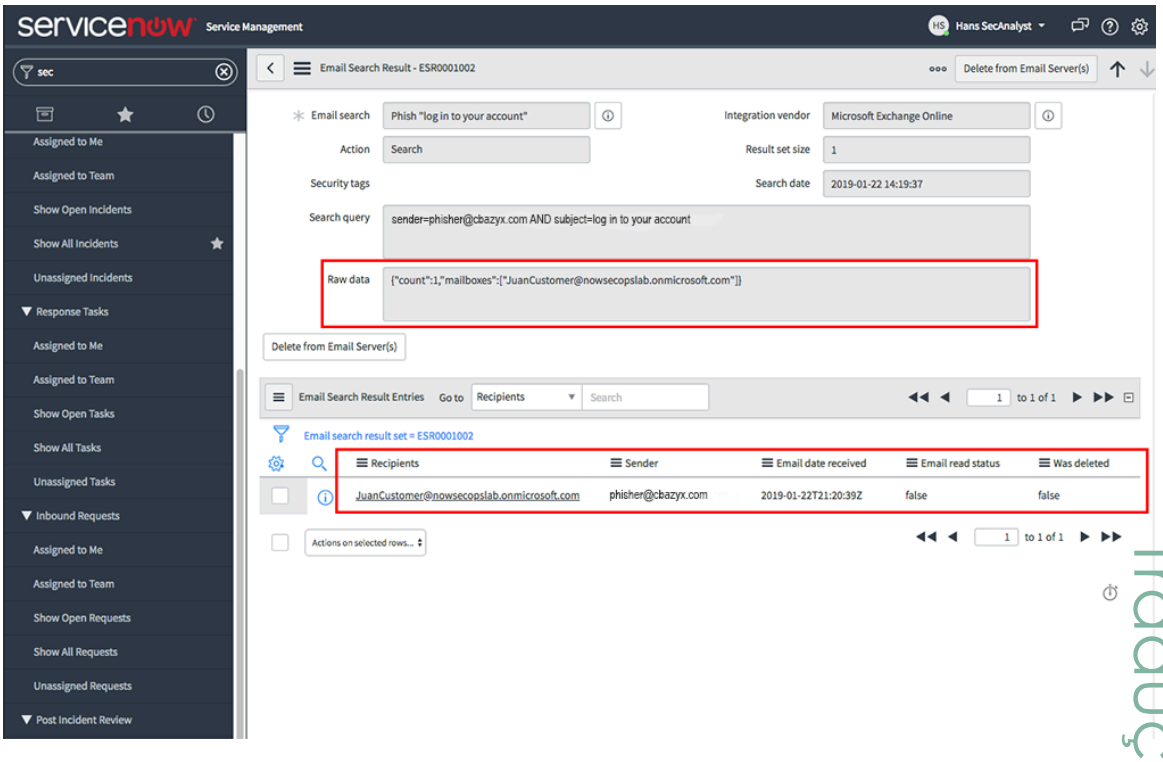
d. No registro Pesquisa de e-mail, clique na lista relacionada Resultados da pesquisa de e-mail.

e. Na coluna Data de pesquisa, clique na data da pesquisa para exibir os dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro do resultado da pesquisa de e-mail é exibido.



Depois que uma pesquisa de e-mail for concluída com sucesso, avalie os resultados. Se você determinar que os e-mails precisam de correção, agora você está pronto para excluir e-mails ou solicitar aprovação de exclusão.

Solicitar aprovação de exclusão para e-mails no serviço online do Microsoft Exchange

Depois que uma pesquisa de e-mail for concluída com sucesso e as mensagens correspondentes forem identificadas, você poderá excluir permanentemente todos os e-mails suspeitos do serviço online do Microsoft Exchange que estão relacionados ao incidente de segurança e à campanha de phishing.

Antes de Iniciar

Função necessária: sn_si.analyst

O sistema executa exclusões nos resultados de pesquisa mais recentes bem-sucedidos.

Por Que e Quando Desempenhar Esta Tarefa

Se as aprovações e notificações por e-mail estiverem habilitadas, envie uma solicitação para excluir e-mails para um grupo de aprovação antes da remoção por e-mail.

Os resultados da pesquisa de e-mail são exibidos com todas as mensagens que foram recebidas. Para garantir que os e-mails de phishing sejam excluídos com sucesso, os resultados da exclusão são publicados nas anotações de trabalho do incidente de segurança associado. Se a marcação estiver habilitada, um marcador de segurança também será exibido no incidente de segurança relacionado. Se o e-mail não for excluído com sucesso, você também será notificado nas anotações de trabalho.

Dependendo das suas políticas organizacionais, pode ser necessário solicitar aprovação antes de excluir e-mails de phishing. O processo de aprovação de exclusão requer informações sobre o número de e-mails a serem excluídos e, potencialmente, acesso a outros detalhes da mensagem. Para processar a solicitação de exclusão, em uma notificação por e-mail, um aprovador recebe a contagem de mensagens de e-mail correspondente, o link do incidente de segurança para acessar os detalhes completos da mensagem e os links de aprovação ou rejeição. Os links neste e-mail permitem que

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

um aprovador aceite ou rejeite a solicitação de exclusão da notificação por e-mail. Uma trilha de auditoria completa com carimbo de data/hora também está disponível para rastrear quando o status de aprovação mudou nas anotações de trabalho. Se um grupo de aprovação for atribuído, um usuário do grupo poderá processar a solicitação para o grupo inteiro. Cada membro do grupo de aprovação recebe uma notificação por e-mail da solicitação.

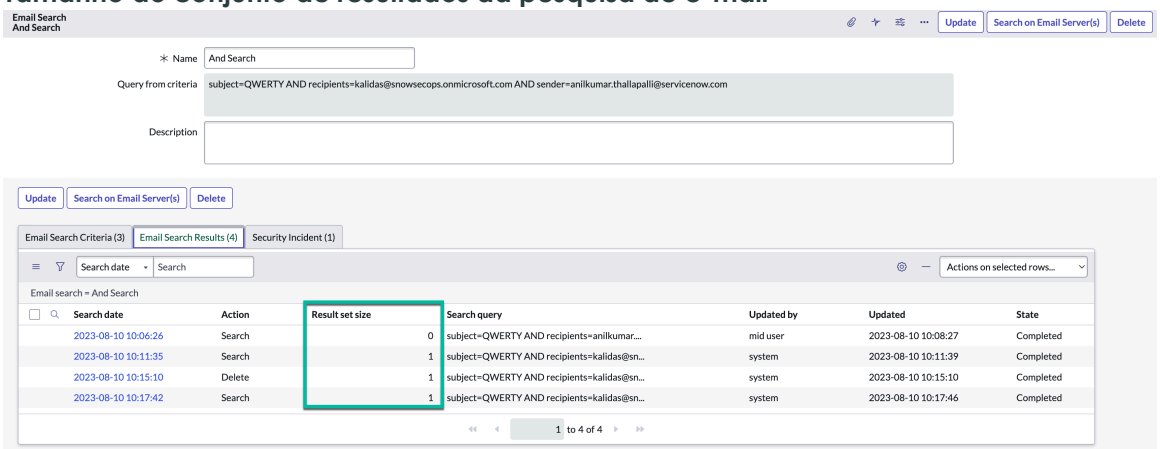
Como um usuário com a função sn_si.analyst, se você determinar que os e-mails precisam de correção, siga as etapas necessárias para excluir e-mails. Se as aprovações estiverem habilitadas, solicite aprovação para excluir e-mails do serviço Microsoft Exchange Online.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança > Mostrar todos os incidentes**.
2. Clique na lista relacionada **Pesquisa de e-mail**.
3. Com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique no nome da sua pesquisa.
   Os resultados da pesquisa são exibidos na lista relacionada Resultados da pesquisa de e-mail.

   Para este exemplo, esta pesquisa encontrou e-mails que correspondem aos seus critérios de pesquisa. Há duas ações de pesquisa listadas no registro. Uma pesquisa não tem correspondências (0) e a outra pesquisa tem um e-mail correspondente (1).

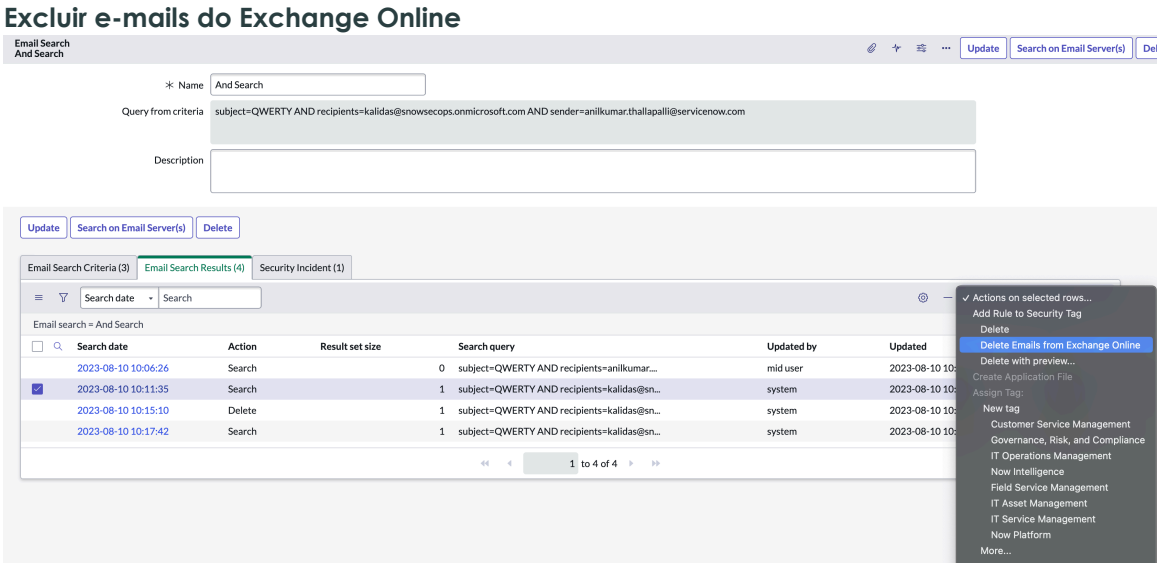
Tamanho do conjunto de resultados da pesquisa de e-mail



4. Para excluir itens de e-mail associados a uma pesquisa, à esquerda da coluna Data de pesquisa, marque a caixa de seleção de um conjunto de resultados de pesquisa.
   Você pode selecionar um único conjunto de resultados ou vários conjuntos de resultados na lista.
5. Selecione os conjuntos de resultados que você deseja excluir.

Tradução automática

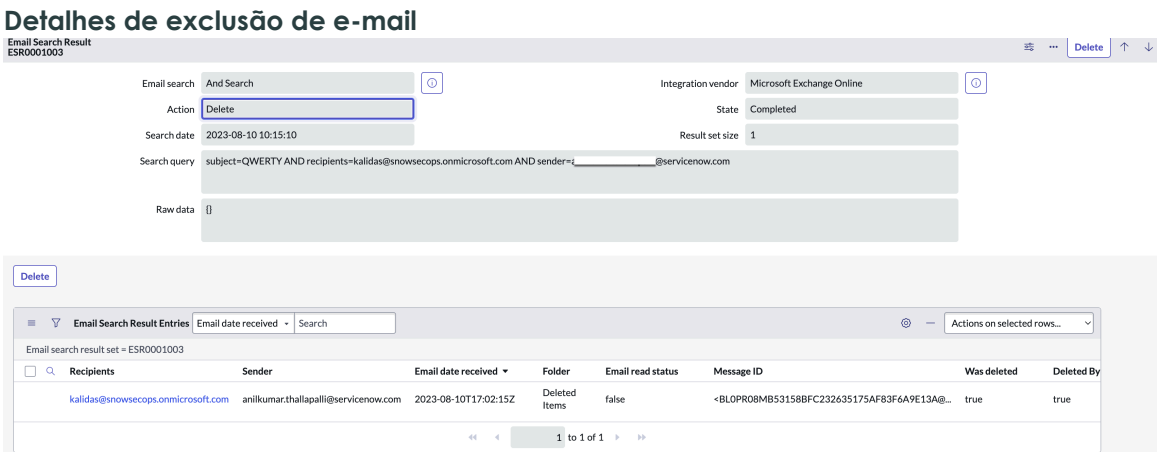
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na parte inferior da lista relacionada Resultados da pesquisa de e-mail, na lista Ações nas linhas selecionadas, selecione **Excluir e-mails do Exchange Online** para excluir todos os itens de e-mail associados a um ou mais conjuntos de resultados do servidor do Exchange Online.
   Se um conjunto de resultados contiver mais de um e-mail, você não precisará abrir o registro Resultado da pesquisa de e-mail e selecionar e-mails individuais para excluí-los. Todos os itens de e-mail com um status `falso` na coluna Foi excluído no registro Resultado da pesquisa de e-mail são excluídos depois que você seleciona **Excluir e-mails do Exchange Online**.

   Se um item de e-mail em um conjunto de resultados já tiver sido excluído, o status na coluna Foi excluído no registro Resultado da pesquisa de e-mail será `verdadeiro`. Esses itens não serão excluídos novamente.

   Se a opção de aprovação estiver desabilitada durante a etapa de configuração, depois de selecionar **Excluir e-mails do Exchange Online**, os e-mails associados ao conjunto de resultados serão excluídos. O conjunto de resultados em si não é excluído. No entanto, o status de todos os itens de e-mail excluídos do conjunto de resultados é atualizado para `verdadeiro` na coluna Foi excluído do registro Resultado da pesquisa de e-mail. Para obter mais informações sobre o recurso de aprovação, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.



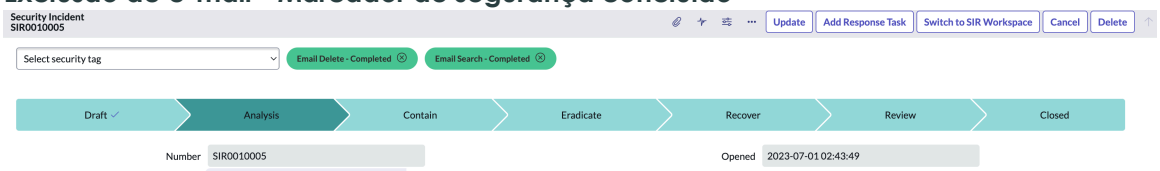
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esses e-mails são excluídos do locatário Microsoft Exchange Online em que você realizou as pesquisas. Uma anotação de trabalho será exibida se os e-mails forem excluídos com sucesso.

No registro de incidente de segurança, o marcador de segurança `Exclusão de e-mail - Concluído` é exibido.

Exclusão de e-mail - Marcador de segurança concluído

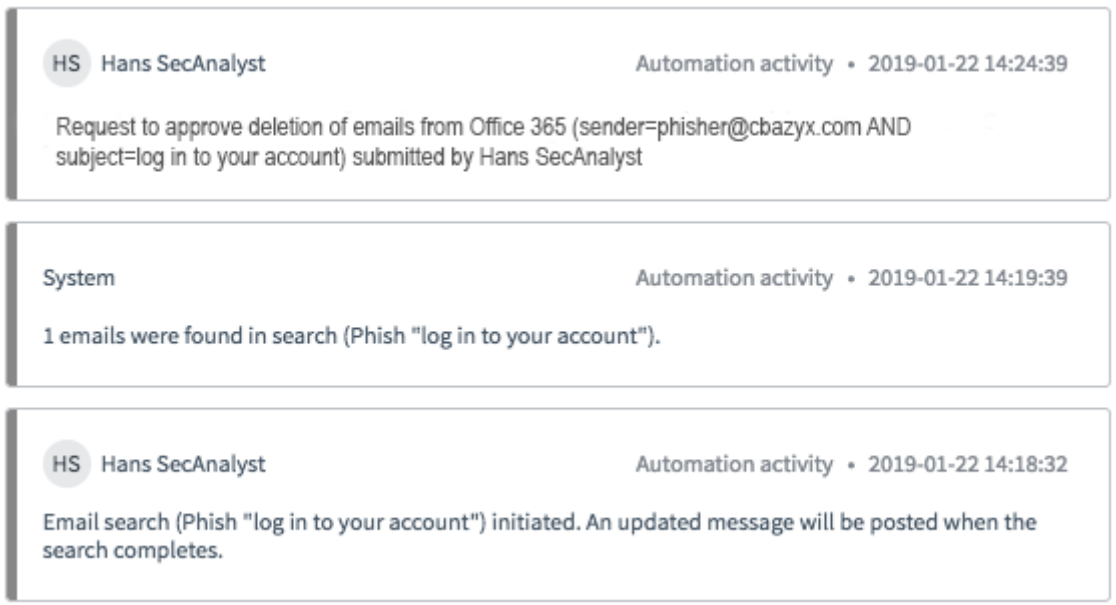


Se as aprovações estiverem desabilitadas para solicitações de exclusão, você excluiu e-mails do locatário Microsoft Exchange Online.

Se as aprovações estiverem habilitadas para solicitações de exclusão durante a etapa de configuração, depois de selecionar **Excluir e-mails do Exchange Online**, uma notificação por e-mail será enviada para cada membro do grupo de aprovação selecionado durante a etapa de configuração.

Se a marcação estiver habilitada durante a etapa de configuração, o marcador de segurança `Exclusão de e-mail - Iniciada` será exibido no registro de incidente de segurança relacionado. Para obter mais informações sobre marcação, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.

As anotações de trabalho são exibidas informando que uma solicitação para excluir e-mails foi enviada pelo usuário com a função sn_si.analyst (`Hans SecAnalyst`).



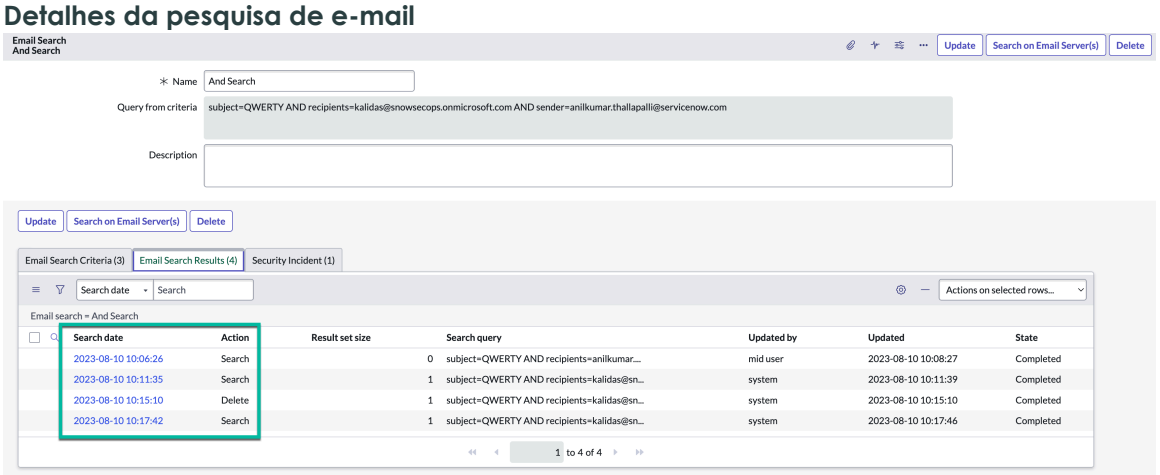
Se as aprovações estiverem habilitadas, a próxima etapa será processar a solicitação de exclusão.

7. Como alternativa, se você quiser exibir os detalhes e itens de e-mail individuais de um registro de pesquisa antes de excluí-lo ou enviar uma solicitação de exclusão, siga estas etapas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Com a lista relacionada Resultados da pesquisa de e-mail selecionada, na coluna Data de pesquisa, clique na data de uma pesquisa que você deseja revisar.



As seguintes informações sobre os e-mails são exibidas:

- Destinatários
- Remetente
- Data de recebimento do e-mail
- Status de leitura de e-mail (`verdadeiro` ou `falso`)
- Foi excluído (`verdadeiro` ou `falso`)
- Excluído por integração (`verdadeiro` ou `falso`)

Nota:

O valor é definido como verdadeiro quando o e-mail é excluído quando o analista inicia a exclusão de servidor(es) de e-mail.

As anotações de trabalho são atualizadas com o número total de registros excluídos, o que inclui os registros excluídos pela integração e pelo usuário.

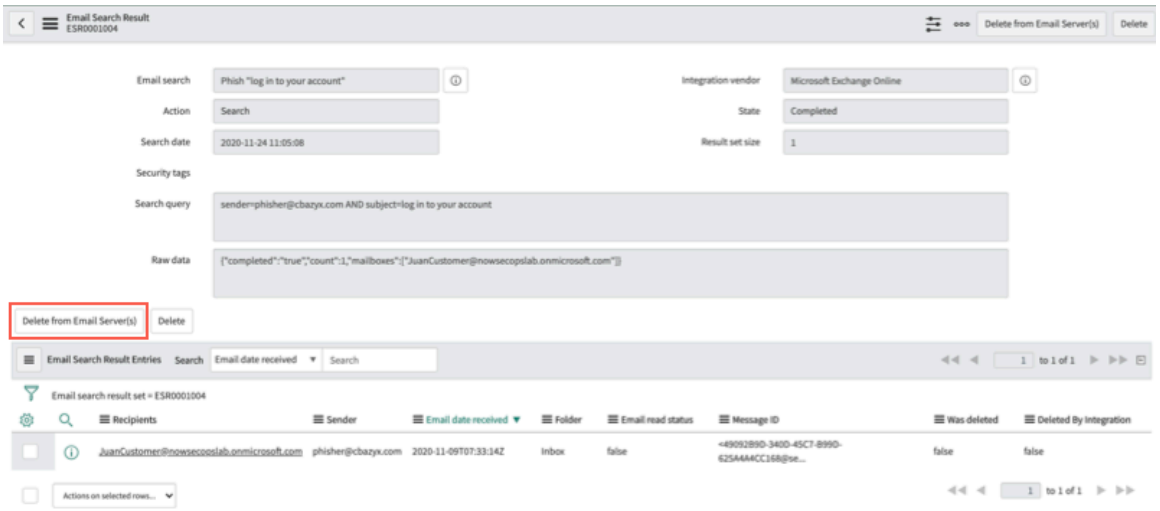
b. Depois de revisar os dados, para excluir todos os e-mails ou enviar uma solicitação para excluir todos os e-mails, clique em **Excluir do(s) servidor(es) de e-mail**.

Conforme descrito no exemplo anterior, se houver mais de um e-mail listado no registro do resultado da pesquisa, você não precisará selecionar os e-mails individuais para removê-los. A solicitação de exclusão remove todos os e-mails associados à pesquisa

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

quando `falso` é exibido na coluna Foi excluído dos resultados da pesquisa mais recentes.



Se as aprovações estiverem habilitadas, você enviou com sucesso uma solicitação para excluir e-mails. Os marcadores de segurança e as anotações de trabalho são exibidos no registro de incidente de segurança relacionado, conforme descrito no exemplo anterior. Como aprovador, a próxima etapa é processar a solicitação de exclusão.

Aprovar solicitações de exclusão de e-mail para a integração Microsoft Exchange Online

Se a opção de aprovação estiver habilitada em sua instância Now Platform, as solicitações para excluir e-mails serão enviadas para cada membro do grupo de aprovação por e-mail. Você seleciona o grupo de aprovação durante a etapa de configuração. As aprovações fornecem à sua organização um nível adicional de controle sobre a exclusão de e-mails.

Antes de Iniciar

Verifique se a opção **Aprovações** está selecionada na guia Configurações adicionais do formulário Configurações de pesquisa e exclusão de e-mails do Exchange Online.

Verifique se você habilitou as opções **Envio**de e- **mail habilitado e Recepção de e-mail habilitada** na sua instância Now Platform para solicitações de aprovação. Para obter mais informações, consulte Configure sua instância Now Platform para a integração Microsoft Exchange Online.

Quando o usuário com a função sn_si.analyst envia solicitações de exclusão de e-mail, por padrão, essas solicitações são enviadas por e-mail para o sn_si.admin. Se você criou um grupo de aprovação, cada membro do grupo receberá uma notificação. Os aprovadores podem processar solicitações de exclusão de e-mail diretamente da notificação por e-mail. Como alternativa, as solicitações podem ser processadas a partir dos registros de resultado da pesquisa de e-mail em Now Platform instâncias. Este tópico mostra ambos os métodos de aprovação.

As informações a seguir descrevem a solicitação na notificação por e-mail:

Número do registro do resultado da pesquisa de e-mail

Número exclusivo atribuído ao registro de pesquisa pelo Now Platform como parte da trilha de auditoria.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do analista que enviou a solicitação

Nome da pessoa que enviou a solicitação como parte da trilha de auditoria.

Link para o incidente de segurança

Um link para o incidente de segurança relacionado ao evento de phishing. Exiba o incidente de segurança com as anotações de trabalho, pesquisas de e-mail e resultados de pesquisa de e-mail diretamente do e-mail.

Aprovar ou rejeitar links

Links para aprovar ou rejeitar a solicitação da notificação por e-mail. Depois de clicar em qualquer link, o sistema inicia automaticamente o fluxo de trabalho relacionado e uma anotação de trabalho é publicada no registro de incidente de segurança.

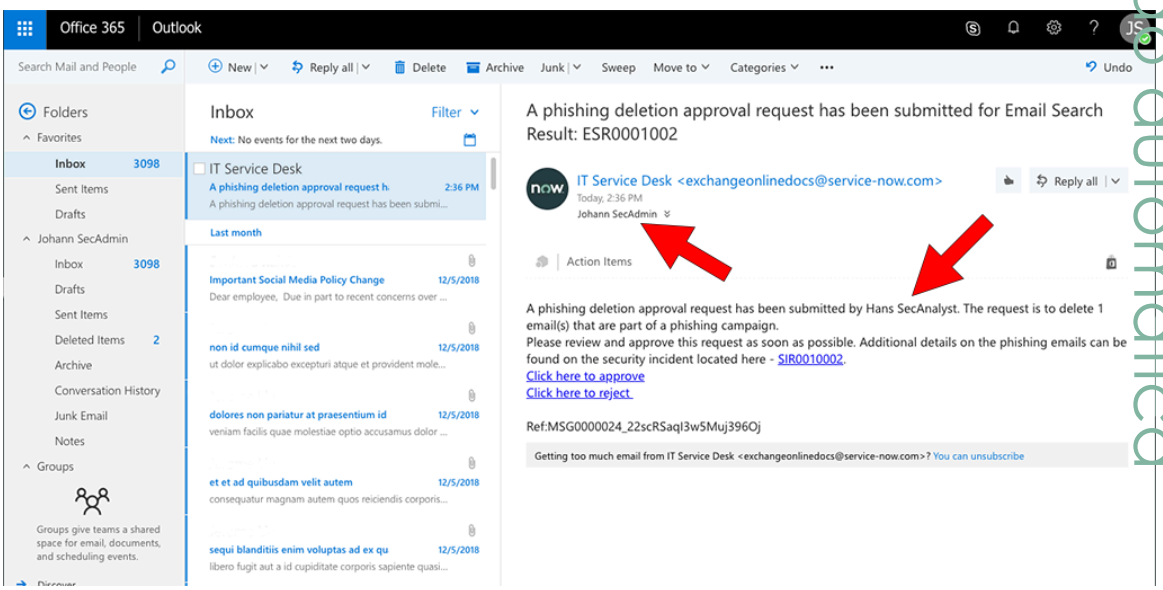
Função necessária: sn_si.admin ou todos os membros de um grupo de aprovação atribuído.

Procedimento

1. Para processar a solicitação de exclusão da notificação por e-mail, siga estas etapas.

a. Como aprovador, localize o e-mail de notificação na conta de e-mail que você configurou em sua conta de usuário Now Platform.

Neste exemplo, o usuário com a função sn_si.analyst (Hans SecAnalyst) envia uma solicitação para excluir um e-mail. Joan SecAdmin é membro do grupo de aprovação.



b. Na notificação por e-mail, escolha uma opção para continuar.

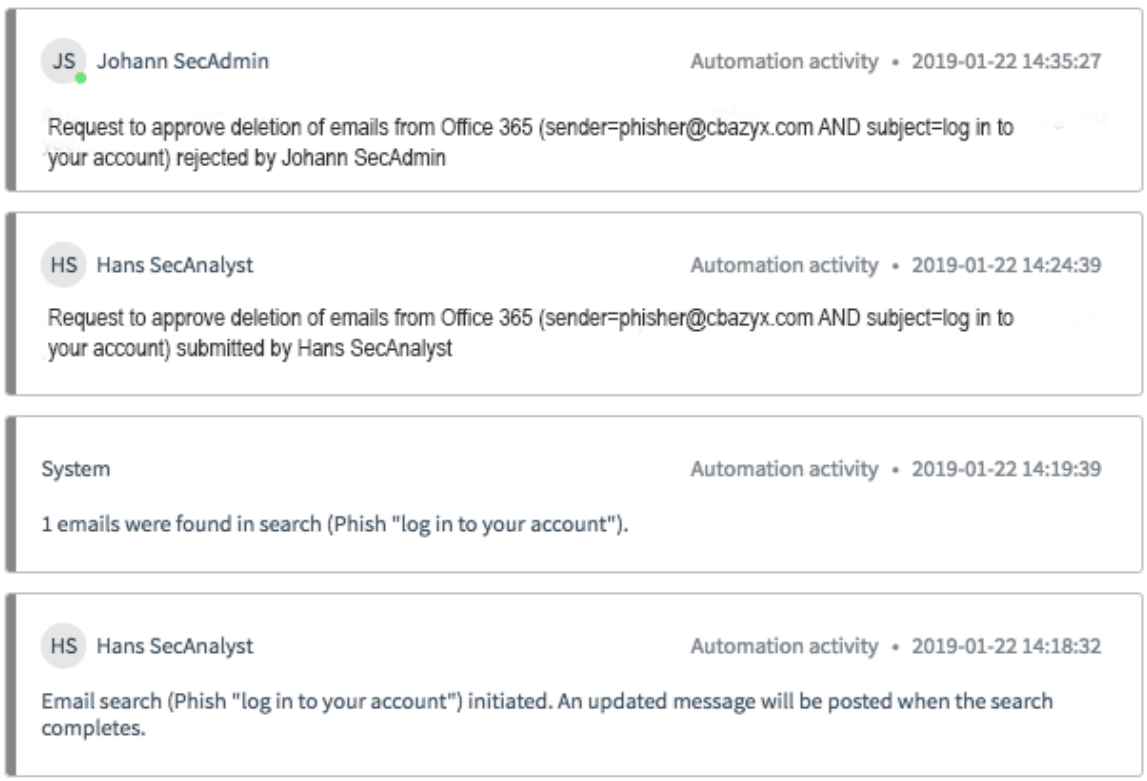
Opção	Descrição
Clique no link Clique aqui para aprovar Aprovar	Aprove a solicitação de exclusão. Todos os itens de e-mail com um status `falso` na coluna Foi excluído que estão associados ao registro de resultado da pesquisa são excluídos automaticamente do locatário Microsoft Exchange Online. O status de todos os itens de e-mail do conjunto de resultados é atualizado para `ver-`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	`dadeiro` na coluna Foi excluído do registro de resultado da pesquisa de e-mail. Uma anotação de trabalho é publicada no registro de incidente de segurança com o número de e-mails excluídos com sucesso. Se a marcação estiver habilitada, o marcador `Exclusão de e-mail - Concluído` substituirá o marcador `Exclusão de e-mail - Iniciado`.
Clique no link Clique aqui para rejeitar	Rejeitar a solicitação de exclusão. Uma anotação de trabalho é publicada com o nome da pessoa que rejeitou a solicitação. Depois que uma solicitação é rejeitada, como o usuário com a função sn_si.analyst, você deve enviar uma nova solicitação de exclusão se determinar que os e-mails devem ser excluídos.
Clique no link para o registro do incidente de segurança (SIR0010002)	Revise o incidente de segurança relacionado e todos os dados de pesquisa relacionados antes de processar a solicitação.

A imagem a seguir mostra um exemplo da trilha de auditoria criada pelas anotações de trabalho no registro de incidente de segurança relacionado a este exemplo. Quando a solicitação é rejeitada na notificação por e-mail por um aprovador, uma anotação de trabalho é publicada em pela pessoa que rejeitou a solicitação. O SecAdmin de SecAdmin rejeita esta solicitação.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na instância Now Platform da pessoa que rejeitou a solicitação (Johann SecAdmin), em **Autoatendimento > Minhas aprovações**, `Rejeitado` é exibido na coluna Estado.

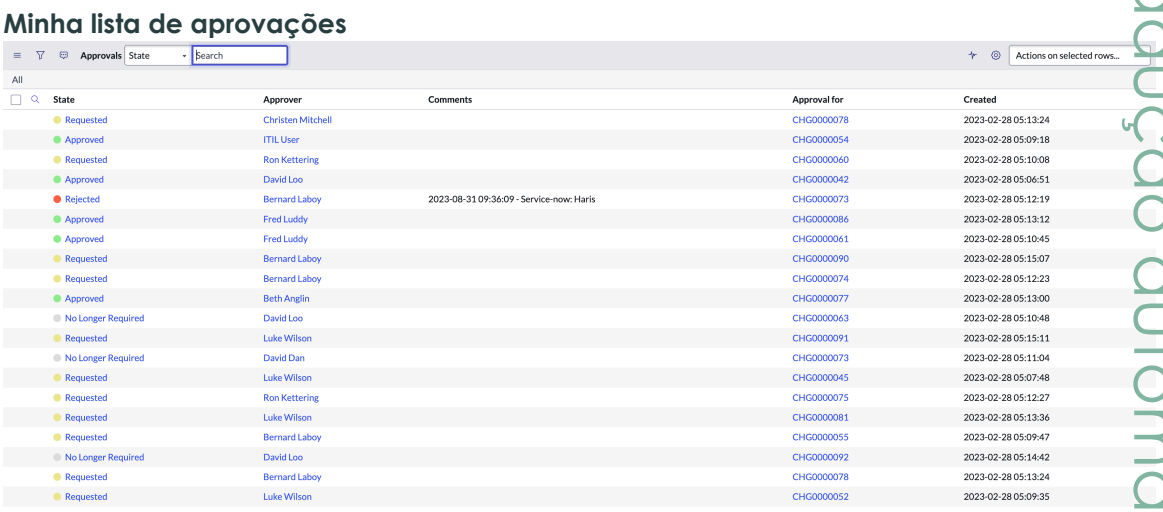
Depois que uma solicitação é rejeitada por qualquer membro do grupo de aprovação, como o usuário com a função sn_si.analyst, você deve enviar uma nova solicitação para excluir esses e-mails se determinar que eles devem ser excluídos.

Para este exemplo, depois que a solicitação é rejeitada, o usuário com a função sn_si.analyst envia uma nova solicitação.

Outro membro do grupo de aprovação, John Approver, recebe um e-mail semelhante ao mostrado no exemplo anterior. O aprovador John também pode processar esta solicitação.

2. Como alternativa, os aprovadores podem navegar até **Autoatendimento > Minhas aprovações** em suas Now Platform instâncias para exibir e processar solicitações de exclusão.
   Para processar uma solicitação de **Minhas aprovações**, siga estas etapas.

   a. Navegar até **Autoatendimento > Minhas aprovações**.

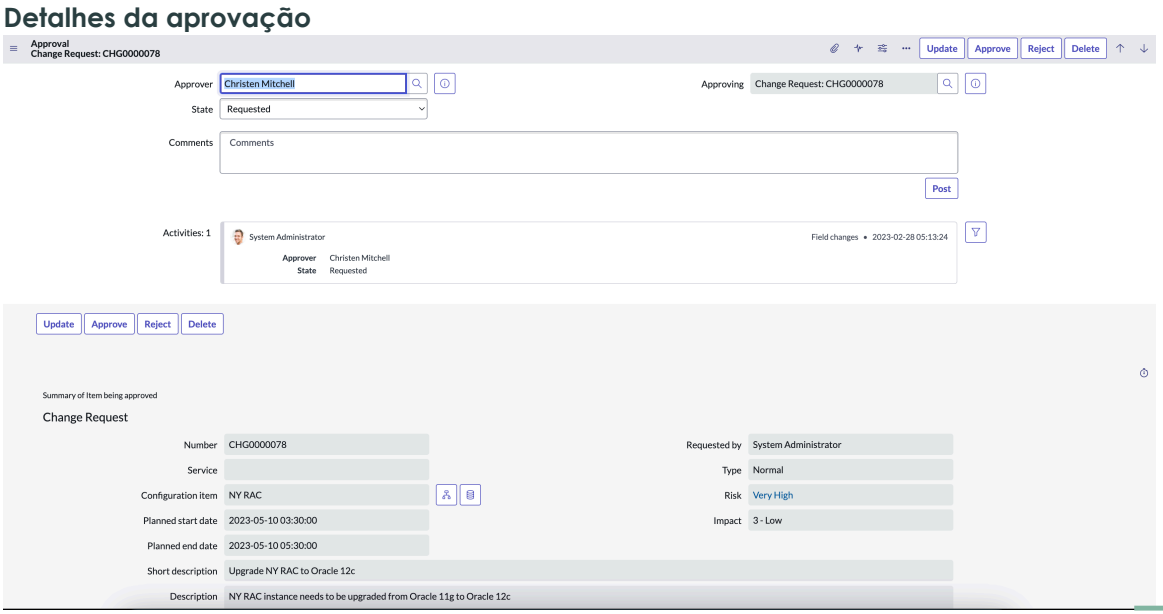


   b. Na coluna Estado, clique no item solicitado.

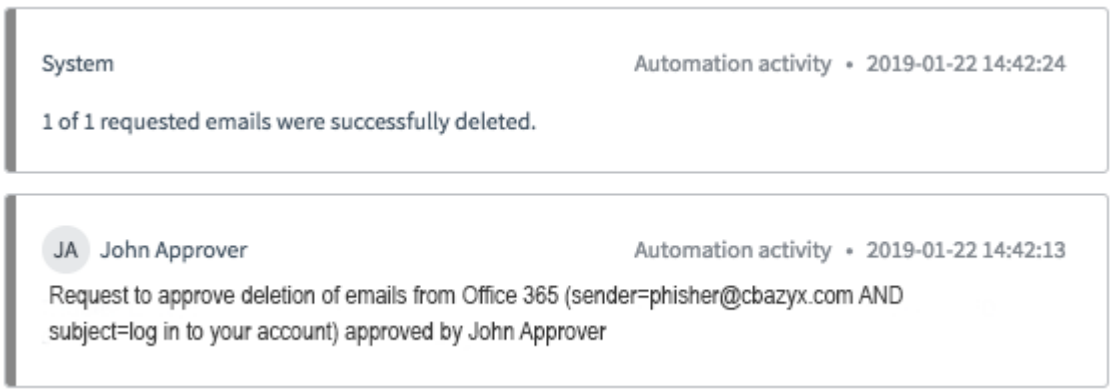
      No registro de aprovação exibido, os dados sobre a pesquisa, a solicitação de pesquisa e os resultados da pesquisa são listados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Neste registro, clique em **Aprovar** para aprovar a solicitação.
Depois que a solicitação é aprovada, o sistema inicia o fluxo de trabalho de exclusão para remover os e-mails. A imagem a seguir mostra um exemplo da trilha de auditoria criada pelas anotações de trabalho no registro de incidente de segurança relacionado a este exemplo. Depois que esta solicitação de exclusão for enviada novamente, ela será aprovada. Independentemente de qual método é usado para aprovar uma solicitação, o número de e-mails excluídos com sucesso é publicado em uma anotação de trabalho.



Depois que os e-mails forem excluídos com sucesso, no registro de incidente de segurança relacionado, se a marcação estiver habilitada, o marcador `Exclusão de e-mail - Concluído` substituirá o marcador `Exclusão de e-mail - Iniciado`.

Recebido(a) **Autoatendimento > Minhas aprovações** para o aprovador (John Approver), o estado muda de `Solicitado` para `Aprovado`.

Recebido(a) **Autoatendimento > Minhas aprovações** para outros membros do grupo de aprovação, por exemplo, Joan SecAdmin, o estado muda para `Não é mais necessário` depois que a solicitação é aprovada.

3. Como alternativa, para confirmar que os e-mails são excluídos no registro Resultado da pesquisa de e-mail no registro de incidente de segurança relacionado, siga estas etapas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

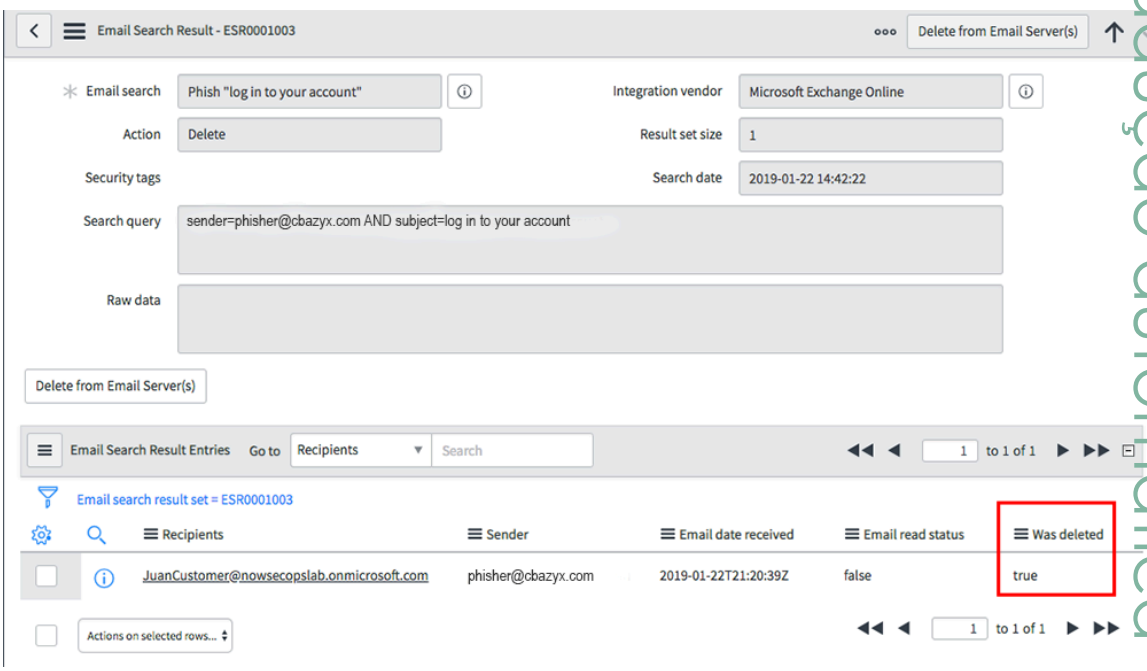
a. Navegar até **Incidentes de segurança > Mostrar todos os incidentes** e localize o incidente de segurança relacionado a phishing.
Na parte inferior do registro, as listas relacionadas são exibidas.

b. Clique na lista relacionada **Pesquisa de e-mail**.

c. Clique no nome da pesquisa na coluna Pesquisa de e-mail (`Phish "faça login na sua conta"`).
O registro de pesquisa de e-mail é exibido. Se a lista relacionada Pesquisa de e-mail não estiver visível, clique no link **Mostrar todas as listas**relacionadas.

d. Clique na lista relacionada **Resultados da pesquisa de e-mail**.
Na coluna Data de pesquisa, as ações de pesquisa e exclusão de e-mail são exibidas com as datas correspondentes.

e. Na coluna Data de pesquisa, clique no item que corresponde à ação de exclusão.
No registro Resultado da pesquisa de e-mail exibido, o status da coluna Foi excluído mostra que o e-mail foi excluído (`verdadeiro`).



Você aprovou com sucesso as solicitações de exclusão de e-mail de uma notificação por e-mail e de um registro de aprovação e confirmou que os e-mails foram excluídos. Para obter mais informações sobre como localizar o registro Resultado da pesquisa de e-mail, consulte Definir critérios de pesquisa de e-mail e solicitar uma pesquisa no serviço Microsoft Exchange Online.

Arquitetura de integração e conexão de sistemas externos para a integração Microsoft Exchange Online

A arquitetura de integração Microsoft Exchange Online foi desenvolvida para oferecer suporte aos recursos de pesquisa e exclusão de ameaças de e-mail no serviço Microsoft Exchange Online. Esta introdução explica por que há etapas de configuração que você deve concluir em suas contas Microsoft antes de instalar a aplicação ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A arquitetura de integração é baseada em avaliações das interfaces de programação de aplicações disponíveis no momento e com a consulta da Microsoft equipe de integração. Essas informações, bem como a terminologia principal sobre os serviços Now Platform e Microsoft Exchange Online, são fornecidas para esclarecer a operação conceitual da integração.

Termos-chave usados para esta integração

Os termos-chave a seguir são usados durante a instalação e a configuração do. Para obter mais informações sobre os termos a seguir, consulte o site de documentação de produtos da ServiceNow e o site de documentos da Microsoft .

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais, como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento de incidentes de segurança desde a descoberta e análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Microsoft Exchange Online

A oferta de serviço de e-mail para Microsoft Exchange Online, que faz parte do pacote Office 365 de produtos Microsoft.

API de gráficos globais

A API fornecida por Microsoft que é usada para acessar informações de caixa de correio em Microsoft Exchange Online.

Autenticação baseada em certificados

Essa autenticação permite que os clientes permitam ou exijam que os usuários se autentiquem diretamente com certificados X.509 em relação ao Azure Active Directory (Azure AD) para login de aplicações e navegadores.

Autenticação OAUTH

Uma ID criada no Microsoft portal do Azure usada para coletar detalhes adicionais da mensagem de e-mail e para excluir e-mails em Microsoft Exchange Online.

Host do Windows

O tipo específico de máquina virtual usada nesta integração.

MID Server

Uma aplicação Now Platform que facilita a comunicação e a movimentação de dados entre a Now Platform e aplicações, fontes de dados e serviços externos. Um MID Server normalmente é necessário para integração com tecnologias no local, mas um MID Server pode ser implantado em determinados casos entre o Now Platform e uma oferta baseada em nuvem quando um componente fornecido pelo cliente é necessário para a integração. Para esta integração de serviços Microsoft Exchange Online, o MID Server facilita a comunicação entre o Now Platform e o servidor PowerShell.

Servidor PowerShell

O servidor PowerShell é uma aplicação da Microsoft que requer as credenciais da sua conta da Microsoft.

Administrador de incidentes de segurança (sn_si.admin)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O usuário com a função sn_si.admin supervisiona a configuração da integração com o produto SIR em sua instância Now Platform. O usuário com esta função também aprova as solicitações de exclusão de e-mails por padrão e atribui a função sn_si.analyst conforme necessário. O usuário com esta função também tem controle total sobre todos os dados Gestão de serviços.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com a função sn_si.analyst interage e analisa incidentes de segurança no produto SIR.

Conexão de sistemas externos para pesquisa e exclusão de e-mail

Esta aplicação usa o serviço do PowerShell da Central de segurança e conformidade do Office 365 e o serviço da API de gráficos globais para recuperar informações do locatário do serviço do Office 365 Exchange Online. Uma conexão HTTPS de saída do MID Server para este ambiente é necessária para que a integração funcione corretamente.

A arquitetura de integração oferece suporte a uma capacidade de pesquisa e exclusão de e-mail no serviço Microsoft Exchange Online. A arquitetura de integração tem como alvo e-mails de phishing, bem como outras ameaças de e-mail que podem comprometer a segurança da sua organização. Para obter e-mails que correspondam a determinados critérios de consulta de pesquisa, o Now Platform se conecta a um locatário de serviço Microsoft Exchange Online usando um MID Server que executa o PowerShell em um servidor Windows.

Depois que o Now Platform estiver conectado ao serviço Microsoft Exchange Online, a integração oferecerá suporte aos seguintes níveis de pesquisas de e-mail:

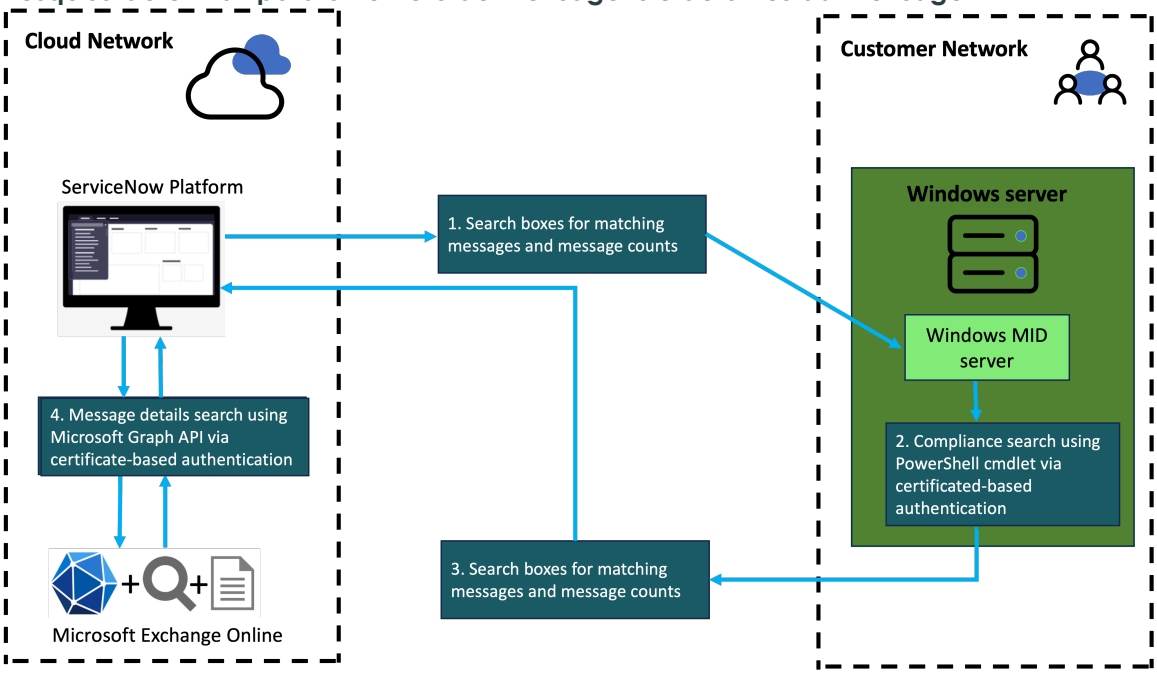
- As mensagens correspondentes: esta pesquisa é realizada por meio do cmdlet do Microsoft PowerShell por meio de um MID Server do Windows que é um componente do Now Platform. Esta pesquisa é baseada em critérios que você configura no Now Platform de um incidente de segurança. O primeiro componente da pesquisa retorna todas as mensagens de e-mail que correspondem aos critérios de pesquisa que você configurou, além dos endereços de caixa de correio específicos onde essas mensagens podem ser encontradas em Microsoft Exchange Online. Os parâmetros de pesquisa compatíveis são Assunto, Remetente e Destinatário da mensagem de e-mail (o valor exibido no campo Para em uma mensagem de e-mail).
- Os detalhes da mensagem: depois que a pesquisa inicial baseada em cmdlet do PowerShell identifica as mensagens correspondentes, essa pesquisa recupera informações adicionais da mensagem usando a Microsoft Global Graph API. Os resultados de e-mail retornados incluem os seguintes detalhes da mensagem:
  - Status de leitura: o status verdadeiro ou falso é rastreado quando os usuários leem e-mails.
  - Endereço do remetente.
  - Endereço do destinatário: esses endereços incluem indivíduos, um grupo e indivíduos que são copiados e copiados nas mensagens.
  - Excluir status: o status verdadeiro ou falso rastreia e-mails excluídos.
  - ID da mensagem: o identificador alfanumérico das mensagens de e-mail.

O fluxo de dados básico do e-mail pesquisa o número de mensagens e os detalhes da mensagem são ilustrados na figura a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de e-mail para o número de mensagens e detalhes da mensagem



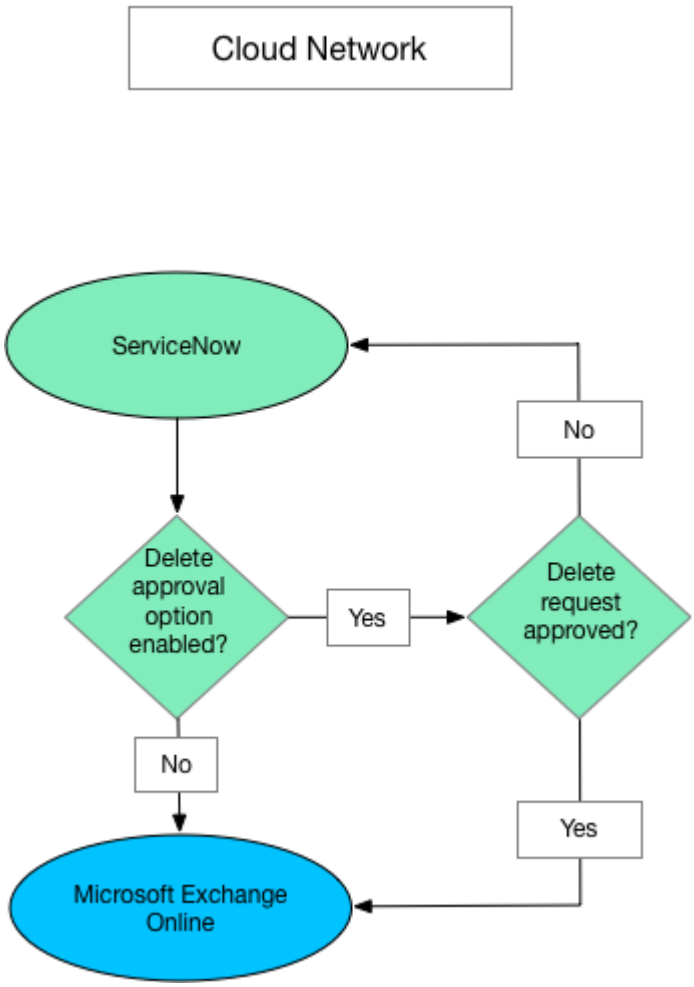
Para exclusão de e-mail, a integração usa a API Graph Global. A recuperação de e-mails excluídos está disponível como uma opção durante a etapa de configuração e é descrita com mais detalhes em Configure a integração Microsoft Exchange Online com sua instância Now Platform.

O fluxo de dados para exclusão de e-mail com o processo de aprovação pré-configurado é ilustrado na figura a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exclusão de e-mail



Fluxos de trabalho

A aplicação Microsoft Exchange Online para pesquisa e exclusão de e-mail inclui os seguintes fluxos de trabalho:

- Exchange Online-E-mails excluídos
- Obter detalhes de e-mail do Exchange Online.
- Microsoft Exchange Online -Pesquisa e exclusão de e-mail.

Para obter mais informações, consulte Introdução aos fluxos de trabalho .

Agora você está pronto para configurar as contas necessárias para a integração.

Recuperar e-mails excluídos no serviço Microsoft Exchange Online

(Opcional) Como administrador do Microsoft Exchange, você pode recuperar e-mails excluídos se a correção de incidentes exigir que você recupere os e-mails excluídos pelo fluxo de trabalho desta integração.

Antes de Iniciar

Para obter mais informações sobre como essa integração exclui e-mails, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre a função administrativa no produto Microsoft Office 365, incluindo informações sobre como recuperar itens excluídos em uma caixa de correio do usuário, consulte Sobre a função de administrador do Exchange Online .

Função necessária: administrador, administrador do Microsoft Exchange

Por Que e Quando Desempenhar Esta Tarefa

Se você selecionar a opção **Recuperar e-mails excluídos** na guia Configurações adicionais durante a etapa de configuração, habilitará a recuperação de e-mails excluídos no seu locatário Microsoft Exchange Online. Os e-mails excluídos usando o fluxo de trabalho de exclusão desta integração são colocados na subpasta Itens excluídos da pasta Itens recuperáveis na caixa de correio do usuário no serviço Microsoft Exchange Online. Se a conta do usuário estiver configurada no locatário Microsoft Exchange Online para que o usuário possa exibir a pasta Itens excluídos, o usuário poderá recuperar esses e-mails usando o serviço Microsoft do Outlook na Web. Como alternativa, o administrador Microsoft Exchange Online pode recuperar e-mails excluídos de uma pasta Itens excluídos de um usuário. Consulte Recuperar itens ou e-mails excluídos no Outlook Web App para obter mais informações.

Função necessária: administrador [Microsoft Exchange Online ou administrador global Microsoft para recuperar e-mails excluídos.

Função necessária: sn_si.admin no Now Platform para habilitar a opção Recuperar e-mails excluídos.

Função necessária: sn_si.analyst no Now Platform para concluir uma pesquisa bem-sucedida de e-mails e verificar se os e-mails foram excluídos com sucesso antes da recuperação.

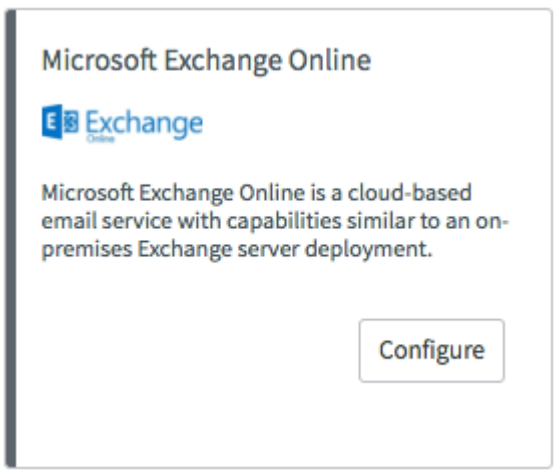
Procedimento

Para habilitar a opção de recuperação de e-mail, siga estas etapas.

a. Navegar até **Operações de segurança** > **Integrações** > **Configurações**.

b. Localize o bloco Microsoft Exchange Online.

c. Clique em **Configurar**.

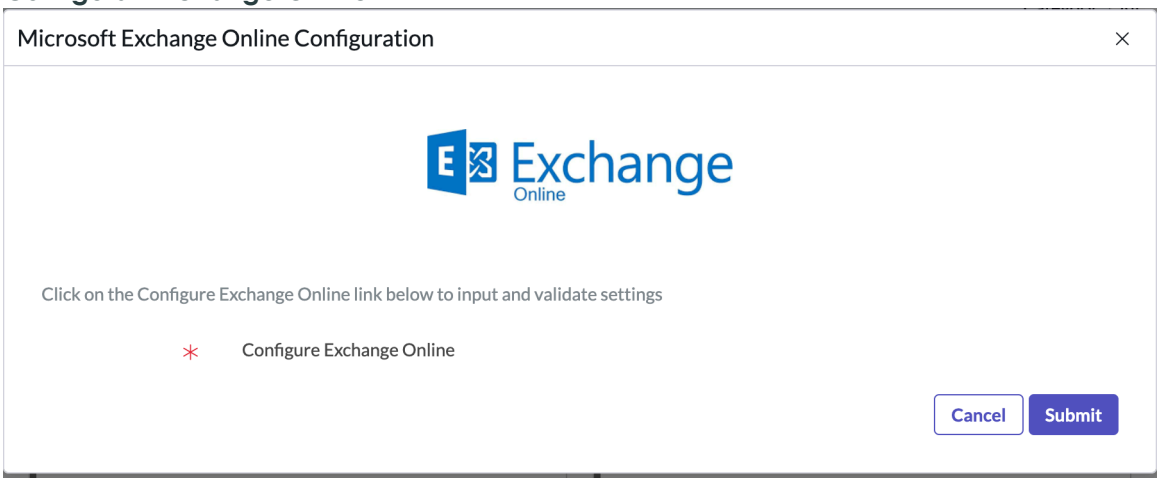


d. Na caixa de diálogo Microsoft Exchange Online Configuração exibida, clique em **Configurar Exchange Online**.

Tradução automática

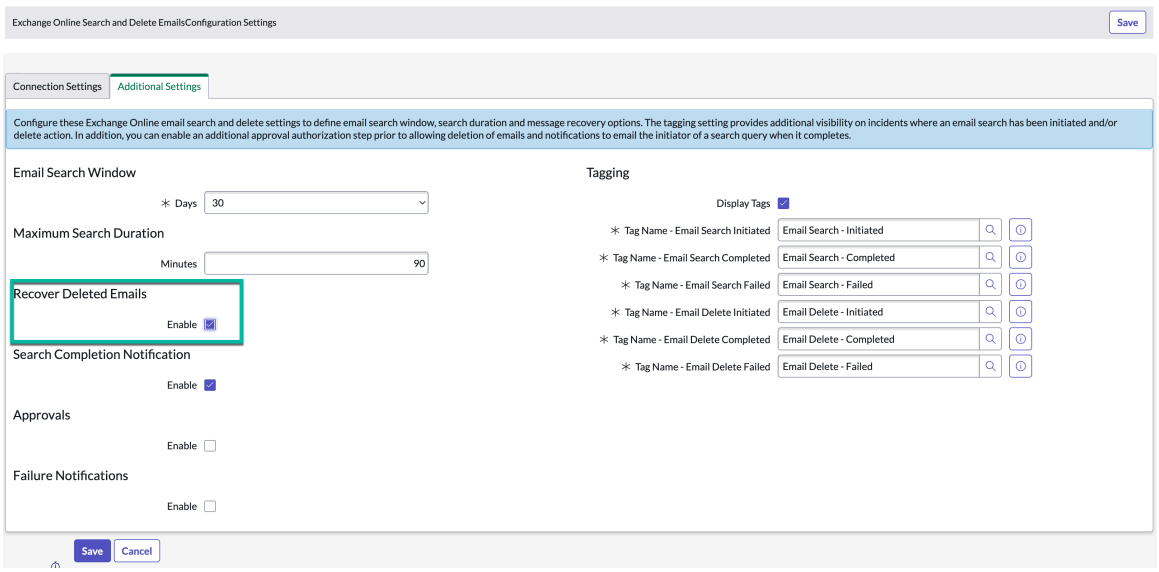
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar Exchange Online



e. Na guia `Configurações adicionais`, em `Recuperar e-mails excluídos`, marque a caixa de seleção **Habilitar**.

Recuperar e-mails excluídos



f. Verifique todas as outras configurações e clique em **Enviar**.

g. Para verificar se uma pesquisa e exclusão de mensagens de e-mail foram concluídas com sucesso para as mensagens de e-mail que você deseja recuperar, navegue até o incidente de segurança que registrou os fluxos de trabalho de pesquisa e exclusão de e-mail.

h. Localize as anotações de trabalho e verifique se o sistema excluiu as mensagens com sucesso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Como administrador Microsoft Exchange Online ou administrador global, faça login na sua conta Microsoft do Office 365.

j. Siga as etapas descritas em Recuperar itens ou e-mails excluídos no Outlook Web App no site de documentação Microsoft.

Editar marcadores de segurança na Now Platform para a integração Microsoft Exchange Online

Você pode editar os nomes e as cores dos marcadores de segurança em sua instância Now Platform® para a integração Microsoft Exchange Online. Esses marcadores de segurança ajudam a identificar rapidamente quando a pesquisa de e-mail é concluída ou falha. Eles também identificam quando as solicitações para excluir e-mails são iniciadas e quando os itens de e-mail são excluídos com sucesso.

Antes de Iniciar

Por padrão, os marcadores de segurança serão habilitados na instância Now Platform® se você selecionar a opção **Exibir** marcadores durante a etapa de configuração. Você pode editar cores e nomes de marcadores e atribuir marcadores a grupos de marcadores de segurança para ajudá-lo a organizá-los em sua instância Now Platform®. Por exemplo, você pode mudar as cores dos marcadores para que o marcador de início de uma capacidade seja de uma cor e o marcador de conclusão seja de outra cor para corresponder aos outros marcadores de segurança habilitados na instância Now Platform®. Essas cores diferentes podem ajudar a identificar rapidamente quando os fluxos de trabalho são iniciados e concluídos com sucesso. Se você decidir que não precisa de um marcador específico, sem desabilitar a marcação para a integração, também poderá desabilitar um único marcador do registro de marcadores. Se desabilitado, este marcador não será mais exibido nos incidentes de segurança relacionados. Para obter mais informações sobre como configurar grupos de marcadores de segurança e marcadores, consulte Configurar grupos de marcadores de segurança e marcadores no site de documentação de produtos da ServiceNow .

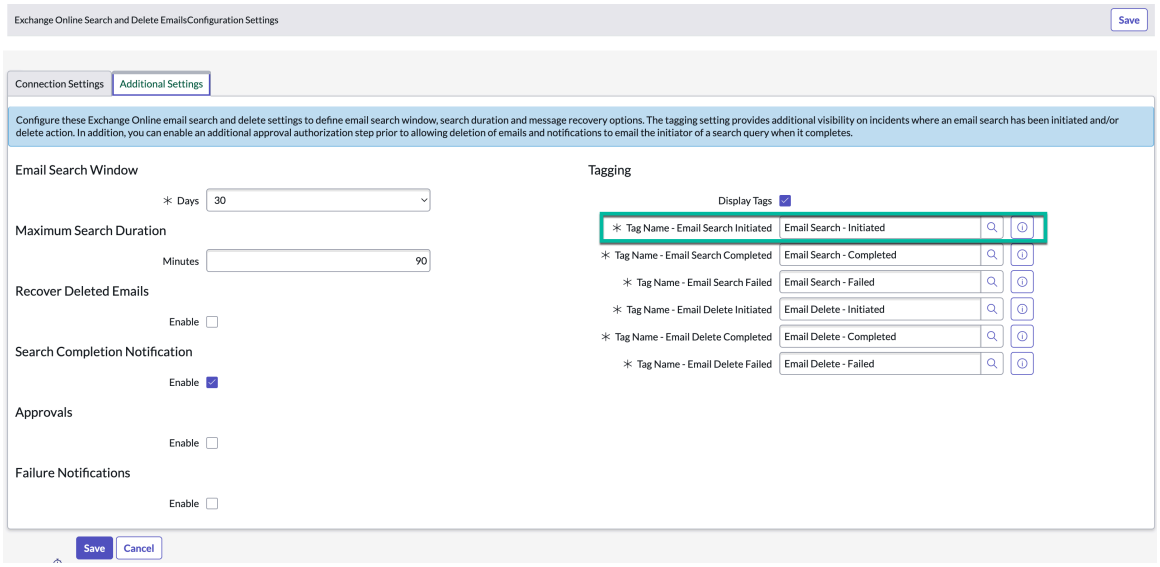
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Integrações** > **Configurações do Exchange Online**.
2. Clique na guia **Configurações adicionais** para selecioná-la.
3. Na guia exibida, se a opção **Exibir** marcadores estiver desmarcada, selecione-a para exibir os nomes dos marcadores.
4. Com os nomes de marcador exibidos, à direita de um marcador, clique no ícone de informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na caixa de diálogo Marcador de segurança exibida, clique em **Abrir registro**.

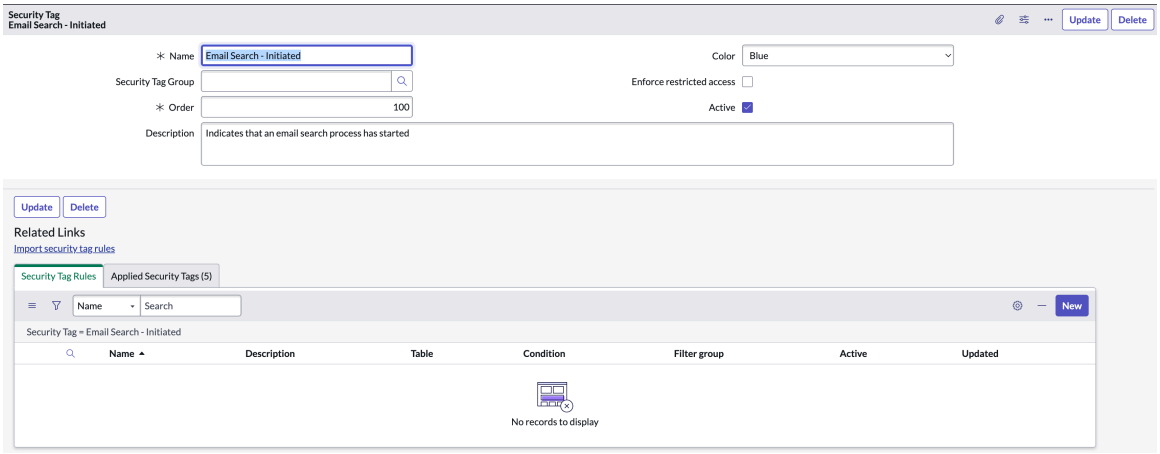
6. No registro exibido, edite os campos.

Opção	Descrição
Nome	Nome exclusivo do marcador de segurança.
Cor	Cor do marcador de segurança. Selecione uma cor na lista de seleção.
Grupo de marcadores de segurança	Nome do grupo de marcadores de segurança. Clique no ícone de informações para exibir os grupos disponíveis. O padrão é Grupo de metatags.
Impor acesso restrito	Selecione esta opção para atribuir funções de leitura e gravação necessárias para os usuários lerem ou gravarem em registros que têm este marcador de segurança. O padrão é limpo.
Ordem	Especifique a ordem em que o marcador aparece em formulários ou em uma lista. O padrão é 100. Para definir a ordem na lista, insira um valor. Por exemplo, 100, 200, 300, 400. O marcador com o número mais baixo é exibido primeiro na lista. O perfil com o número mais alto é exibido por último.
Ativo	Ative ou desative este marcador. O padrão é selecionado (ativo)
Descrição	Descrição do marcador.

7. Clique em **Atualizar** para salvar suas mudanças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Agora você editou com sucesso o registro de marcador de um marcador de segurança.

Check-list para a integração Microsoft Exchange Online

Use esta check-list para se orientar nas tarefas de ponta a ponta da integração. A check-list a seguir inclui tarefas de configuração e instalação, exemplos de casos de uso e resultados esperados para a aplicação.

Antes de Iniciar

Acompanhe o andamento da configuração, instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada etapa identifica as funções necessárias para executar as tarefas e faz referência aos tópicos numerados do guia de instalação e configuração desta integração.

Funções necessárias: as funções são listadas para cada etapa na tabela a seguir.

Procedimento

Para acompanhar o andamento da integração, siga as etapas na tabela na ordem em que são apresentadas

Check-list

☐	Como Microsoft administrador do Office 365, configure sua Microsoft conta do Office 365. Crie uma conta de API que permita o acesso ao Centro de segurança e conformidade no Microsoft Office 365.
☐	Como administrador do Microsoft Azure, configure sua conta do Microsoft Azure. Crie uma conta que usa uma ID de aplicação para coletar detalhes adicionais da mensagem de e-mail e excluir mensagens de e-mail. Para obter as etapas para configurar a conta, consulte Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online.
☐	Como administrador Now Platform, configure sua instância Now Platform para a integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Para tarefas e mais informações, consulte Configure sua instância Now Platform para a integração Microsoft Exchange Online. **a.** Atribua Now Platform funções. **b.** Configure um MID Server em sua instância Now Platform. **c.** Instale as aplicações Now Platform (SIR) e Operações de segurança do ServiceNow Store e ative-as em sua instância. **d.** Habilite os recursos de envio e recebimento de e-mail. **e.** Atribua a função de leitura e gravação de e-mail ao sn_si.analyst. **f.** Crie um grupo de aprovação.
☐	Como Now Platform administrador, instale a aplicação para a integração a partir do ServiceNow Store. Para obter as etapas de instalação, consulte Instalar a aplicação Microsoft Exchange Online para a integração ServiceNow Microsoft Exchange Online.
☐	Como sn_si.admin, conclua as guias de definições de configuração para estabelecer conectividade e ativar os fluxos de trabalho de pesquisa e exclusão. Para definições de conexão e configuração, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.
☐	Como sn_si.analyst, configure os critérios de pesquisa de e-mail e solicite uma pesquisa de e-mails correspondentes no servidor Microsoft Exchange Online. Para obter um exemplo, consulte Definir critérios de pesquisa de e-mail e solicitar uma pesquisa no serviço Microsoft Exchange Online. **a.** Localize incidentes de segurança relacionados a eventos de phishing. **b.** Configure os critérios de pesquisa de e-mail. **c.** Solicite uma pesquisa de e-mails. **d.** Localize os resultados da pesquisa e os detalhes da mensagem nas listas relacionadas ao incidente de segurança.
☐	Como sn_si.analyst, exclua e-mails do servidor Microsoft Exchange Online. Para obter um exemplo, consulte Solicitar aprovação de exclusão para e-mails no serviço online do Microsoft Exchange. **a.** Localize o incidente de segurança com os resultados da pesquisa. **b.** Exclua e-mails ou solicite aprovação para excluir e-mails. **c.** Verifique se os e-mails foram excluídos dos resultados publicados nas anotações de trabalho e nas listas relacionadas no incidente de segurança.
☐	Como sn_si.admin ou, como membro de um grupo de aprovação, processa solicitações de exclusão por e-mail por meio de notificações por e-mail.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Para obter um exemplo, consulte Aprovar solicitações de exclusão de e-mail para a integração Microsoft Exchange Online.

Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.

Solução de problemas de integração do Microsoft Exchange Online

Depois de configurar com sucesso a aplicação Microsoft Exchange Online e configurar sua instância Now Platform, se você tiver problemas de pesquisa de e-mail, poderá executar testes de diagnóstico com base em critérios específicos.

Antes de Iniciar

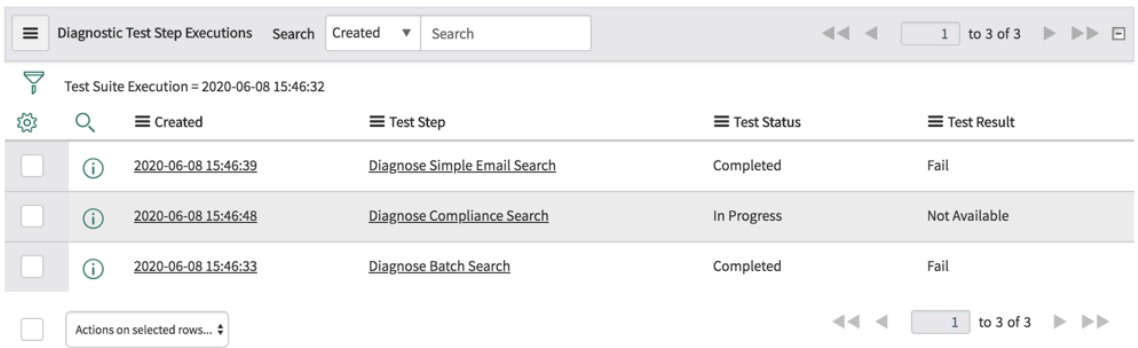
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Os resultados desses testes podem ajudar o ServiceNow Suporte ao cliente a identificar e solucionar os problemas.

Procedimento

1. Navegar até **Todos** > **Diagnósticos do Exchange Online** > **Iniciar testes de diagnóstico**.
2. Insira os seguintes detalhes:
   - Insira o Remetente e um ou mais endereços de e-mail do Destinatário para restringir os critérios de pesquisa e fornecer resultados mais precisos.
   - Especifique o Assunto para o qual os testes de diagnóstico estão sendo realizados. Este é um campo obrigatório.
3. Clique em **Enviar**.
4. Para exibir os resultados dos testes de diagnóstico, navegue até **Diagnósticos do Exchange Online** > **Exibir Resultados de testes de diagnóstico**.
   A coluna Status mostra os seguintes status:
   - Concluído – Aprovado: os testes foram concluídos com sucesso.
   - Concluído - Falhas: os testes foram concluídos com alguns erros.
   - Em andamento: os testes ainda estão em execução e não foram concluídos.
5. Clique em Execução do pacote de testes de diagnóstico para ver os detalhes da execução de testes.



Os seguintes tipos de testes de diagnóstico são executados:

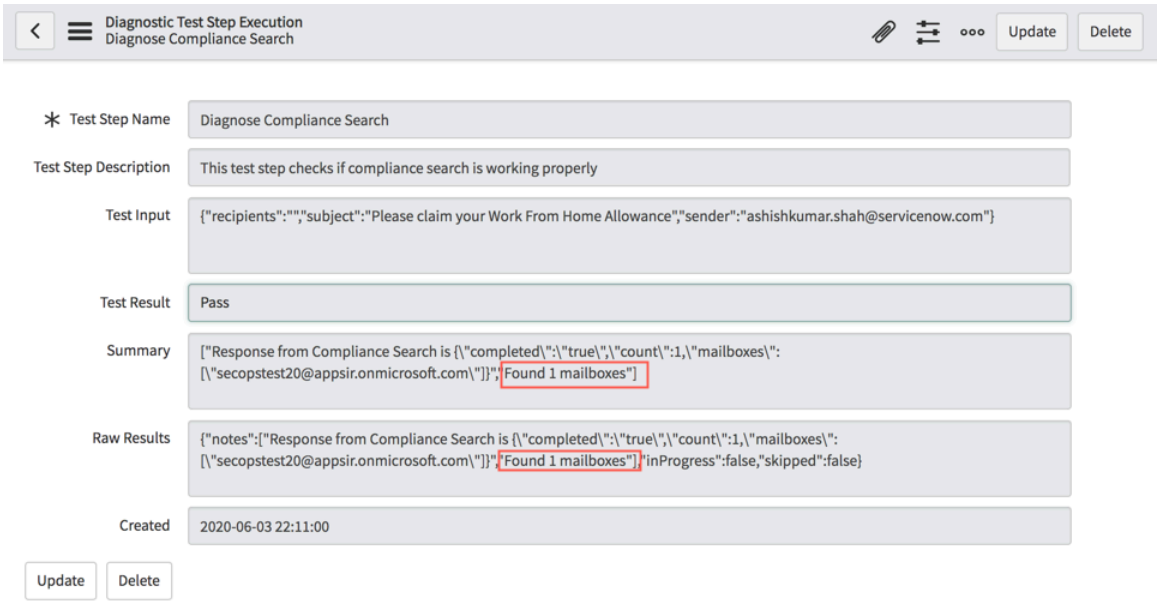
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Diagnosticar pesquisa de conformidade: gera uma lista de caixas de correio de e-mail de destinatários executando uma pesquisa de conformidade.
- Diagnosticar pesquisa de e-mail simples: pesquisa caixas de correio de e-mail fazendo chamadas REST separadas para pesquisar cada pasta do destinatário.
- Diagnosticar pesquisa em lote – pesquisa caixas de correio em uma consulta em lote, combinando várias pesquisas em uma chamada REST.

Para executar os testes 2 e 3, você deve especificar os endereços de e-mail dos destinatários na página Iniciar testes de diagnóstico. Se eles não forem especificados, os testes não serão realizados.

6. Clique no link Criado na página Execução do pacote de testes de diagnóstico para exibir os resultados de testes em detalhes.



A imagem acima mostra os resultados detalhados da execução da etapa Diagnóstico de conformidade Teste de pesquisa e mostra a contagem de caixas de correio encontradas na pesquisa.

Importante: Para obter mais cenários e problemas de solução de problemas, consulte KB1501969: Configuração e solução de problemas da autenticação baseada em certificados para integração do Exchange Online

Integração do Microsoft Exchange no Local

A integração Microsoft Exchange no local fornece ferramentas para os analistas de segurança conterem e erradicarem ameaças de e-mail de phishing e Spear Phishing em instâncias no local.

Explorar Integrações do Security Incident Response	**Configurar** Introdução à integração com o Microsoft Exchange no local
Usar Pesquisar e excluir e-mails de phishing	**Desenvolver**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução à integração com o Microsoft Exchange no local

A integração Microsoft Exchange no local fornece ferramentas para que os analistas de segurança contenham e corrijam ameaças de e-mail de phishing e Spear Phishing em instâncias no local. Antes de poder usar a integração Microsoft Exchange no local, você deve baixá-la do ServiceNow Store e identificar os servidores Exchange e MID apropriados.

Antes de Iniciar

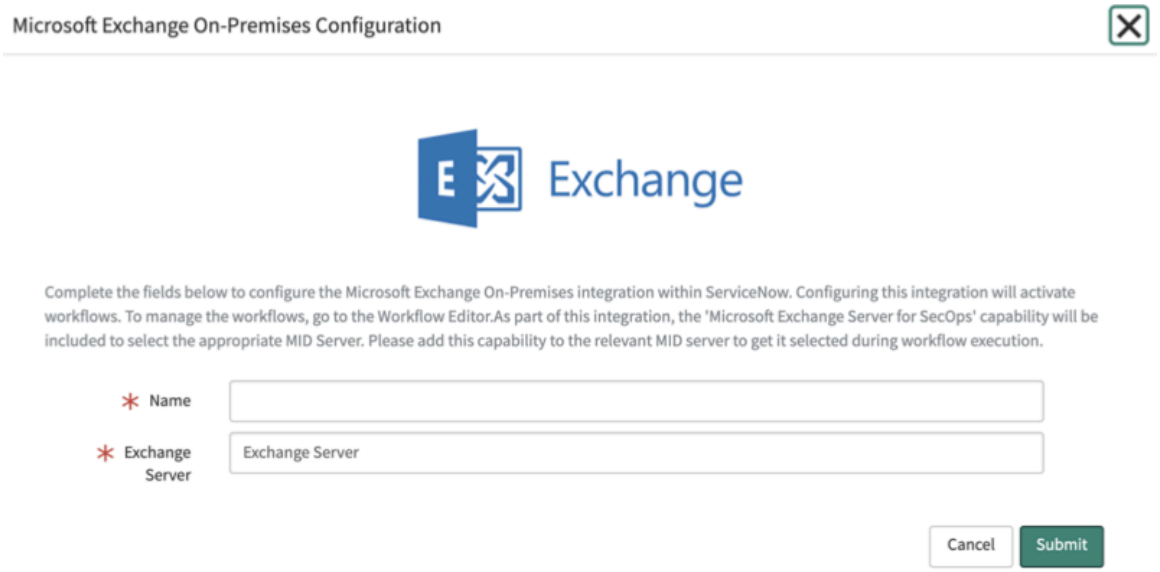
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação do sistema operacional for concluída, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão Microsoft Exchange No local, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



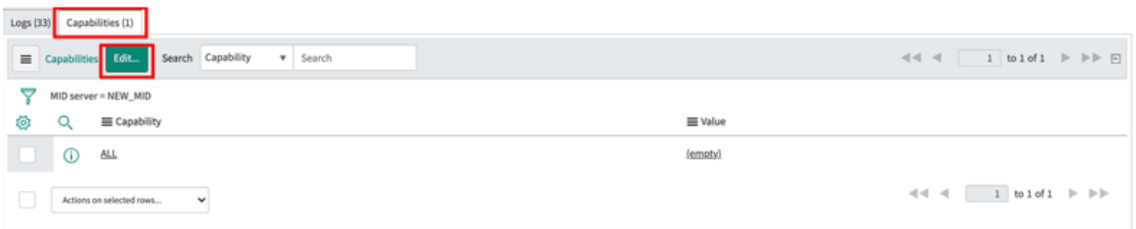
4. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Exchange Server	Especifique o servidor do Exchange a ser usado.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.
8. Navegar até **Orquestração** > **MID Servers**.
9. Abra o registro e verifique o status do MID Server que pode ser acessado pelo Exchange Server e se a opção **Status** está definida como **Ativo** e a opção **Validado** como **Sim**.
10. Adicione a capacidade do MID server:
    - Selecione o respectivo MID Server para adicionar a capacidade.
    - Clique na lista relacionada **Capacidades** e clique em **Editar**.

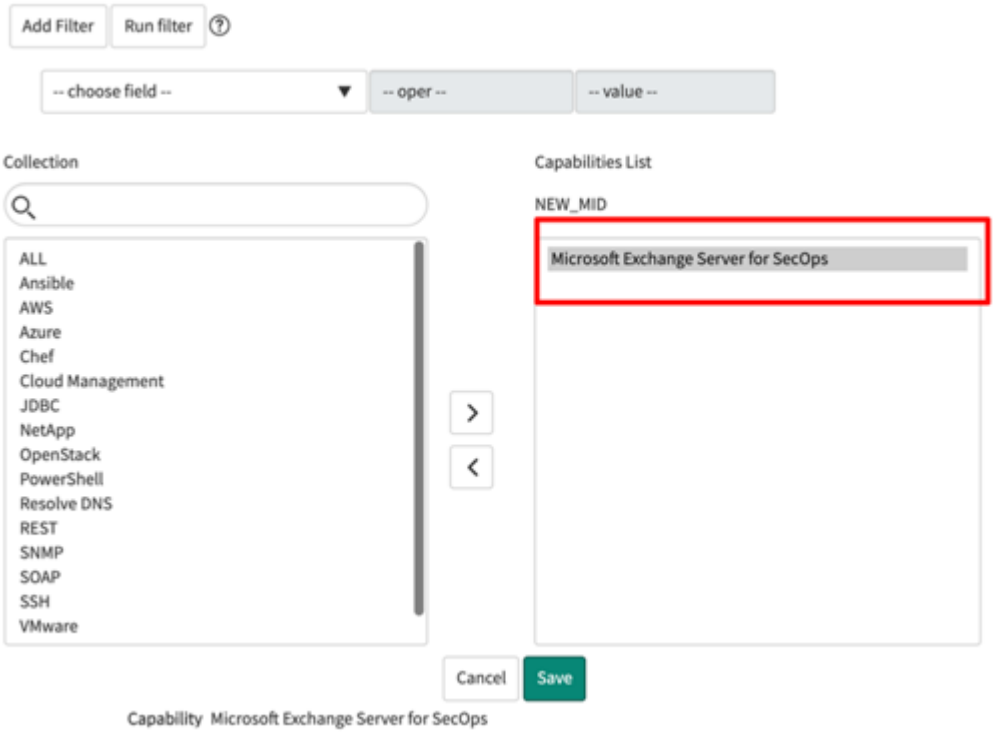
Capacidade do MID Server



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

◦ Remover **tudo** e adicionar **o Microsoft Exchange Server para SecOps**.



◦ Selecione os **Intervalos de IP** na seção **Listas relacionadas** e defina o valor como **TODOS** ou qualquer valor desejado.

◦ Selecione as **Aplicações compatíveis** na seção **Listas relacionadas** e defina o valor como TODOS ou Orquestração.

◦ **Salve** o registro.

11. Valide as conexões e credenciais.

12. Depois que as credenciais forem validadas, a configuração na instância da ServiceNow estará concluída e pronta para executar operações de pesquisa e exclusão de e-mail usando esta integração.

Microsoft Exchange - Executar fluxo de trabalho de pesquisa e exclusão de e-mail

Quando o fluxo de trabalho **Microsoft Exchange - Executar pesquisa e exclusão de e-mail** é executado, ele pesquisa o servidor do Exchange usando a consulta de pesquisa fornecida e retorna os detalhes para a instância no local.

Antes de Iniciar

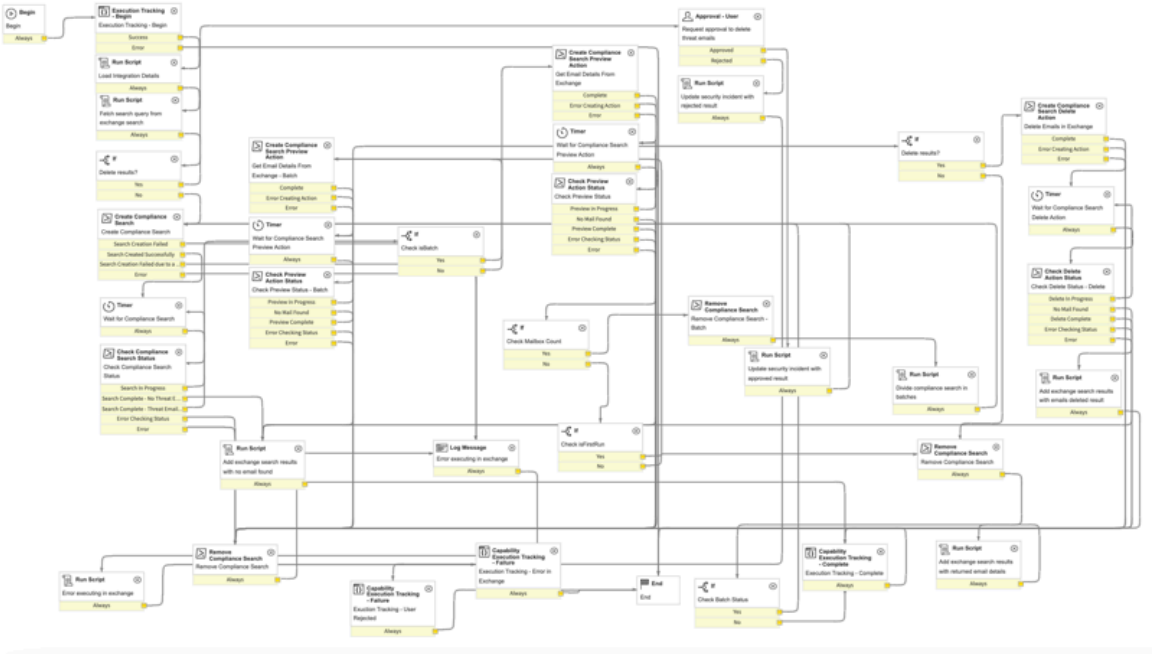
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Microsoft Exchange - Executar Pesquisa e Exclusão de E-mail** é executado quando as pesquisas de e-mail são configuradas e o botão **Excluir do(s) Servidor(es)de E-mail ou Pesquisar no(s) Servidor(es) de E-mail** é pressionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades de fluxo de trabalho incluem:

- Criar atividade de pesquisa de conformidade
- Atividade Verificar status de pesquisa de conformidade

Criar atividade de ação de visualização da pesquisa de conformidade

A atividade Criar ação de visualização de pesquisa de conformidade cria uma nova ação de pesquisa de conformidade do tipo visualização no servidor do Exchange para a pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.
pesquisarNome	Nome obrigatório da pesquisa de conformidade criada no servidor do Exchange.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Concluir	Quando a ação de pesquisa de conformidade é criada com sucesso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de Saída

Variável	Descrição
Erro ao criar ação	Quando a criação da ação de pesquisa de conformidade falha devido a uma exceção no servidor do Exchange.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Atividade Verificar status da ação de visualização

A atividade Visualizar status da ação verifica o status da ação de pesquisa de conformidade do tipo visualização e retorna as informações de visualização dos e-mails encontrados, como destinatário, remetente, assunto e data de recebimento do e-mail.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.
pesquisarNome	Nome obrigatório da pesquisa de conformidade criada no servidor do Exchange.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da ação de pesquisa de conformidade e as informações de visualização do e-mail encontrado como parte da pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Visualização em andamento	Quando o status da ação de pesquisa de conformidade está em andamento.
Nenhum e-mail encontrado	Quando o status da ação de pesquisa de conformidade é concluído e nenhum e-mail é encontrado como parte da pesquisa de conformidade.
Exibição concluída	Quando o status da ação de pesquisa de conformidade é concluído, os e-mails são encontrados como parte da pesquisa de conformidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de Saída

Variável	Descrição
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no servidor do Exchange.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Criar atividade de ação de exclusão de pesquisa de conformidade

A atividade Criar ação de exclusão de pesquisa de conformidade cria uma nova ação de pesquisa de conformidade do tipo limpeza no servidor do Exchange para a pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.
pesquisarNome	Nome obrigatório da pesquisa de conformidade criada no servidor do Exchange.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Concluir	Quando a ação de pesquisa de conformidade é criada com sucesso.
Erro ao criar ação	Quando a criação da ação de pesquisa de conformidade falha devido a uma exceção no servidor do Exchange.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Atividade Verificar status da ação de exclusão

A atividade Verificar status da ação de exclusão verifica o status da ação de pesquisa de conformidade do tipo limpeza e executa a operação de exclusão reversível no servidor do Exchange para os e-mails encontrados como parte da pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
pesquisarNome	Nome obrigatório da pesquisa de conformidade criada no servidor do Exchange.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da ação de pesquisa de conformidade e a contagem de e-mails excluídos que foram encontrados como parte da pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Exclusão em Andamento	Quando o status da ação de pesquisa de conformidade está em andamento.
Nenhum e-mail encontrado	Quando o status da ação de pesquisa de conformidade é concluído, nenhum e-mail é excluído como parte da pesquisa de conformidade.
Exclusão concluída	Quando o status da ação de pesquisa de conformidade é concluído, os e-mails são excluídos como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no servidor do Exchange.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Remover atividade de pesquisa de conformidade

A atividade Remover pesquisa de conformidade remove a pesquisa de conformidade criada do servidor do Exchange.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.
pesquisarNome	Nome obrigatório da pesquisa de conformidade criada no servidor do Exchange.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de ingestão de alerta da API de segurança do Microsoft Graph

Use a integração API de Segurança do Microsoft Graph para ingerir alertas de provedores de segurança do Microsoft Graph e criar incidentes de segurança automaticamente.

Visão geral

O API de Segurança do Microsoft Graph é um serviço intermediário (ou agente) que fornece uma única interface programática para conectar vários provedores de segurança (nativo para Microsoft e parceiros da ServiceNow).

A integração API de Segurança do Microsoft Graph resolve esses problemas usando o API de Segurança do Microsoft Graph para se conectar a diferentes tecnologias de segurança da Microsoft, como Azure Sentinel, Proteção Avançada contra Ameaças do Microsoft Defender e Proteção Avançada contra Ameaças do Azure. Os alertas dos provedores de segurança da Microsoft são ingeridos e os incidentes de segurança são criados automaticamente em Security Incident Response.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Descoberta de API de Segurança do Microsoft Graph alertas que são candidatos a incidentes de segurança e automatizam a criação de incidentes de segurança.
- Mapeamento de campos de alerta para campos de incidente de segurança.
- Agregação de alertas semelhantes a incidentes de segurança abertos existentes em vez de criar incidentes de segurança duplicados.
- Visualize os valores do campo de alerta e valide seus mapeamentos no incidente de segurança.
- Atualização automática de status de alerta para criação e fechamento de incidentes de segurança.
- Configure a ingestão programada de alertas para criar incidentes de segurança periodicamente.

Configurar sua instância da Now Platform para a integração da API de segurança do Microsoft Graph

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação a partir do ServiceNow Store.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response.	As funções a seguir são necessárias para a instalação, configuração e uso da integração em sua instância Now Platform®.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	• Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®: ◦ Nomeia, cria e edita perfis de alerta. ◦ Seleciona e mapeia campos de dados de alerta da API de segurança do Microsoft Graph para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão de alertas contínuos. ◦ Habilita atualizações de alerta quando um incidente Security Incident Response é criado e fechado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e como atribuir funções a usuários, consulte Funções no site de documentação de produtos da Servicenow .
Registre sua aplicação no portal Microsoft Azure.	Antes de ingerir alertas, você deve configurar sua aplicação no portal Microsoft Azure. Consulte Configurar o portal do Microsoft Azure para obter detalhes.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Ingestão de eventos e alertas para Operações de segurança: esta aplicação requer:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	◦ com.glide.hub.integration.runtime => Tempo de execução do IntegrationHub da ServiceNow ◦ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in Event and Alert Ingestion. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

Configurar o portal do Microsoft Azure

Para recuperar alertas de segurança de uma aplicação disponível no locatário do Microsoft Azure usando o API de Segurança do Microsoft Graph, você deve registrar a aplicação no portal Microsoft Azure e conceder acesso de leitura e gravação a eventos de segurança para a aplicação.

Antes de Iniciar

Função necessária:

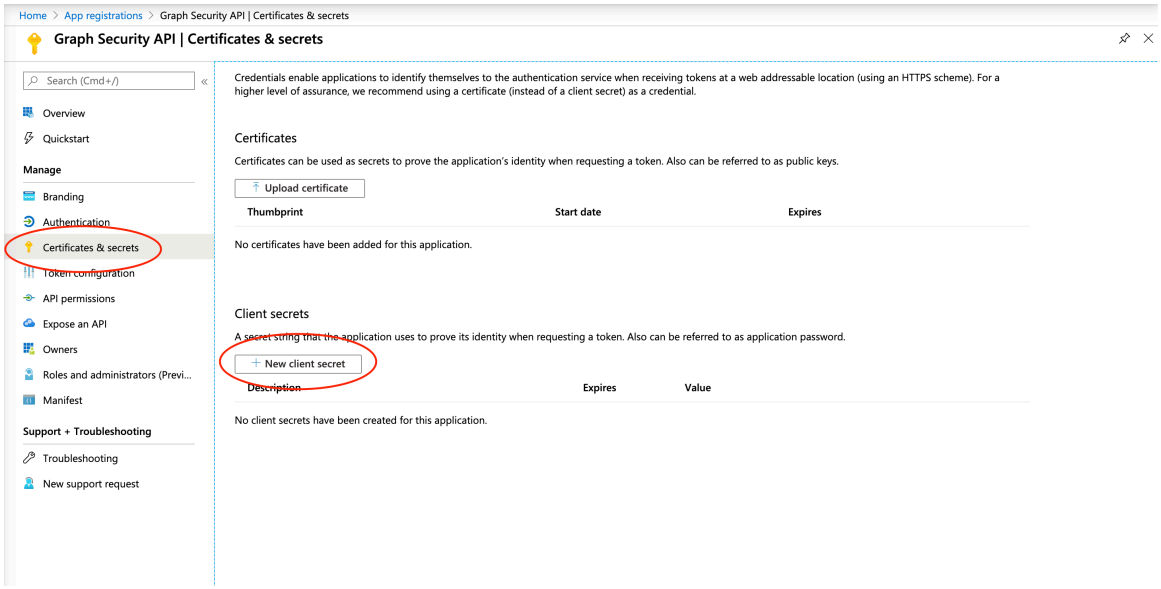
- Desenvolvedor de aplicações: necessário para registrar a aplicação.
- Administrador de locatário: o administrador de locatário Microsoft Azure deve conceder permissões à aplicação fazendo uma chamada para o endpoint de consentimento do administrador.

Procedimento

1. Faça login no portal Microsoft Azure.
2. Insira **Registros de app** na caixa **Pesquisar**.
3. Clique **em Novo registro**.
4. Insira um nome para sua aplicação e o URI de redirecionamento, por exemplo, http://localhost e clique em **Registrar**.
   O URI de redirecionamento é usado ao fornecer o consentimento do administrador para a aplicação.
5. Na página Registros de aplicações, selecione a aplicação que você registrou, por exemplo, Graph Security Demo.
6. Em **Gerenciar**, selecione **Certificados e segredos**.

Tradução automática

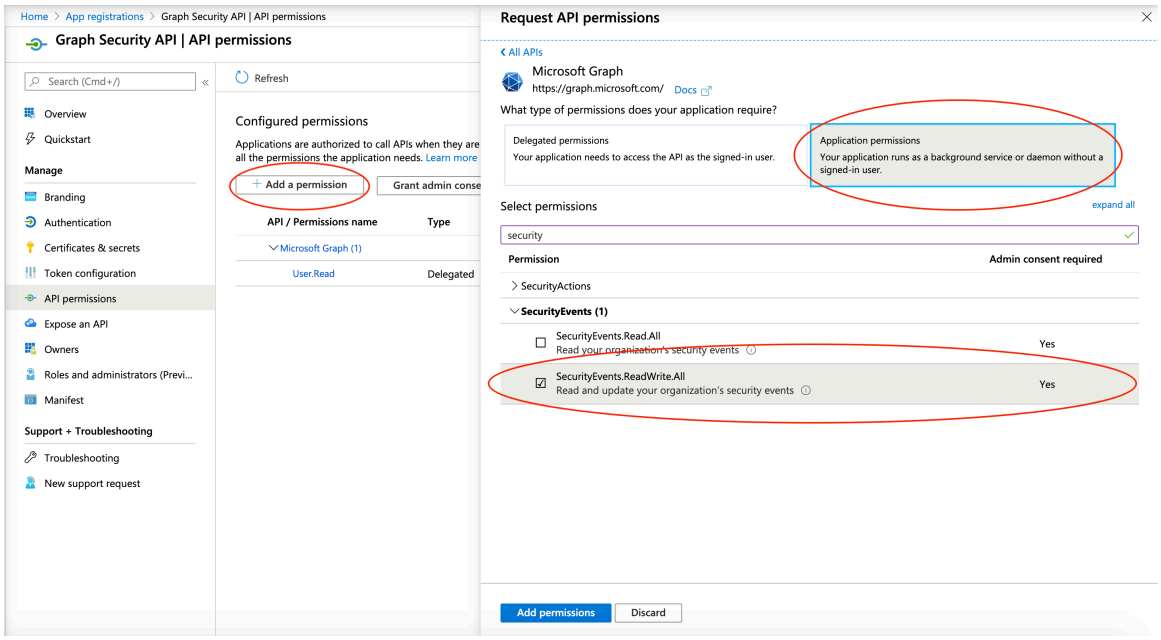
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Selecione **Novo segredo do cliente** para criar um segredo do cliente.
   Copie o segredo do cliente e salve-o, pois ele não ficará visível posteriormente. Caso você tenha esquecido o segredo do cliente, é possível gerar um novo segredo do cliente.

   Nota: Se você esquecer o segredo do cliente, poderá gerar um novo seguindo as instruções nas etapas 4 e 5.

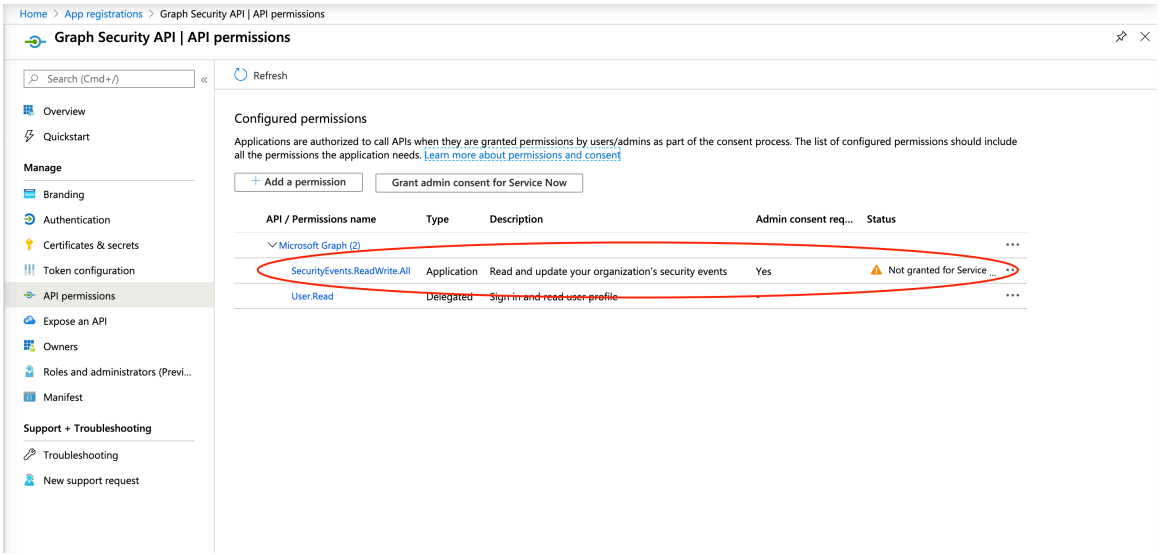
8. Clique em **Exibir permissões de API** na página Visão geral.
9. Adicione novas permissões de API no nível da aplicação para eventos de segurança SecurityEvents.ReadWrite.All.



10. Conceda consentimento de administrador para as permissões de API recém-adicionadas. Para obter mais informações, consulte Permissões do Microsoft Graph Modelo de permissão do Microsoft Graph.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Faça login como um administrador de locatário e forneça consentimento para a aplicação.
    As etapas são fornecidas abaixo:

    a. Navegue até o seguinte URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

    Insira o APPLICATION_ID da aplicação que você registrou.

12. Clique em **Aceitar** para aceitar as permissões solicitadas pela aplicação criada acima. Você pode usar a aplicação para ler eventos de segurança. Consulte a documentação de autorização de segurança do Microsoft Graph para obter mais detalhes.

Instalar e configurar a aplicação ServiceNow para integração de ingestão de alertas da API de segurança do Microsoft Graph

Antes de executar a integração em sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Operações de segurança em sua instância Now Platform.

Antes de Iniciar

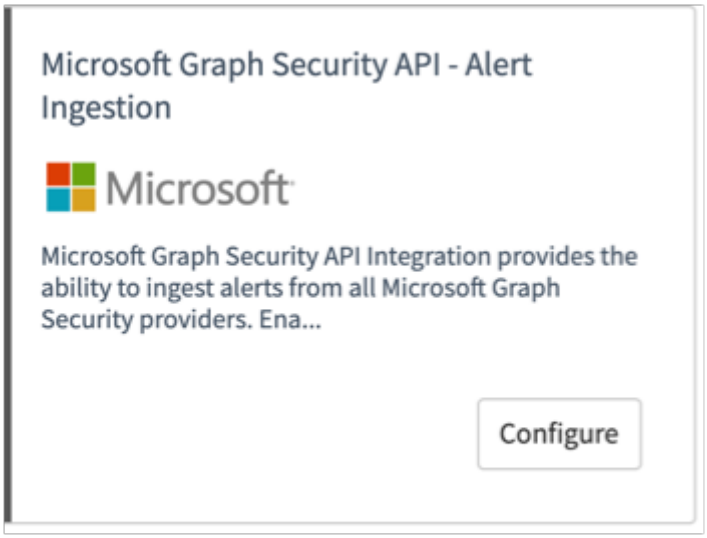
Função necessária: sn_si.admin

Procedimento

1. Se você não instalou a aplicação [API de Segurança do Microsoft Graph de ServiceNow Store para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize o bloco API de segurança do Microsoft Graph - Ingestão de alertas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

3. Para configurar a aplicação, clique em **Configurar**.
4. Na caixa de diálogo Configuração de ingestões de alerta exibida, preencha os campos.

Campo	Descrição
Nome	Nome da instância da nuvem Microsoft Azure. Você pode inserir somente valores alfanuméricos e hifens (-) neste campo.
ID de locatário	O Microsoft Azure ID do locatário. Esta é a instância da qual todos os alertas no portal Microsoft Azure são recuperados.
ID de cliente	O ID de cliente da aplicação que você registrou no portal Microsoft Azure. Consulte Configurar o portal do Microsoft Azure para obter detalhes.
Segredo do cliente	A senha da sua aplicação registrada.

5. Clique em **Enviar**.
   Depois de validadas e enviadas com sucesso, cada configuração do servidor de ingestão de alertas é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de alerta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um perfil para a integração de ingestão de alertas da API de segurança do Microsoft Graph

Como um usuário com a função sn_si.admin, você cria um perfil de alerta em sua instância Now Platform e determina quais alertas criam incidentes de segurança. Antes que os incidentes de segurança sejam criados a partir de alertas ingeridos, os valores de campo dos alertas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será exibido.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A integração permite ingerir diferentes tipos de alertas, como tentativas de acesso não autorizado e malware, por exemplo. Esses alertas são ingeridos com base nos perfis que você configura no ambiente Operações de segurança da sua instância. Todos os alertas são ingeridos inicialmente para um tipo de alerta configurado em um perfil. Os alertas ingeridos podem ser filtrados para especificar quais alertas criam incidentes de segurança.

Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para alertas identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de alertas ingeridos, os valores de campos individuais nos alertas filtrados são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização. Todos os alertas que atendem aos critérios de seleção em seu locatário Microsoft Azure e estão disponíveis em API de Segurança do Microsoft Graph são ingeridos inicialmente em sua instância Now Platform.

Identificar a origem do perfil

Especifique o nome e a origem do perfil.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para um alerta em sua instância Now Platform, navegue até **Integração da API de segurança do Microsoft Graph** > **Perfil da API de segurança do Microsoft Graph**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

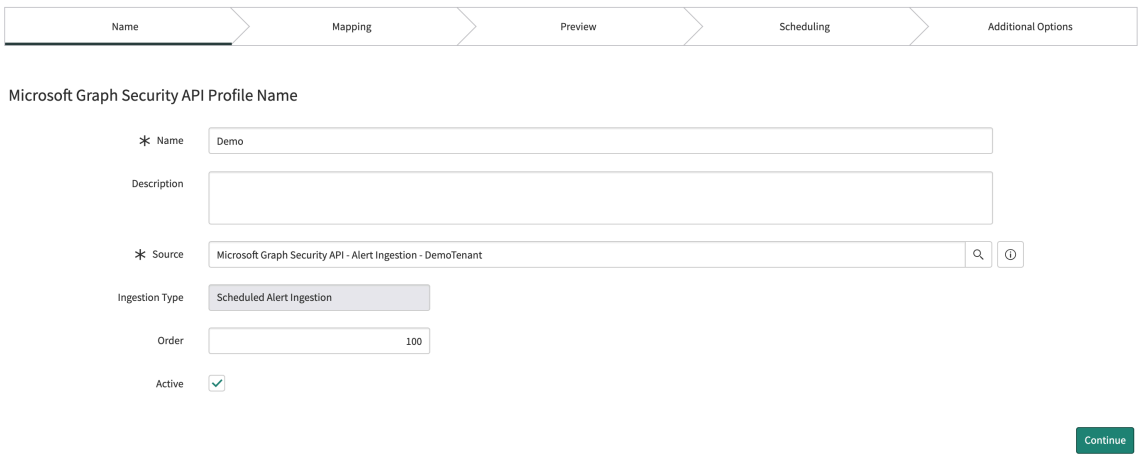
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e nomes de perfil duplicados não serão salvos. Os nomes de perfil em sua instância Now Platform devem ser exclusivos.
Ativo	A caixa de seleção está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Você deve concluir todas as seções no perfil antes de torná-lo ativo.
Origem	O locatário Microsoft Azure que você configurou para ingerir alertas. Se você tiver vários locatários configurados, selecione o locatário apropriado para os tipos de alerta que você planeja ingerir para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem as mesmas condições de acionamento. Quanto menor o valor do pedido, maior será a prioridade.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

A próxima etapa é mapear os campos de alerta.

Mapeamento de campos de alerta para integração de ingestão de alertas da API de segurança do Microsoft Graph

Depois de identificar as origens para ingestão de alertas programada, a próxima etapa é mapear campos de alerta individuais para os campos em um Now Platform SIR incidente de segurança.

Para a etapa de mapeamento, você deve primeiro ingerir alertas de amostra do locatário Microsoft Azure. Em seguida, você deve garantir que todos os dados de campo de alerta relevantes estejam mapeados para o local apropriado no formulário de incidente SIR e visualizar o incidente SIR na seção de visualização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O mapeamento dos campos de alerta de amostra envolve o seguinte:

- Ingerir exemplos de alertas da API de segurança do Microsoft Graph
- Mapeamento de alertas para campos de resposta a incidentes de segurança

Ingerir exemplos de alertas da API de segurança do Microsoft Graph

Ingerir alertas de exemplo do seu locatário Microsoft Azure.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

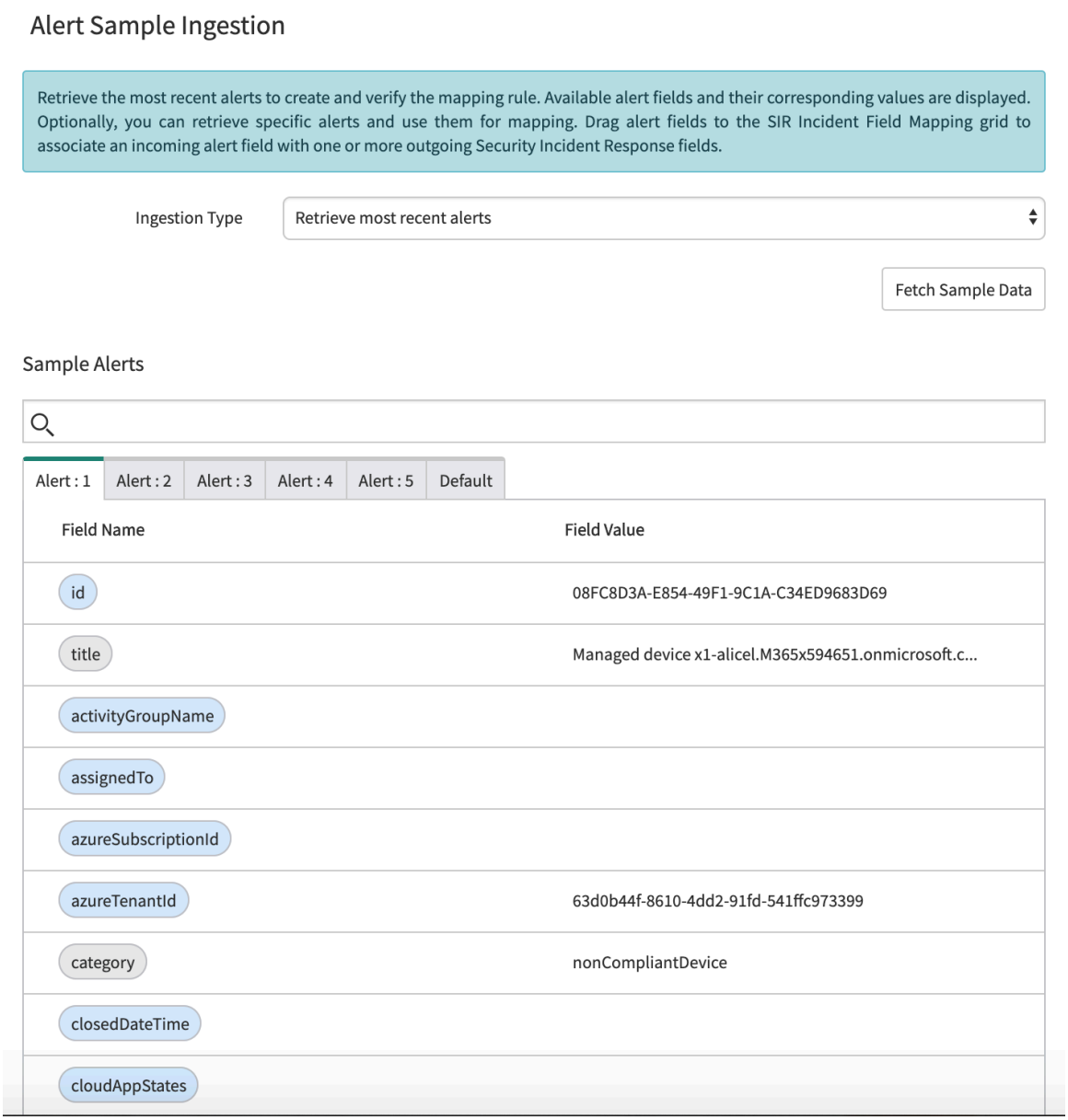
1. Você pode extrair os 5 alertas de amostra mais recentes ou fornecer os IDs de alerta exclusivos para os alertas específicos que deseja usar para sua experiência de mapeamento.
   Na lista de seleção **Preferência de ingestão**, selecione uma das seguintes opções:
   - Recuperar alertas mais recentes: os 5 alertas mais recentes são recuperados.
   - Selecionar alertas com base no ID de alertas: especifique o ID de alerta dos alertas a serem recuperados. Você pode especificar no máximo 5 IDs de alerta separados por vírgulas.
2. Clique em **Buscar dados de amostra** para extrair os dados de alerta de amostra mais recentes do locatário Microsoft Azure.
   A extração de alertas de amostra pode levar alguns minutos.

   Os valores do campo de alerta de amostra são preenchidos no lado esquerdo do formulário quando os alertas de amostra são ingeridos pelo perfil. Esses são os alertas que

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

você mapeia para os campos de incidente de segurança SIR. Os campos de alerta e os resultados dos valores são exibidos como guias individuais.



Tradução automática

O que Fazer Depois

Depois de obter os dados de amostra, a próxima etapa é mapear os campos de alerta para o incidente de segurança.

Mapeamento de alertas para campos de resposta a incidentes de segurança

Mapeie campos de alerta individuais de alertas acionados para campos em um incidente de segurança Now Platform.

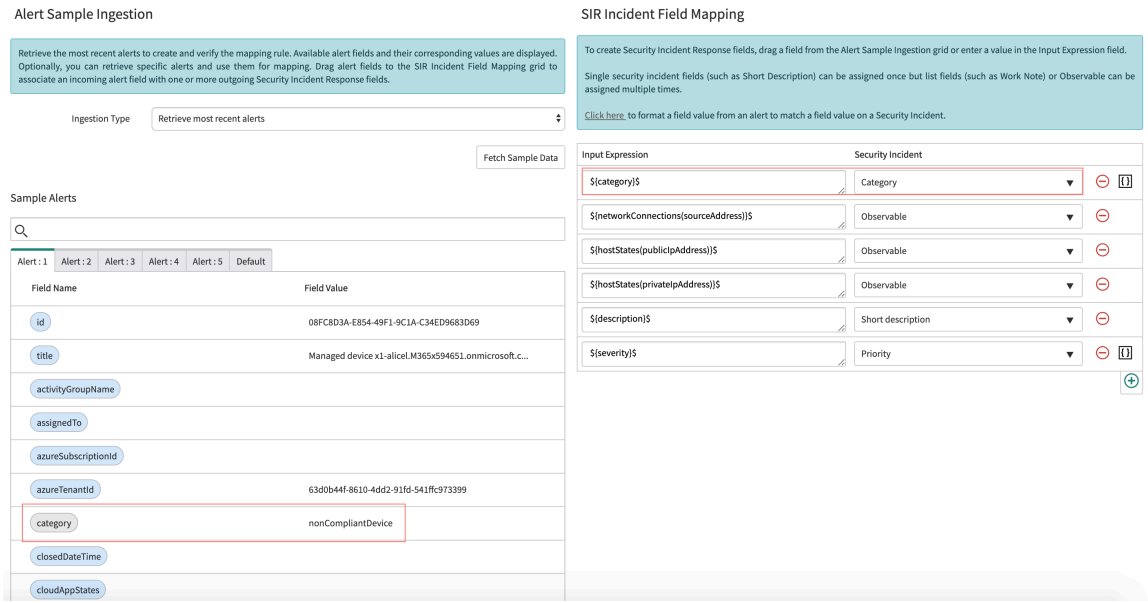
Mapeamento de campo de alerta

Como um usuário com a função sn_si.admin, use os campos da seção Alertas de amostra à esquerda e mapeie-os para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR no painel direito. Edite a configuração de mapeamento arrastando os campos de alerta do lado esquerdo e soltando-os na seção de mapeamento de incidente SIR à direita. O mapeamento à direita associa o campo de alerta de entrada a um campo de incidente de segurança de saída.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Depois de obter os dados de amostra, a próxima etapa é mapear os campos de alerta para o incidente de segurança. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
2. Arraste o nome do campo, por exemplo, `categoria`e solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, a `categoria` é mapeada para o campo `Categoria` no incidente de segurança.



No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo à direita. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudá-lo a garantir que nenhum campo de alerta seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação de cores dos campos de alerta ajuda a rastrear os valores de alerta que você já mapeou conforme eles ficam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de alerta importante restante permanece não mapeada.

Os campos em azul claro à esquerda indicam que um campo de alerta ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de alerta de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

a. Para inserir manualmente um valor no campo Expressão de entrada, insira-o no formato ${fieldname}$. O campo de alerta será mapeado para o campo de incidente de segurança.

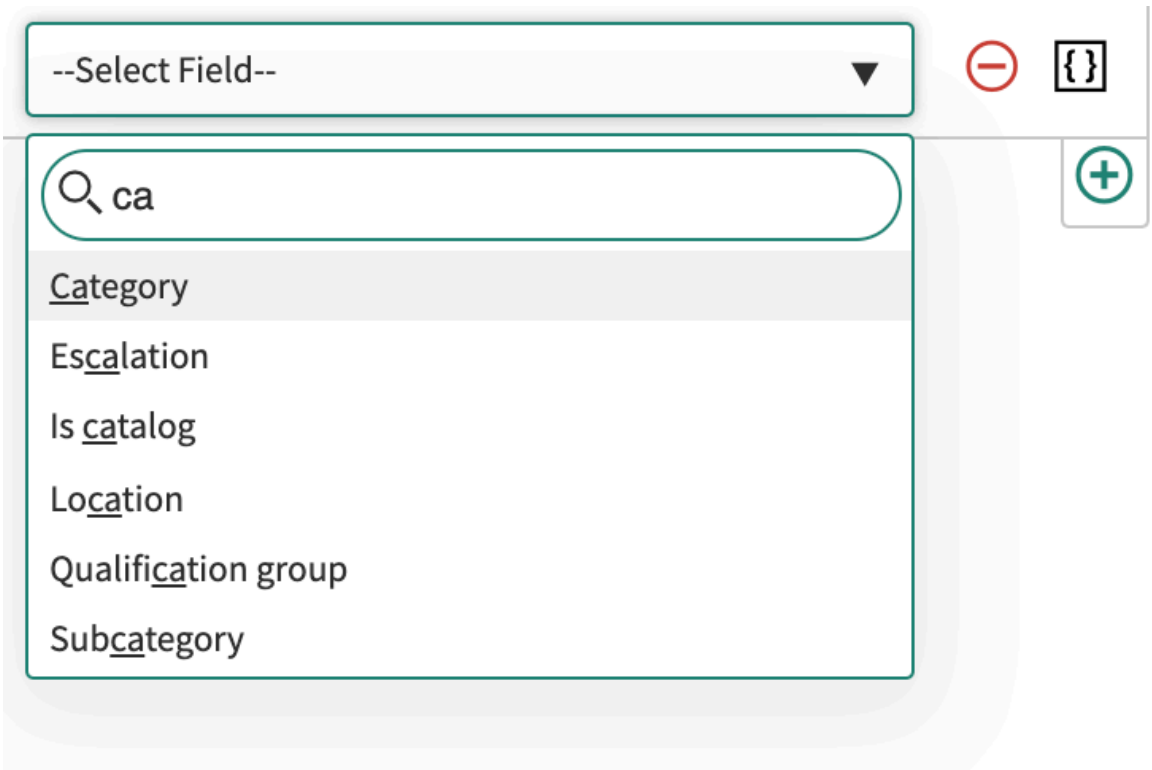
b. Você não pode mapear alertas ingeridos para os campos MITRE-ATT&CK da estrutura na seção de mapeamento de incidentes de segurança. Se você ainda mapear os campos, as informações não estarão disponíveis como parte do cartão [MITRE-ATT&CK na seção MITRE-ATT&CK da estrutura do formulário de incidente de segurança. Para associar as técnicas MITRE-ATT&CK, use o recurso de extração automática disponível como parte da estrutura MITRE-ATT&CK] no módulo Inteligência contra ameaças.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário na seção SIR Mapeamento de campo de incidente, na parte inferior da grade, clique no ícone de adição (+). Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

Na lista de seleção expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, a categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores para os campos de alerta no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidentes SIR já mapeados.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> **Nota:** Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

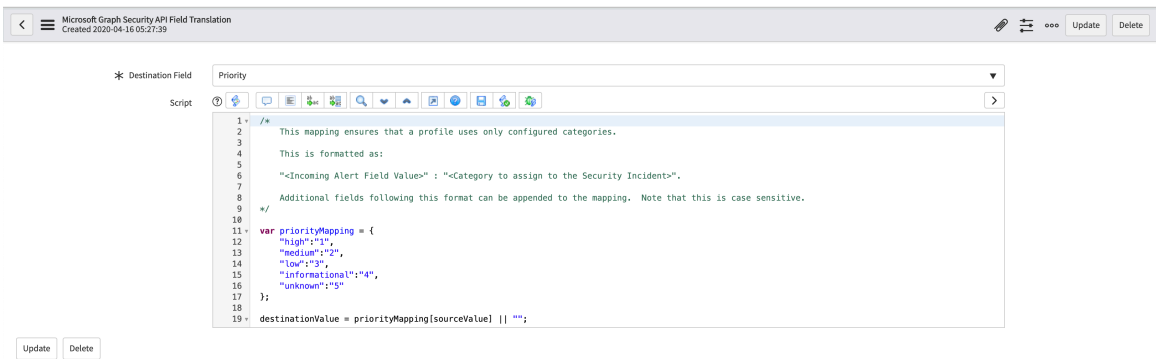
d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o ID de alerta desejado no campo Expressão de entrada. Com o recurso de arrastar e soltar, mapeie-o ao lado do novo campo.

4. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.
5. Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um alerta de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

Formatar tradução de campo

Em determinados casos, os valores do campo de alerta em API de Segurança do Microsoft Graph podem não ser convertidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de Malware e Infecção de Vírus pode ter valores de campos diferentes para a categoria de origem, mas ambos os valores podem ser convertidos para uma Atividade de Código Mal-Intencionado comum no campo Categoria no incidente de segurança SIR usando o Formato Funcionalidade de tradução de campo.

Para usar o editor de script, clique no ícone {}. O editor de script é exibido.



Condições de geração de incidentes

Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais alertas devem criar incidentes de segurança e quais alertas devem ser filtrados, por exemplo, alertas de baixa prioridade. Você pode usar os mesmos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

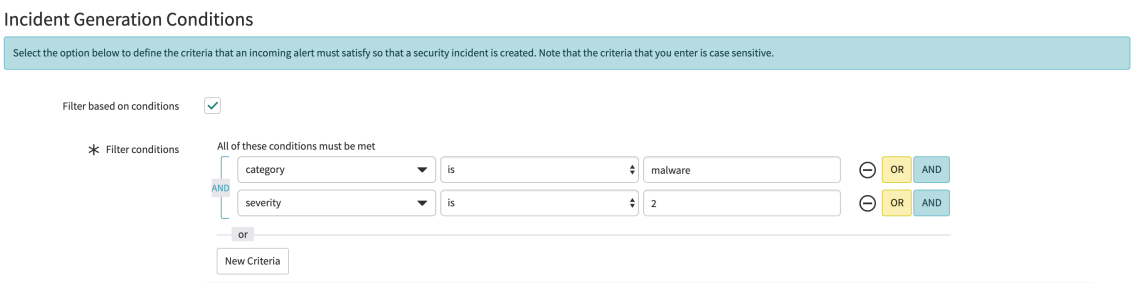
valores de campos no construtor Condições de geração de incidentes para definir critérios adicionais que um alerta de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até a seção Condições de geração de incidente no formulário e selecione a opção Filtrar com base nas condições. O Construtor de condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção do primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de alerta do alerta que você ingeriu. Esses campos são dinâmicos e mudam dependendo do alerta que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores do alerta. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao locatário do Microsoft Azure e revisar os alertas para as palavras-chave.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   - Se **E**for selecionado, todas as condições deverão ser atendidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Na segunda linha, defina uma segunda condição de filtro

   A imagem a seguir é um exemplo com duas condições que devem ser atendidas antes que os incidentes de segurança sejam criados.



   Você definiu as condições de acionamento para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

   Esse tipo de filtragem ajuda a isolar alertas de segurança e limita o número de incidentes de segurança que você cria. Se critérios de filtragem adicionais forem definidos, somente os alertas necessários serão ingeridos sem a necessidade de alterar a consulta ou a configuração do alerta acionado.

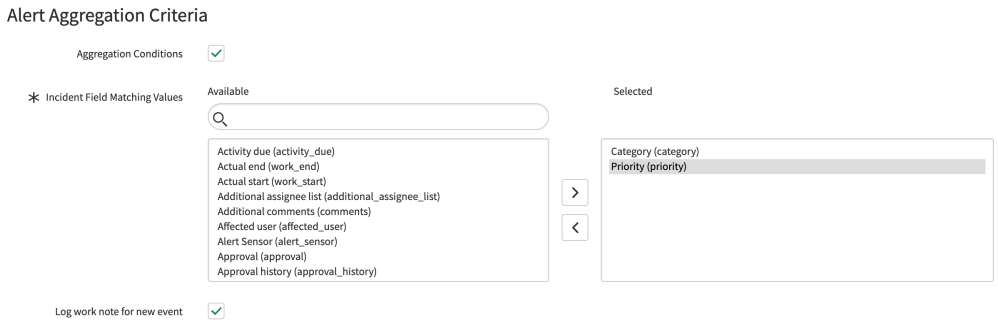
Critérios de agregação de alertas para lidar com alertas semelhantes e evitar incidentes duplicados

Defina critérios de agregação de alertas adicionais que agregam um alerta de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de alerta relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Role até a seção Critérios de Agregação de Alertas no formulário e selecione a opção Condições de Agregação. As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.
2. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes na Now Platform e mova-os para a lista Selecionado. Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de alerta mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de alertas não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para mapeamento de campos de vários valores.



Se um novo alerta corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o alerta será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os alertas agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os alertas agregados em um incidente de segurança são exibidos na lista relacionada Alertas agregados do Microsoft Graph. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que os alertas são adicionados aos incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.

3. (Opcional) Para registrar uma anotação de trabalho para um novo alerta adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra que um novo alerta foi adicionado junto com um link para os detalhes do alerta e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Você mapeou com sucesso valores de um alerta para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem. Você também anexou alertas ou eventos a incidentes de segurança SIR existentes.

4. Clique em **Continuar** para continuar com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizar o incidente de segurança para a integração da API de segurança do Microsoft Graph

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um Now Platform SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de alerta que deseja exibir no incidente de segurança.

Antes de Iniciar

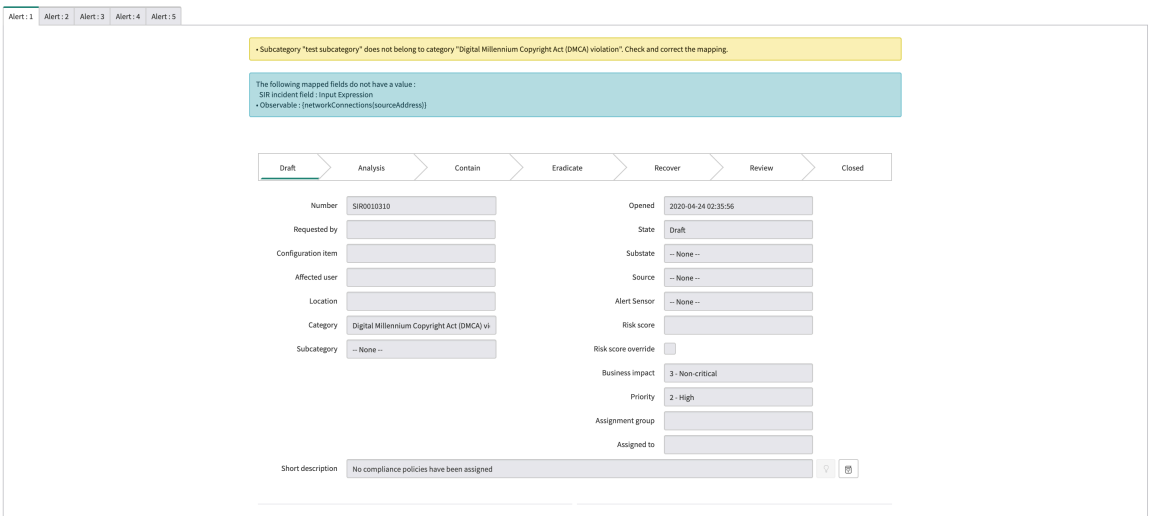
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
   Todos os alertas ingeridos e os mapeamentos de campo definidos na página Mapeamento são exibidos.
2. Clique em um ID de alerta para ver uma visualização do incidente de segurança.
   Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de alerta no incidente de segurança.



   A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois
Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campos no incidente de segurança, a próxima etapa será definir a programação.

Definir programação para integração da API de segurança do Microsoft Graph

Verifique as configurações padrão para recuperação de alertas ou modifique a programação conforme necessário. Esta etapa permite filtrar a recuperação do alerta com base em um intervalo de datas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você também escolhe com que frequência pesquisará alertas futuros que correspondam à configuração do perfil de alerta. Para perfis de ingestão de alertas automatizados, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação do alerta. Esta etapa é necessária para perfis de alerta programados.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de alertas API de Segurança do Microsoft Graph é afetado pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

Procedimento
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os alertas são extraídos do locatário Microsoft Azure.

Opção	Descrição
Ingestão contínua de alertas selecionada	Com base na configuração padrão, a instância da Now Platform extrai do locatário Microsoft Azure novos alertas a cada cinco minutos. Os incidentes de segurança serão criados se os alertas acionados forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar a ingestão de alertas em relação à carga do servidor e para extrair os dados mais atuais, cinco minutos é a configuração que você pode preferir. No entanto, este valor pode ser modificado conforme necessário.
◦ Ingestão contínua de alertas selecionada ◦ Definir tempo de ingestão do alerta inicial	Tempo de ingestão inicial Se você quiser programar a ingestão inicial em um horário específico, siga estas etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	◦ Selecione os campos Ingestão de alertas contínuos e Definir tempo de ingestão do alerta inicial. ◦ Especifique o tempo no campo Tempo de ingestão do alerta inicial de entrada. A ingestão inicial ocorrerá no horário especificado aqui. As ingestões subsequentes serão baseadas na programação definida no campo Incremento de pesquisa (minutos). Como um exemplo de programação, se você tiver um trabalho de alerta diário que é executado uma vez por dia às 4h no horário local, poderá configurar o perfil de alerta correspondente em sua instância da Now Platform para ser executado às 4h05 no horário local para capturar o alerta imediatamente e crie um incidente de segurança. Insira 04 05 00 no campo Ingestão de alerta inicial. No campo Incrementar (minutos), insira 1440 (24 horas) para programar a próxima ingestão de alertas por 24 horas a partir da ingestão de alertas inicial. O tempo de ingestão do alerta inicial e o tempo de ingestão do próximo alerta são exibidos nos campos. Para definir as configurações neste exemplo, siga estas etapas: ◦ Selecione a opção **Ingestão de alertas contínuos**. ◦ No campo Incremento de pesquisa (minutos), insira 1440 (24 horas). ◦ Clique na opção **Definir tempo de ingestão do alerta inicial** para habilitar a edição dos campos Tempo de ingestão do alerta inicial e Tempo de ingestão do próximo alerta (estimado). ◦ No campo Tempo de ingestão do alerta inicial, insira 04 05 00. No campo Tempo da próxima ingestão de alertas (estimado), a hora da próxima ingestão de alertas é exibida.
Campo de recuperação única selecionado	Recuperação Única Use esta configuração se quiser que uma extração única inclua alertas históricos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Quando esta configuração é definida, um perfil é usado uma vez para recuperar alertas de eventos históricos que são baseados em um intervalo de datas. À direita do campo Data desde, clique no ícone de calendário. No calendário exibido, selecione a data em que deseja começar a extrair alertas. Começando com o valor de data Desde, os alertas são recuperados até a data atual. Observe que você pode retroceder até sete dias a partir da data atual. Esta funcionalidade não se destina a recuperar quantidades significativas de alertas históricos, mas sim uma quantidade mínima de alertas em andamento que estão sendo trabalhados ativamente no momento da ativação do perfil. Depois que os alertas forem extraídos, esta configuração não recuperará mais alertas para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todos os alertas encontrados para o intervalo inserido.

3. Clique em **Continuar** para navegar até a página Opções adicionais.

Automatizar atualizações de alerta e fechamento com base no status do incidente SIR

A integração de ingestão de alertas API de Segurança do Microsoft Graph tem uma interface bidirecional que permite que ambos os alertas criem incidentes de segurança, bem como a capacidade de atualizar os alertas depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como SIR incidente número, grupo de atribuição, SIR URL do incidente e assim por diante. T

Antes de Iniciar

Função necessária: sn_si.admin

Nota: Os status de alerta inicial e de fechamento serão atualizados somente se esta funcionalidade for compatível com o provedor de serviços. Para obter detalhes, consulte a documentação API de Segurança do Microsoft Graph e a documentação do provedor de segurança.

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração de atualização de alertas quando o incidente de segurança for criado.

Opção ou campo	Descrição
Atualizar alertas após a criação do incidente SIR	Selecione esta opção se quiser atualizar o status do alerta e adicionar comentários adicionais quando um incidente de segurança for criado a partir do alerta. Isso po-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	de ocorrer para os alertas de gatilho iniciais que criam o incidente de segurança, bem como para os alertas agregados.
Atualização de status de alerta inicial	Selecione um status de alerta inicial na lista. Este status será definido para todos os alertas quando um incidente de segurança for criado para um alerta ingerido. Isso inclui alertas que criam novos incidentes e alertas que são ingeridos e agregados a um incidente em aberto existente. **Nota:** Com base no status de alerta selecionado aqui, o status de alerta usado pelos provedores de segurança será atualizado correspondentemente.
Comentários iniciais retornados para o alerta	Com base na fase selecionada, os comentários padrão são exibidos. Você pode modificar o texto padrão e usar o formato ${field name}$ para adicionar ou modificar quaisquer campos disponíveis no formulário de incidente de segurança.
Fechar alertas após o fechamento do incidente de SIR	Selecione esta opção se quiser usar a opção de fechamento de alerta automatizado. Isso pode ocorrer para os alertas de gatilho iniciais que criam o incidente de segurança, bem como para os alertas agregados. O status do alerta será atualizado no provedor de segurança com os comentários de status e fechamento após o SIR incidente ser fechado no Now Platform.
Atualização de status de alerta de fechamento	Selecione um status de alerta na lista. Selecione o valor de status a ser definido para todos os alertas quando um incidente de segurança for encerrado para um alerta ingerido.
Comentários de fechamento retornados para o alerta	Os comentários de fechamento padrão são exibidos aqui. Você pode editar o texto padrão e usar o formato ${field name}$ para adicionar ou modificar quaisquer campos disponíveis no formulário de incidente de segurança.

3. Clique em **Concluir** para concluir a configuração e mover o perfil para o estado **Aguardando**.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair alertas do locatário Microsoft Azure com base em sua programação. Um máximo de 1.000 incidentes de segurança podem ser criados em um período de 24 horas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de configuração de integração da API de segurança do Microsoft Graph

Use esta opção para modificar as API de Segurança do Microsoft Graph propriedades do sistema padrão de integração de ingestão.

Antes de Iniciar

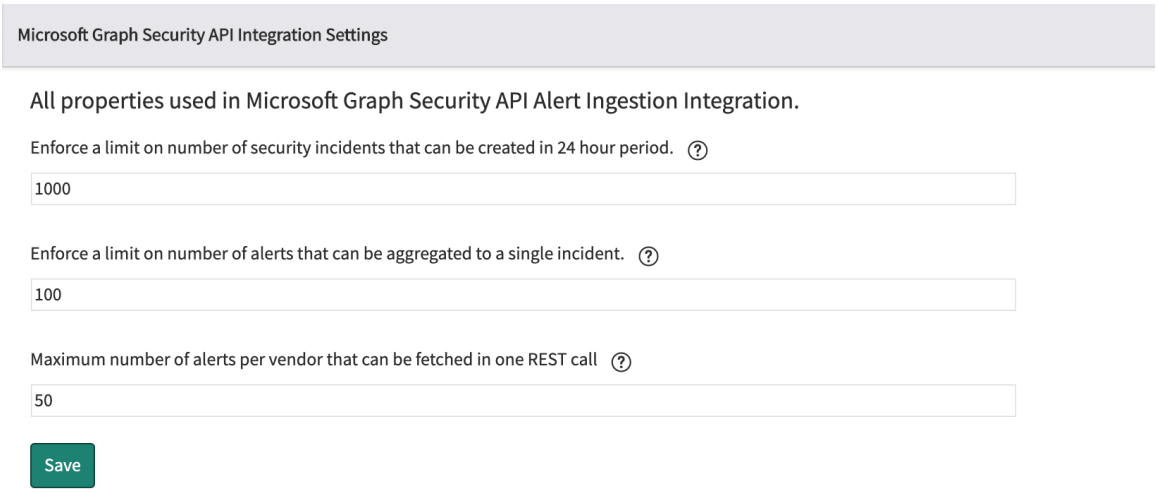
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Modifique as propriedades de configuração padrão para limitar o número de incidentes de segurança que podem ser criados durante um período de 24 horas ou o número de alertas que podem ser agregados em um incidente de segurança.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Integração da API de segurança do Microsoft Graph** > **Configuração de integração da API de segurança do Microsoft Graph**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.



Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Formulário do Security Incident Response após ingestão de alertas

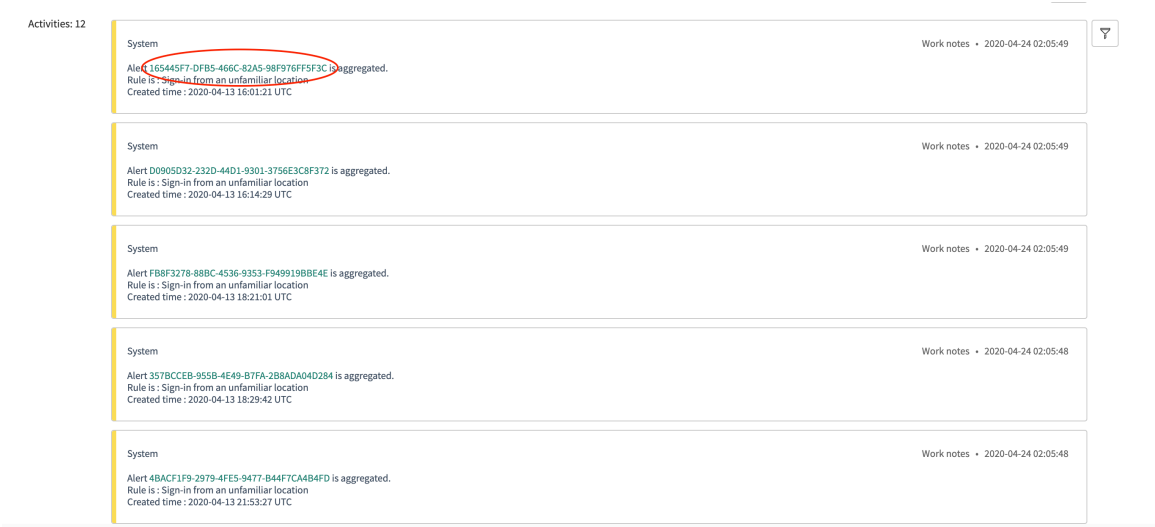
Depois que um alerta API de Segurança do Microsoft Graph é ingerido, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro do incidente de segurança.

Anotações de trabalho

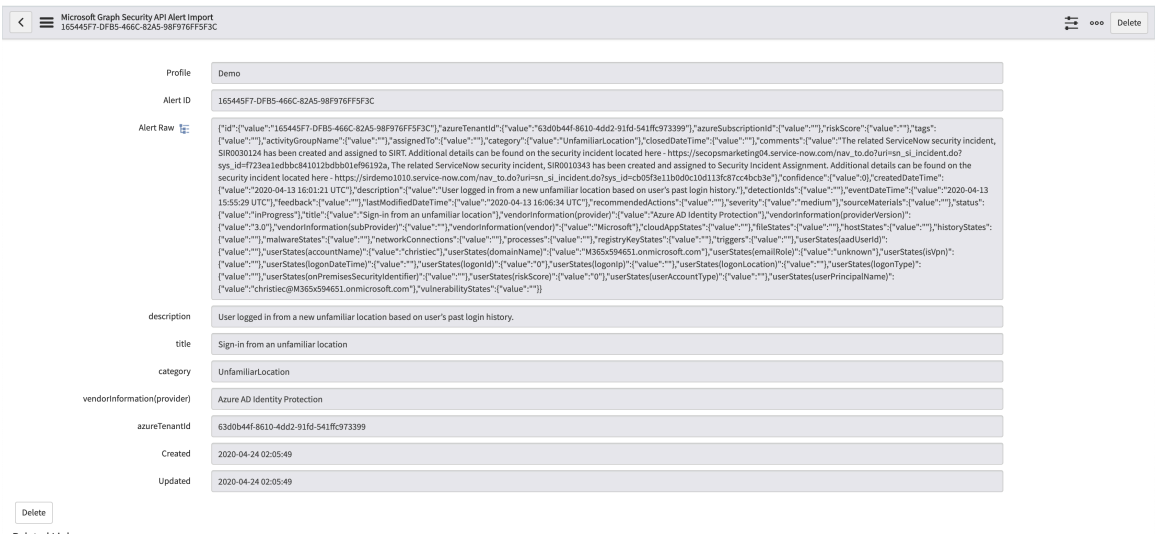
Se você selecionou a opção **Registrar anotação de trabalho para novo alerta** nos Critérios de Agregação de alertas conforme descrito em Mapeamento de alertas para campos de resposta a incidentes de segurança, uma anotação de trabalho será publicada quando o alerta for agregado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

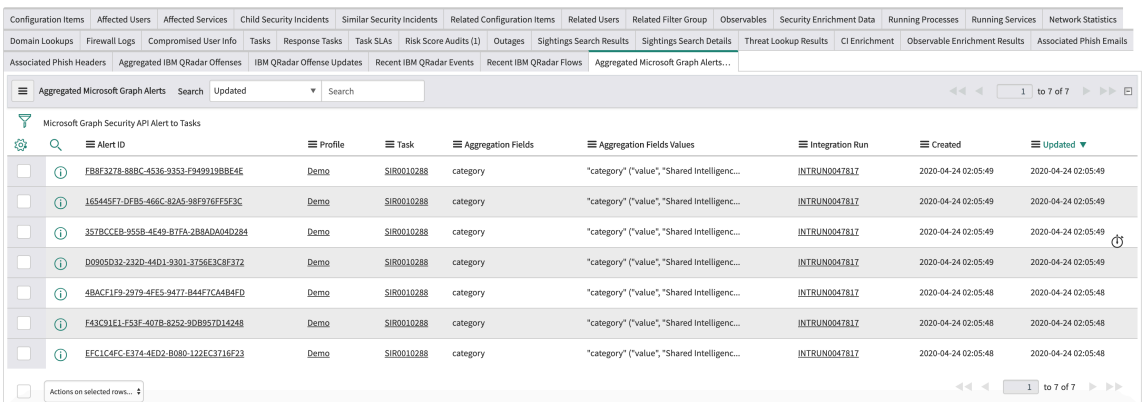


Clique no link do alerta para navegar até o registro de importação de alerta interno que contém dados brutos de alerta.



Alertas agregados

Clicar **Listas relacionadas** > **Alertas de segurança agregados do Microsoft Graph** para exibir os alertas agregados ao incidente de segurança.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Criar incidente de segurança**: selecione um alerta na lista, clique no menu **Ações** e clique em **Criar incidente de segurança**. Esta opção cria um novo incidente de segurança para o alerta e este alerta é desagregado do incidente de segurança primário.
- **Excluir registro de alerta**: selecione um alerta na lista, clique no menu **Ações** e clique em **Excluir**. Esta opção exclui o registro do alerta.

Opcional: copiar um perfil da API de segurança do Microsoft Graph

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar os perfis para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Todos** > **Integração da API de segurança do Microsoft Graph** > **Perfil da API de segurança do Microsoft Graph**.
2. Na lista API de Segurança do Microsoft Graph Perfis exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.
   O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (`verdadeiro`), a cópia está desabilitada neste ponto (`falso`). Você pode preferir editar valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.

   Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativo** está definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Separação de domínios e ingestão de alertas API de Segurança do Microsoft Graph

A separação de domínios é compatível com esta aplicação. A integração API de Segurança do Microsoft Graph ingere alertas de provedores de segurança do Microsoft Graph e cria automaticamente incidentes de segurança. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

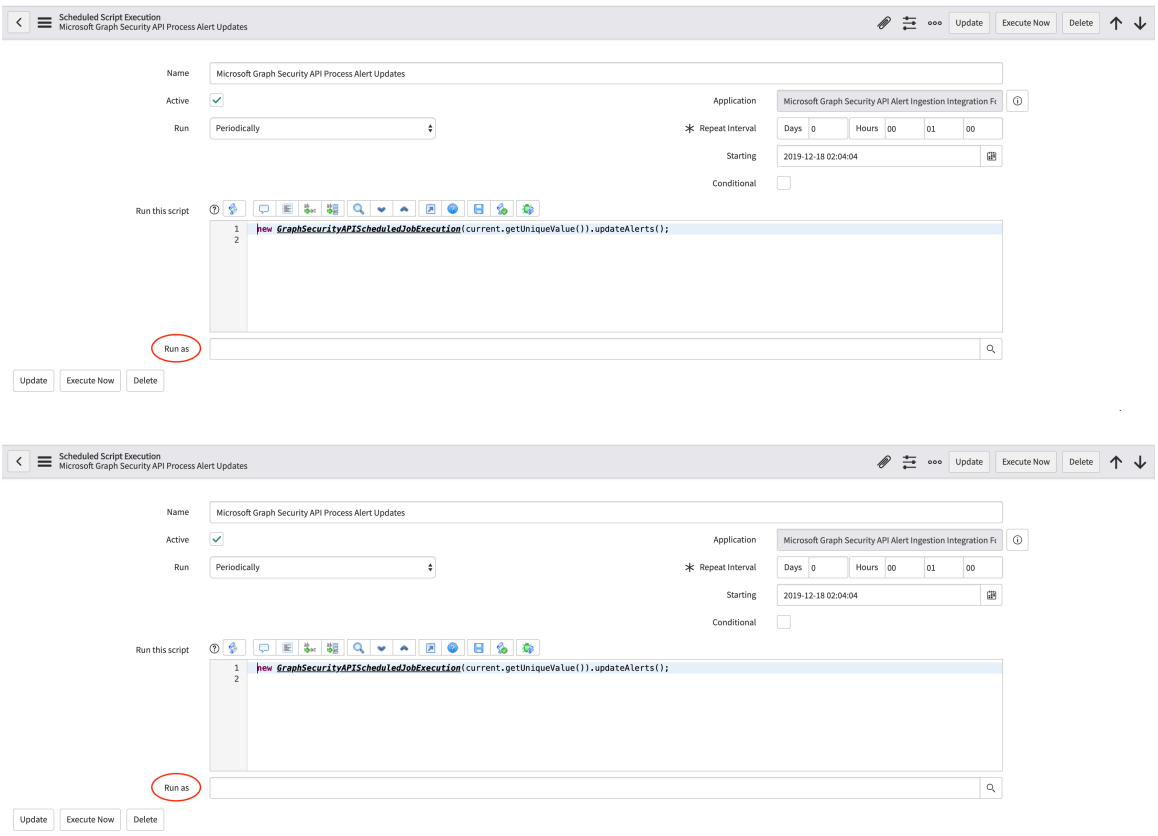
- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, emissão de relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no API de Segurança do Microsoft Graph

Para obter a separação de domínio, replique os trabalhos agendados API de Segurança do Microsoft Graph Processo de perfil e SIR Atualizações de alerta de processo e altere a **opção Executar como** usuários. Por padrão, os usuários do sistema executam esses trabalhos agendados. Altere **Executar como** para um usuário com a função sn_si.admin no respectivo domínio e execute o trabalho agendado.



Informações relacionadas

Domain Separation para provedores de serviço

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uso do Flow Designer e do Hub de integração na integração da API de segurança do Microsoft Graph

Usando o Flow Designer e a funcionalidade do Hub de integração, vários subfluxos e ações foram criados como parte da integração API de Segurança do Microsoft Graph.

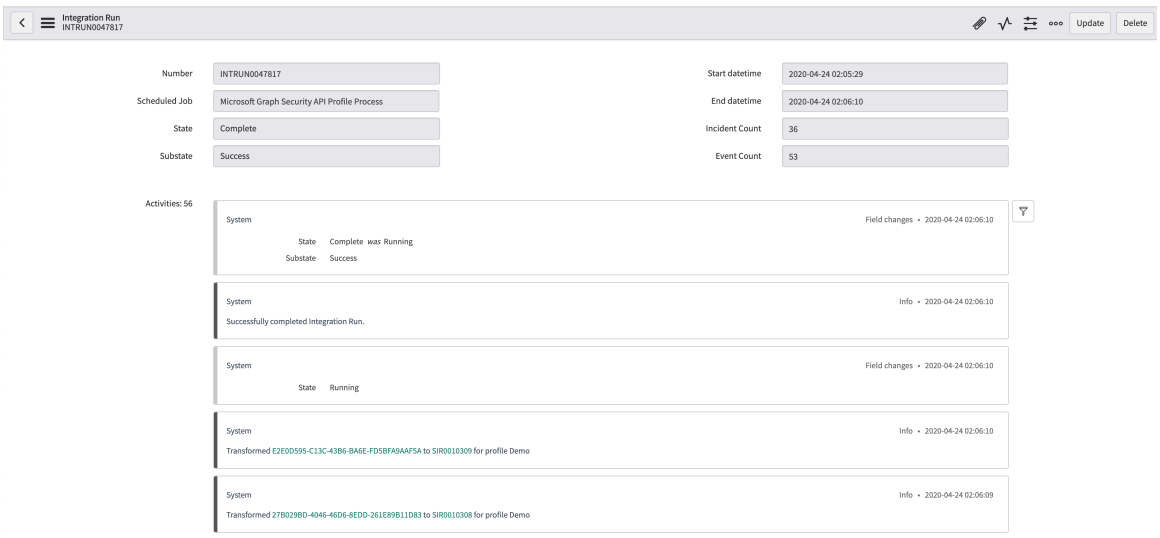
Os seguintes subfluxos estão disponíveis:

- API de Segurança do Microsoft Graph Validação de configuração: usada no bloco de configuração para validar as credenciais na configuração inicial.
- Chamada REST para API de Segurança do Microsoft Graph: é usado para todas as interações com a API de segurança do Microsoft Graph usando chamadas REST.
- Recuperar alertas de amostra: é usado na seção Mapeamento da configuração do perfil para buscar dados de amostra. Este subfluxo é acionado de forma assíncrona.

Solução de problemas de integração da API de segurança do Microsoft Graph

Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas à integração de ingestão de alertas API de Segurança do Microsoft Graph.

- **Execução de integração**: quando um trabalho agendado começa a ser executado, um registro de execução de integração com logs, erros e avisos é exibido. O número de alertas extraídos e o número de incidentes criados em uma execução de trabalho agendado também são exibidos. Usuários com a função `sn_si.analyst` podem ver se houve falha na extração de erros/perfis durante a execução da integração. Usuários com a função `sn_si.analyst` podem verificar a tabela `sn_event_ingestion_integration_run` em busca de erros ocorridos. Para solucionar quaisquer problemas de integração, você deve primeiro verificar a execução da integração. Os erros são registrados como anotações de trabalho nos registros de execução de integração para cada execução de trabalho agendado.



- **Perfil incompleto**: ao configurar o perfil, na seção Opções adicionais (Automatizar atualizações de alerta e fechamento com base no status do incidente SIR), você deve clicar no botão **Concluir** para garantir que o perfil seja movido para o estado Aguardando, indicando que está aguardando a ingestão.
- **Validar perfil**: para validar se a integração está funcionando corretamente, verifique os estados do perfil, a data da última extração do perfil, a tabela de importação de alertas, o alerta para os registros da tabela de tarefas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Problemas de SSL**: ao se conectar por meio de API de Segurança do Microsoft Graph, certifique-se de que a instância tenha um certificado de CA válido que não tenha expirado. Você pode importar o RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Consulte KB0778285 para obter detalhes.

Integração de Palo Alto Networks - AutoFocus

O sistema de base de integração Palo Alto Networks - AutoFocus inclui um fluxo de trabalho e uma série de atividades de fluxo de trabalho que você pode usar para integrar Palo Alto Networks - AutoFocus com sua instância.

Explorar Integrações do Security Incident Response	**Configurar** Ativar e configurar a integração Palo Alto Networks - AutoFocus
Usar • Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor • Obter fluxo de trabalho de aprimoramento de informações da sessão do AutoFocus	**Desenvolver** • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Ativar e configurar a integração Palo Alto Networks - AutoFocus

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo Palo Alto Networks - AutoFocus. Antes de poder usar o Palo Alto Networks - AutoFocus, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. .
2. Quando a instalação estiver concluída, acesse o site de suporte da Palo Alto Networks e obtenha a chave de API.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em sua instância, navegue até **Operações de segurança** > **Configuração de Integração**.
4. No cartão Palo Alto Networks AutoFocus, clique em **Configurar**.
5. Insira (ou cole) a **chave de API** que você adquiriu no site de suporte da Palo Alto Networks.
6. Clique em **Enviar**.

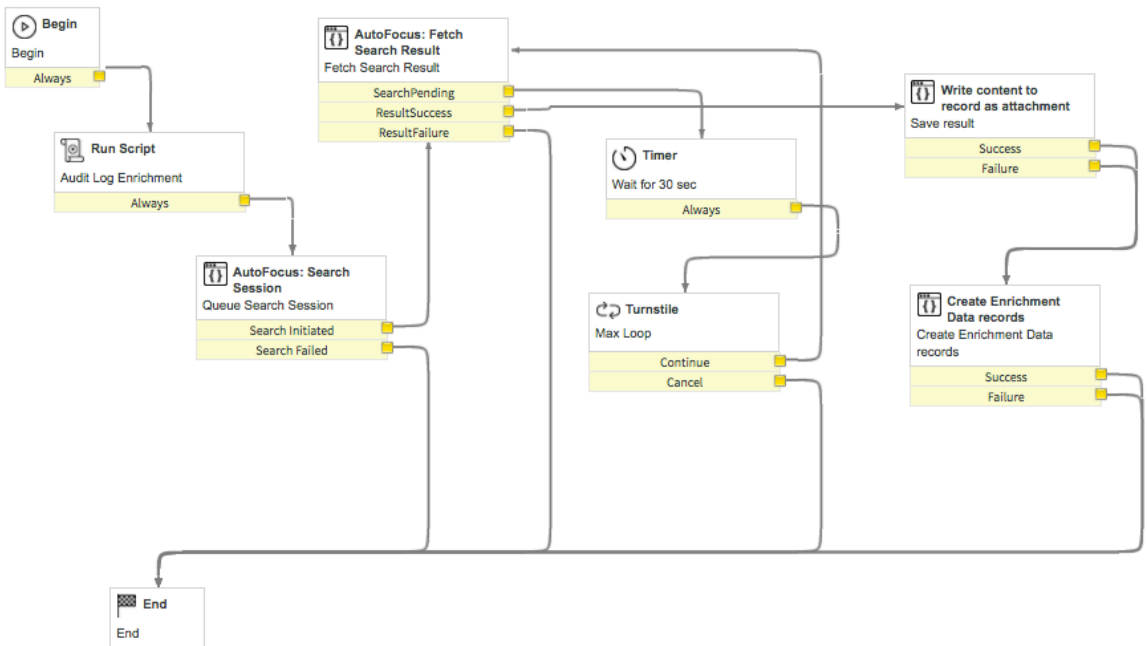
Obter fluxo de trabalho de aprimoramento de informações da sessão do AutoFocus

Quando o fluxo de trabalho do **Security Operations Palo Alto Networks - Obter aprimoramento de informações da sessão do AutoFocus** é executado, ele enfileira uma consulta de pesquisa com o AutoFocus para coletar informações sobre um IP de origem especificado. Se o AutoFocus tiver conhecimento sobre sessões anteriores originadas desse endereço IP, um relatório no formato JSON será retornado.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho **de aprimoramento de informações da sessão do Security Operations Palo Alto Networks - AutoFocus** é executado quando o campo **IP de origem** em um incidente de segurança é modificado e o registro é atualizado. O fluxo de trabalho busca o endereço IP e envia uma solicitação de consulta para o AutoFocus. Se o AutoFocus tiver identificado anteriormente sessões originadas do endereço IP, um relatório no formato JSON será retornado.

Operações de segurança Palo Alto Networks - Obter fluxo de trabalho de aprimoramento de dados do WildFire



Procedimento
1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Clique na guia **Indicadores de comprometimento** e preencha o campo **IP de origem**.
3. Clique em **Atualizar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O AutoFocus verifica as informações do endereço IP e um arquivo de texto no formato JSON é anexado ao incidente de segurança.

As atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade de sessão de pesquisa de foco automático

A atividade de fluxo de trabalho **Sessão de pesquisa do AutoFocus** carrega informações de um endereço IP atribuído a um incidente de segurança para o AutoFocus e as enfileira para uma consulta de pesquisa.

Variáveis de entrada

Nota:

Quando a atividade é executada, ela enfileira uma consulta de pesquisa com o AutoFocus para coletar informações para um IP de origem especificado. Se o AutoFocus tiver identificado anteriormente sessões originadas desse endereço IP, um relatório no formato JSON será retornado.

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
searchSessionQuery [cadeia de caracteres]	A consulta de pesquisa para informações da sessão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
requestStatus [booliano]	Verdadeiro se uma consulta de pesquisa foi programada para execução no AutoFocus.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.
afcookie [cadeia de caracteres]	Um identificador para a consulta de pesquisa do AutoFocus usado pelo Atividade Buscar resultados de pesquisa para recuperar os resultados da pesquisa.

Atividade Buscar resultados de pesquisa

A atividade de fluxo de trabalho **Buscar resultados** de pesquisa busca resultados de pesquisa identificados por um cookie para a consulta de pesquisa iniciada pela atividade de **sessão de pesquisa** com foco automático.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
afcookie [cadeia de caracteres]	O cookie AutoFocus para a solicitação de pesquisa gerada pelo Atividade de sessão de pesquisa de foco automático.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
pesquisaPendente [Booliano]	Verdadeiro se a solicitação de pesquisa ainda estiver sendo processada no AutoFocus.
resultado [cadeia de caracteres]	Os dados dos resultados da pesquisa.
status [booliano]	Verdadeiro se a pesquisa for concluída e os resultados tiverem sido gerados com sucesso.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.

Integração de Palo Alto Networks - Firewall

Para executar a integração Palo Alto Networks - Firewall, certifique-se de ter um MID Server configurado com credenciais SSH. Se um firewall ainda não estiver configurado, adicione um.

Explorar Integrações do Security Incident Response	**Configurar** • Ativar e configurar a integração de firewall da Palo Alto Networks • Configurar credenciais SSH para o MID Server
Usar Integração de Operações de segurança Palo Alto Networks Fluxo de trabalho do inicializador de firewall	**Desenvolver** • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução de problemas de integração
- Fazer ou responder a perguntas na comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configurar credenciais SSH para o MID Server

O firewall da Palo Alto Networks envia chamadas de API para o MID Server. Como tal, certifique-se de que as credenciais SSH tenham sido criadas para o MID Server.

Antes de Iniciar

- O plug-in Orquestração deve ser ativado.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Orquestração** > **Credenciais e Conexões** > **Credenciais**.
2. Clique em **Nova**.
3. Na tela do Interceptador, clique em **Credenciais SSH**.
4. Preencha os campos conforme necessário.

Credenciais SSH

Campo	Descrição
Nome	Insira um nome para a credencial.
Ativo	Marque esta caixa de seleção para ativar esta credencial.
Aplica-se a	Selecione **Todos os MID servers** ou **MID servers específicos**.
MID Servers	Se você selecionou **MID Servers específicos**, clique no ícone de cadeado e selecione os MID Servers aos quais deseja aplicar essas credenciais.
Ordem	Selecione a ordem na qual as credenciais são testadas pelo servidor. Números menores são testados primeiro.
Nome de usuário	Insira o nome de usuário do usuário associado a essas credenciais, se houver.
Senha	Se você inseriu um **Nome de usuário**, insira a senha do usuário.
Marcador	Insira um marcador a ser usado para critérios de pesquisa. O campo **Marcador** deve conter o mesmo valor que o **Nome**.

Ativar e configurar a integração de firewall da Palo Alto Networks

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo Palo Alto Networks - Firewall. Antes de poder usar o Palo Alto Networks - Firewall, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

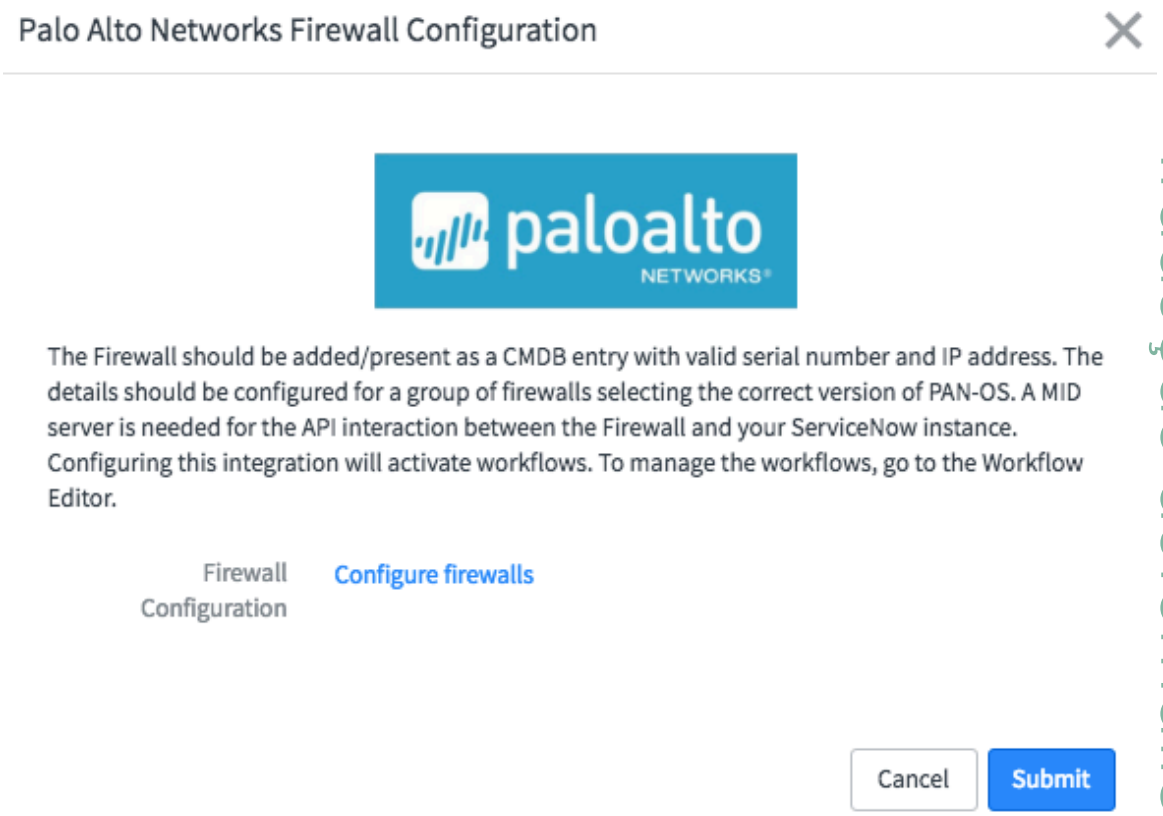
Função necessária: sn_si_admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Antes de ativar e configurar a integração, acesse o painel do Firewall da Palo Alto Networks.
   Anote os nomes da lista dinâmica de IP, lista dinâmica de URL ou lista dinâmica de domínio que você está usando para o bloqueio do firewall.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão do firewall da Palo Alto Networks, clique em **Configurar**.



5. Clique **em Configurar firewalls**.
6. Na tela Configurações do firewall, clique em **Novo**.
7. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Firewalls	Clique no ícone de cadeado e selecione o firewall a ser configurado.
Versão do firewall	Selecione a versão do firewall da Palo Alto Networks.**PAN-OS-7.1** é a versão recomendada. A seleção de versões anteriores pode retornar resultados inconsistentes.
Nome de usuário	Insira o nome de usuário a ser usado ao se conectar ao firewall por meio de endpoints REST.
Senha	Insira a senha do usuário de conexão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Lista dinâmica de IPs	Insira o nome da Lista Dinâmica Externa ou da Lista de Bloqueios Dinâmicos que você usa para endereços IP.
Lista dinâmica de URLs	Insira o nome da Lista dinâmica externa ou Lista de bloqueios dinâmicos que você usa para URLs.
Lista dinâmica de domínio	Insira o nome da Lista dinâmica externa ou Lista de bloqueios dinâmicos que você usa para domínios.

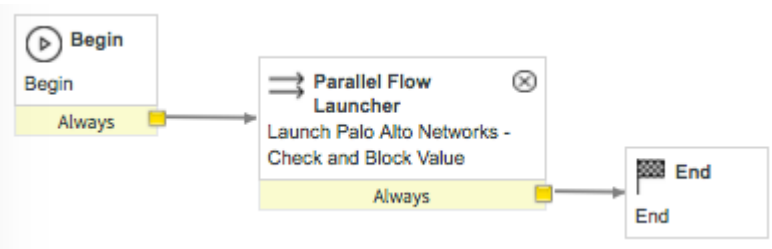
8. Clique em **Enviar**.

Integração de Operações de segurança Palo Alto Networks Fluxo de trabalho do inicializador de firewall

O fluxo de trabalho do inicializador do firewall da Palo Alto Networks para integração de Operações de segurança é a implementação do firewall da Palo Alto Networks iniciada pelo fluxo de trabalho da capacidade **Integração de operações de segurança - Solicitação de bloqueio**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor.



Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor

Como os incidentes de segurança são criados e triados para identificar possíveis ameaças, você pode usar o fluxo de trabalho **Palo Alto Networks - Verificar e bloquear valor das Operações de segurança** para verificar e atualizar automaticamente endereços IP, URLs e domínios usando listas dinâmicas externas definidas em Palo Alto Networks - Firewall.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho **Security Operations Palo Alto Networks - Verificar e bloquear valor** é executado quando as solicitações de bloqueio do firewall são enviadas. A solicitação de bloqueio especifica o firewall a ser usado, o tipo de observável a ser verificado e bloqueado (se necessário) e o valor do bloco. Ou seja, o endereço IP, a URL ou o domínio em questão.

Durante a execução do fluxo de trabalho, os comandos definidos em **Palo Alto Networks Integration** > **Firewall** > **Comandos** são executados. Os comandos Mostrar tipo (por exemplo, Show-IP-ExternalDynamicList) determinam se o valor existe no firewall. Os comandos de tipo

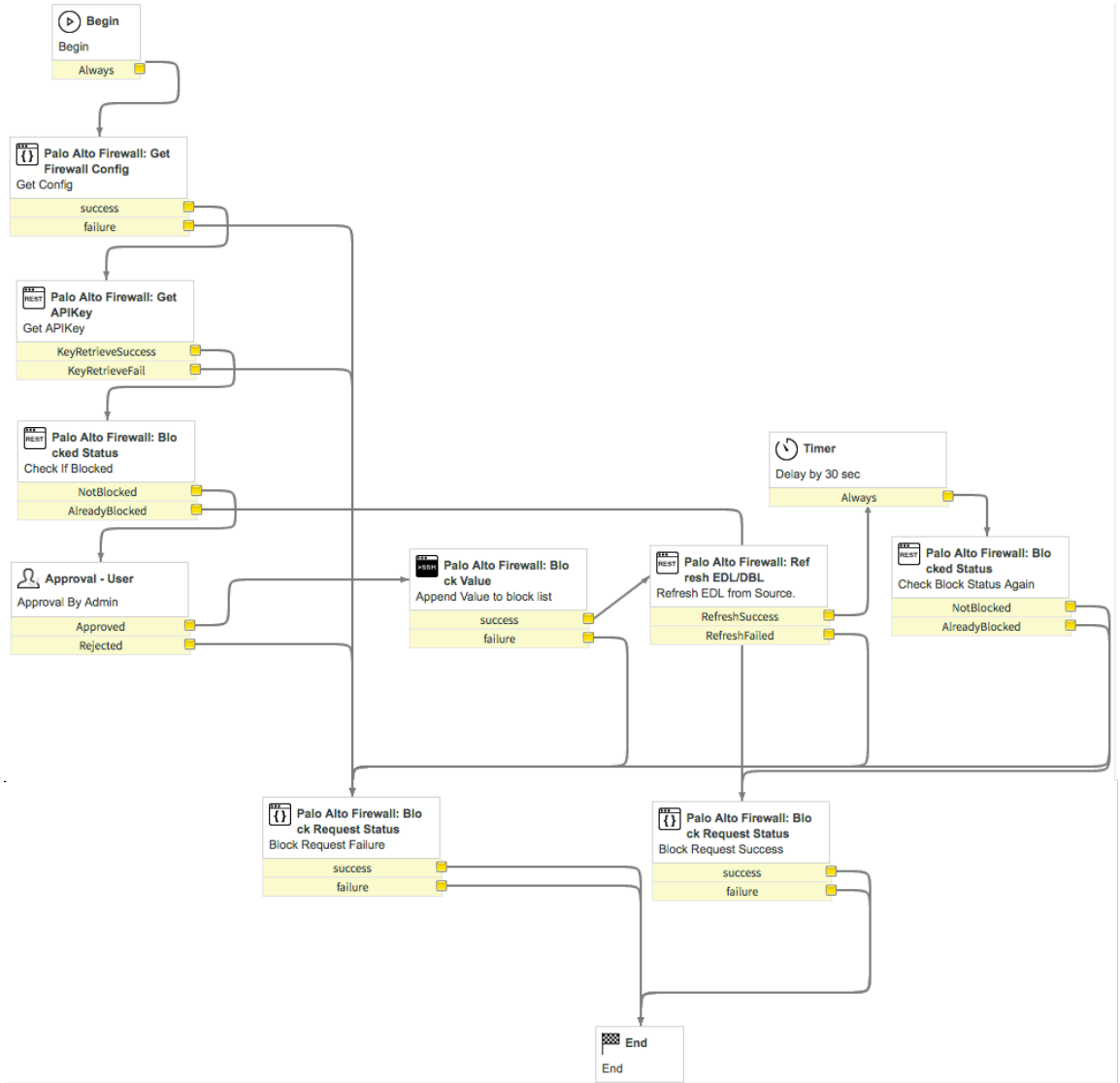
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de atualização (por exemplo, Refresh-IP-ExternalDynamicList) adicionam à lista de bloqueios um valor que não existe no firewall.

Depois que a atividade Status bloqueado é executada, é necessária a aprovação de um administrador do sistema para que o fluxo de trabalho possa prosseguir.

Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor



Procedimento

1. Navegar até **Palo Alto Networks Integration** > **Firewall** > **Bloquear solicitações**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Firewall	Selecione o firewall a ser usado.
Tipos de bloco	Selecione o tipo de valor a ser verificado:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ IP ◦ URL ◦ DOMÍNIO
Valor do bloco	Insira o valor do tipo selecionado a ser verificado no firewall.

4. Clique em **Enviar**.

Firewall da Palo Alto - Atividade Bloquear status da solicitação

Esta atividade é chamada por outras atividades para definir o status da solicitação de bloqueio do Firewall como sucesso ou falha.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
firewallBlockRequestSysid [cadeia de caracteres]	O ID do sistema da solicitação de bloqueio do firewall. Esta variável de entrada é obrigatória.
status [cadeia de caracteres]	Indica se o trabalho de atualização foi executado: sucesso ou falha.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se o trabalho de atualização foi bem-sucedido ou não.

Firewall Palo Alto - Atividade Bloquear valor

Depois que o fluxo de trabalho identifica um valor que não está no firewall, o registro é roteado para aprovação. Após a aprovação, esta atividade se conecta ao MID Server por meio de suas credenciais SSH e invoca um script que adiciona o valor à lista de bloqueios externos do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Nota: Você deve inserir manualmente as variáveis de entrada para esta atividade e publicar o fluxo de trabalho. Se o fluxo de trabalho não for publicado, as variáveis de entrada não serão salvas para usuários não administradores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
toBeBlockedValue [cadeia de caracteres]	O valor a ser adicionado ao EDL, caso ainda não esteja presente. Esta variável de entrada é obrigatória.
typeToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado: IP, URL ou domínio. Esta variável de entrada é obrigatória.
targetHost [cadeia de caracteres]	O MID Server no qual o script é executado.
SSHCredentialTag [cadeia de caracteres]	O marcador de credencial SSH definido no MID Server.
scriptCommand [cadeia de caracteres]	O script AppendValueToList.sh usado para adicionar o valor ao EDL. Ele requer o caminho completo para o MID Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	O resultado foi passado para o EDL.

Atividade Firewall Palo Alto - Status bloqueado

Esta atividade verifica se o valor (IP, URL ou domínio) está incluído na respectiva lista dinâmica externa/lista de bloqueios dinâmicos (EDL/DBL) no firewall. Os detalhes de EDL/DBL são obtidos do firewall usando um comando operacional e uma rotina é executada para verificar se o valor está bloqueado no firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
valueToBeChecked [cadeia de caracteres]	O valor na solicitação de bloqueio.
showEDLDetailsCommand [cadeia de caracteres]	O comando Lista dinâmica externa que está sendo usado para determinar se o valor existe no firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall usado.
FirewallApiKey [cadeia de caracteres]	A chave de API do firewall.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente usando a mensagem da API Palo Alto Firewall Operational Command.

Variáveis de saída

Variável	Descrição
commandResult [cadeia de caracteres]	Os resultados do firewall para o comando mostrar detalhes de EDL.
blockStatus [booliano]	Verdadeiro indica bloqueado. Falso indica que não está bloqueado.
commandResponse [cadeia de caracteres]	O status de resposta obtido do firewall para o comando mostrar detalhes de EDL.

Firewall Palo Alto: atividade Obter chave de API

Esta atividade recupera a chave de API do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
Nome de usuário [string]	O nome de usuário do administrador do firewall.
Senha [cadeia de caracteres]	A senha do administrador do firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
APIKey [cadeia de caracteres]	A chave de API do firewall.

Firewall Palo Alto: atividade Obter configuração do firewall

A atividade de fluxo de trabalho **Palo Alto Firewall: Obter configuração** de firewall obtém todas as informações de configuração de firewall relacionadas do banco de dados e as disponibiliza para uso pela atividade subsequente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
firewallSysid [cadeia de caracteres]	O ID do sistema do firewall. Esta variável de entrada é obrigatória.
typeOfValueToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado no firewall: IP, URL ou domínio.
firewallIPAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
ipEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para endereços IP.
urlEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para URLs.
domainEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para domínios.
firewallVersionSysId [cadeia de caracteres]	O ID do sistema para a versão do firewall.
updateEDLCommand [cadeia de caracteres]	O comando a ser usado para atualizar o EDL da origem.
ShowEDLDetailsCommand [cadeia de caracteres]	O comando a ser usado para obter os detalhes do EDL.
status [booliano]	Verdadeiro indica sucesso. Falso indica falha.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.
endpoint [Criptografado]	O endpoint criptografado do banco de dados.

Firewall Palo Alto - Atualizar atividade de EDL/DBL

Esta atividade executa um comando operacional no firewall para atualizar a lista dinâmica externa da origem configurada no firewall. A saída desta atividade indica se o trabalho de atualização foi enfileirado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall que está sendo atualizado.
FirewallApiKey [cadeia de caracteres]	A chave de API do firewall atualizada.
FirewallCommand [cadeia de caracteres]	O comando operacional a ser executado para enfileirar o trabalho de atualização.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
activity.Output.result [cadeia de caracteres]	Uma cadeia de caracteres de texto para indicar se o trabalho de atualização foi enfileirado para ser executado: sucesso ou falha.

Fluxo de trabalho Obter dados de log

Se Security Incident Response, Inteligência contra ameaçase Palo Alto Networks - Firewall estiverem ativados, o fluxo de trabalho **Palo Alto Networks - Obter dados de log das Operações de segurança** será executado automaticamente quando o IP de origem dos observáveis em um incidente de segurança for alterado.

Antes de Iniciar

Função necessária: sn_si.analyst

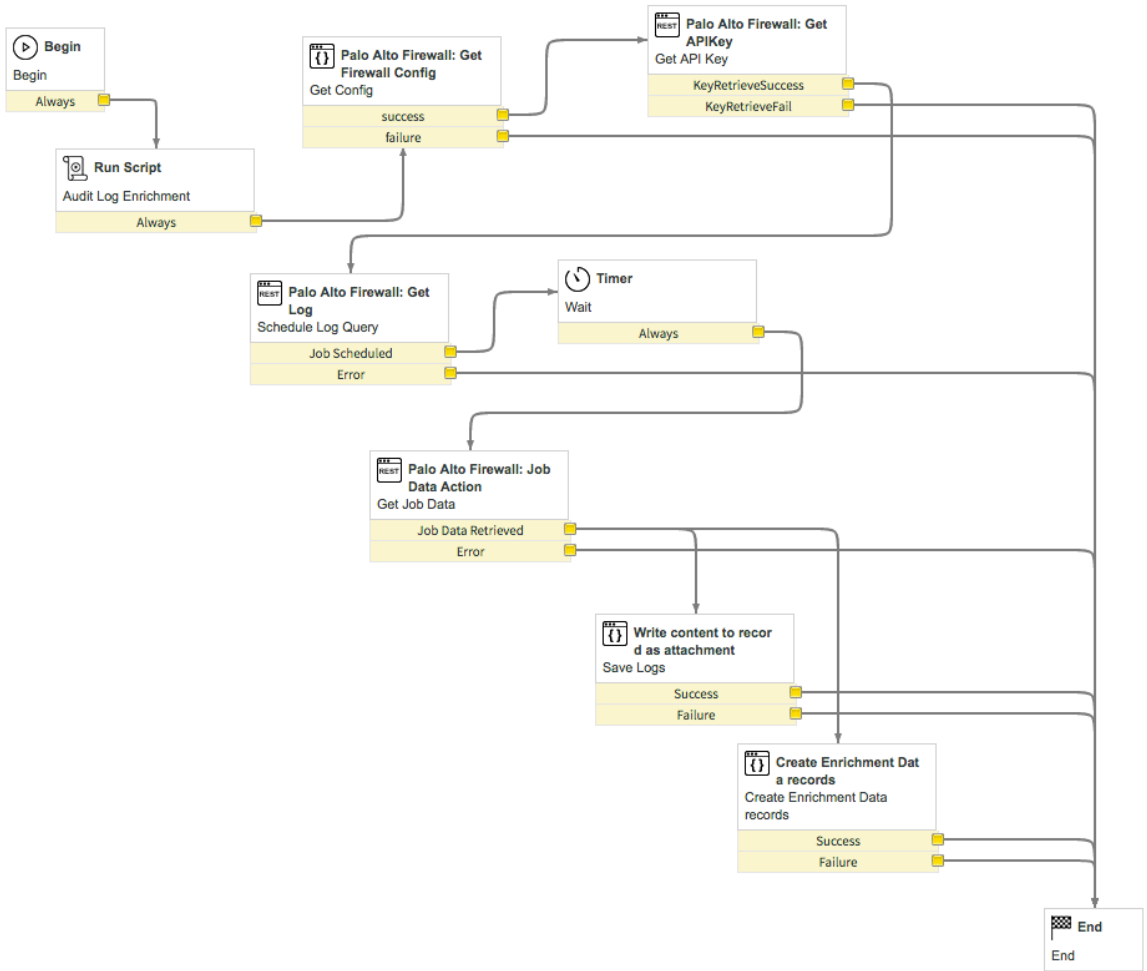
Por Que e Quando Desempenhar Esta Tarefa

Durante a execução do fluxo de trabalho, as informações de configuração do firewall são recuperadas do banco de dados e a chave de API é recuperada do firewall. A atividade Obter log enfileira uma consulta de pesquisa no firewall. Quando a consulta é executada, ela retorna um ID de trabalho que é usado para recuperar dados de logs de ameaças do firewall. Ele anexa os dados de log como um arquivo XML ao incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança Palo Alto Networks - Fluxo de trabalho Obter dados de log



Procedimento

1. Navegue até um incidente de segurança que contém observáveis.
2. Clique na guia **Observáveis de incidentes de segurança**.
3. Em **IP de origem**, adicione ou modifique o endereço IP.
4. Clique em **Atualizar**.
   O fluxo de trabalho **Security Operations Palo Alto Networks - Obter dados** de log é executado e os dados de log de ameaças aprimorados são anexados ao incidente de segurança. As informações também são analisadas e exibidas na seção **Logs do firewall** na guia **Dados** de aprimoramento.

Firewall Palo Alto: atividade Obter chave de API

Esta atividade recupera a chave de API do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
Nome de usuário [string]	O nome de usuário do administrador do firewall.
Senha [cadeia de caracteres]	A senha do administrador do firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
APIKey [cadeia de caracteres]	A chave de API do firewall.

Firewall Palo Alto: atividade Obter configuração do firewall

A atividade de fluxo de trabalho **Palo Alto Firewall: Obter configuração** de firewall obtém todas as informações de configuração de firewall relacionadas do banco de dados e as disponibiliza para uso pela atividade subsequente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
firewallSysid [cadeia de caracteres]	O ID do sistema do firewall. Esta variável de entrada é obrigatória.
typeOfValueToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado no firewall: IP, URL ou domínio.
firewallIPAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
ipEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para endereços IP.
urlEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para URLs.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
domainEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para domínios.
firewallVersionSysId [cadeia de caracteres]	O ID do sistema para a versão do firewall.
updateEDLCommand [cadeia de caracteres]	O comando a ser usado para atualizar o EDL da origem.
ShowEDLDetailsCommand [cadeia de caracteres]	O comando a ser usado para obter os detalhes do EDL.
status [booliano]	Verdadeiro indica sucesso. Falso indica falha.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.
endpoint [Criptografado]	O endpoint criptografado do banco de dados.

Firewall Palo Alto - Atividade Obter log

A atividade de fluxo de trabalho **Palo Alto Firewall: Obter log** programa uma consulta no firewall para recuperar logs e retorna um JobID usado para recuperar os dados de log.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall. Esta variável de entrada é obrigatória.
FirewallApiKey [cadeia de caracteres]	A chave de acesso de API do firewall. Esta variável de entrada é obrigatória.
FirewallLogType [cadeia de caracteres]	O tipo de dados de log a serem recuperados (definido como ameaça). Esta variável de entrada é obrigatória.
FirewallLogFilterQuery [cadeia de caracteres]	A consulta a ser executada para pesquisar logs no firewall. Esta variável de entrada é obrigatória.
LogDirection [cadeia de caracteres]	Especifica se os logs são mostrados na ordem mais antiga (para trás) ou mais recente (para frente).
LogNumber [cadeia de caracteres]	Especifica o número de logs a serem recuperados.
LogSkipCount [cadeia de caracteres]	Especifica o número de logs a serem ignorados ao fazer uma recuperação de log.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
QueuedJobID [cadeia de caracteres]	O ID do trabalho retornado do firewall.
Trabalho programado [cadeia de caracteres]	Especifica (sucesso ou falha) se o trabalho foi enviado para o firewall.
erro [cadeia de caracteres]	Todos os erros retornados.

Firewall Palo Alto - Atividade de ação de dados de trabalho

Depois que a atividade **Palo Alto Firewall: Obter log** enfileira a consulta de pesquisa no firewall e o trabalho é executado, a atividade **Palo Alto Firewall: Ação de dados do trabalho** recupera os dados do log de ameaças do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todos os campos de entrada são obrigatórios.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.
FirewallApiKey [cadeia de caracteres]	A chave de acesso de API do firewall.
JobID [cadeia de caracteres]	O ID do trabalho na fila.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
commandStatus [cadeia de caracteres]	Especifica (sucesso ou falha) se os dados foram recuperados do firewall.
Dados do trabalho [cadeia de caracteres]	Os dados coletados do firewall.
erro [cadeia de caracteres]	Todos os erros retornados.

Integração de Palo Alto Networks - WildFire

Palo Alto Networks - WildFire é uma aplicação baseada em nuvem que interage com o firewall do sistema.

Explorar

Integrações do Security Incident Response

Configurar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Ativar Operações de segurança Palo Alto Networks - WildFire
Usar Obter fluxo de trabalho de aprimoramento de dados do WildFire	**Desenvolver** • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Ativar Operações de segurança Palo Alto Networks - WildFire

Antes de poder usar a integração Palo Alto Networks - WildFire das Operações de segurança, você deve baixar a integração do ServiceNow Store.

Antes de Iniciar
Função necessária: administrador

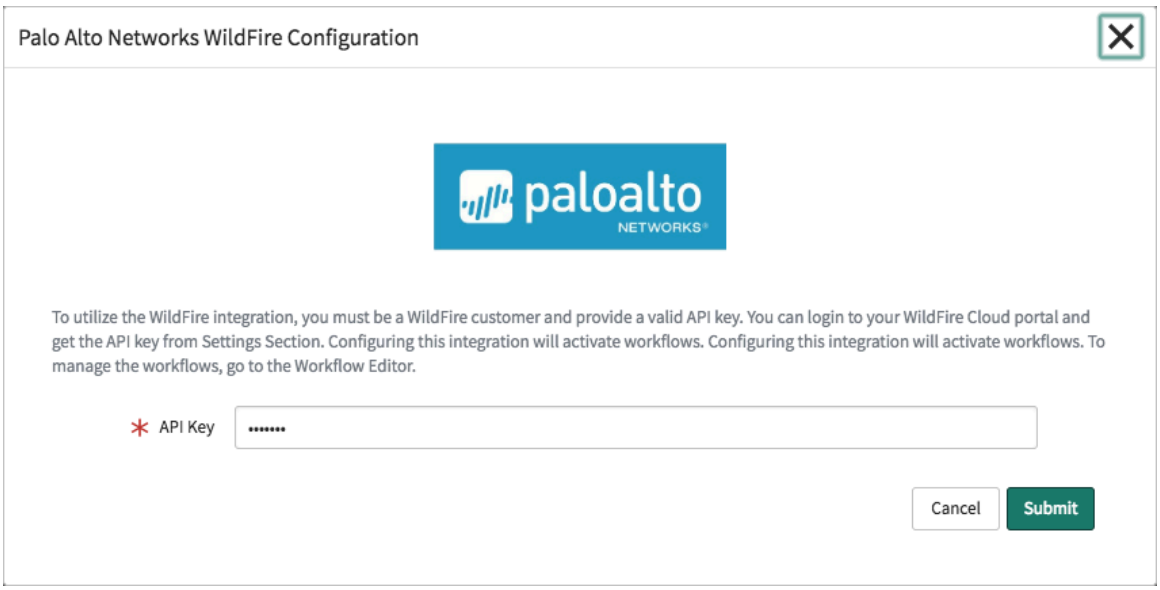
Procedimento

1. Baixe a integração do ServiceNow Store.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No cartão Carbon Black, clique em **Configurar**.



4. Insira a chave de API e clique em **Enviar**.
   O cartão de configuração de integração é exibido.
5. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Obter fluxo de trabalho de aprimoramento de dados do WildFire

Quando o fluxo de trabalho **Operações de segurança Palo Alto Networks - Obter aprimoramento de dados do WildFire** é executado, um arquivo hash é carregado no WildFire. Os dados são aprimorados e os relatórios são baixados para a instância para ajudar no processamento de possíveis ataques de malware.

Antes de Iniciar

Função necessária: sn_si.analyst

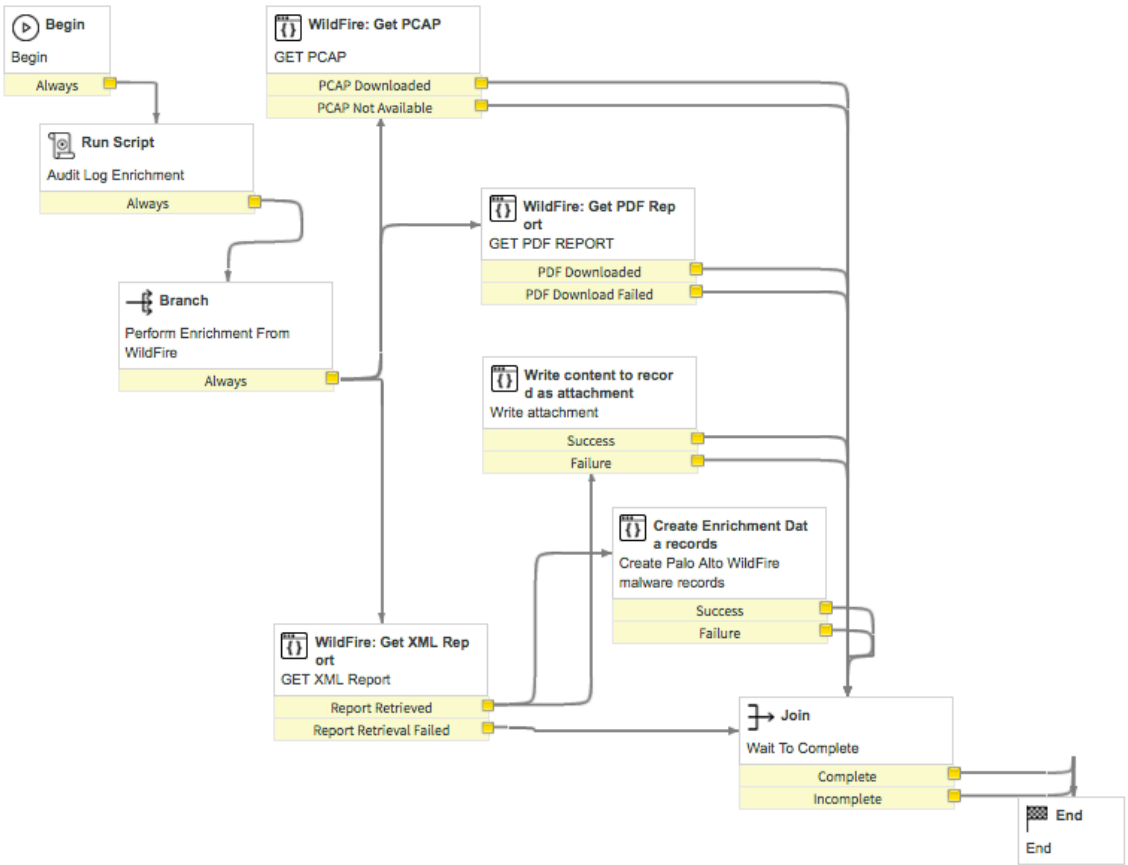
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Operações de segurança Palo Alto Networks - Obter aprimoramento de dados do WildFire** é executado quando um incidente de segurança é criado a partir de um alerta recebido da aplicação Palo Alto Network Firewall. Um hash de malware da notificação por e-mail recebida do firewall é inserido na guia **IoC** do incidente de segurança e o registro é atualizado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança Palo Alto Networks - Obter fluxo de trabalho de aprimoramento de dados do WildFire



Procedimento

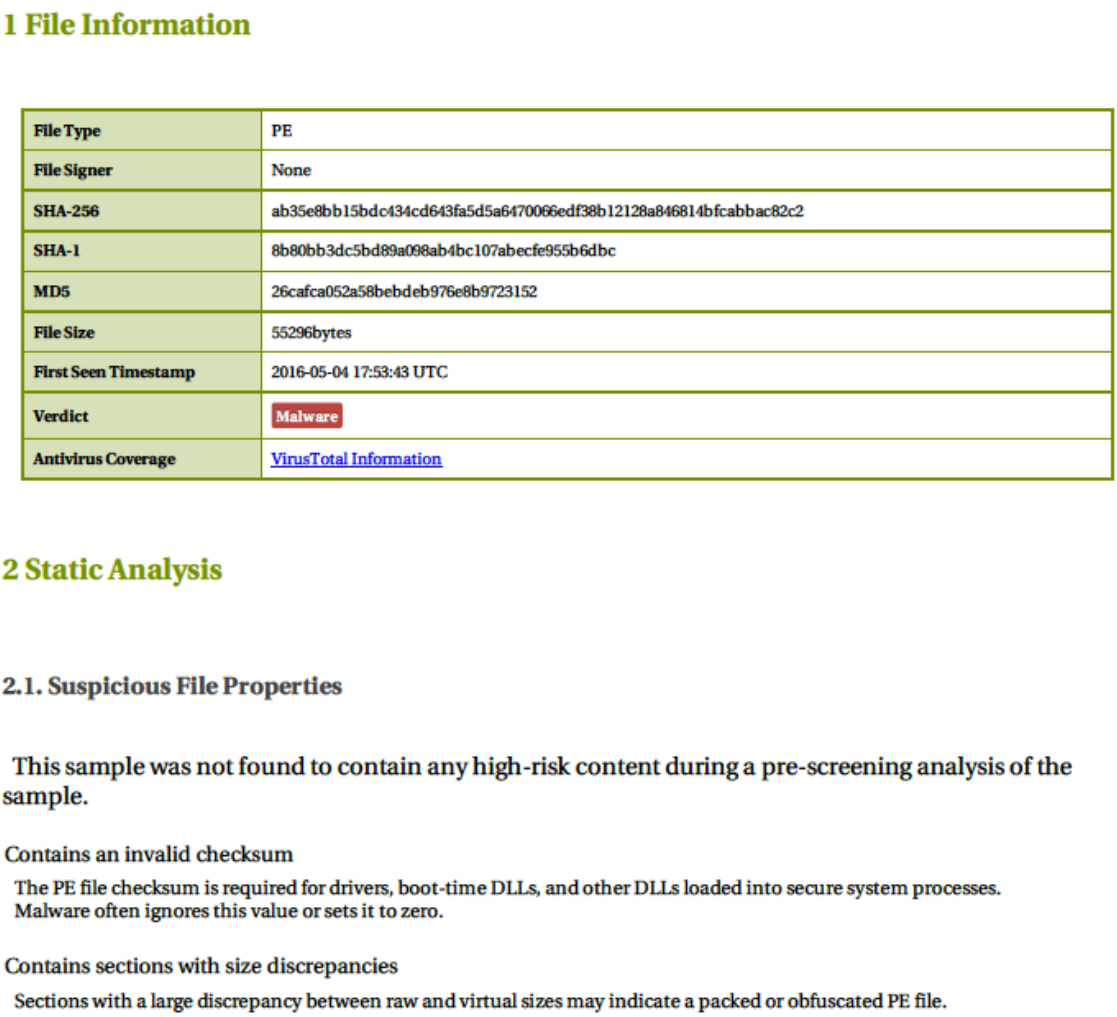
1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Com base na notificação por e-mail recebida do firewall, localize e abra o incidente de segurança que foi criado.
3. Clique na guia **Indicadores de comprometimento** e preencha o **hash de malware** com o hash que você recebeu no alerta.
4. Clique em **Atualizar**.
   O fluxo de trabalho faz com que o arquivo hash seja carregado no WildFire, onde os dados são aprimorados. Relatórios nos formatos PDF e XML são anexados ao registro (incidente de segurança ou IoC) em sua instância para ajudar no processamento de possíveis ataques de malware.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se os dados aprimorados incluírem informações de captura de pacotes, as informações de PCAP também serão baixadas. Os dados de PCAP capturam quais ações o arquivo estava executando. Por exemplo, ele pode relatar em quais servidores o arquivo estava entrando em contato. Para exibir arquivos PCAP, você precisa de um analisador de pacotes, como o Wireshark .

Exemplo de PDF gerado pelo WildFire



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Tradução automática

WildFire - obter atividade de PCAP

A atividade de fluxo de trabalho **WildFire: Obter PCAP** obtém as informações de captura de pacotes (PCAP) geradas durante a análise de um hash de arquivo especificado no WildFire. O resultado desta atividade é anexado a um registro específico conforme identificado pelo **TableName** e pelo **RecordId**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
ArquivoSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Palo Alto Network Firewall.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
TableName [cadeia de caracteres]	A tabela afetada.
RecordId [cadeia de caracteres]	O incidente de segurança ou IoC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
commandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na atividade.

Atividade WildFire - obter relatório em PDF

A atividade de fluxo de trabalho **WildFire: Obter relatório em PDF** obtém o relatório gerado durante a análise de um hash de arquivo especificado no WildFire no formato PDF. O resultado desta atividade é anexado a um registro específico conforme identificado pelo **TableName** e pelo **RecordId**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
TableName [cadeia de caracteres]	A tabela afetada.
ArquivoSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Palo Alto Network Firewall.
RecordId [cadeia de caracteres]	O incidente de segurança ou IoC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
commandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade WildFire- obter relatório XML

A atividade de fluxo de trabalho **WildFire: Obter relatório XML** obtém o relatório gerado durante a análise de um hash de arquivo especificado no WildFire no formato XML. O resultado desta atividade é anexado a um registro específico conforme identificado pelo **TableName** e pelo **RecordId**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
TableName [cadeia de caracteres]	A tabela afetada.
ArquivoSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Palo Alto Network Firewall.
RecordId [cadeia de caracteres]	O incidente de segurança ou IoC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
commandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na atividade.

Integração de Palo Alto Networks Next-Generation Firewall

Depois de instalado e configurado, o analista de incidentes de segurança usa essa integração para bloquear endereços IP, URLs e domínios mal-intencionados usando recursos de lista dinâmica externa (EDL) com os produtos ServiceNow Security Incident Response (SIR). O analista de incidentes de segurança cria entradas para um EDL a partir de observáveis determinados como mal-intencionados em ServiceNow SIR incidentes de segurança.

Um EDL é um arquivo de texto hospedado em um servidor Web externo. Para esta integração, este servidor Web é sua instância Now Platform, o que permite que o Palo Alto Networks Next-Generation Firewall importe objetos que estão incluídos na lista, endereços IP, URLs e domínios e aplique a política.

Para impor a política nas entradas de EDL, a lista é referenciada em uma regra ou perfil de política. Conforme as entradas de EDL são modificadas, o firewall importa dinamicamente a lista no intervalo configurado e impõe a política sem uma mudança de configuração ou uma confirmação no firewall. Para esta integração, Now Platform criou uma tabela contendo entradas de EDL que são recuperadas pelo autorizado Palo Alto Networks Next-Generation Firewall nos intervalos de recuperação configurados.

A integração inclui os seguintes recursos:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Flexibilidade para criar vários EDLs que se aplicam a diferentes políticas de negação ou permissão do firewall.
- Relatórios detalhados sobre os tipos de sites que estão sendo bloqueados (phishing, malware e sites permitidos).
- Marcação de Now Platform incidentes de segurança com entradas de EDL pelo tipo de observável (URL, domínio, endereço IP).
- Configurar períodos de expiração de EDL para manter o tamanho da lista de EDL expirando ou removendo automaticamente entradas mais antigas.
- Pesquisar, excluir ou migrar entradas de EDL entre listas de EDL.
- Vincular entradas de EDL a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

A integração requer que os plug-ins (com.snc.security_incident) e (com.snc.secops.orchestration) do produto Security Incident Response estejam ativados.

Esta integração é compatível somente com Palo Alto Networks (PAN-OS 8.x). Versões anteriores não são compatíveis.

Essa integração é compatível com as versões Kingston, London, Madrid e New York do Now Platform®.

Nota: Os tópicos a seguir estão numerados. Para uma instalação, configuração e verificação sem problemas dos resultados esperados, siga os tópicos na ordem em que são apresentados.

Criar um perfil de certificado para o Palo Alto Networks Next-Generation Firewall

A integração requer um perfil de certificado para validar e autenticar a conexão segura entre o servidor Now Platform® e o servidor Palo Alto Networks Next-Generation Firewall.

Antes de Iniciar
Função necessária: Palo Alto Networks Next-Generation Firewall Administrador

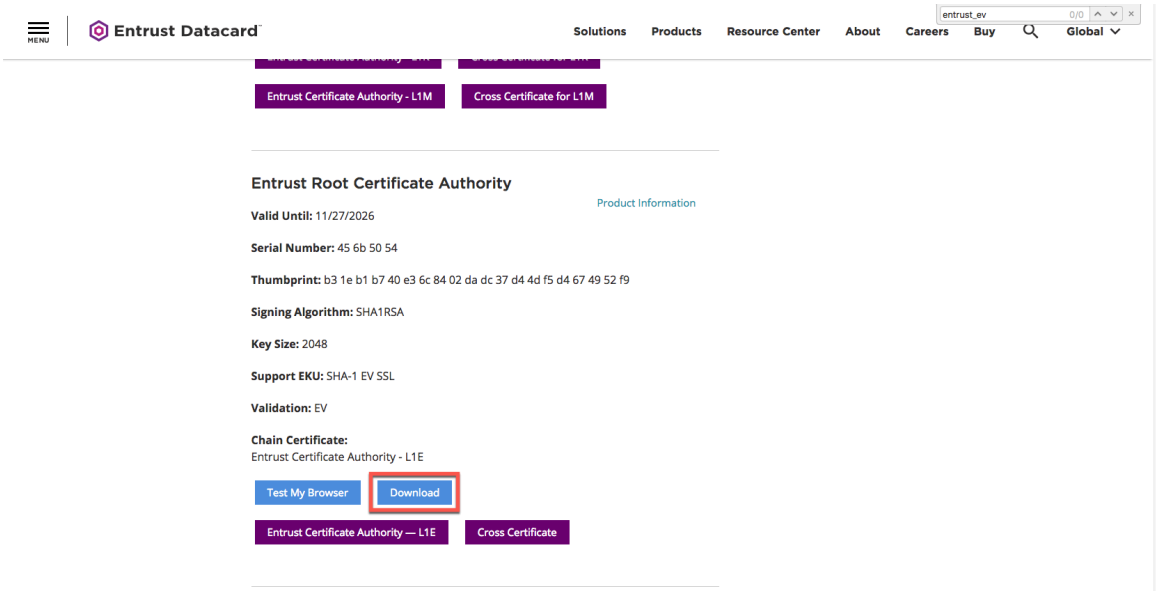
Por Que e Quando Desempenhar Esta Tarefa
Um Palo Alto Networks Next-Generation Firewall autentica em uma instância Now Platform®, recupera entradas de EDL da tabela de banco de dados e incorpora as entradas nas regras de política de firewall correspondentes. Esta recuperação requer a função de conta de usuário da API na instância Now Platform®, que é usada pelo administrador do firewall do PAN para acessar a API Now Platform®.

O administrador Palo Alto Networks Next-Generation Firewall cria um perfil de certificado em Palo Alto Networks. Este certificado valida e autentica a conexão segura entre o servidor [Now Platform® e o servidor de firewall Palo Alto Networks.

Now Platform® usa Entrust como uma autoridade de certificação e o perfil de certificação necessário é criado usando o certificado `entrust_ev_ca.cer`. Este certificado está disponível para download no site do cartão EntrustData™. Para garantir que você esteja obtendo as versões mais atuais, baixe esses certificados diretamente do site da Entrust.

Procedimento
1. Navegue até Certificados raiz Download .
2. No site da Entrust, role até o **certificado da autoridade de certificação raiz Entrust**, conforme mostrado na figura a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique **em Download**.
   O nome do arquivo baixado é **entrust_ev_ca.cer**.
4. Consulte a documentação Palo Alto Networks para saber como configurar o perfil de certificado depois de baixá-lo.
   Os requisitos podem ser encontrados no site Palo Alto Networks.

Informações relacionadas

"Configurar um perfil de certificado" no Guia do administrador do PAN-OS 10.0

Configurar e instalar Palo Alto Networks Next-Generation Firewall

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação sem problemas.

Antes de Iniciar

Função necessária: (admin)

Configuração de tarefa	Descrição
Verifique se você tem as funções Now Platform e Security Incident Response atribuídas.	As seguintes funções são necessárias: • O administrador do sistema (admin) instala o aplicativo e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e cria, ativa e remove EDLs. Esta função também atribui a função sn_si.analyst. • O (admin) atribui a função de conta de API Now Platform® (sn_sec_panfw.api_account_access), que é usada exclusivamente para inserir credenciais necessárias para autenticação em Palo Alto Networks, para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	que os firewalls possam recuperar EDLs de Now Platform®. • (sn_si.analyst) ou Analista do Centro de Operações de Segurança (SOC), cria entradas de EDL e trabalha com incidentes de segurança.
Verifique se você está usando Palo Alto Networks Next-Generation Firewall versão-OS 9.x e 10.x.	Esta integração é compatível somente com Palo Alto Networks Next-Generation Firewall OS 9.0 e posterior.
Configure perfis de EDL, regras de política de segurança e perfis de certificado em Palo Alto Networks, conforme recomendado na documentação de Palo Alto Networks.	Consulte Palo Alto Networks a documentação geral e os requisitos no: site de documentação da Paloalto Networks .
Verifique se você baixou e configurou o certificado Entrust™ da autoridade de certificação raiz.	A integração requer este certificado para validar e autenticar a conexão segura entre o servidor Now Platform e o servidor Palo Alto Networks Next-Generation Firewall. Para obter mais informações sobre como configurar o certificado, consulte "Configurar um perfil de certificado" no Guia do administrador do PAN-OS 10.0 . Para o download, consulte Criar um perfil de certificado para o Palo Alto Networks Next-Generation Firewall e Download de certificados raiz .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posterior Para a versão Madrid e as versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	3. Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .
Se sua organização tiver Now Platform® processos de aprovação e gestão de mudanças para exclusão de e-mail, verifique se a capacidade de envio/ recebimento de e-mail está habilitada.	Para verificar se a capacidade de envio/ recebimento de e-mail está habilitada em sua instância Now Platform®, navegue até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**. Em Configuração de e-mail de saída, verifique se **o envio** de e- **mail e o recebimento de** e-mail estão selecionados.

Procedimento

Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.

Criar a função de conta de API para Palo Alto Networks Next-Generation Firewall

Uma função de conta de API é necessária em sua instância Now Platform® para esta integração. O nome de usuário e a senha associados a esta conta são criados em Now Platform® e inseridos em Palo Alto Networks, portanto, Palo Alto Networks Next-Generation Firewall é autenticado com Now Platform® ao recuperar entradas de EDL.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O administrador Now Platform® cria uma função de conta de API (sn_sec_panfw.api_account_access). Esta conta é usada exclusivamente para inserir credenciais necessárias para autenticação em Palo Alto Networks para que os firewalls possam recuperar EDLs de Now Platform®. Esta conta é uma conta de usuário de API separada e exclusiva na instância Now Platform® e atribuída ao administrador Palo Alto Networks Next-Generation Firewall.

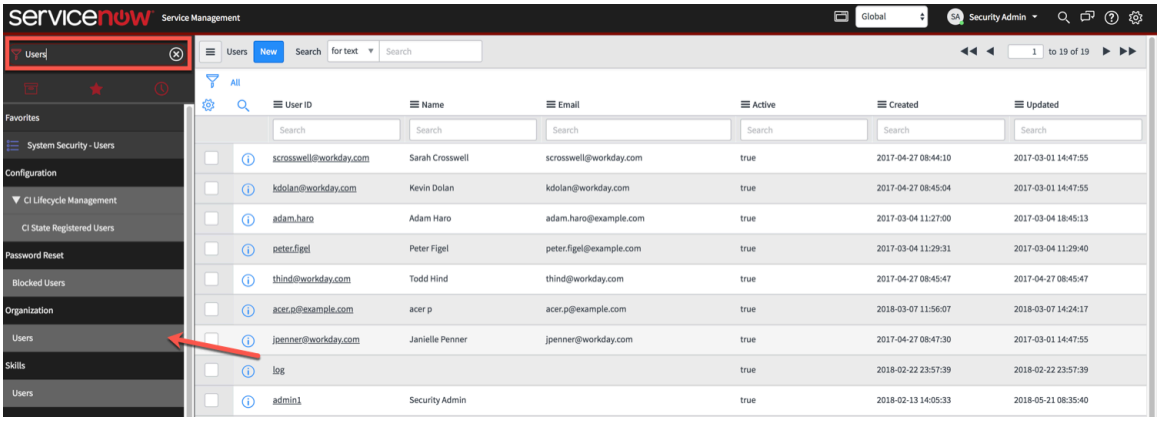
Procedimento

1. Navegar até **Todos** > **Organização** > **Usuários**.

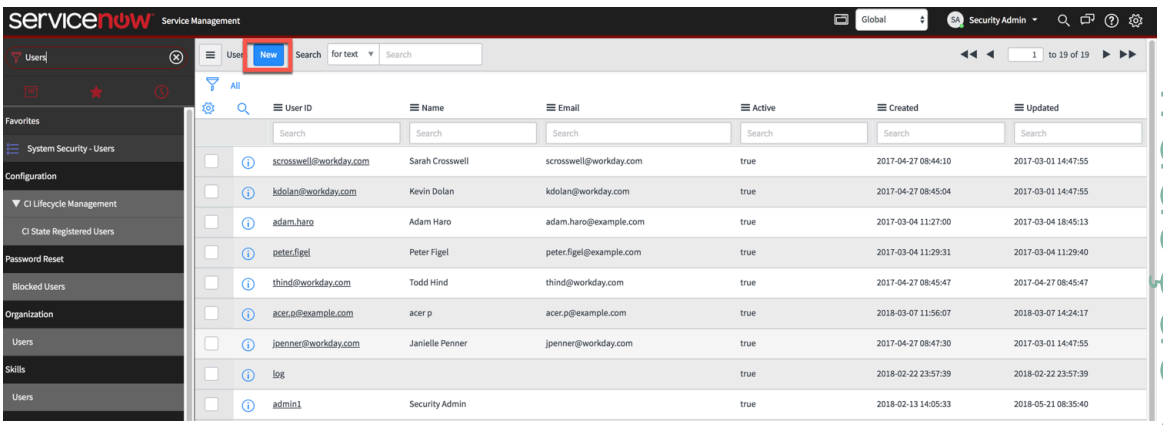
2. Clique no módulo **Usuários**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na lista Usuários exibida, clique em **Novo**.



Um novo formulário de usuário é exibido.

4. Preencha o formulário.

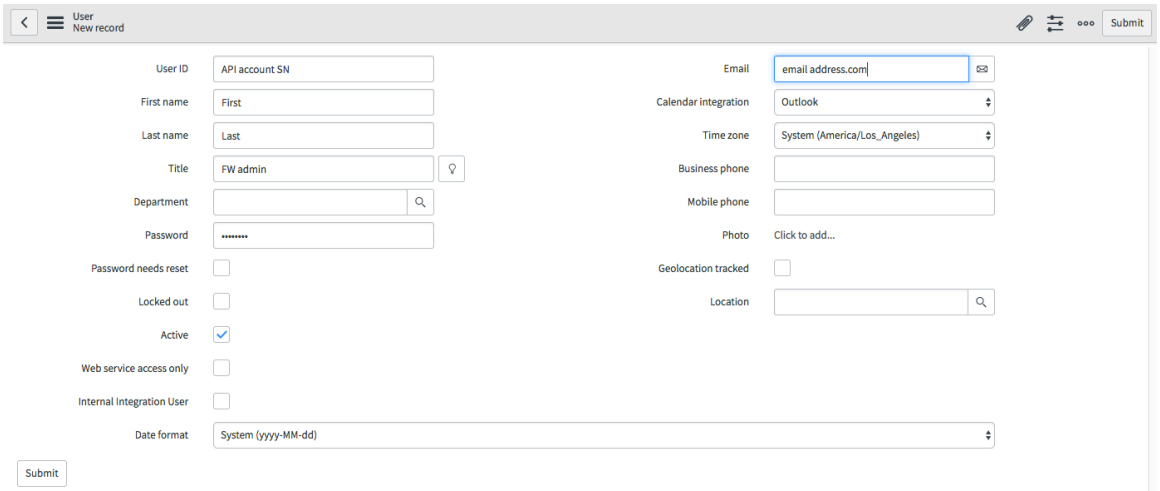
Nota: Os valores de título do ID do usuário e endereço de e-mail mostrados na tabela e na figura a seguir são valores de exemplo.

Campo	Descrição
ID do Usuário	ID de usuário exclusivo para a função em sua instância Now Platform®. Este ID de usuário é inserido no campo **Nome** de usuário na seção **Autenticação de cliente** da caixa de diálogo Listas dinâmicas externas no site Palo Alto Networks. Um exemplo é `a conta de API SN`.
Nome	Pessoa que você está atribuindo.
Sobrenome	Pessoa que você está atribuindo.
Título	Cargo, por exemplo, `FW admin`.
Senha	Senha exclusiva criada para esta função. Esta senha é inserida no campo **Senha** na seção **Autenticação de cliente** da caixa de diálogo Listas dinâmicas externas no site Palo Alto Networks.

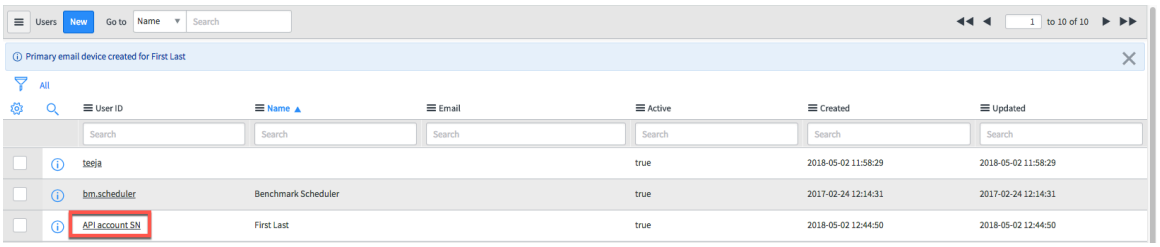
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

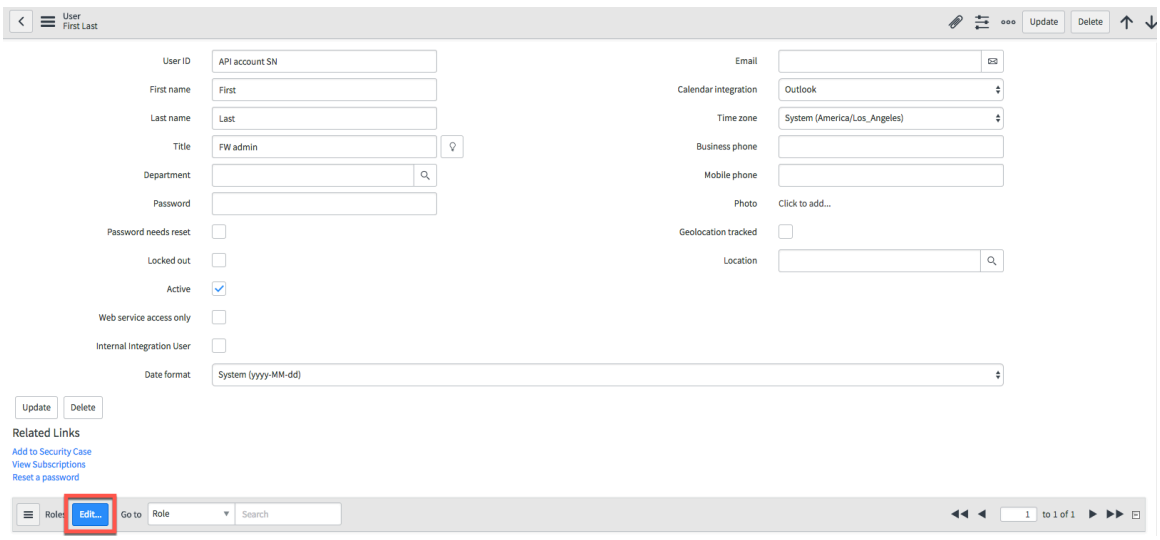
Campo	Descrição
E-mail	Endereço de e-mail exclusivo.



5. Clique em **Enviar**.
   Depois de enviado, você pode atribuir a função.
6. Na lista Usuários na coluna **ID** do usuário, clique no nome do ID do usuário que você inseriu, `SN da conta de API`, por exemplo.



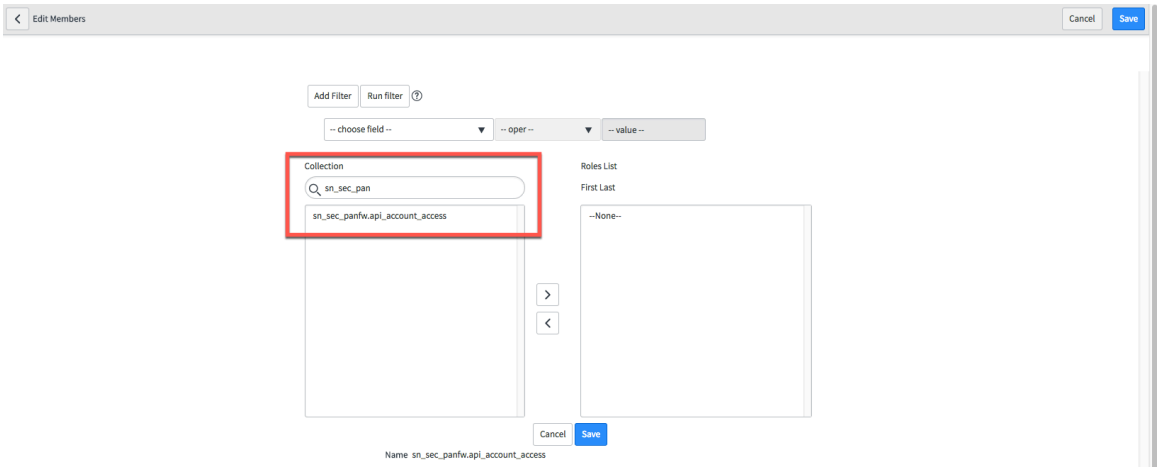
7. No registro aberto na seção Funções, clique em **Editar**.



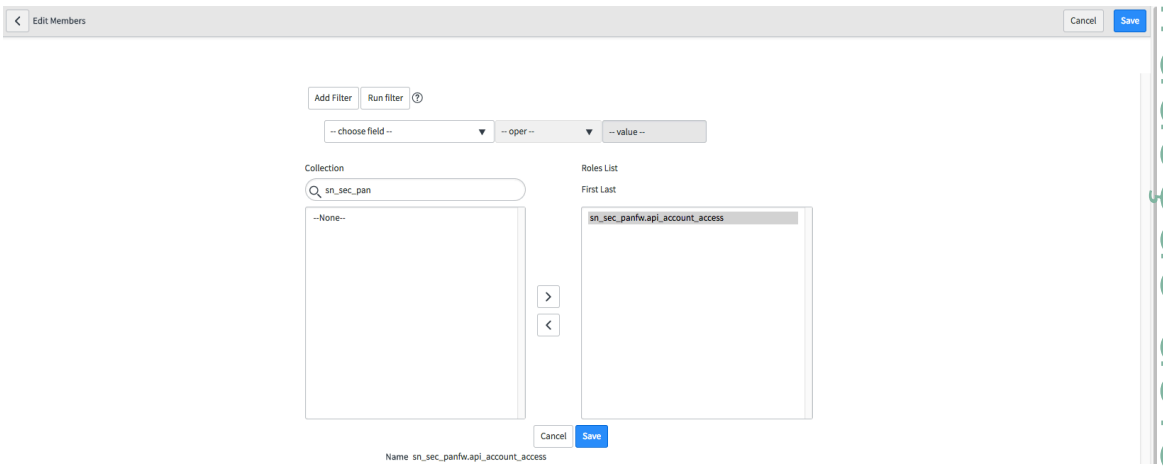
8. No formulário **Editar Membros**exibido, insira `sn_sec_panfw.api_account_access` no campo **Coleção**.
   Abaixo do campo **Coleção**, a função é exibida na coluna.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



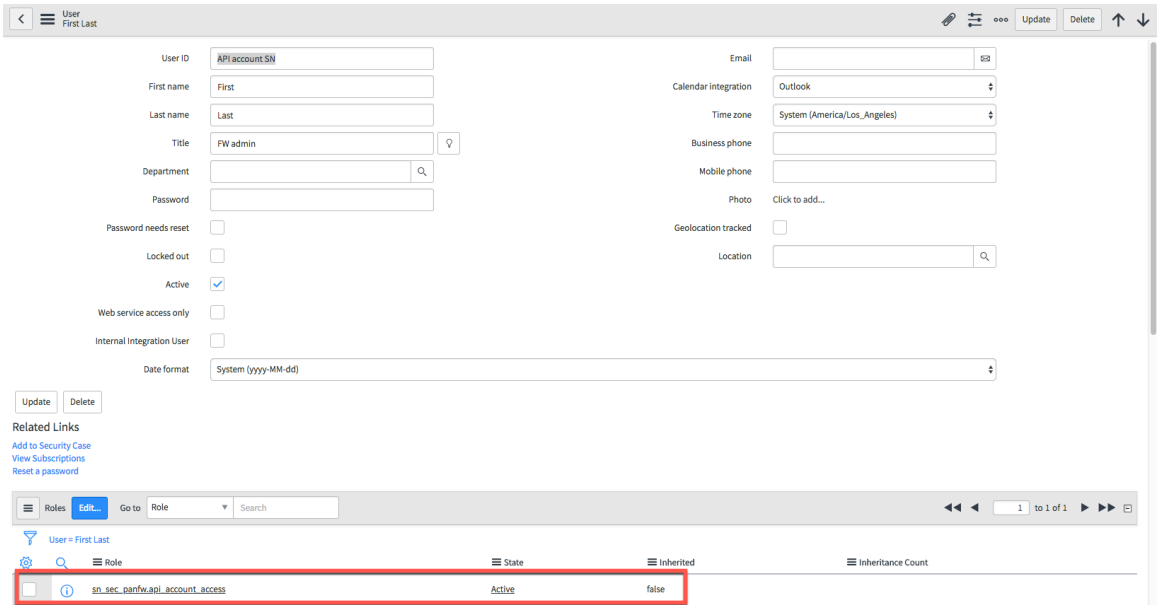
9. Na coluna **Coleção**, selecione e mova `sn_sec_panfw.api_account_access` para a **Lista de funções**.



10. Clique em **Salvar**.
11. Navegue até **Usuários**e, na coluna **Usuário** da lista, clique no nome do ID que você criou para a função (`SN da conta da API`).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro do usuário é exibido. Este registro verifica se a conta do usuário foi atribuída. O **estado** está ativo e a função não é herdada.

Listas dinâmicas externas compatíveis com Palo Alto Networks Next-Generation Firewall

A integração ServiceNow Palo Alto Networks Next-Generation Firewall é compatível com listas dinâmicas externas (EDLs) que aceitam IP, URL e observáveis de domínio.

EDLs e observáveis compatíveis

Uma lista dinâmica externa é um arquivo de texto hospedado em um servidor webexterno que, para esta integração, é a instância Now Platform. O Palo Alto Networks Next-Generation Firewall pode importar objetos - endereços IP, URLs, domínios - incluídos na lista e impor a política. Para impor a política nas entradas de EDL, a lista é referenciada em uma regra ou perfil de política.

Esta integração oferece suporte a três tipos de EDLs:

- IP (isso inclui um único endereço IP, bem como blocos CIDR (intervalos) de endereços).
- URL
- Domínio

A tabela a seguir lista as descrições dos observáveis compatíveis com esta integração e exemplos de formatos para cada tipo.

Observáveis e formatos de exemplo compatíveis

Observável	Formatos de exemplo	Descrição
Endereço IP	• 95.153.103.54 (IPv4) • (IPv6): 2001:00B8:130F:FE03:0000:09C0:080E:1305	Representa um endereço de interface único e distinto. A integração é compatível com os formatos IPv4, IPv6 e CIDR. O suporte para observáveis de endereço IP inclui

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observáveis e formatos de exemplo compatíveis

Observável	Formatos de exemplo	Descrição
		intervalos CIDR (Roteamento entre domínios sem classe), por exemplo, 95.153.100.0/22. Observação: uma mensagem de erro é exibida quando você tenta anexar um único endereço IP a um EDL que você já bloqueou como parte de um intervalo de CIDR. Por exemplo, o endereço único 95.153.103.54 faz parte do intervalo CIDR representado por 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.example.com • www.example.com/article.html • example.com • *.exemplo.com	Caracteres curinga são compatíveis. O Now Platform reformata as entradas de URL para atender aos requisitos de formato Palo Alto Networks da EDL.
Domínio	• www.exemplo.com • example.com • mail.example.com	Caracteres curinga não são compatíveis.

Para obter mais informações sobre diretrizes de formatação e EDLs, consulte "Diretrizes de formatação para uma lista dinâmica externa" no Guia do administrador do PAN-OS 10.0 no site Palo Alto Networks.

Criar uma EDL para o firewall de última geração da Palo Alto Networks

Crie uma lista dinâmica externa (EDL) em sua instância Now Platform. Depois de aprovado e ativado, você pode criar entradas para EDLs a partir de observáveis determinados como mal-intencionados em Now Platform Security Incident Response incidentes (SIR) e solicitar aprovação para bloqueá-los.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Crie a EDL em sua instância Now Platform para que o firewall possa importar objetos (endereços IP, URLs, domínios) incluídos na lista e impor a política. Para impor a política nas entradas de EDL, a lista é referenciada em uma regra ou perfil de política.

As imagens na seção a seguir são mostradas com os **Formulários** com guia limpos em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

formulários com guias, consulte a seção "Exibir formulários com guias" em Configuração do layout do formulário .

Procedimento

1. Depois que a instalação da aplicação estiver concluída, navegue até **Integrações** > **Configurações de Integração**.
2. Localize o bloco Palo Alto Networks Next-Generation Firewall e clique em **Configurar**.

3. Clique **em Criar nova lista de EDL**.

4. No formulário, preencha os campos.

Palo Alto Networks Formulário Lista dinâmica externa do firewall

Campo	Descrição
Nome	Palo Alto Networks Nome da lista dinâmica do firewall. Inclua o tipo de observável (URL, IP, domínio) neste campo para que o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	analista de segurança possa reconhecer facilmente a intenção da EDL pelo nome. O nome também deve indicar claramente para qual política de firewall esses objetos EDL estão mapeados. Alguns exemplos de nomes de EDL são IP de malware de saída ou URL de phishing de saída.
Ativo	Esta caixa de seleção está desmarcada por padrão para indicar que a EDL está inativa. Quando inativo, o EDL não pode receber entradas adicionais. Quando a caixa de seleção está marcada, a EDL é ativada e fica disponível para entradas de EDL.
Marcador de exibição	A caixa de seleção é marcada por padrão para marcar automaticamente o observável e o registro de incidente de segurança associado se o observável estiver bloqueado em uma EDL. Quando selecionado, o tipo de marcador e o marcador EDL para campos de observáveis ficam disponíveis no formulário. **Nota:** Um nome de marcador é criado por padrão a partir do valor inserido no campo **Nome** com um prefixo EDL-, por exemplo, EDL-Malware OutBound IP. Você pode mudar o nome e a cor do marcador. Consulte: (Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall. O nome do marcador é exibido no campo Marcador da EDL para observáveis quando a EDL é salva. Quando a caixa de seleção está desmarcada, nenhum marcador é criado e o tipo de marcador e o marcador EDL para campos de observáveis não estão disponíveis no formulário.
Tipo de observável	Selecione um tipo de observável que este EDL aceita na lista de seleção: IP (incluindo CIDR), URL ou domínio.
Tipo de marcador	Marcadores que estão disponíveis na lista de seleção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Uma lista de bloqueios é uma lista de observáveis que você deseja que o Palo Alto Networks Next-Generation Firewall bloqueie. Uma lista de permissões é uma lista de observáveis que você deseja que o Palo Alto Networks Next-Generation Firewall permita. Por padrão, a cor do marcador da Lista de bloqueios é preta e a cor do marcador da Lista de permissões é cinza. Você pode mudar a cor. Consulte: (Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em sua instância Now Platform, que estão anexadas ao registro de EDL. A solicitação de mudança é usada para configurar o URL de recuperação da lista de EDL no servidor Palo Alto Networks Next-Generation Firewall. Esta opção é recomendada se o administrador do firewall também estiver usando o Now Platform para mudanças de política ou regra de firewall. Se você criar uma solicitação, depois que ela for fechada, a lista de EDL será ativada automaticamente. Desmarque a caixa de seleção para ativar manualmente o EDL após receber um aviso por e-mail do administrador do firewall de que a configuração em Palo Alto Networks foi concluída. Quando a caixa de seleção de Criar solicitação de mudança está desmarcada, o campo Solicitação de mudança fica indisponível.
Marcador de EDL para observáveis	Este campo será exibido somente se a caixa de seleção Exibir marcador estiver marcada. O campo é preenchido automaticamente depois que a EDL é salva com um valor padrão do campo Nome.

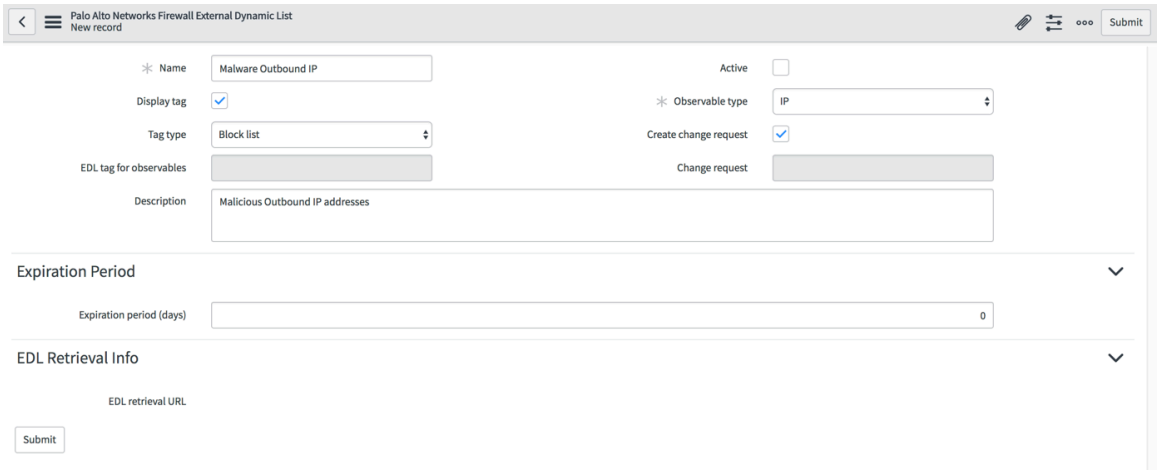
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

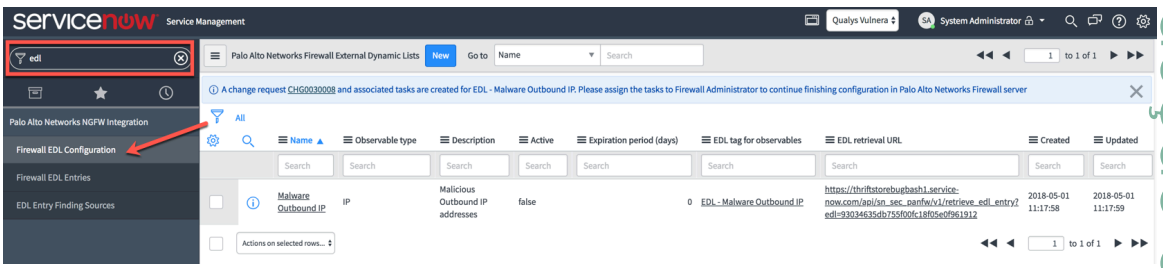
Campo	Descrição
	Para obter mais informações sobre como alterar o nome e a cor do marcador padrão, consulte (Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall
Solicitação de mudança	Quando a caixa de seleção Criar solicitação de mudança está marcada, o número da solicitação de mudança é exibido na instância Now Platform depois que a EDL é salva. Quando a caixa de seleção de Criar solicitação de mudança está desmarcada, este campo não é exibido.
Descrição	Descrição da lista dinâmica do firewall da Palo Alto Networks. O nome geralmente contém os tipos de sites e observáveis que você espera que estejam neste EDL e você pode usar este campo para obter mais detalhes.
Período de expiração (dias)	Período de expiração da EDL. 0 (o padrão) indica que a entrada de EDL nunca expira. Se você alterar este valor, esta entrada ficará ativa pelo número de dias inserido. Você pode inserir um valor mínimo de 1 e não há valor máximo. Por exemplo, se você inserir `30` dias às 14h01 do dia 1º de maio, a EDL expirará às 14h01 do dia 31 de maio. Todas as entradas nesta EDL herdam este valor por padrão, a menos que você substitua o valor com base na entrada individual.

Tradução automática

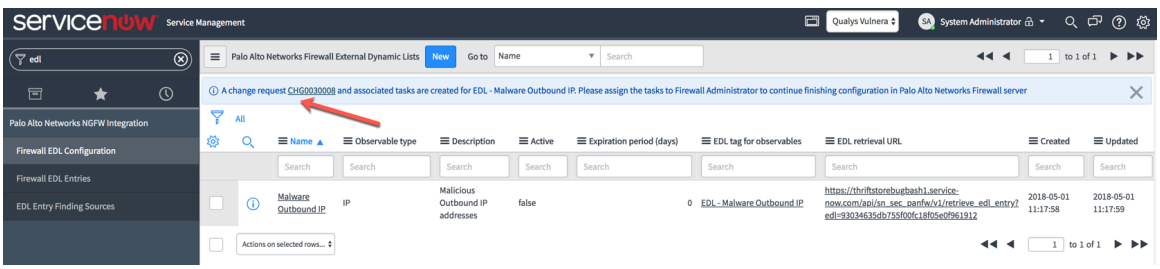
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
6. Se a lista Listas dinâmicas externas do firewall da Palo Alto Networks não for exibida, navegue até **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall** e clique em **Configuração de EDL do firewall**.



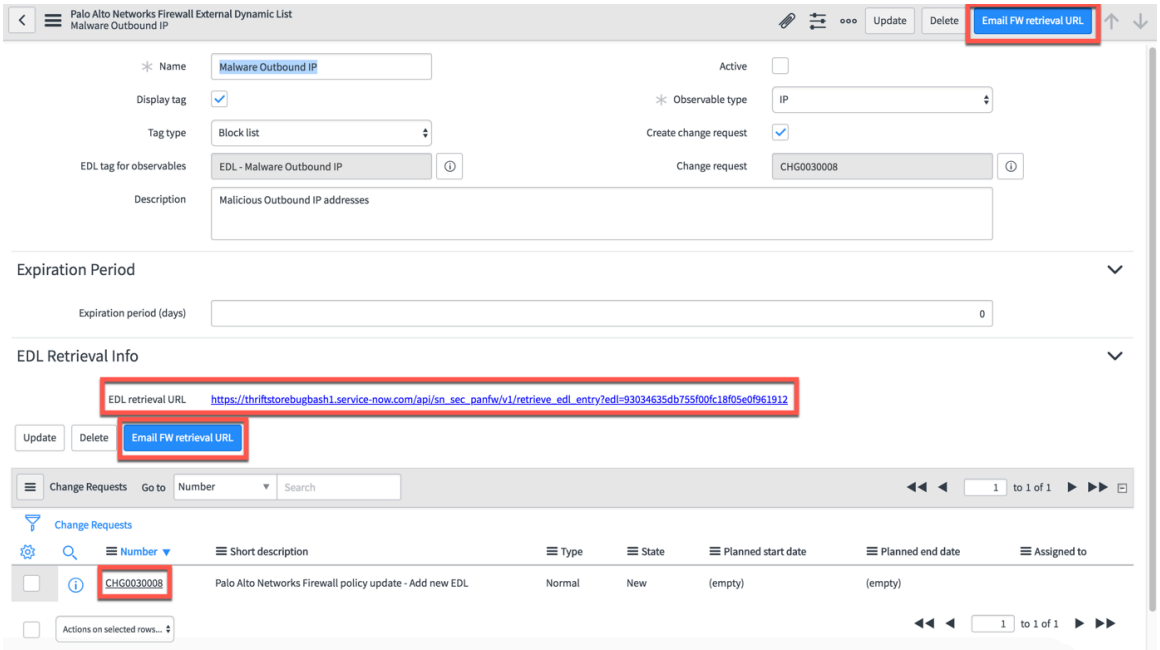
O novo EDL é exibido. O status da EDL ainda está inativo (`falso`), o que significa que a EDL não está disponível para aceitar entradas. Se **Criar solicitação de mudança** tiver sido configurado, uma mensagem será exibida indicando que uma solicitação de mudança e tarefas foram criadas em sua instância Now Platform.



7. Na coluna **Nome**, clique em um item para abrir o registro.
   O registro de EDL é exibido. Este exemplo mostra um EDL de IP de saída de malware. Os campos, opções e links a seguir são exibidos no novo registro após o envio e descritos na tabela a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



URL de recuperação e links de solicitação de mudança no registro de EDL

Opção	Descrição
URL de recuperação do firmware do e-mail	Envia por e-mail um aviso de que o link da EDL está disponível para configuração ao administrador do firewall Palo Alto Networks.
URL de recuperação da EDL	Este URL é colocado no campo **Origem** na caixa de diálogo de autenticação Listas dinâmicas externas na guia **Criar lista** no site Palo Alto Networks. O link de URL que o administrador do firewall Palo Alto Networks usa para configuração no firewall Palo Alto Networks é gerado e exibido automaticamente. **Nota:** Se você tiver as Configurações do sistema definidas como **Formulários com guias**, este link será exibido na guia **Informações de recuperação de EDL** na parte inferior do registro.
Now Platform solicitação de mudança	Um link para o registro de solicitação de mudança é exibido na seção Solicitações de mudança quando configurado, e o número da solicitação é exibido no campo Solicitação de mudança.
Atualizar	Modifique os dados e atualize os campos editáveis.
Excluir	Exclua o registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Crie e adicione mais EDLs conforme necessário.
   Os EDLs são exibidos na lista Palo Alto Networks Listas dinâmicas externas.

O que Fazer Depois

Ative uma EDL manualmente ou com uma solicitação de mudança Now Platform.

Ativar uma EDL para Palo Alto Networks Next-Generation Firewall

Depois que a lista dinâmica externa (EDL) foi criada no seu Now Platform® e o URL está disponível, o administrador do firewall do Palo Alto Networks configura o EDL no Palo Alto Networks Next-Generation Firewall. O URL de recuperação é usado pelo administrador do firewall Palo Alto Networks para configurar o EDL no servidor Palo Alto Networks Next-Generation Firewall. Antes que possa aceitar entradas de EDL, a EDL deve ser configurada em Palo Alto Networks e ativada em Now Platform®.

Antes de Iniciar

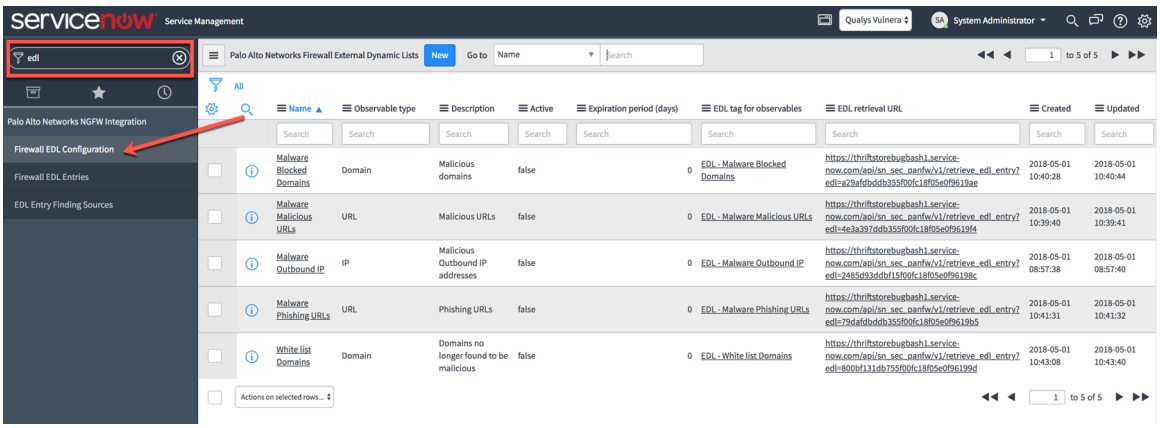
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Depois que a EDL for configurada, como administrador do incidente de segurança, você poderá ativar a EDL manualmente ou a EDL será ativada automaticamente após a conclusão de uma Now Platform® Solicitação de Mudança. A EDL deve ser aprovada e movida do estado inativo para o estado ativo antes que possa aceitar entradas de EDL.

Procedimento

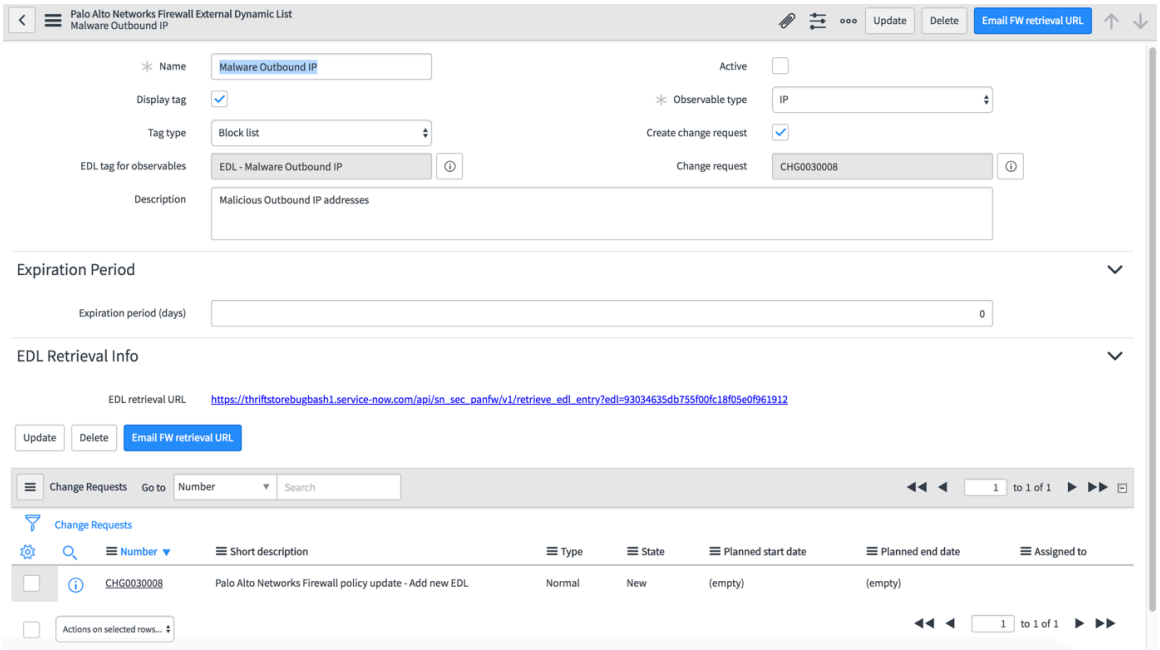
1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall** e selecione o módulo **Configuração de EDL do firewall**.



2. Na lista Listas dinâmicas do firewall da Palo Alto Networks exibida, selecione sua nova EDL na coluna Nome.
3. No registro exibido, observe os botões de **URL de recuperação de FW de e-mail**, o link da URL de recuperação de EDL ativo e, se configurado, a solicitação de mudança Now Platform® na seção Solicitações de mudança.
   Certifique-se de que a caixa de seleção **Ativo** esteja desmarcada.

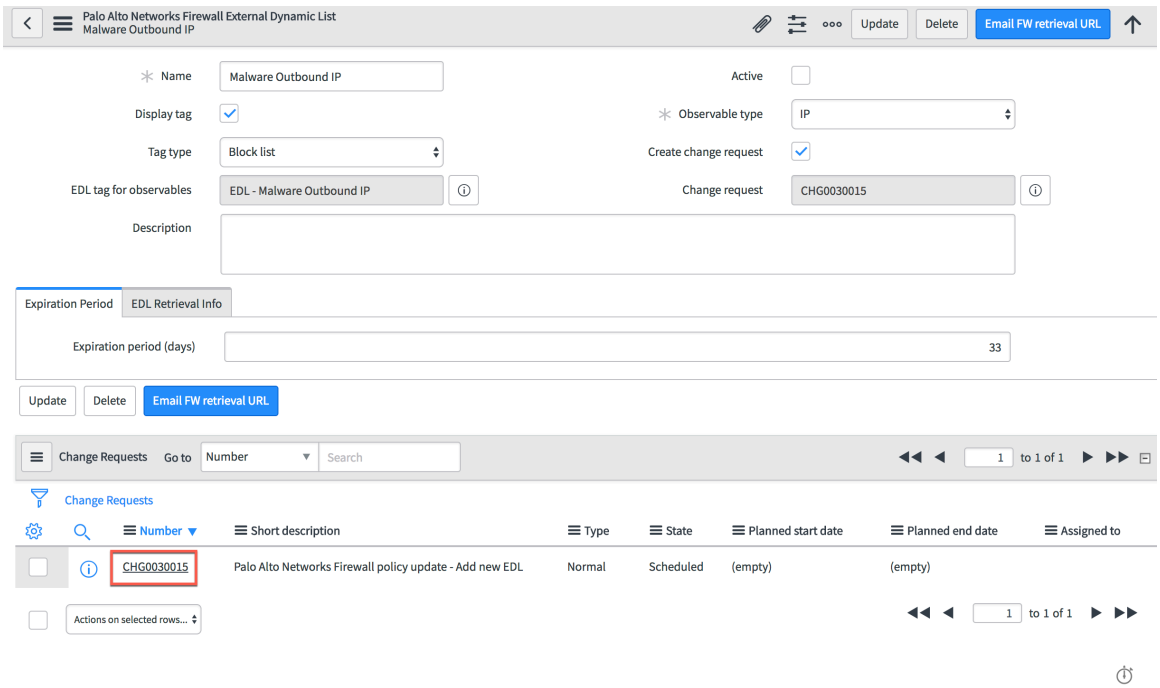
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Com os **formulários com guias** limpos nas configurações do sistema, a URL de recuperação de EDL aparecerá na seção **Informações de recuperação** de EDL, conforme mostrado na figura anterior.

A figura a seguir mostra as **informações de recuperação de EDL** exibidas como uma guia com os **formulários** com guia selecionados nas configurações do sistema. Clique na guia **Informações de recuperação de EDL** para exibir o URL de recuperação. O link para a solicitação de mudança (**CH0030015**) também é exibido.



4. Para concluir a configuração e mover o EDL de inativo para ativo, você deve escolher uma das seguintes opções para notificar o administrador do firewall de que o URL de recuperação está disponível.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Clique **em URL de recuperação de FW de e-mail**.	Envie a URL de Recuperação de EDL por e-mail diretamente para o administrador do firewall. Esta opção permite que o administrador do firewall conclua a configuração na plataforma Palo Alto Networks. Escolha esta opção se o administrador do firewall não estiver usando o Now Platform® . **Nota:** O administrador de incidentes de segurança ativa manualmente o EDL no Now Platform® depois de receber um aviso de que a configuração do Palo Alto Networks Next-Generation Firewall foi concluída. Consulte: Ativar um EDL manualmente para Palo Alto Networks Next-Generation Firewall.
Conclua a solicitação de mudança Now Platform® e atribua as tarefas de configuração ao administrador do firewall.	Esta opção estará disponível somente se o administrador de firewall para Palo Alto Networks também estiver usando o Now Platform®e os processos de aprovação e gestão de mudanças Now Platform® estiverem configurados. **Nota:** Usuários com a função sn_si.admin podem aprovar a solicitação de mudança Now Platform®. Depois que as tarefas de configuração são concluídas e a solicitação de mudança é encerrada, a EDL é ativada automaticamente. Consulte: Ativar uma EDL para Palo Alto Networks Next-Generation Firewall com uma solicitação de mudança.

Depois de notificar o administrador do firewall de que o URL de recuperação está disponível e você confirmar que a EDL foi configurada em Palo Alto Networks, como administrador de incidentes de segurança, a próxima etapa é ativar a EDL. Você ativa o EDL manualmente ou, se configurado, usa o formulário de solicitação de mudança Now Platform para ativar o EDL.

Informações relacionadas

Configurar um EDL em Palo Alto Networks Next-Generation Firewall

Ativar um EDL manualmente para Palo Alto Networks Next-Generation Firewall

Se o administrador do firewall da Palo Alto Networks não estiver usando o Now Platforme você for notificado diretamente de que o Palo Alto Networks Next-Generation Firewall está configurado, você poderá ativar a lista dinâmica externa (EDL) manualmente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Em Palo Alto Networks, atribua um objeto EDL, uma política e a URL de origem à EDL que você criou. Para obter mais informações sobre como configurar o EDL para Palo Alto Networks Next-Generation Firewall em Palo Alto Networks, consulte Configurar um EDL em Palo Alto Networks Next-Generation Firewall.

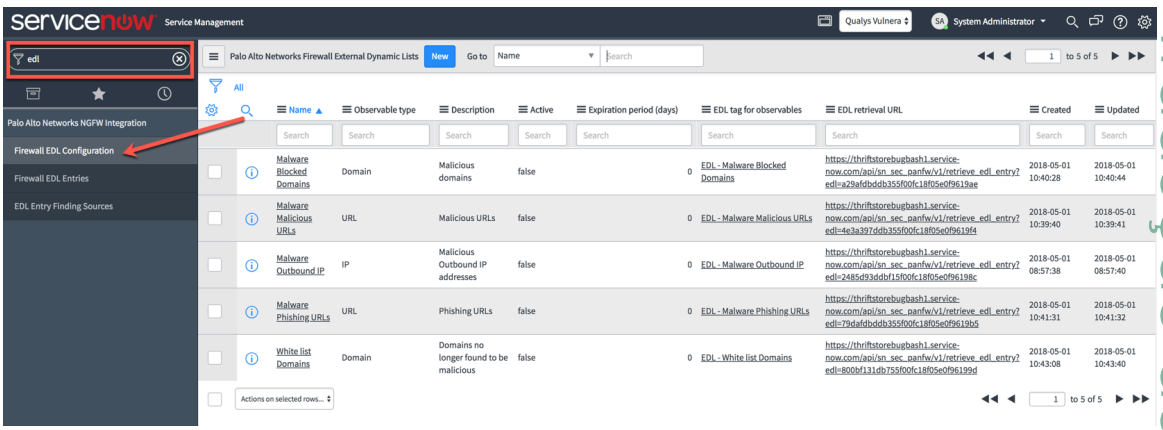
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

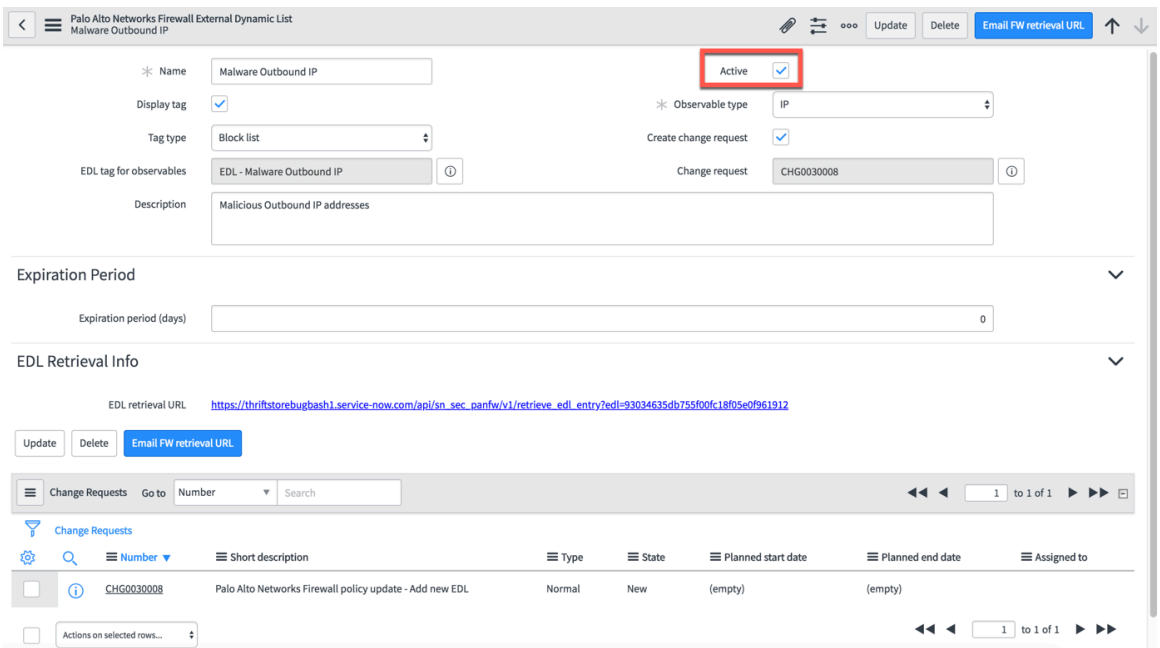
Como o Now Platform administrador de incidentes de segurança, você será notificado pelo Palo Alto Networks administrador do firewall quando a configuração do EDL for concluída no Palo Alto Networks Next-Generation Firewall.

Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.



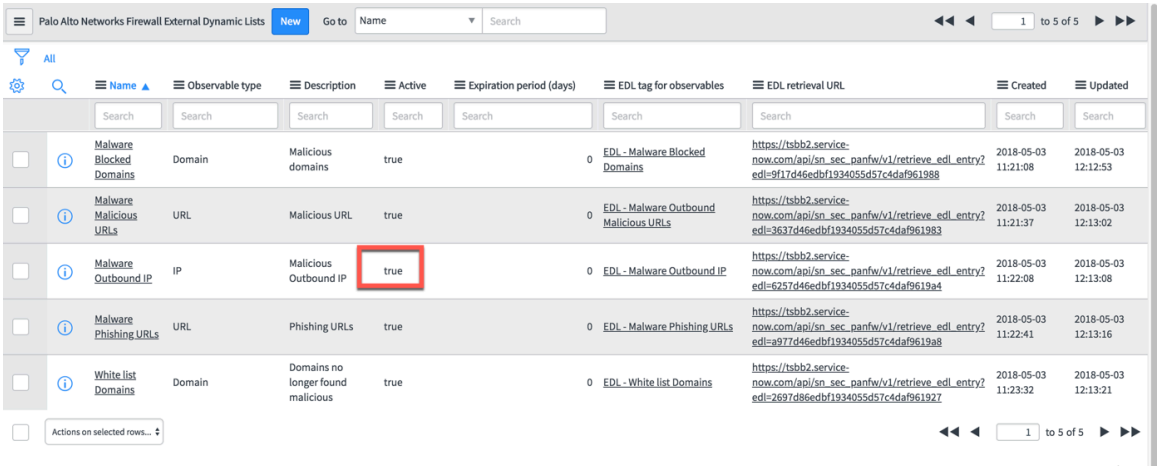
2. Selecione o módulo **Configuração de EDL do firewall**.
3. Na lista Listas dinâmicas externas do firewall da Palo Alto Networks, clique em um item na coluna **Nome** para abri-lo.
4. No registro que é aberto, marque a caixa de seleção **Ativo**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Atualizar**.
   Na coluna **Ativo** da lista Listas dinâmicas externas do firewall da Palo Alto Networks, `verdadeiro` é exibido para o estado da EDL.



Resultados
A EDL está ativada e pronta para receber entradas de EDL

O que Fazer Depois
Envie entradas de EDL de um incidente de segurança ou da lista de bloqueios.

Configurar um EDL em Palo Alto Networks Next-Generation Firewall

O Palo Alto Networks administrador de firewall configura um EDL para o Palo Alto Networks Next-Generation Firewall depois de notificado que a URL de recuperação está disponível no Now Platform. Antes que a EDL possa aceitar entradas de EDL, ela deve ser configurada em Palo Alto Networkse ativada em Now Platform®.

Antes de Iniciar
Função necessária: Palo Alto Networks administrador de firewall

Por Que e Quando Desempenhar Esta Tarefa
O administrador Palo Alto Networks Next-Generation Firewall cria um objeto EDL e atribui a URL (Recuperação) de origem e a política à EDL. Essas tarefas são realizadas em Palo Alto Networks antes que a EDL seja ativada em Now Platform.

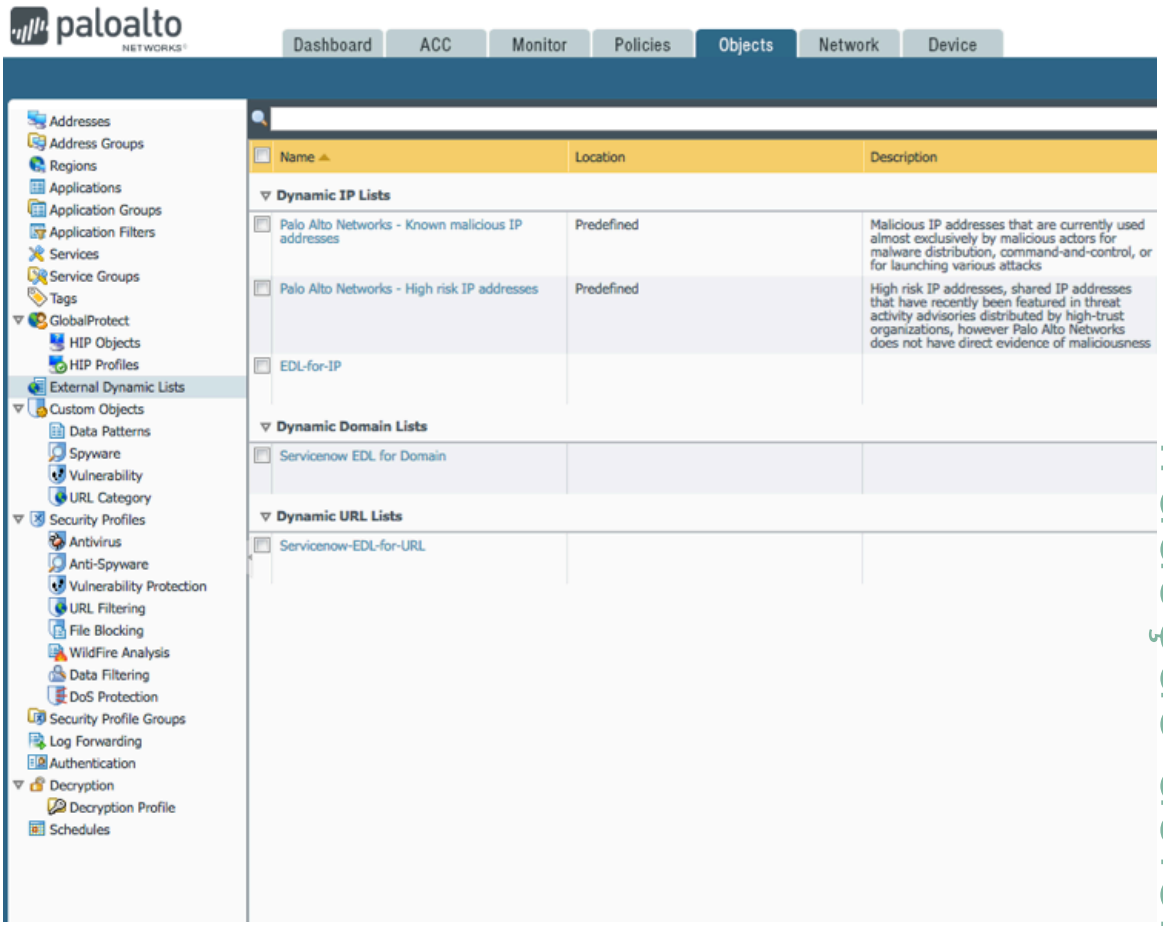
As imagens na seção a seguir são usadas com permissão e são PRIVILEGIADAS e PROPRIETÁRIAS.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

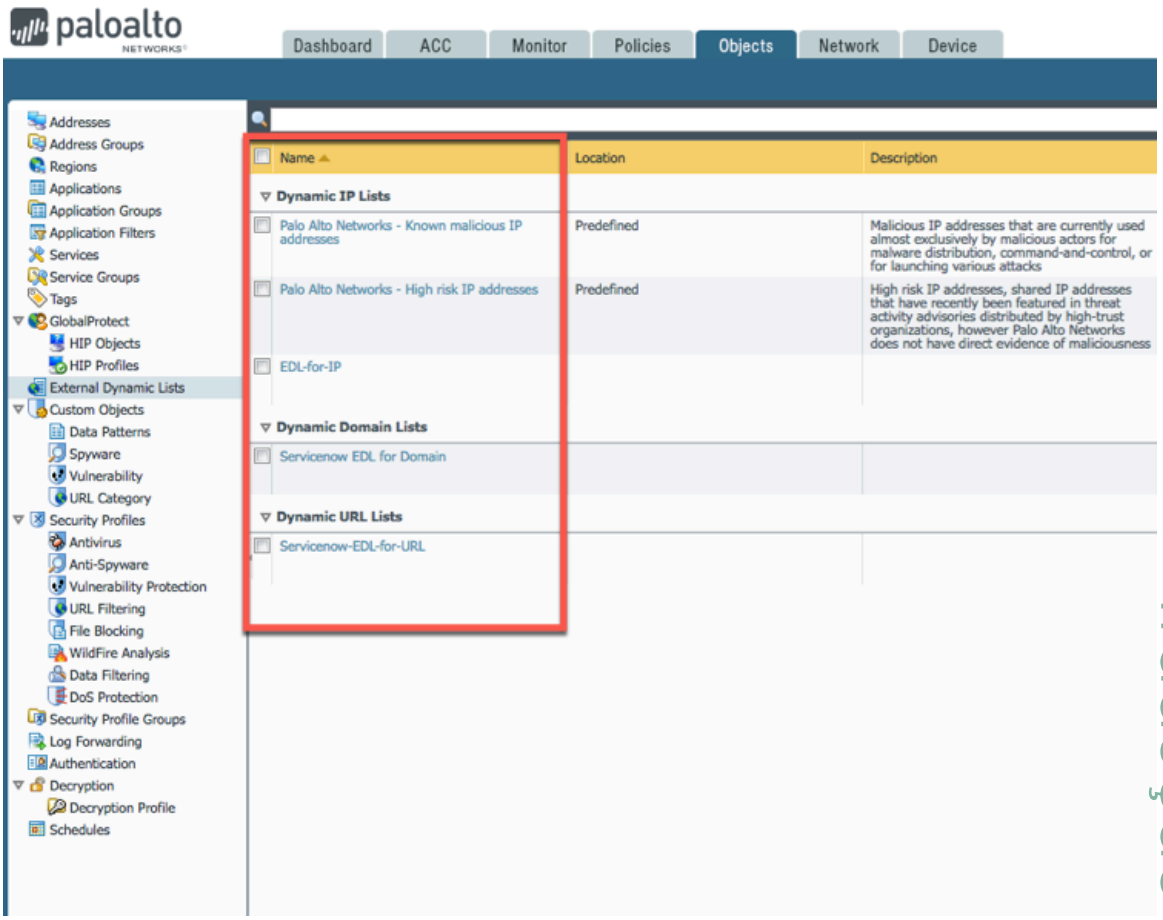
1. Se você não configurou o EDL para o firewall, navegue até **Listas dinâmicas externas** > **Objetos** in Palo Alto Networks.



2. Na coluna **Nome**, selecione o ServiceNow EDL que você deseja configurar na lista, por exemplo, **ServiceNow EDL para URL**.

Tradução automática

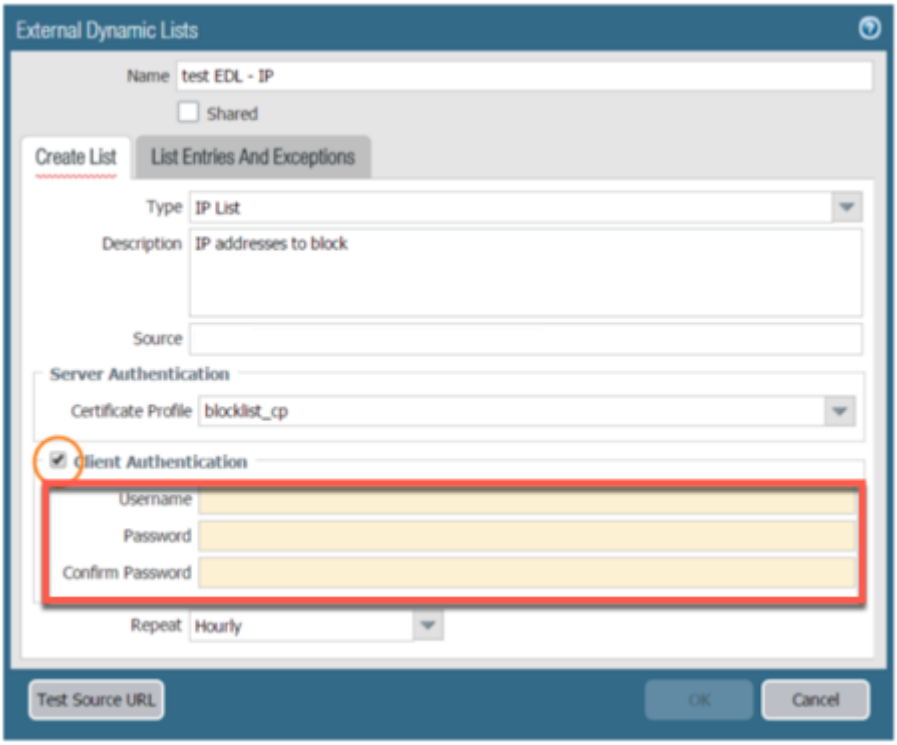
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



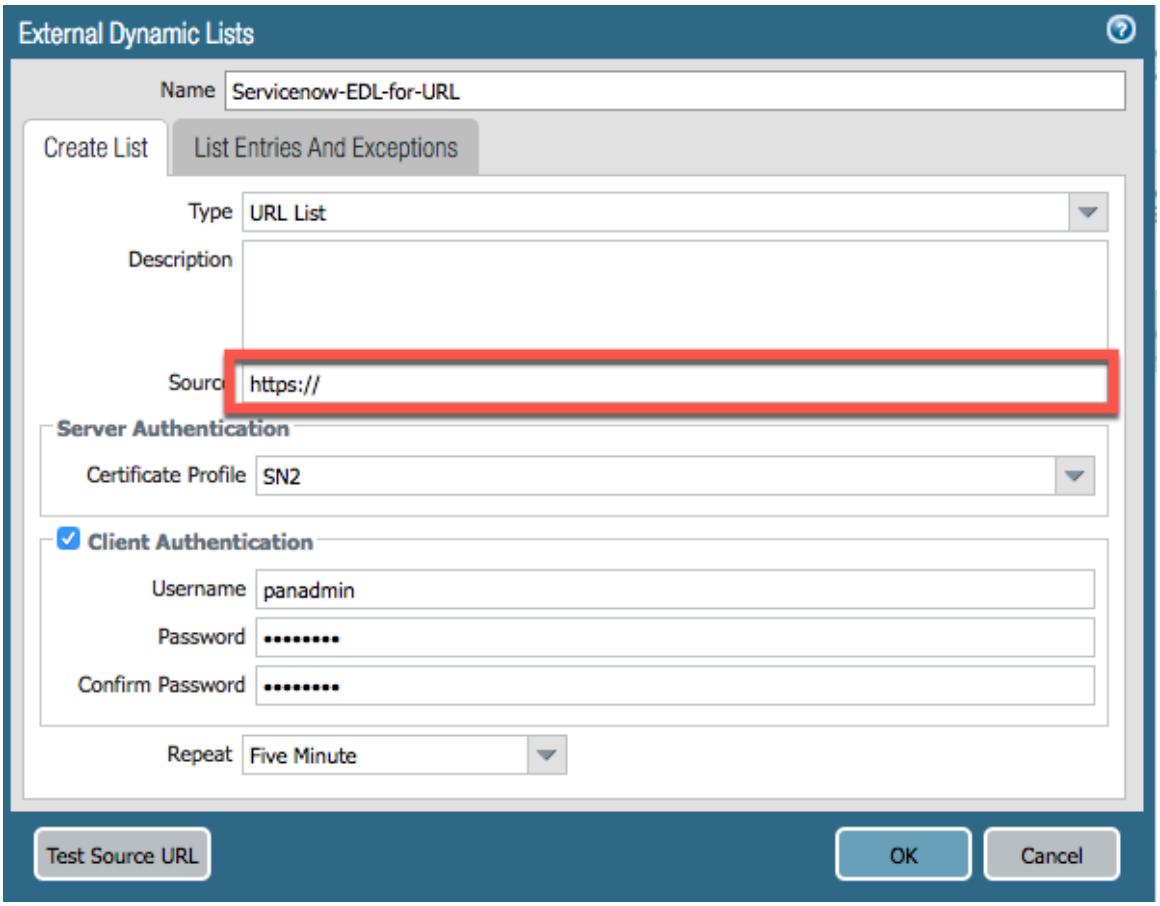
3. Na caixa de diálogo Listas dinâmicas externas, insira o Nome de usuário e a Senha para autenticar com Now Platform®.
Essas credenciais são o nome de usuário e a senha que você criou para a função de conta da API (sn_sec_panfw.api_account_access) em sua instância ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No campo Origem, insira o URL que foi gerado na lista de EDL em sua instância ServiceNow.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione um Perfil de certificado na lista de seleção, `SN2`, por exemplo.
6. Clique em OK.

Ativar uma EDL para Palo Alto Networks Next-Generation Firewall com uma solicitação de mudança

Se configurado, o formulário de solicitação de mudança ServiceNow será usado para ativar a lista dinâmica externa (EDL). Esta opção é recomendada se o administrador do firewall também estiver usando o Now Platform para mudanças de política ou regra de firewall. A EDL é ativada automaticamente e está pronta para receber entradas de EDL após o fechamento da solicitação de mudança Now Platform.

Antes de Iniciar

Nota: As imagens na seção a seguir são mostradas com os **formulários com guias** selecionados em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar formulários com guias, consulte a seção intitulada Exibir formulários com guias em Configuração do layout do formulário no site de documentação de produtos da ServiceNow .

Função necessária: sn_si.admin para aprovar a solicitação de mudança e as tarefas de mudança

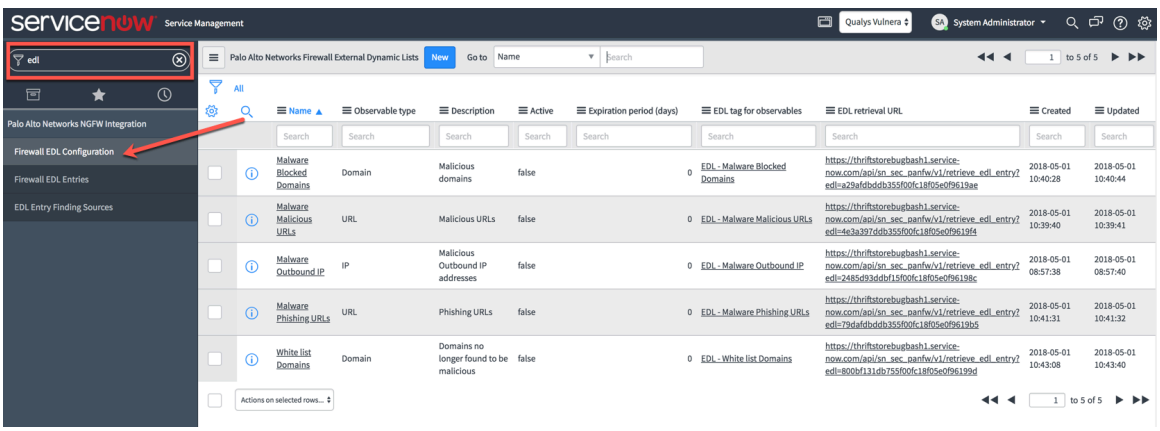
Palo Alto Networks administrador de firewall para concluir tarefas de configuração em Palo Alto Networks

Por Que e Quando Desempenhar Esta Tarefa

Se configurado, monitore sua solicitação de mudança Now Platform e atribua todas as tarefas necessárias para configurar o Palo Alto Networks Next-Generation Firewall. Depois que essas tarefas forem concluídas, feche a solicitação de mudança Now Platform para ativar o EDL automaticamente.

Procedimento

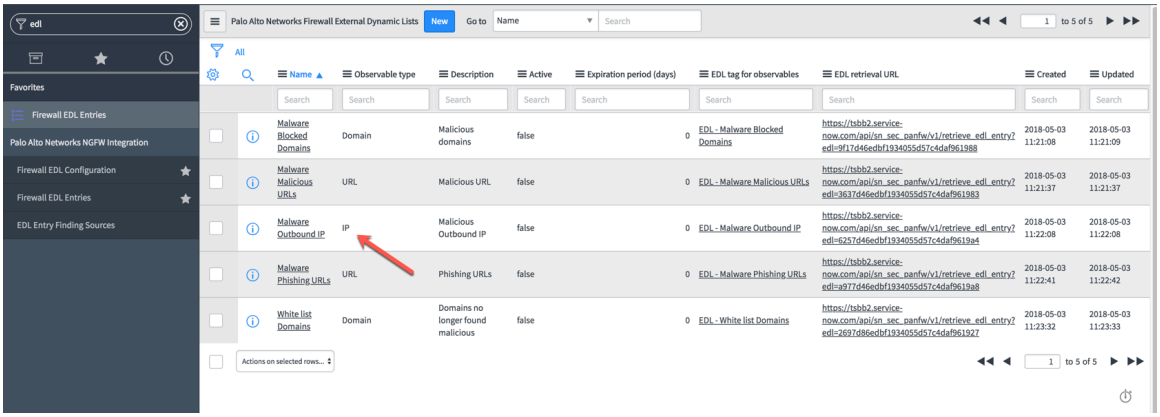
1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.



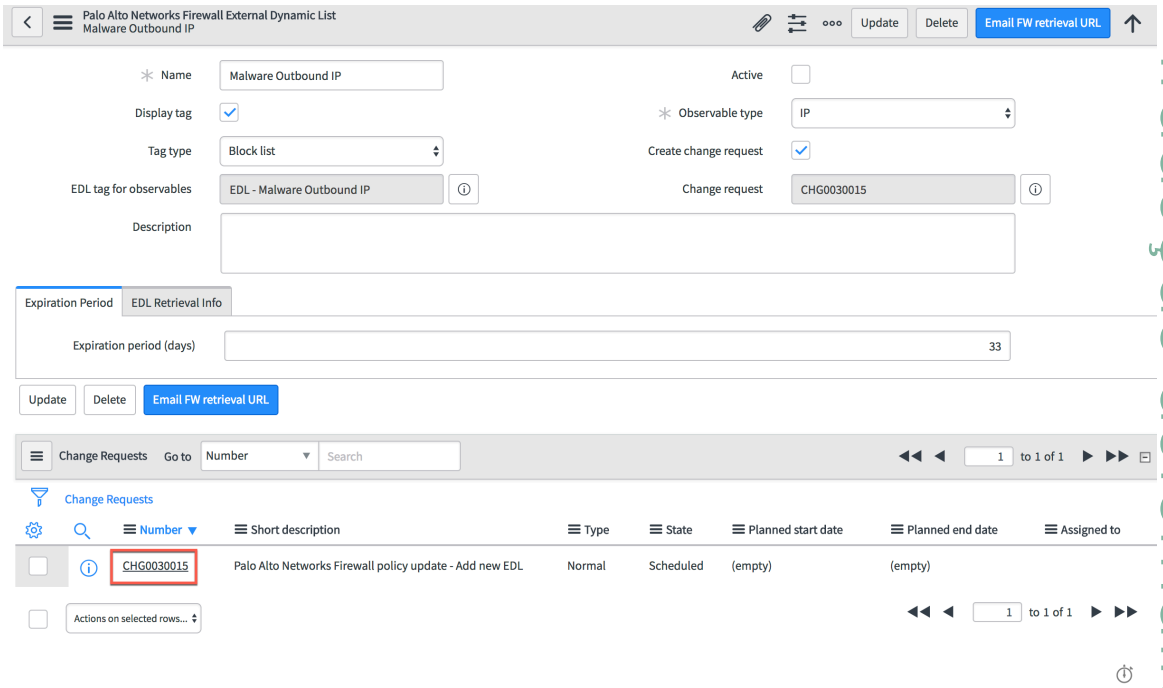
2. Selecione o módulo EDL e clique em um EDL na coluna **Nome**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



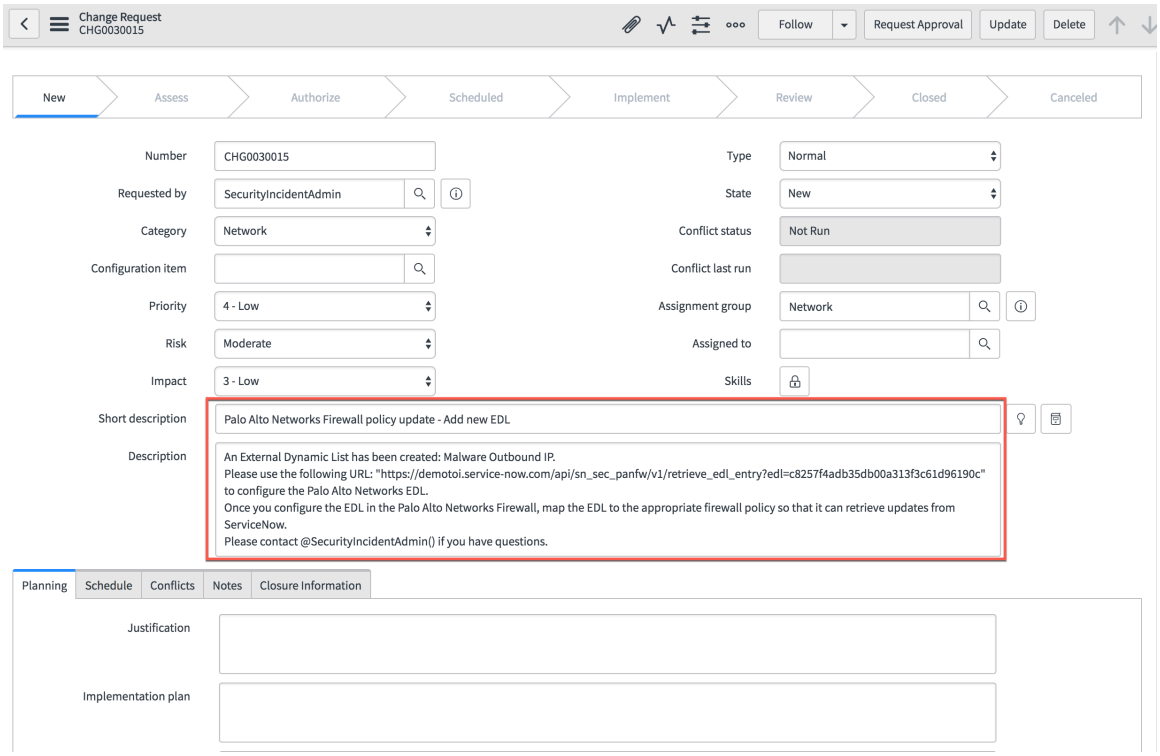
3. No registro de EDL aberto, clique no número da solicitação de mudança na lista relacionada Solicitações de mudança.



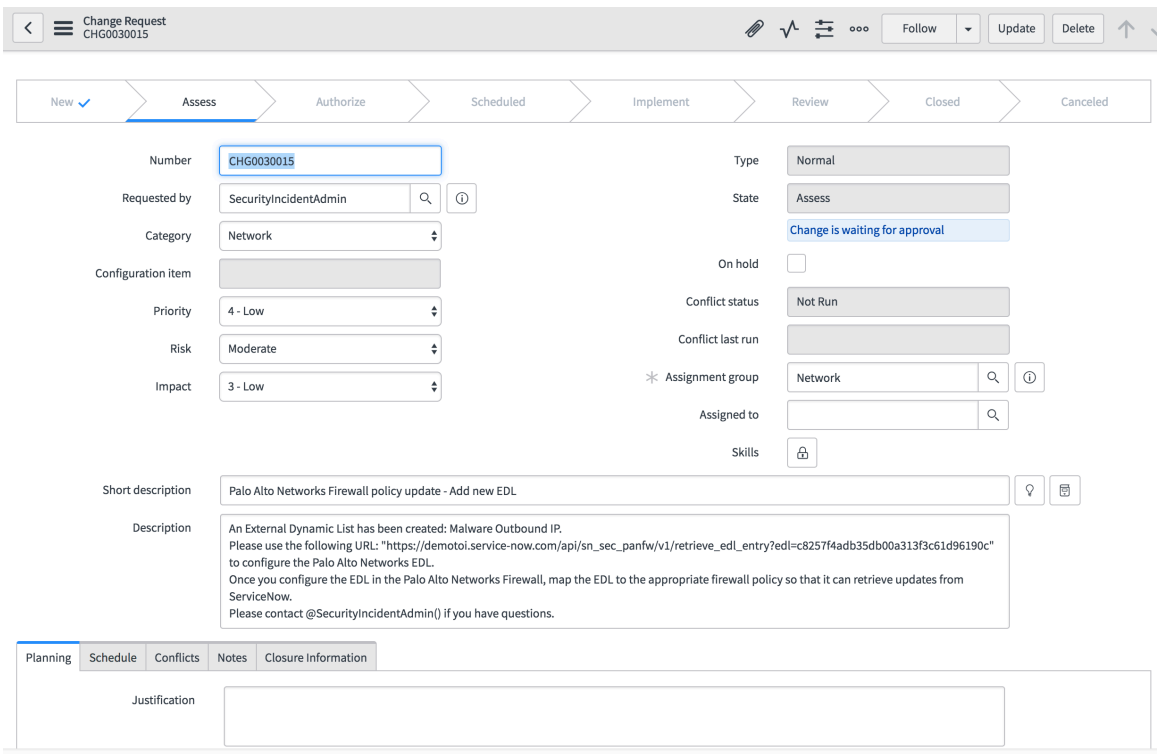
O registro da solicitação de mudança é exibido. O campo **Descrição** lista o URL de recuperação usado para configurar o Palo Alto Networks EDL. Detalhes sobre como mapear o EDL para a política Palo Alto Networks Next-Generation Firewall apropriada também estão incluídos. No campo **Descrição resumida**, um comentário indica que há uma solicitação para adicionar uma nova EDL.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No canto superior direito do registro, clique em **Solicitar aprovação**.
O Estado muda para Avaliar e uma mensagem é exibida informando que a solicitação de mudança está aguardando aprovação.

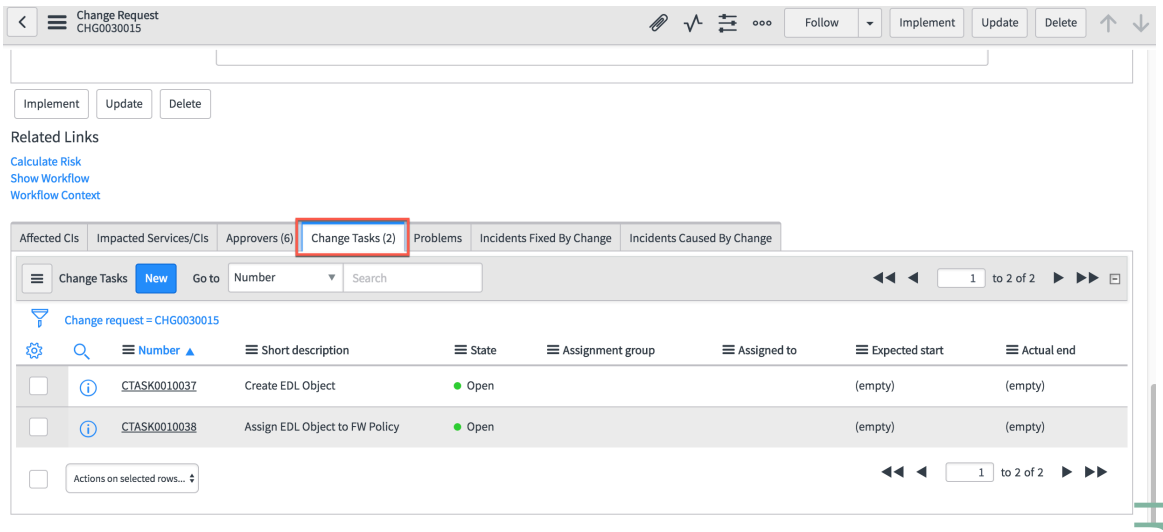


5. Para concluir a solicitação de mudança e ativar o EDL, siga as etapas para atribuir as tarefas e fechar a solicitação de mudança.

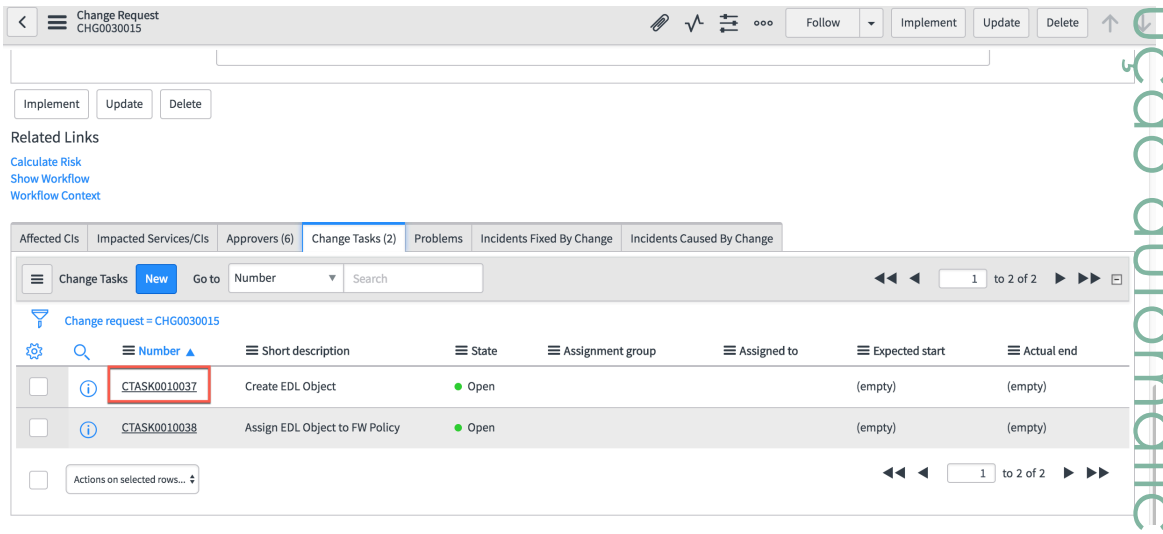
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Se não for exibido, abra a solicitação de mudança e selecione a guia **Tarefas de mudança**.



b. Clique na tarefa associada à criação do objeto EDL para abri-lo.

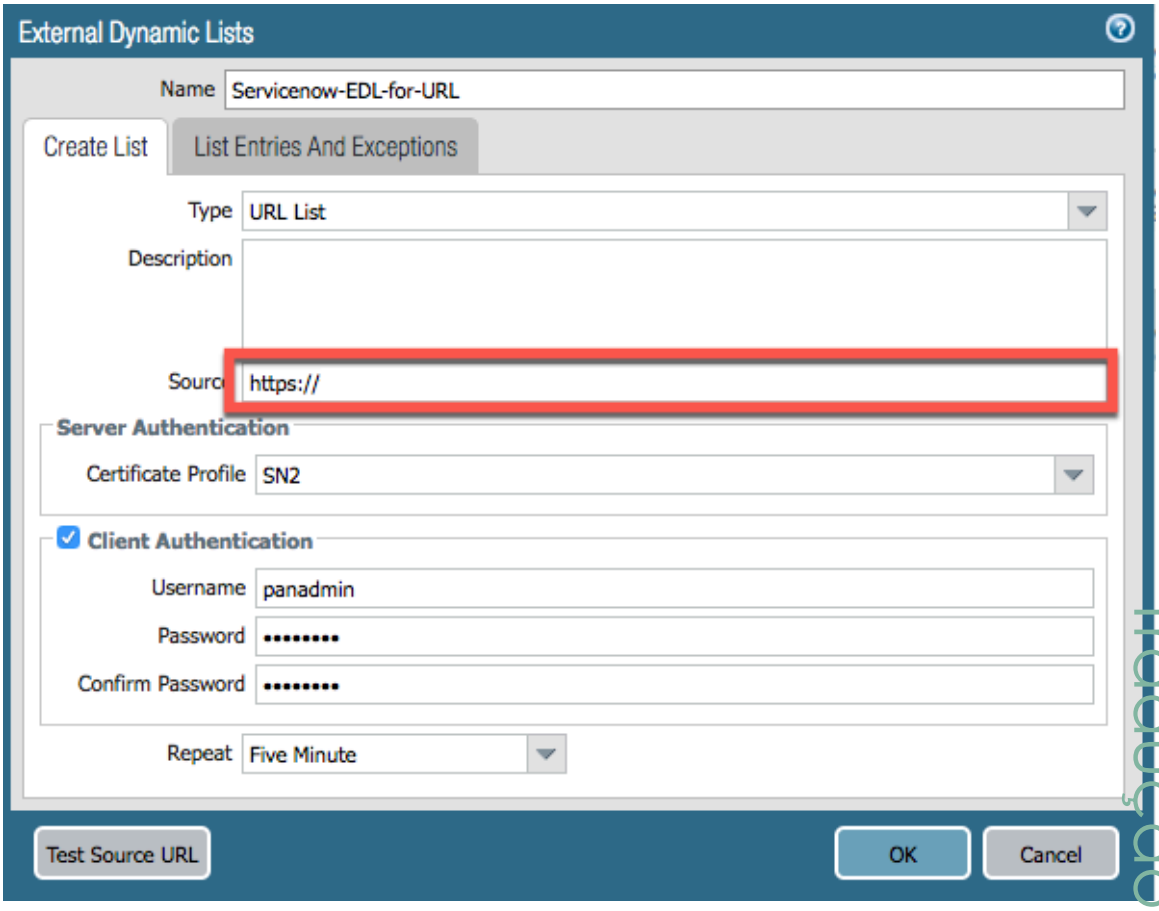


c. No registro exibido, atribua a tarefa ao administrador de firewall Palo Alto Networks e clique em **Atualizar**.
O administrador do firewall é notificado e cria o objeto EDL no Palo Alto Networks Next-Generation Firewall.

Para criar o objeto EDL, a URL de recuperação Now Platform é copiada em Palo Alto Networks em **Listas dinâmicas externas** > **Criar listas** > **Origem**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

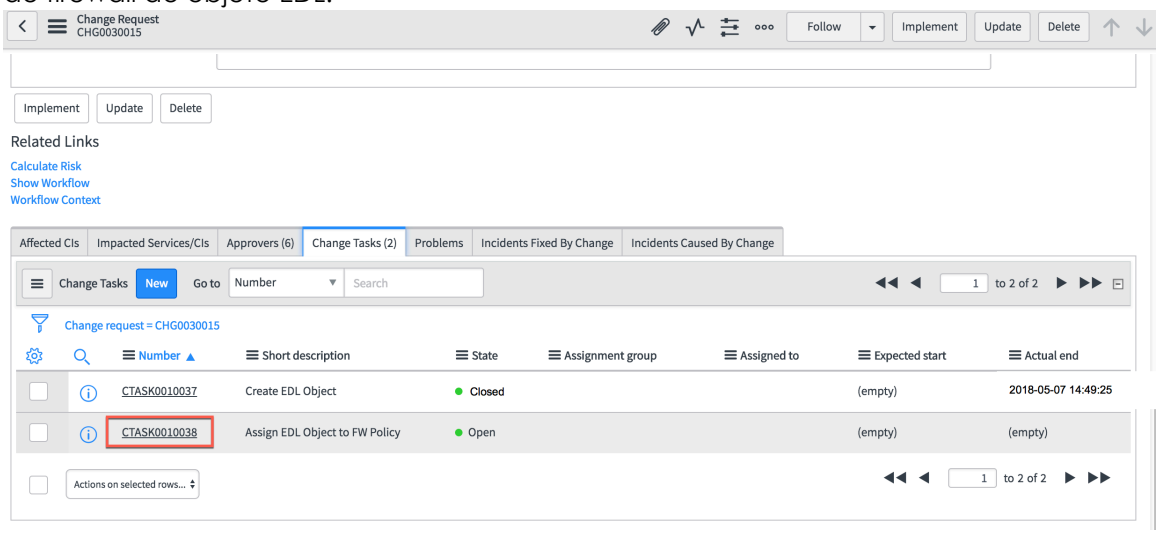


A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

d. Depois de verificar que o objeto EDL foi criado em Palo Alto Networks, em Now Platform, navegue até a solicitação de mudança associada à criação do objeto EDL e clique em **Tarefa de fechamento**.

No registro de tarefa deste exemplo, `CTASK0010037` foi encerrado para esta tarefa.

e. Navegue até a guia Tarefas de mudança e clique na tarefa para atribuir uma política de firewall ao objeto EDL.



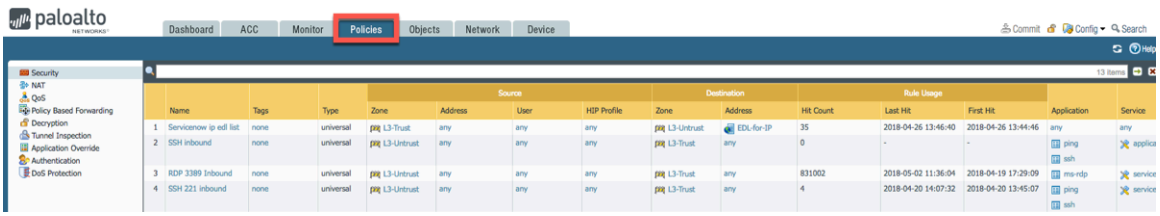
O status de `CTASK0010037` é `Encerrado`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

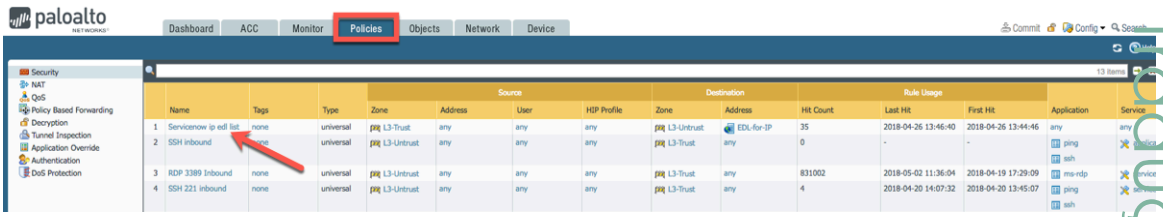
f. Abra o registro e atribua a próxima tarefa.

Depois que a tarefa tiver sido atribuída, em Palo Alto Networks, o administrador do firewall navegará até a guia **Políticas** para atribuir a política.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

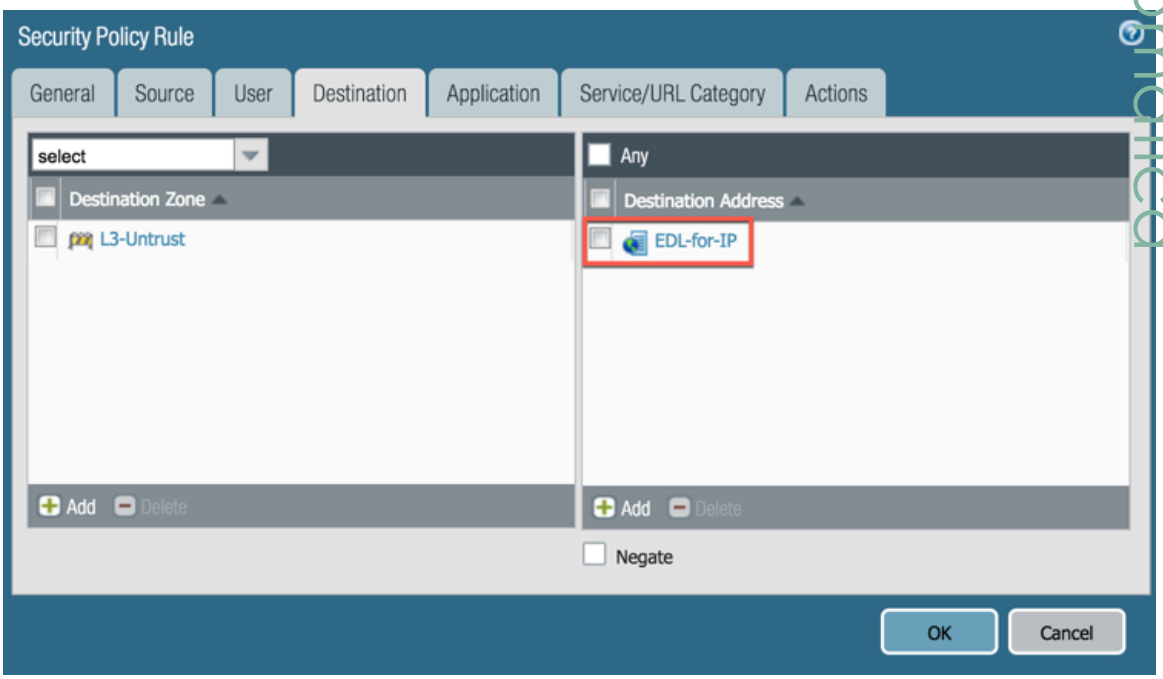
g. Na coluna **Nome**, localize e clique na regra de política de segurança à qual você deseja adicionar o EDL, por exemplo, **ServiceNow ip edl list**.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

h. Na caixa de diálogo Regra de política de segurança, selecione a guia **Destino** para adicionar uma EDL no campo **Endereço de destino**.

i. Para exibir todos os EDLs disponíveis, clique no ícone **Adicionar**.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

j. Clique em **OK**.

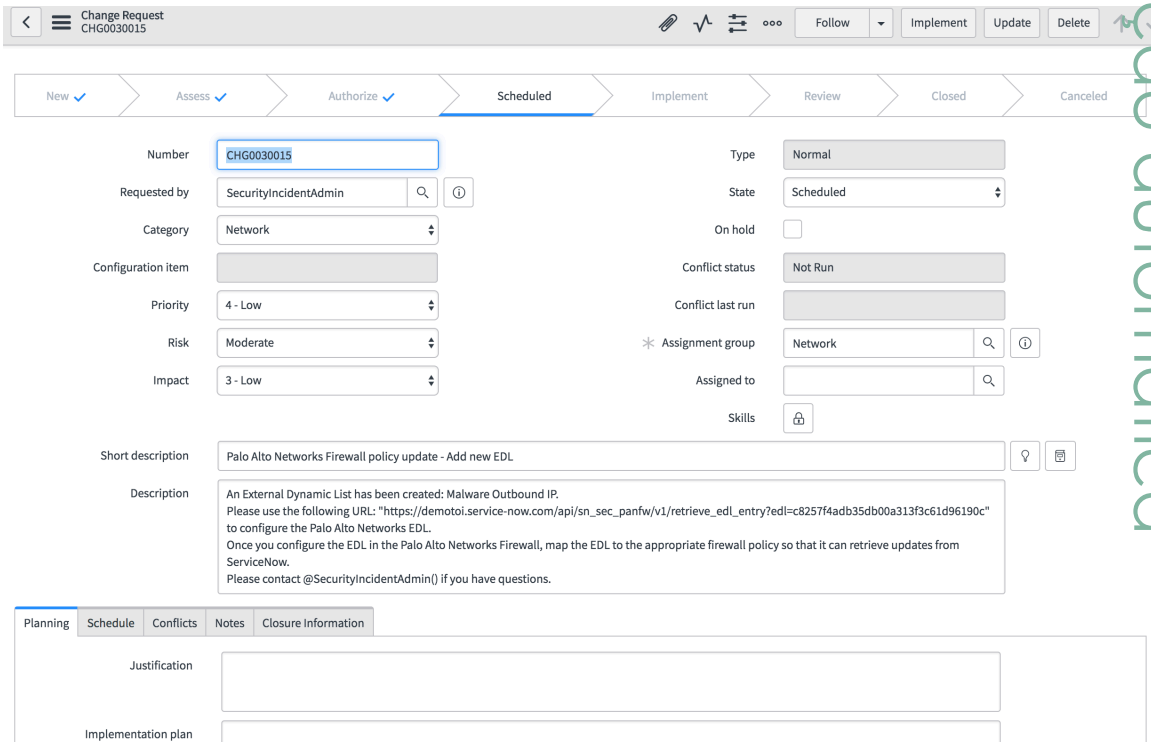
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

k. Depois de verificar que o objeto EDL foi atribuído a uma política de segurança, no Now Platform, navegue até a solicitação de mudança, abra a tarefa associada à atribuição do objeto EDL e clique em **Tarefa de fechamento**.
Depois que ambas as tarefas forem encerradas, a solicitação de mudança estará pronta para aprovação.

l. No registro de solicitação de mudança, clique na lista relacionada de **Aprovadores** e selecione um item na coluna **Estado** para abrir a solicitação usada para criar a EDL.

m. No formulário de solicitação de aprovação em aberto, clique em **Aprovar**.
O estado da solicitação de mudança é movido para Programado.



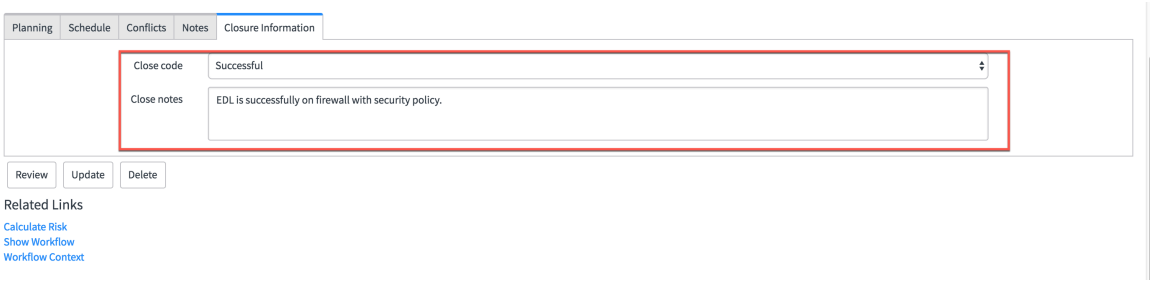
n. Clique em **Implementar**.

o. Clique na guia relacionada **Informações de fechamento** e insira anotações para fechar a solicitação.

Uma entrada neste campo é necessária para fechar a solicitação de mudança.

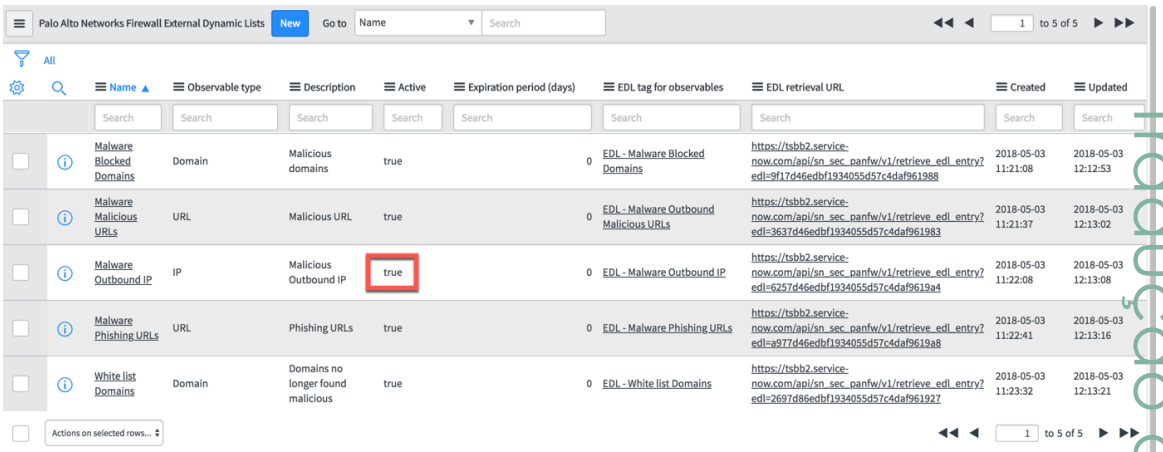
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

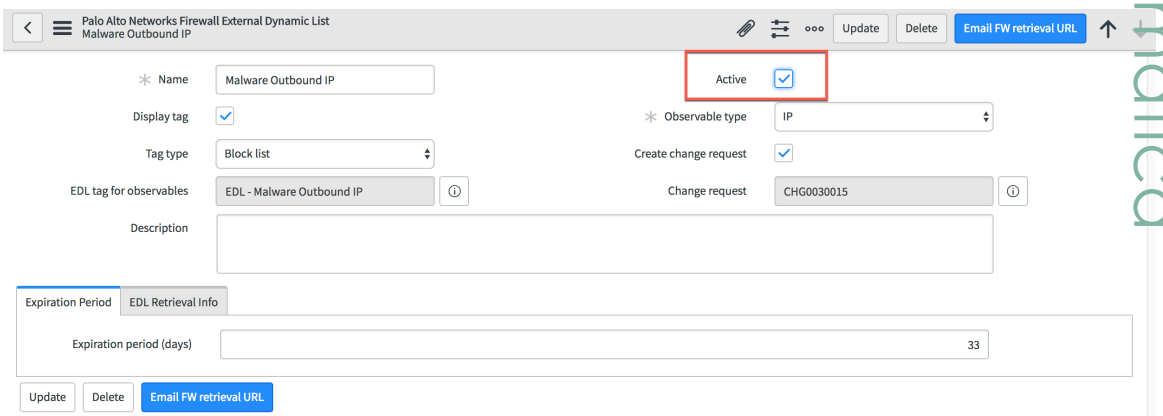


Depois que a solicitação de mudança é fechada, o EDL é ativado automaticamente. Se você não verificou se a EDL está ativada, navegue até **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.

Na coluna Ativa da lista, observe que o status da EDL é (`verdadeiro`).



Na coluna Nome, clique no nome do EDL e, no registro aberto, observe que a caixa de seleção **Ativo** também está marcada.



A EDL agora está pronta para aceitar entradas de EDL.

O que Fazer Depois

Envie entradas de EDL de um incidente de segurança ou da lista de bloqueios.

Enviar entradas de EDL de um registro de incidente de segurança para Palo Alto Networks Next-Generation Firewall

Os observáveis anexados a um registro de incidente de segurança são enviados para aprovação como entradas de lista dinâmica externa (EDL) para EDLs. Um processo de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aprovação para entradas de EDL faz parte do fluxo de trabalho pré-configurado. O firewall importa entradas de EDL - endereços IP, URLs, domínios - que estão incluídas nas listas de EDL e impõem a política.

Antes de Iniciar

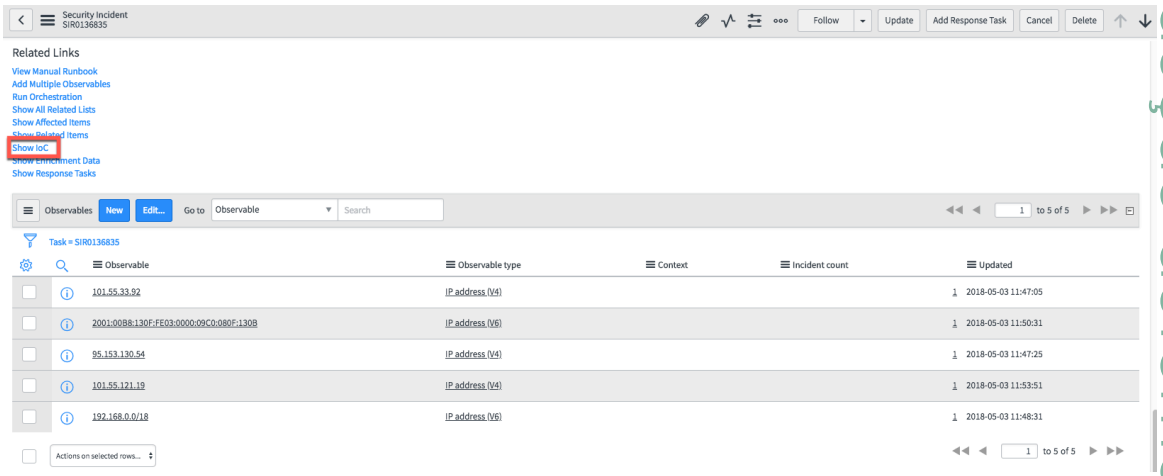
Função necessária: sn_si.analyst para enviar entradas de EDL. Para aprovar entradas de EDL: a aprovação é atribuída a sn_si.admin por padrão, mas essa autoridade pode ser atribuída conforme exigido por sua organização.

Por Que e Quando Desempenhar Esta Tarefa

Usuários com a função sn_si.analyst enviam entradas de EDL solicitando um bloco em observáveis anexados a um registro de incidente de segurança. Depois de enviada, uma entrada de EDL com um status Pendente é gerada e enviada para aprovação. O exemplo a seguir mostra uma solicitação de bloqueio para um observável de URL.

Procedimento

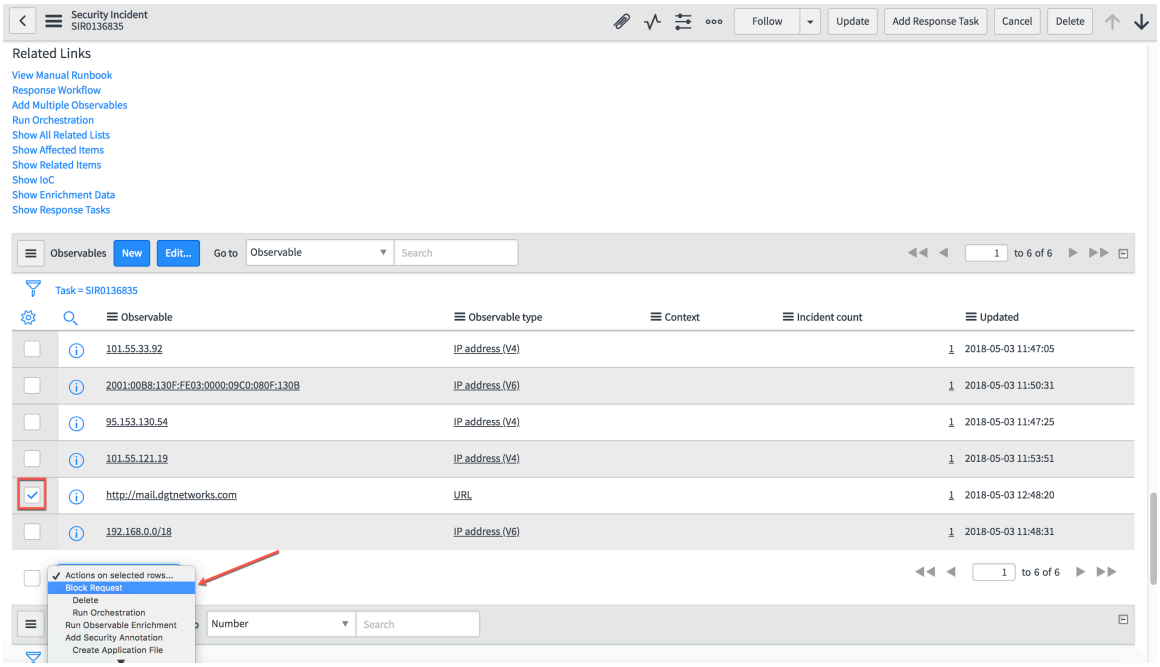
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**e clique em um registro de incidente de segurança para abri-lo.
2. Clique no link relacionado **Mostrar IoC**.



3. Na lista relacionada Observáveis, selecione os observáveis que você deseja bloquear e, na lista **Ações nas linhas selecionadas**, selecione **Bloquear solicitação**.

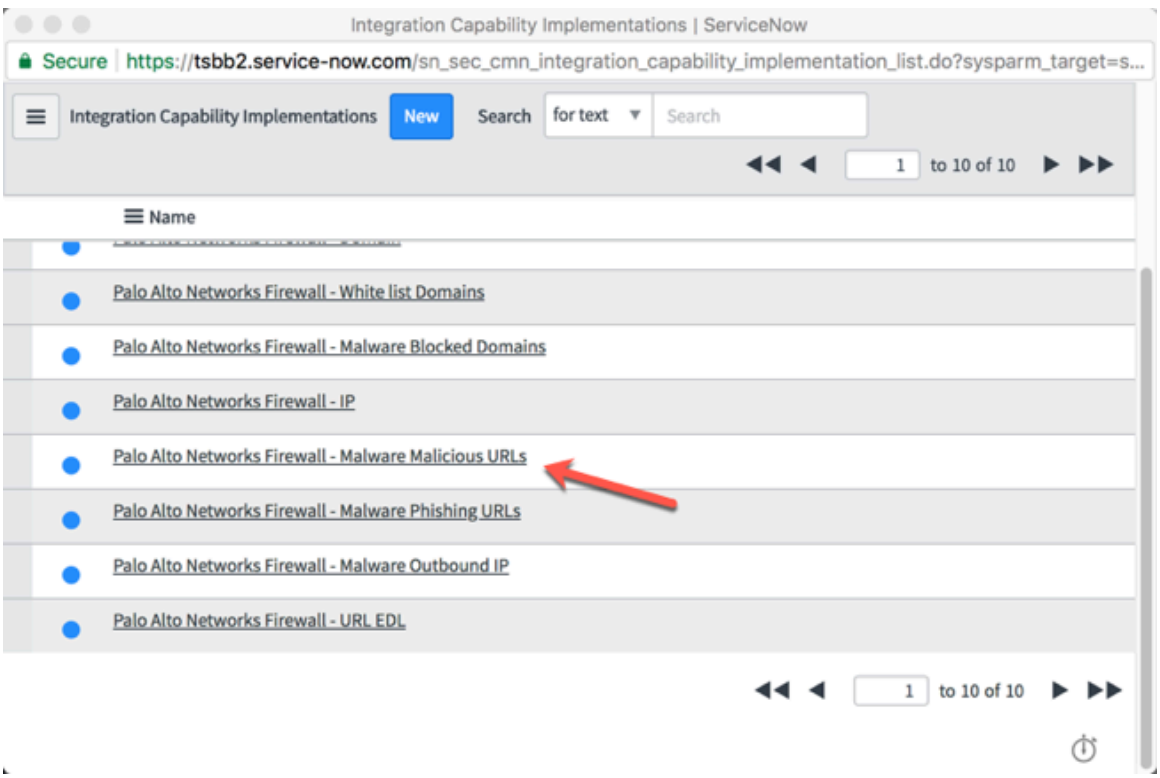
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo exibida, clique no ícone de pesquisa (ícone de 🔍).
5. Na lista exibida, selecione o EDL ao qual deseja anexar esta entrada.

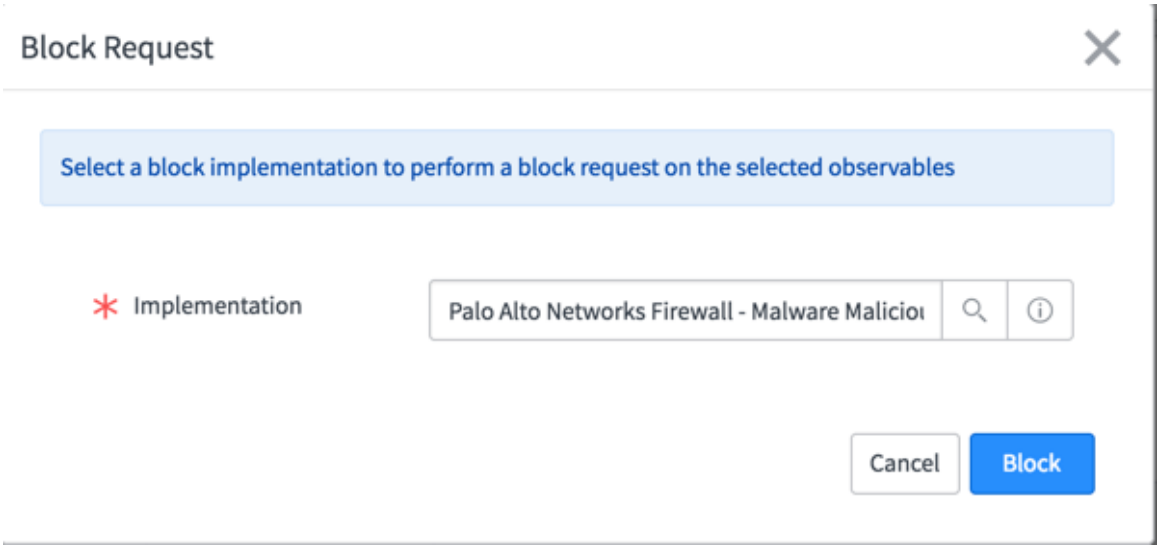
> **Nota:** Para este exemplo, o tipo de observável de entrada (URL) deve corresponder ao tipo de observável EDL (URL).



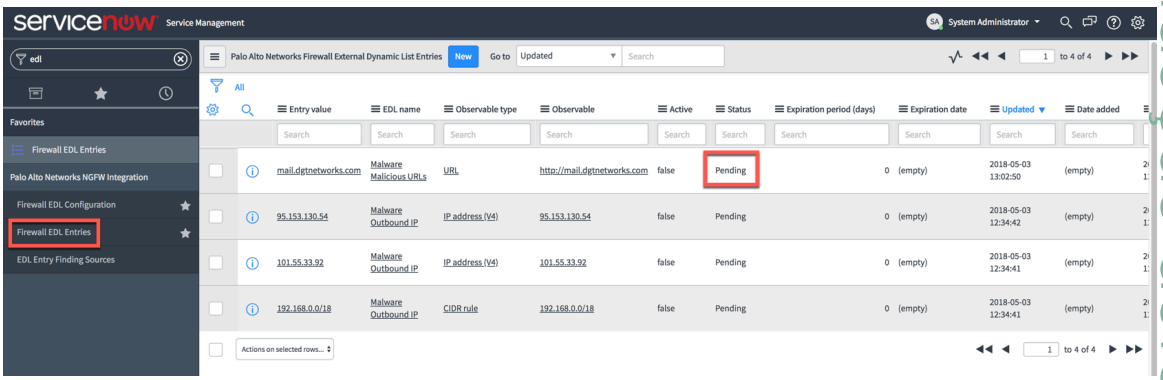
6. Na caixa de diálogo Solicitação de bloqueio com o nome da EDL exibido no campo **Implementação**, clique em **Bloquear**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

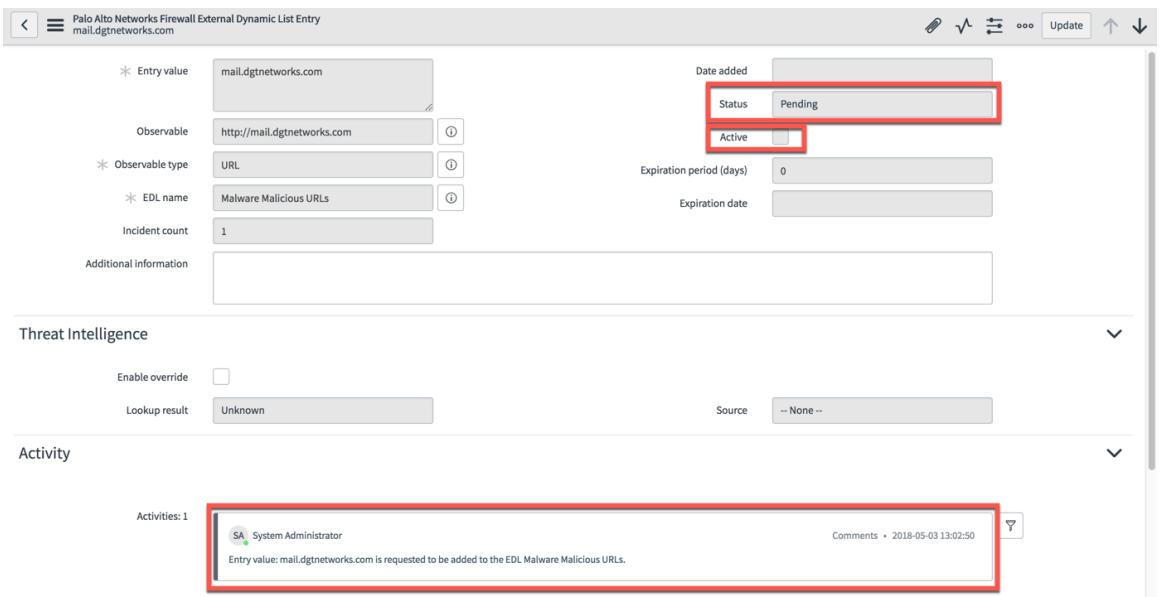


7. Navegar até **Integração de NGFW com a Palo Alto Networks** > **Entradas de EDL do Firewall** e clique em **Entradas de EDL do firewall**.



8. Na lista Entradas da lista dinâmica externa do firewall da Palo Alto Networks, clique no seu observável na coluna **Valor de entrada** para abrir o registro.

   Para este exemplo, o registro de **mail.dgtnetworks.com** é exibido.

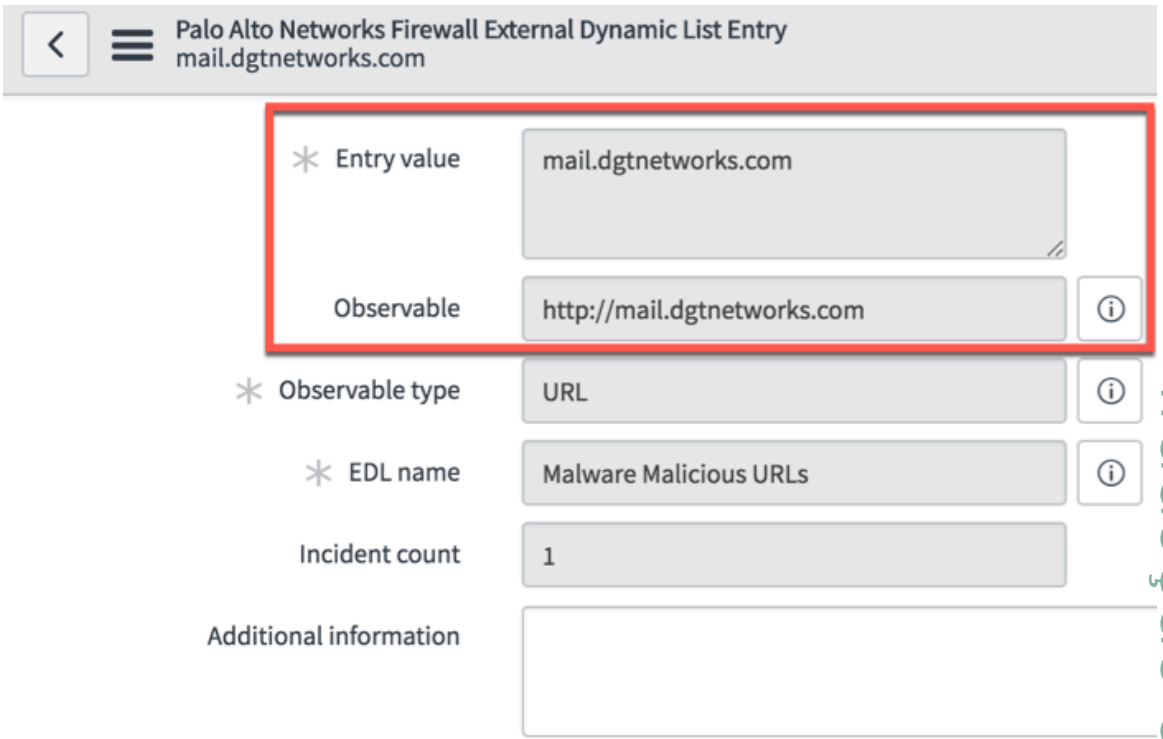


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O status é Pendente, a caixa de seleção Ativo está desmarcada e as anotações de trabalho mostram que há uma solicitação para adicionar o observável. Esta solicitação de entrada de EDL está pronta para aprovação.

Os campos Valor de entrada e Observável mostram formatos diferentes para o observável de URL.



O ícone ao lado do campo `Observável` é um link para a tabela Observável Now Platform®.

O valor no campo `Observável` (`http://mail.dgtnetworks.com`) está vinculado à tabela Observável e corresponde ao formato que foi trazido do evento de acionamento de incidente Security Incident Response.

O Now Platform® pode modificar automaticamente as entradas de EDL para que sejam compatíveis com o formato de URL de EDL Palo Alto Networks.

Neste exemplo, o observável foi criado com o protocolo http:// (`http://mail.dgtnetworks.com`) e este formato é exibido no campo Observável. O protocolo http:// é removido automaticamente do observável pelo Now Platform®, portanto, é compatível com Palo Alto Networks e pode ser recuperado. Como resultado, `mail.dgtnetworks.com` é exibido no campo `Valor de entrada`.

O que Fazer Depois
Aprovar entradas de EDL.

Informações relacionadas

Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enviar entradas de EDL da lista de bloqueios para Palo Alto Networks Next-Generation Firewall

Para observáveis determinados como mal-intencionados e não associados a um incidente de segurança Now Platform específico, você envia entradas da lista dinâmica externa (EDL) da lista de bloqueios.

Antes de Iniciar

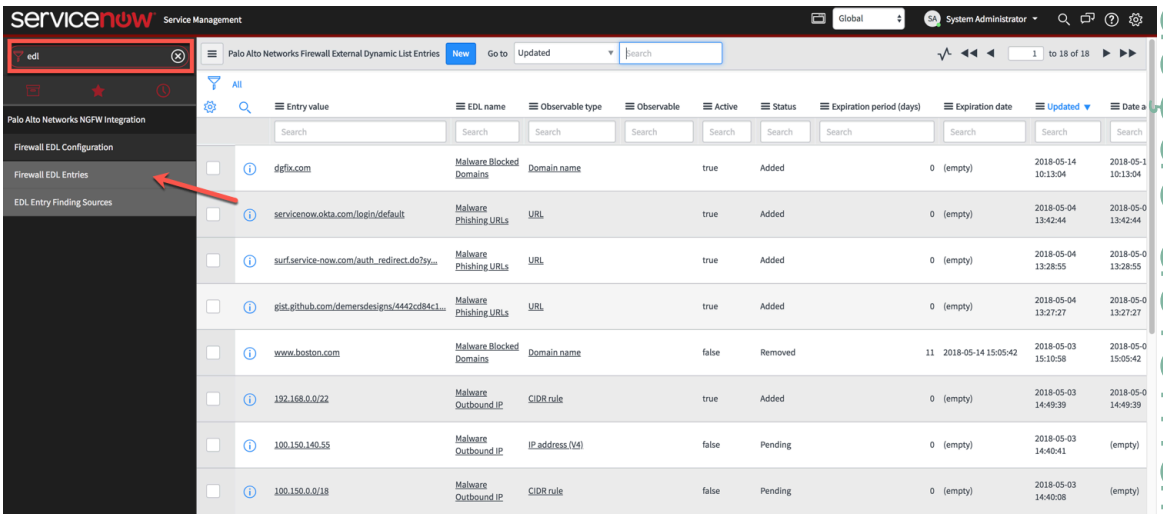
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Quando você quiser bloquear um observável que você determinou que é mal-intencionado ou permitir que um observável que você determinou que não seja mal-intencionado e o observável não esteja associado a um registro de incidente de segurança Now Platform específico, envie entradas de EDL diretamente da lista de bloqueios. Exemplos desses tipos de entradas de EDL podem ser URLs ou domínios para sites específicos.

Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Entradas de EDL do Firewall**.



2. Clique no módulo **Entradas de EDL do firewall**.
3. Na lista Entradas da lista dinâmica externa do firewall da Palo Alto Networks, clique em **Novo**.
4. No novo registro exibido, no campo **Valor de entrada**, insira um valor para o observável. Os dois resultados possíveis desta entrada:

   Os campos restantes no formulário são preenchidos automaticamente.

   Um observável correspondente é encontrado e uma mensagem é exibida informando que existe um observável correspondente. Selecione a EDL à qual deseja anexar esta entrada e clique em **Enviar**. Selecione a EDL à qual deseja anexar esta entrada antes de definir o período de expiração.

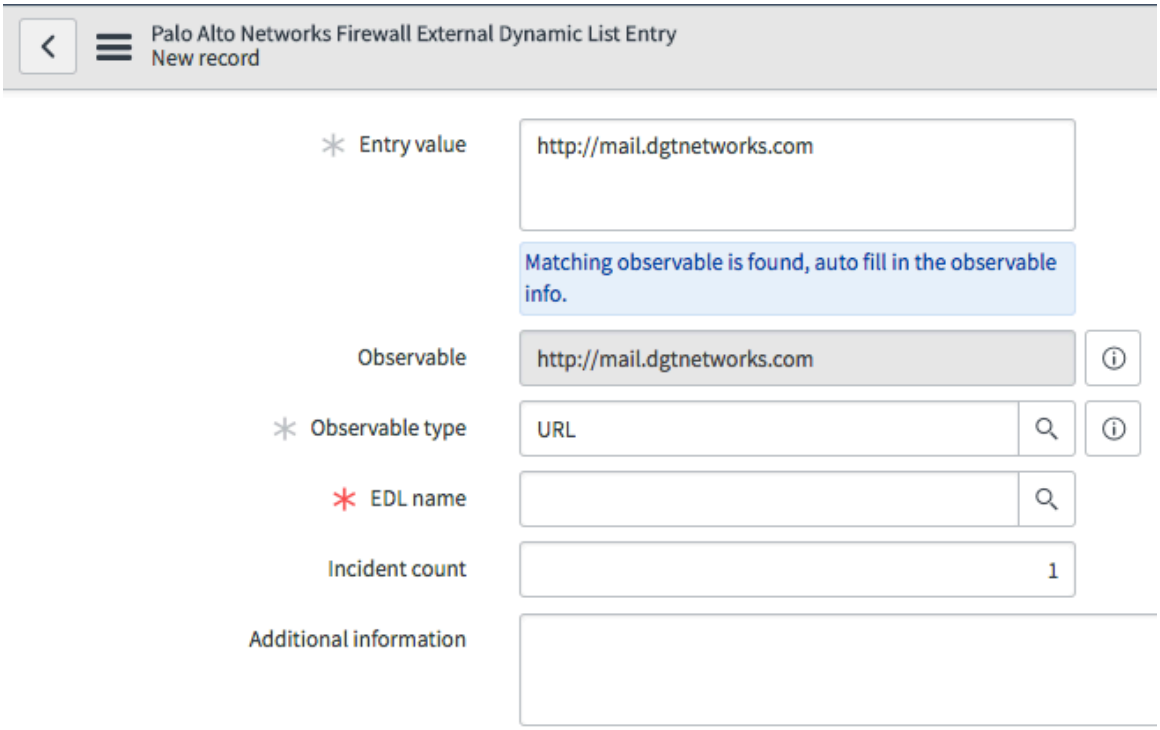
   Uma mensagem será exibida instruindo você a preencher o formulário.

   Um observável correspondente não foi encontrado e você deve preencher o formulário. Depois de concluir, selecione a EDL à qual deseja anexar o observável e clique em **Enviar**. Um registro observável é criado.

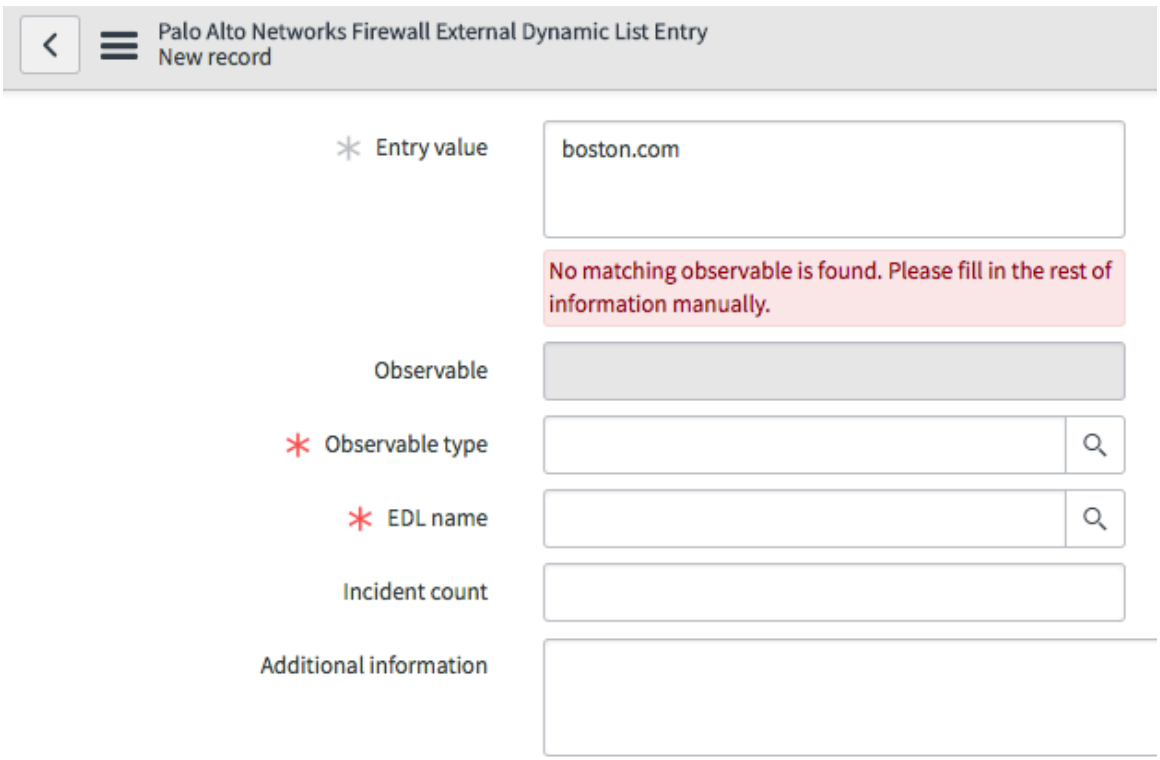
   A figura a seguir mostra um exemplo de um observável de domínio existente e como os campos são preenchidos automaticamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique no ícone de pesquisa para selecionar o EDL ao qual você deseja anexar a entrada.
6. Clique em **Enviar**.
   Se você tiver a aprovação por e-mail configurada no fluxo de trabalho, uma solicitação de aprovação por e-mail será enviada.
7. Se for exibida uma mensagem solicitando que você preencha o restante das informações manualmente, preencha os campos.



Tradução automática

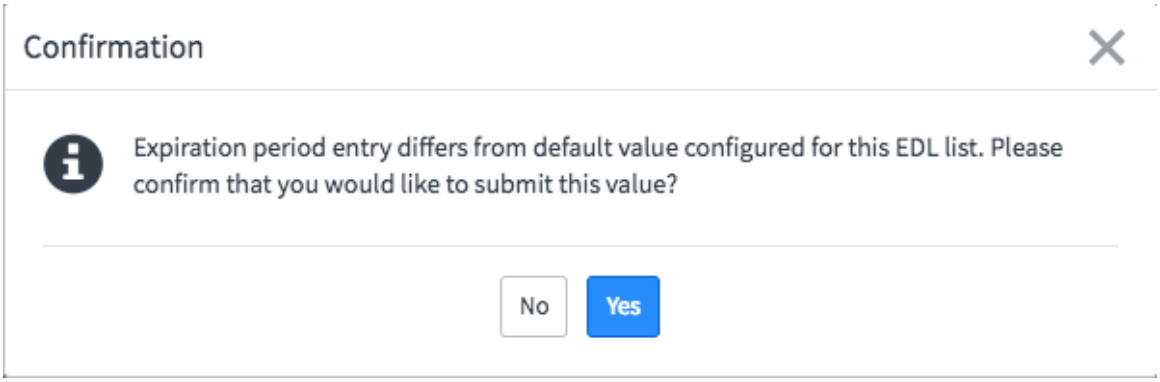
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de observável	Tipo de observável compatível com a caixa de diálogo.
Nome da EDL	EDL ao qual você deseja anexar a entrada. **Nota:** Selecione a EDL à qual deseja anexar a entrada antes de definir o período de expiração.
Habilitar substituição (o padrão é selecionado)	Resultado ou origem da pesquisa. Quando configurado, permite que você insira um **resultado de pesquisa** e a origem usada para encontrar os resultados. Esses campos são normalmente preenchidos quando um registro de incidente de segurança é criado. Nesse caso, não há resultado de pesquisa ou origem e você preenche esses campos manualmente.
Resultado da pesquisa	Selecione **Desconhecido** ou **Mal**-intencionado .
Origem	Origem que executa uma pesquisa de ameaças na entrada de EDL, por exemplo, ThreatCrowd etc.
Período de expiração	O período de expiração herdado da EDL por padrão. Você pode substituir este valor, mas somente durante a criação da entrada. `0` indica que a entrada de EDL nunca expira. Se você alterar este valor, esta entrada ficará ativa pelo número de dias inserido. Você pode inserir um valor mínimo de `1`e não há valor máximo. Por exemplo, se você inserir `30` dias às 14h01 do dia 1º de maio, a entrada de EDL expirará às 14h01 do dia 31 de maio.

8. Clique em **Enviar**.
   Se você alterou o período de expiração padrão da entrada de EDL, uma caixa de diálogo de confirmação de aviso será exibida indicando que o período é diferente do EDL selecionado.

Tradução automática

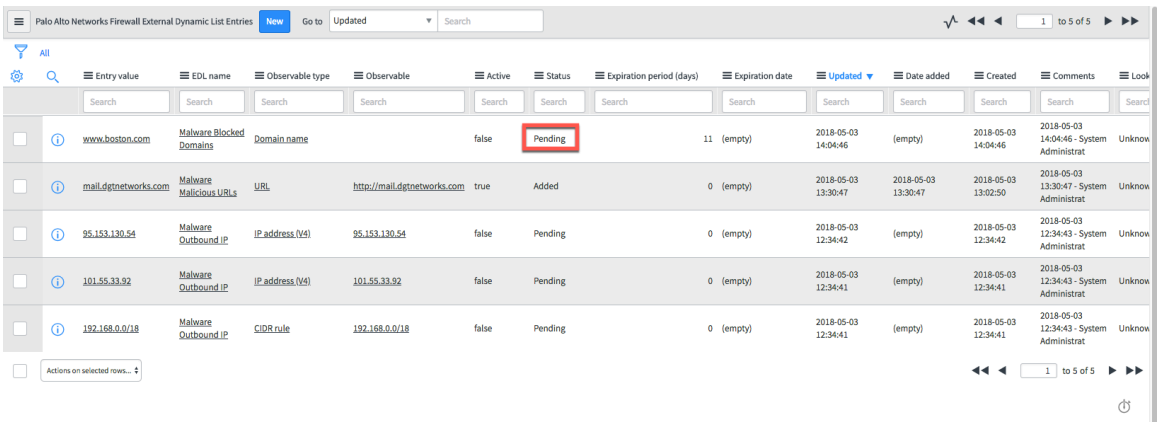
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Escolha uma opção para configurar o período de expiração.

Opção	Descrição
Sim	Confirma a substituição da expiração, salva o registro e retorna você para a lista de **entradas da lista dinâmica externa do firewall da Palo Alto Networks**. Se você tiver a aprovação por e-mail configurada no fluxo de trabalho, uma solicitação de aprovação por e-mail será enviada.
Não	Cancela a substituição. Neste ponto, você pode alterar o valor do **Período de expiração**. Depois de alterar o valor, clique em **Enviar** para retornar à lista de **Entradas da lista dinâmica externa do firewall da Palo Alto Networks**.

10. Se não for exibido, navegue até a **Lista dinâmica externa do firewall da Palo Alto Networks lista Entradas** e observe que o status da entrada é Pendente.



A entrada agora está pronta para aprovação.

O que Fazer Depois

Aprovar entradas de EDL.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Aprovar entradas de EDL para Palo Alto Networks Next-Generation Firewall

Um processo de aprovação para entradas da lista dinâmica externa (EDL) faz parte do fluxo de trabalho pré-configurado. Você aprova as entradas de EDL antes que as entradas sejam ativadas em EDLs. Depois que você aprovar a entrada de EDL, o firewall recuperará a entrada e seu observável será bloqueado desse ponto em diante.

Antes de Iniciar

Função necessária: a aprovação para entradas de EDL é atribuída a sn_si.admin por padrão, mas essa autoridade pode ser atribuída conforme exigido por sua organização. No exemplo a seguir, o administrador Now Platform tem autoridade de aprovação.

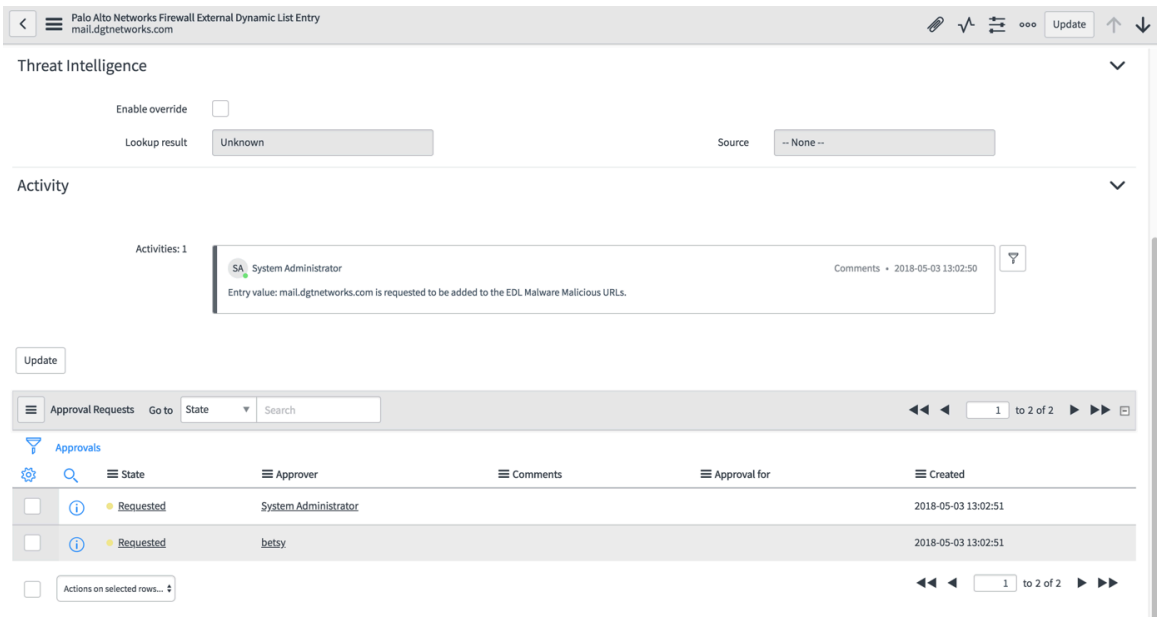
Por Que e Quando Desempenhar Esta Tarefa

Quando o processo de aprovação está habilitado, uma entrada de EDL não é ativada ou desativada na EDL até que seja aprovada.

Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Entradas de EDL do Firewall** e abra o registro de EDL.
2. No registro de EDL, role até a seção Solicitações de aprovação.

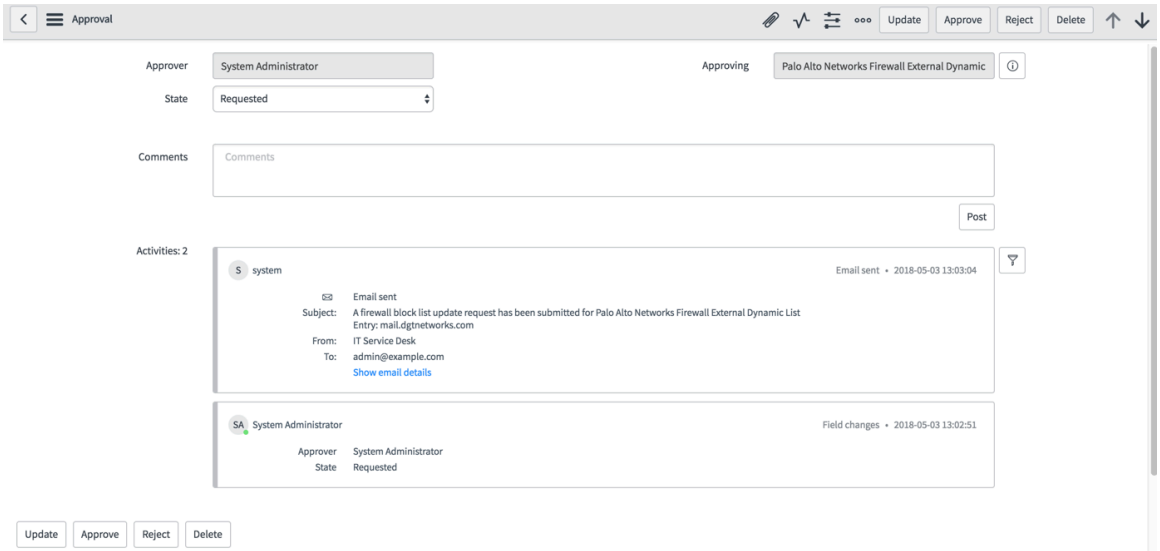
   Nota: Se você tiver Formulários com guias selecionados em Configurações do sistema, a seção aparecerá como uma guia no registro.



3. Em Solicitações de aprovação, clique em um item na coluna **Estado** para abri-lo.
   O registro de aprovação é exibido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



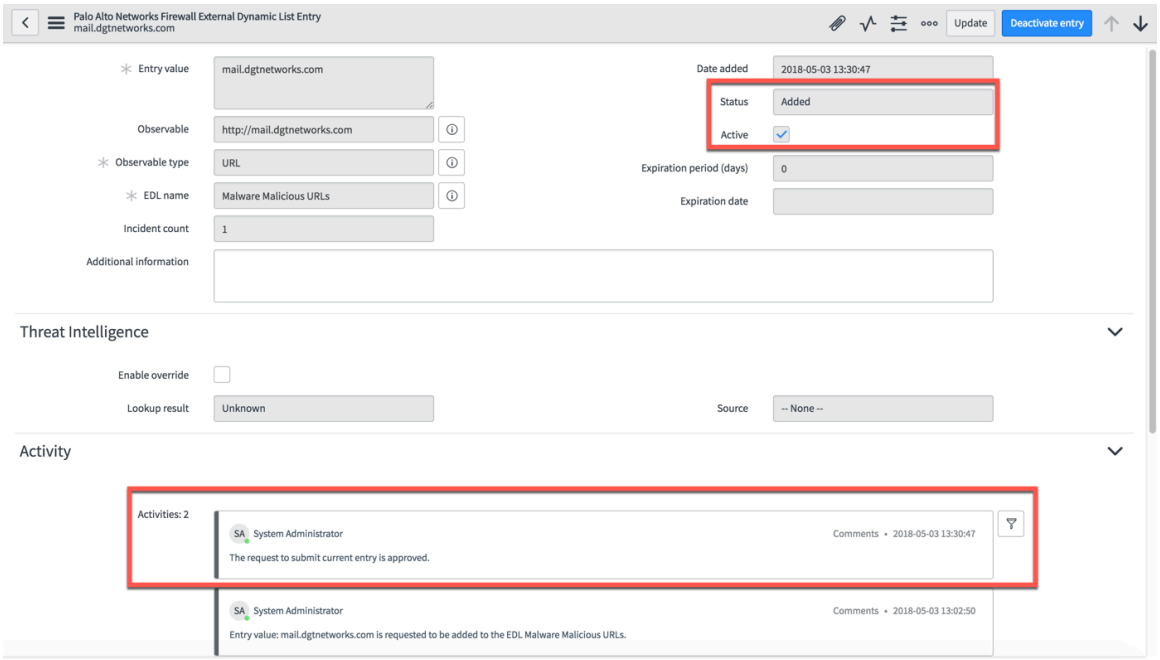
4. Escolha uma opção para aprovar a entrada de EDL.

Opção	Descrição
Aprovar	No registro de entrada, o campo **Status**muda para `Adicionado`e a caixa de seleção **Ativo** é marcada. O botão **Desativar**é exibido e ativo. As anotações de trabalho mostram que a solicitação da entrada de EDL foi aprovada.
Rejeitar	No registro de entrada, o campo Status muda para **Rejeitado**e a caixa de seleção **Ativo** é desmarcada, indicando que a entrada não está bloqueada no firewall. As anotações de trabalho mostram que a solicitação da entrada de EDL foi rejeitada.

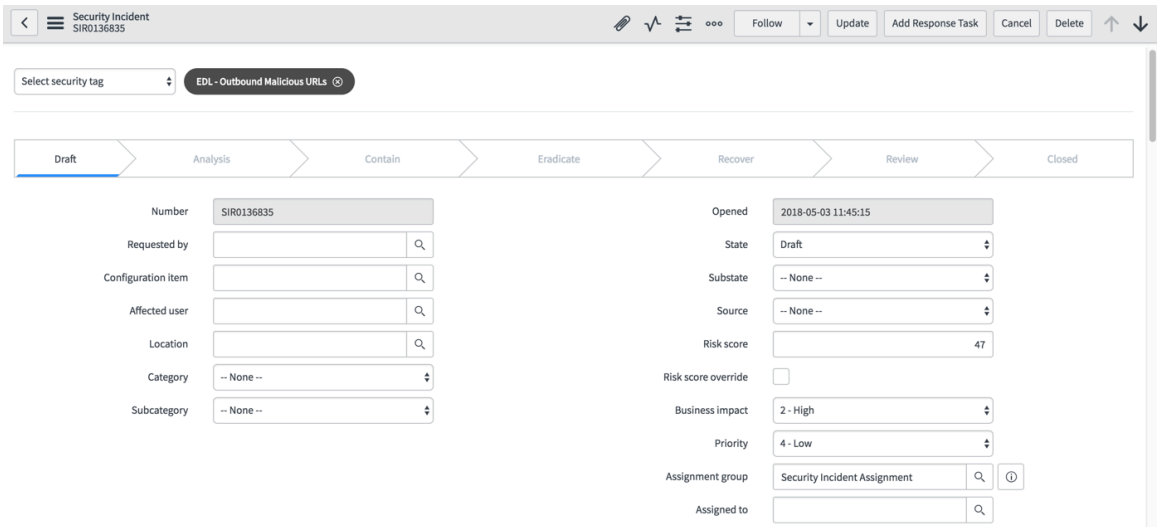
Depois de aprovar a entrada de EDL e ela ser ativada, o Palo Alto Networks Next-Generation Firewall recupera a entrada de EDL após o próximo intervalo de recuperação. Depois que a entrada é recuperada, o observável é bloqueado desse ponto em diante. Na figura a seguir, observe que a caixa de seleção Ativo está marcada, o status é Adicionado e as anotações de trabalho indicam que a solicitação foi aprovada.

Tradução automática

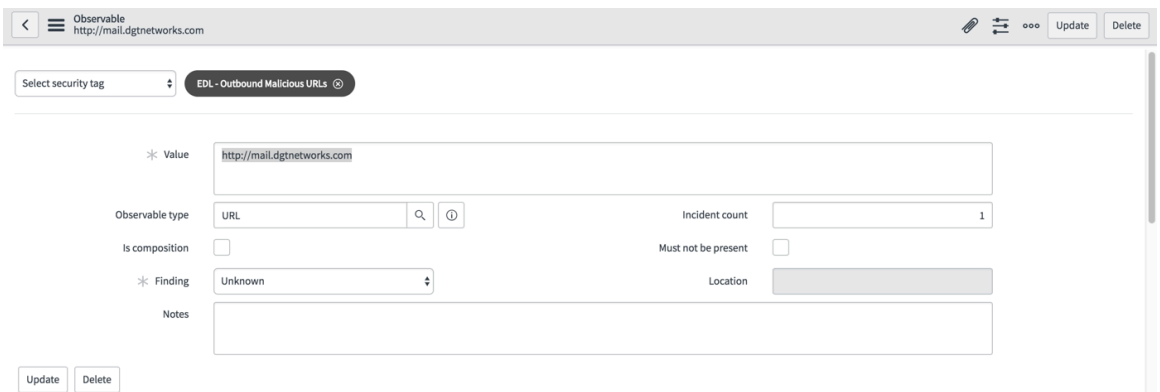
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que a entrada de EDL é aprovada e ativada, o registro do incidente de segurança é marcado com um marcador de segurança. O marcador é exibido na parte superior do registro.



O marcador de segurança também é exibido no registro do observável.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

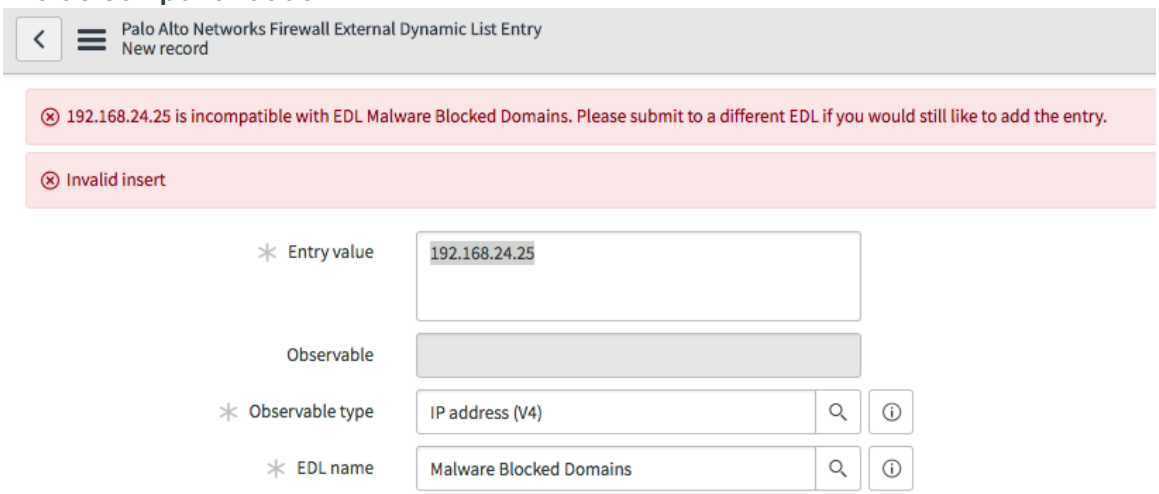
Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Há restrições para adicionar entradas de lista dinâmica externa (EDL) a EDLs. Se houver conflitos duplicados, de compatibilidade ou de CIDR (Roteamento entre domínios sem classe) quando você tentar adicionar entradas de EDL a EDLs, serão exibidas mensagens de erro que ajudarão a resolver esses erros.

Exceção de compatibilidade

Cada EDL aceita somente entradas compatíveis com seu tipo de observável. Se você criar um EDL de domínio e tentar anexar um observável de endereço IP a ele, uma mensagem de erro incompatível será exibida. Por exemplo, uma EDL de domínio só pode aceitar observáveis de domínio, conforme ilustrado na figura a seguir.

Erro de compatibilidade



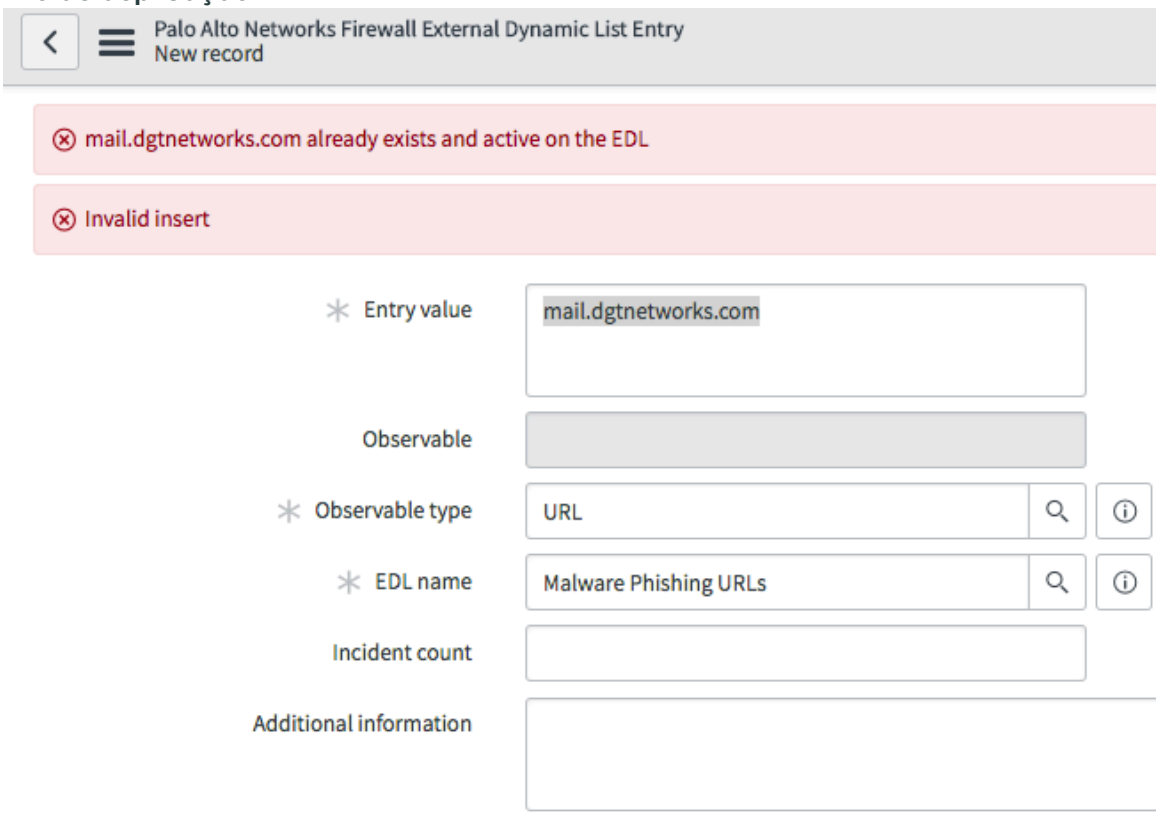
Exceção de duplicação

Um observável não pode ser ativado em vários EDLs do mesmo tipo de observável. Se um observável de URL já estiver ativado em uma EDL de URL e você tentar ativar o mesmo observável em uma EDL de URL de phishing, será exibida uma mensagem de erro de duplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erro de duplicação



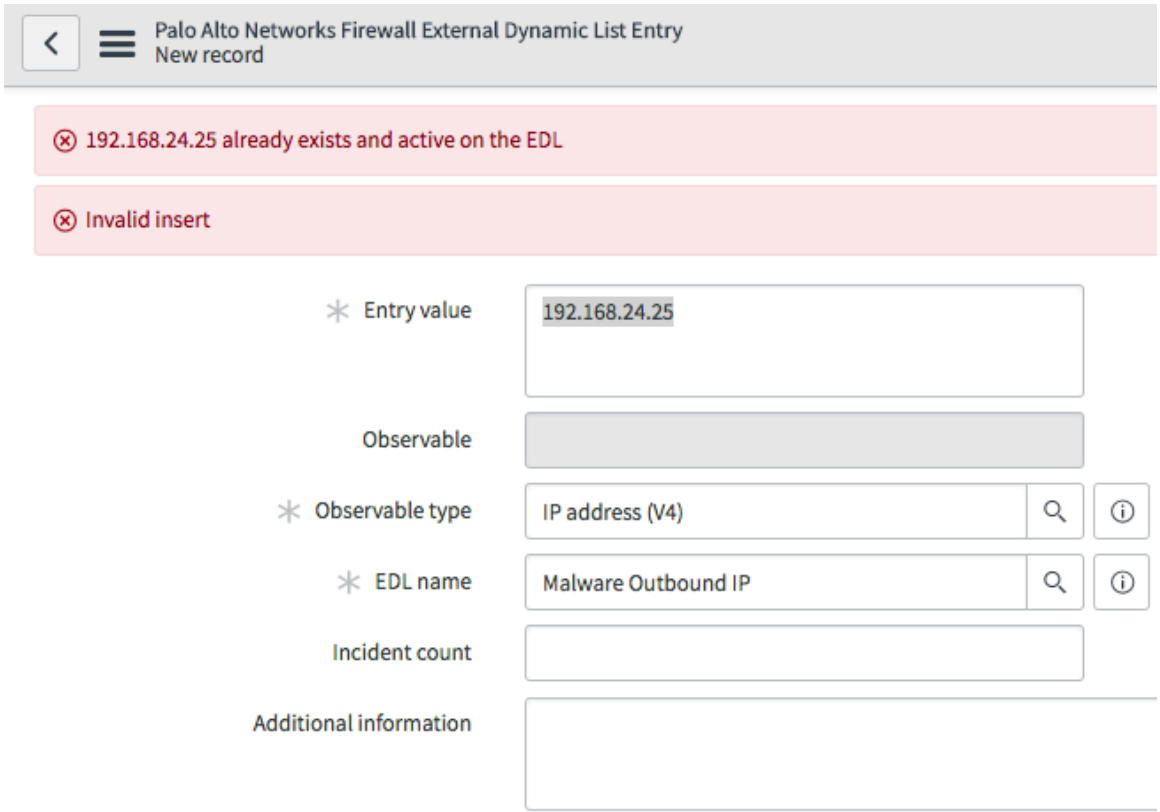
Exceção de CIDR (Roteamento entre domínios sem classe)

Se você tentar anexar um único endereço IP a uma EDL e esse endereço IP fizer parte de um observável CIDR já em uma EDL, será exibido um erro de conflito de CIDR. Este erro indica que o único endereço IP já está incluído na EDL como parte do observável CIDR. Por exemplo, `192.168.24.25` faz parte do bloco CIDR `192.168.0.0/22`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conflito de CIDR



(Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall

Se a caixa de seleção **Exibir marcador** estiver marcada ao criar o registro da lista dinâmica externa (EDL), você poderá editar os nomes dos marcadores e as cores dos marcadores de segurança. Os marcadores de segurança ajudam a rastrear observáveis que já estão bloqueados.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

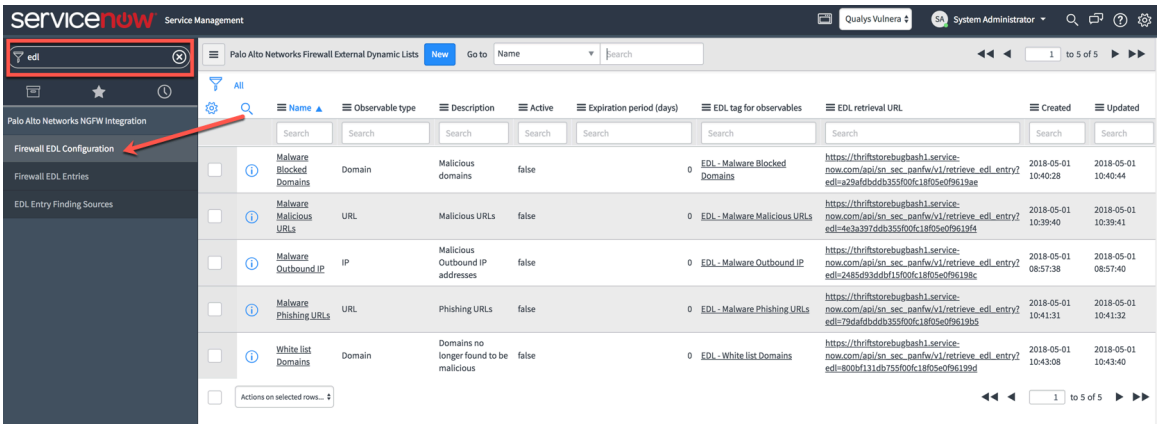
Os marcadores de segurança ajudam a identificar rapidamente quais incidentes de segurança têm observáveis em uma lista de bloqueios. Os marcadores também ajudam a identificar se um observável já está bloqueado ou se foi removido de uma EDL. Por padrão, a cor do marcador de segurança é preta para entradas da lista de bloqueios e cinza para entradas da lista de permissões. Você pode mudar os nomes e as cores dos marcadores para ajudá-lo a reconhecer determinados marcadores com mais facilidade.

Tradução automática

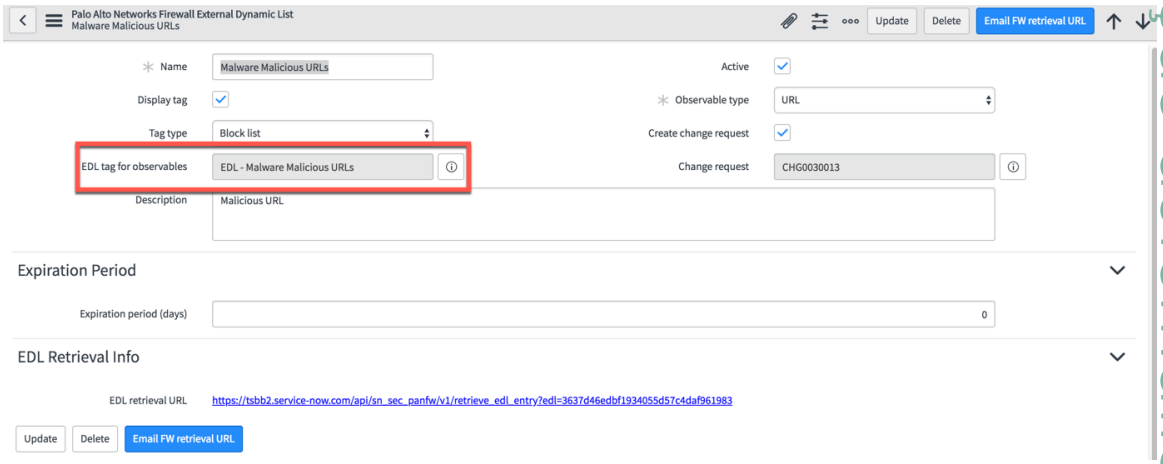
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

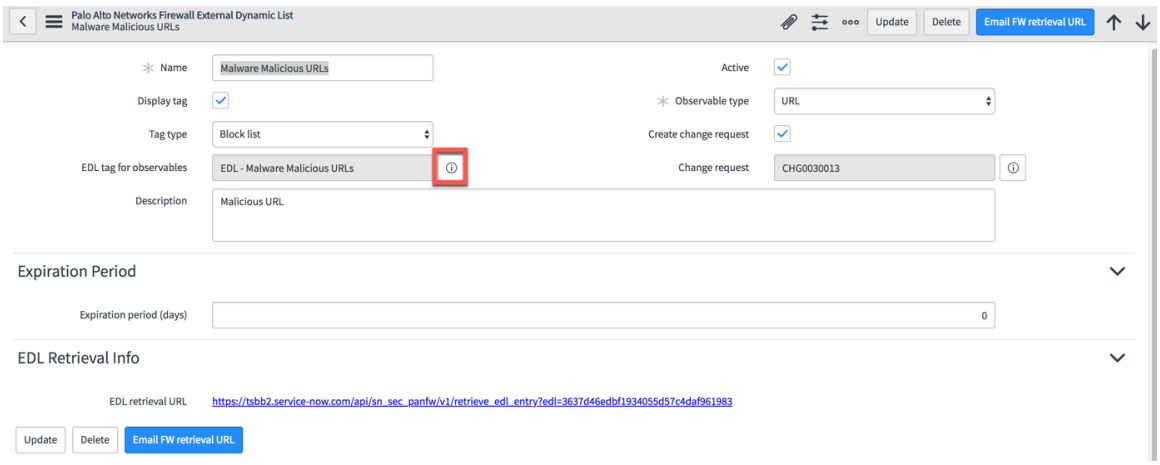
1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.



2. Clique em um item na coluna **Nome** para abri-lo
   O registro de EDL é exibido. Por padrão, o nome do marcador de segurança é o mesmo valor que você inseriu no campo **Nome** da EDL ao criá-la. Por padrão, o nome também inclui um prefixo EDL, por exemplo, EDL – URLs de malware malicioso.



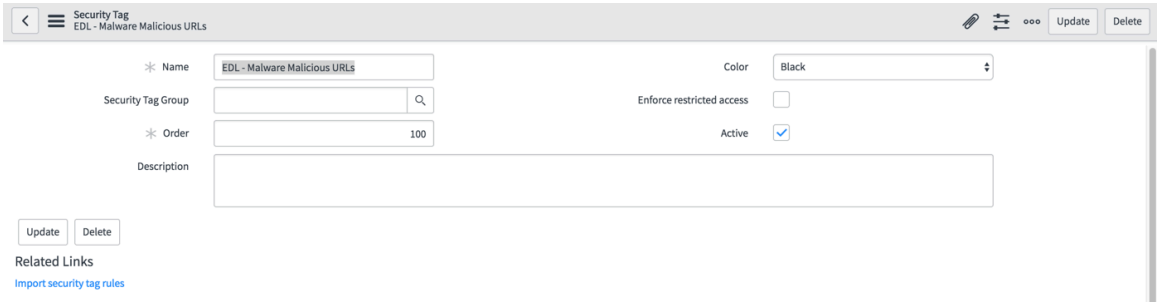
3. Clique no ícone de informações (ícone ⓘ) ao lado do **marcador EDL para observáveis** e, em seguida, em **Abrir registro**.



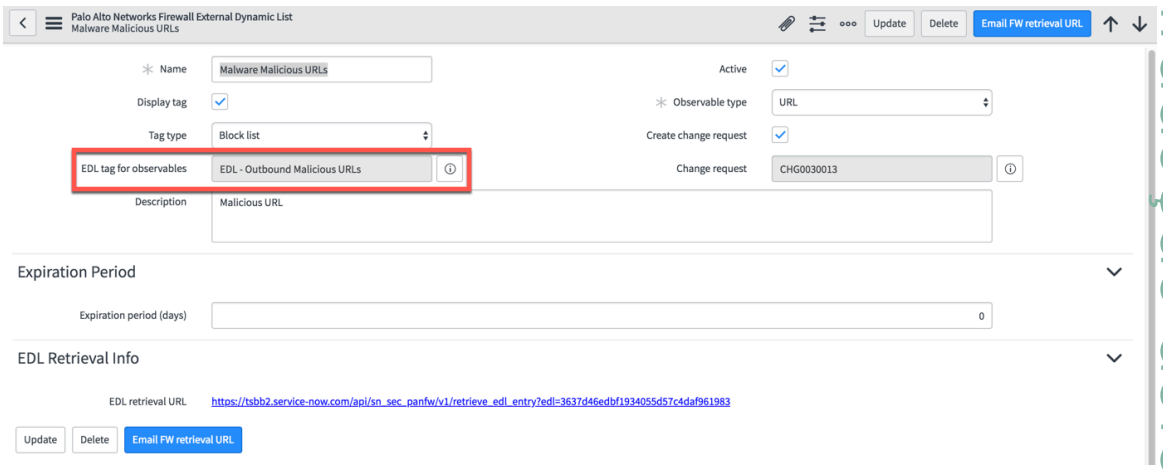
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

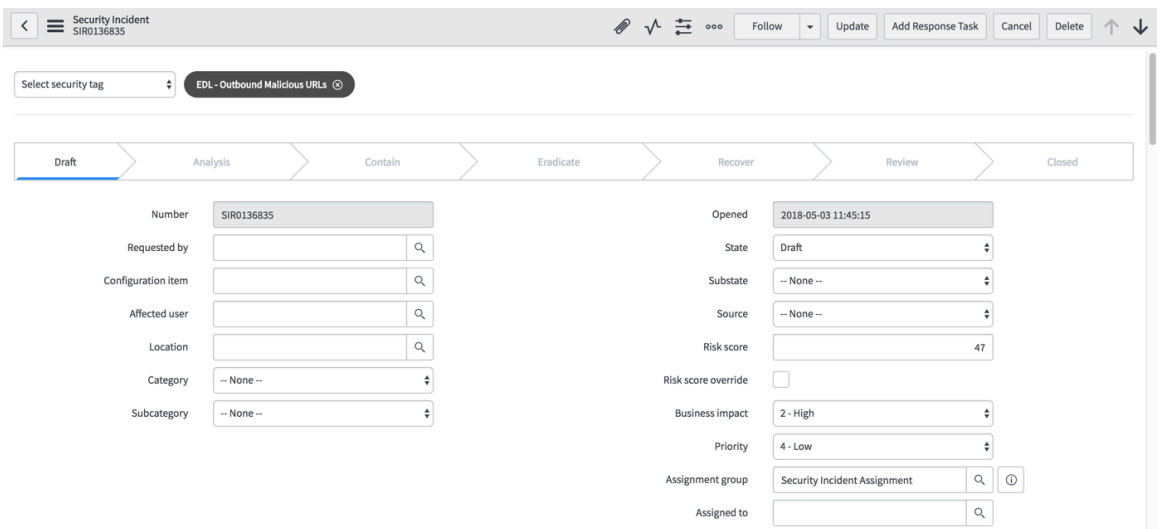
O formulário de marcador de segurança é exibido.



4. No campo **Nome**, modifique o nome do marcador de segurança e clique em **Atualizar**. O registro de EDL atualizado é exibido com o nome do marcador modificado. No exemplo a seguir, `Saída` foi adicionado ao nome do marcador. Mantenha o prefixo `EDL` no novo nome do marcador para ajudá-lo a identificar que o marcador está associado à integração Palo Alto Networks Next-Generation Firewall.



Os marcadores de segurança são exibidos para cada tipo de observável (IP, URL, domínio) no registro de incidente de segurança e no registro do observável sempre que esse observável é adicionado a um EDL.



Se um observável já tiver sido adicionado a um EDL e um marcador de segurança for exibido em um incidente de segurança para este observável, o marcador de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

EDL também será exibido automaticamente em todos os registros de incidentes de segurança subsequentes que forem criados. Essa duplicação informa que o observável já está em uma lista de bloqueios. Você não precisa adicionar este observável e bloqueá-lo novamente.

Quando um observável não está mais bloqueado, um marcador de segurança não é exibido no registro de incidente de segurança ou no registro do observável. Nesta instância, nenhum marcador de segurança indica que a data de expiração do observável pode ter passado ou que o observável foi desativado de uma EDL.

Desinstalar Palo Alto Networks Next-Generation Firewall

Se você quiser desinstalar Palo Alto Networks Next-Generation Firewall da instância Now Platform e remover todos os remanescentes da integração, consulte o site de documentação ServiceNow para obter instruções sobre como desinstalar aplicações.

Antes de Iniciar

Função necessária: administrador do sistema (admin)
Consulte Desinstalar aplicações no site de documentação de produtos da ServiceNow .

Integração de PhishTank

PhishTank é um sistema de verificação de phishing baseado na comunidade no qual os usuários enviam ameaças suspeitas e outros usuários no sistema votam para determinar se as ameaças de phishing são legítimas. Quando integrados ao produto Now Platform Operações de segurança, os resultados de inteligência contra ameaças fornecem aos analistas informações adicionais sobre incidentes ou investigações de segurança relacionados a phishing.

A integração PhishTank realiza pesquisas em possíveis URLs de sites de phishing.

O fluxo de trabalho verifica se há novos observáveis conforme eles chegam nos incidentes de segurança. Se os observáveis forem de um tipo reconhecido pela integração de API, os observáveis serão avaliados. Os observáveis determinados como mal-intencionados são marcados.

Instalar e configurar PhishTank

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que a aplicação PhishTank se integre corretamente a Now Platform Operações de segurança.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Tarefas de configuração	Descrição
Verifique se você atribuiu as funções Now Platform necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o aplicativo e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	esperados. Esta função também tem acesso ao módulo Operações de segurança.
Obtenha uma chave de API.	Visite o site PhishTank para obter informações sobre chaves de API e para criar uma conta: Site PhishTank .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posterior Para a versão Madrid e as versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .

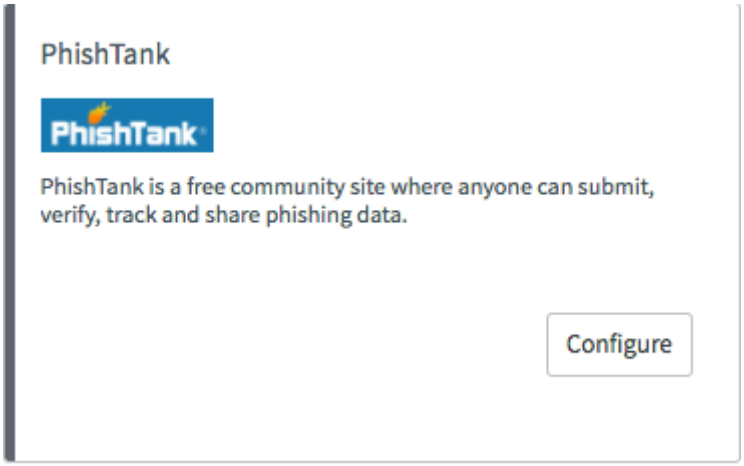
Função necessária: administrador

Procedimento

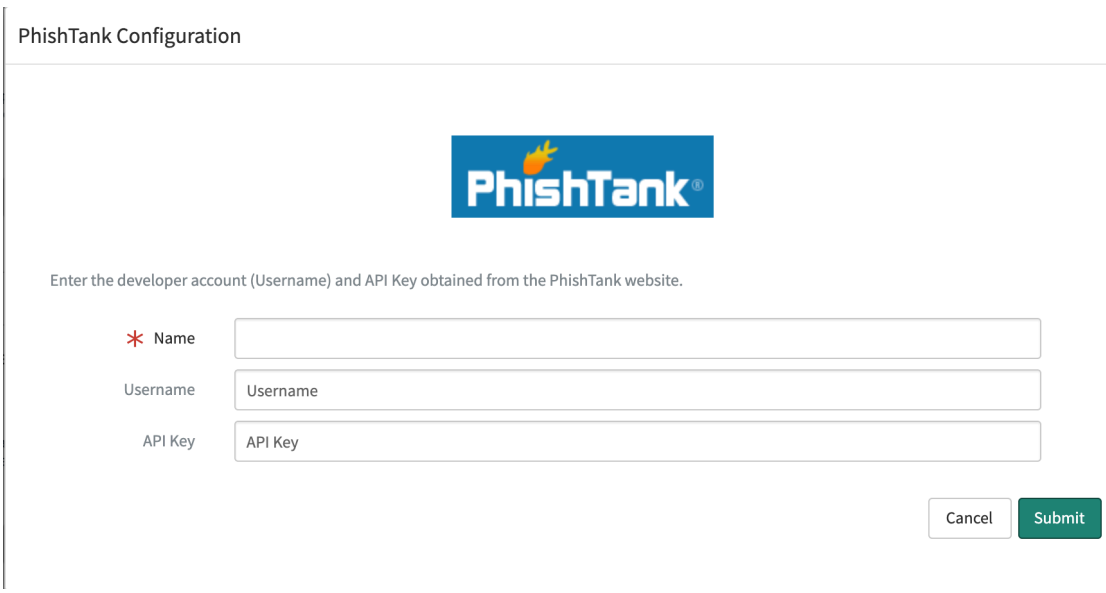
1. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.
2. Depois que a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco PhishTank.
3. Clique em **Configurar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo **Configuração do PhishTank**, insira o Nome da configuração, o Nome de usuário (conta de desenvolvedor criada no PhishTank) e a chave de API que você obteve no site PhishTank e clique em **Enviar**.



5. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, a chave de API PhishTank pode ser inválida.

Verificar resultados esperados para PhishTank

Os observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Os resultados da pesquisa são exibidos na guia Resultados da pesquisa de ameaças na parte inferior do registro de incidente de segurança.

Antes de Iniciar

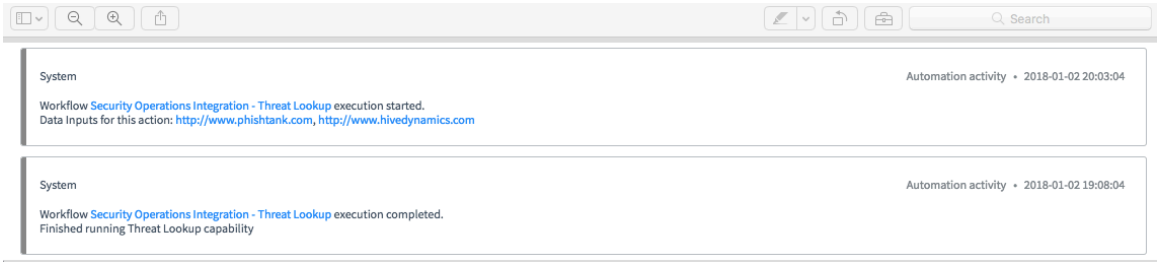
Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o formulário de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

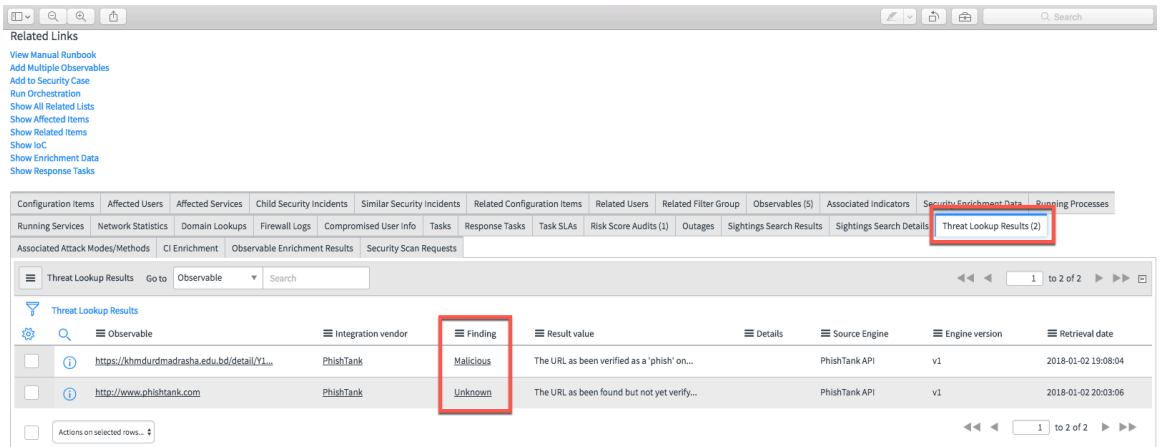


   Depois que a aplicação é configurada, o fluxo é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no registro de incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

3. Navegue até a parte inferior do incidente de segurança e clique no link relacionado **Mostrar todas as listas** relacionadas.

   Nota: As imagens nas etapas a seguir são mostradas com a configuração **Formulários com guias** ativa nas Configurações do sistema. Se os formulários com guias não forem exibidos, no canto superior direito da faixa superior, clique no ícone de engrenagem Configurações. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se Formulários **com guias** e **Com o formulário** estão selecionados.



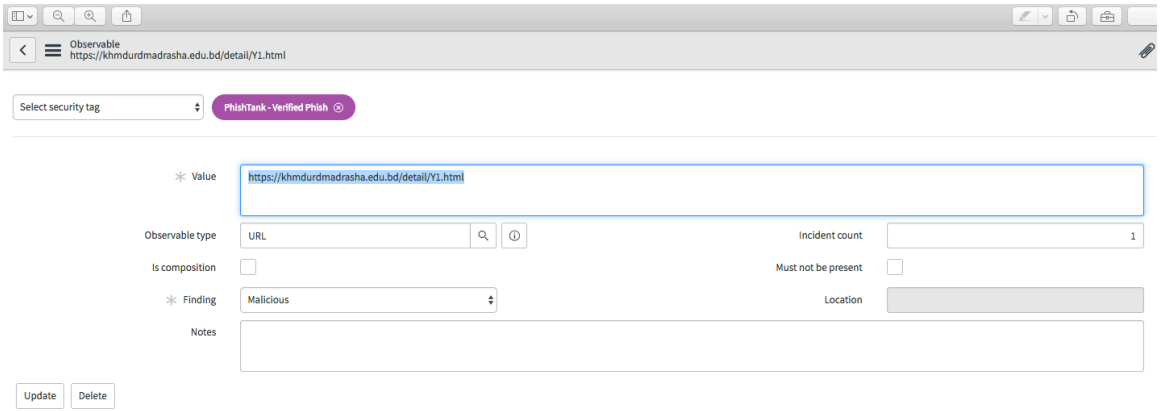
   A guia **Resultados da pesquisa de ameaças** na parte inferior do registro do incidente de segurança exibe os resultados da pesquisa.

   A coluna **Descoberta** exibe `Desconhecido` para registros não determinados como mal-intencionados. Para resultados correspondentes a mal-intencionados, `Mal` -intencionado é exibido na coluna **Descoberta**.

4. Na coluna **Observável**, clique em um observável para abrir um registro e exibir mais informações.

Tradução automática

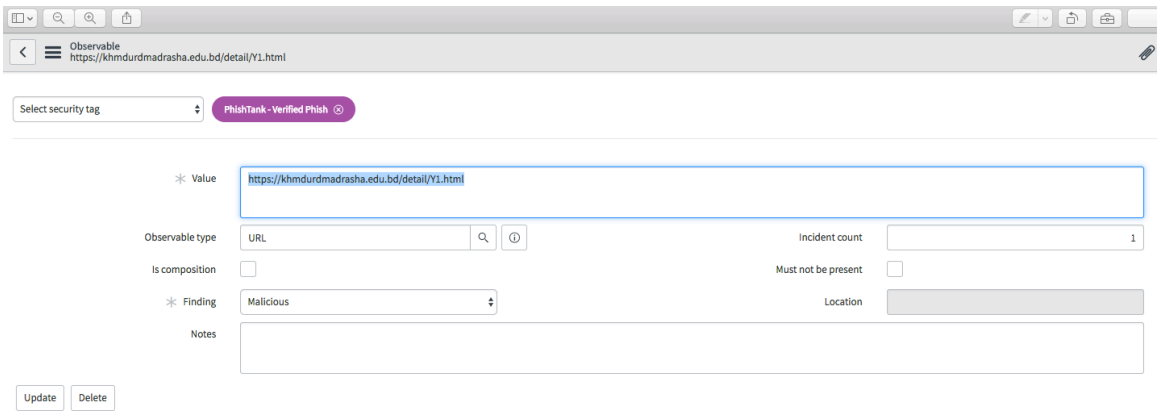
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



No registro do observável, para pesquisas correspondentes a mal-intencionadas, `Mal-intencionado` é exibido no campo **Descoberta**. O observável está marcado com a origem Inteligência contra ameaças que o considerou mal-intencionado, neste caso, a aplicação PhishTank.

5. Para exibir dados brutos, navegue de volta para o incidente de segurança e clique no ícone de informações azul ao lado de um observável.

6. Na janela que é exibida, clique em **Abrir registro**.



O link criado pela API e o campo **Descoberta** exibido com os resultados.

Trouble?
Se você não vir os resultados na guia **Resultados da pesquisa de ameaças**, verifique se o observável é de um tipo compatível com a pesquisa pela integração.

(Opcional) Anexar manualmente um observável para PhishTank

Você pode anexar observáveis manualmente a um incidente de segurança. Você anexa observáveis manualmente quando deseja executar pesquisas de ameaças em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

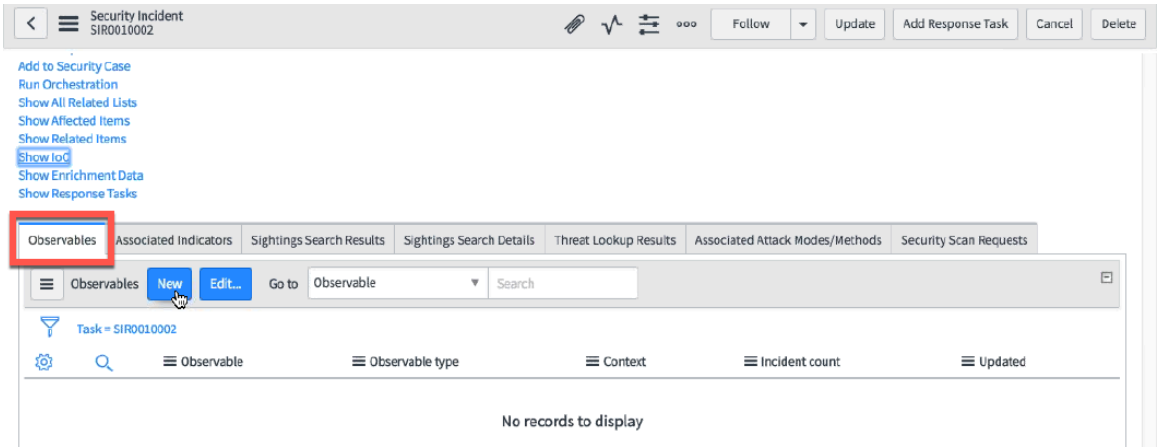
Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

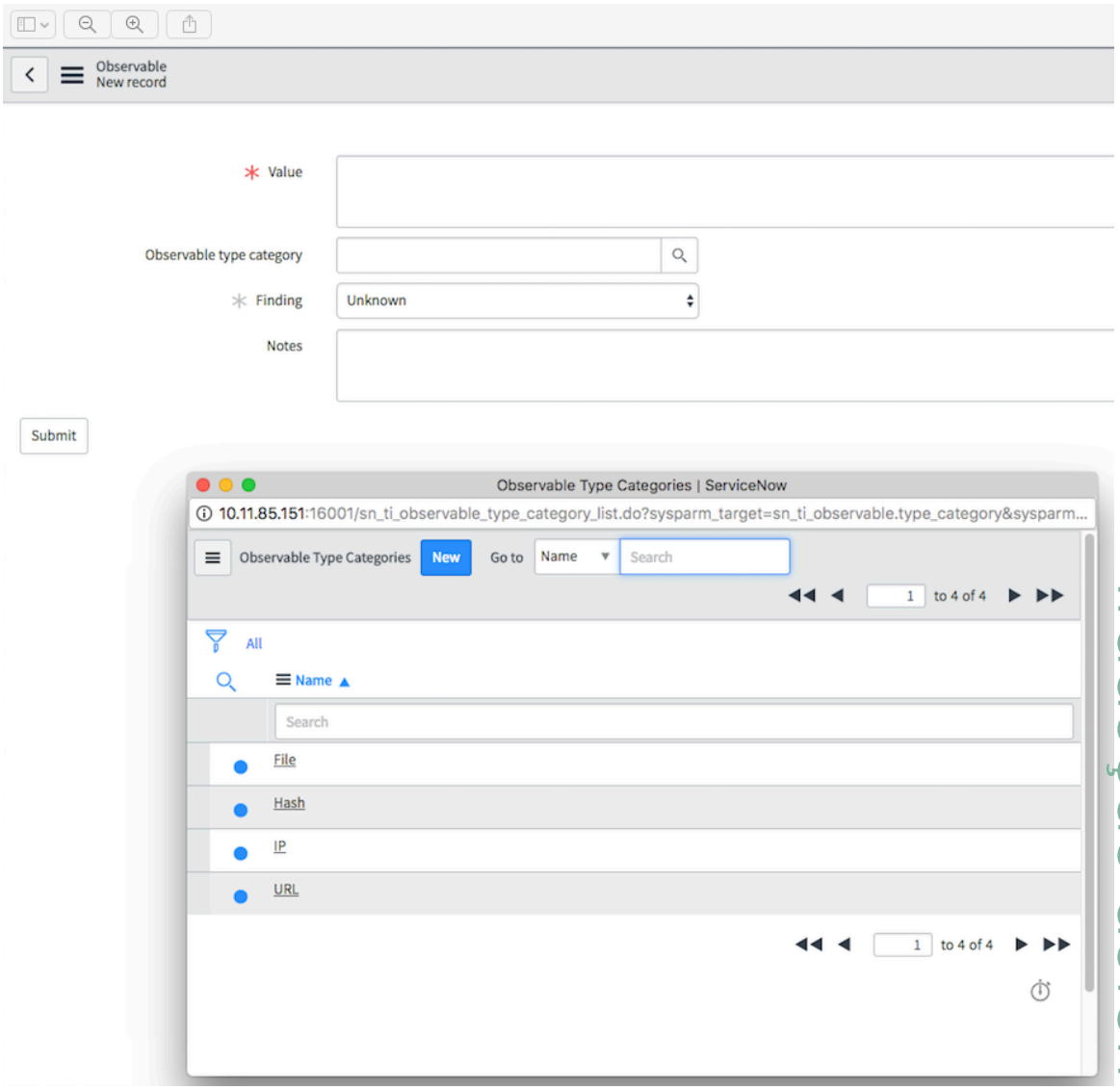
1. Navegue até o seu incidente de segurança aberto.
2. No registro de incidente de segurança aberto, clique no link **Mostrar IoC**em **Links relacionados** para exibir a guia **Observáveis**.



3. Clique em **Nova**.
   O formulário Observável é exibido.
4. No campo **Valor**, insira um URL.
5. Clique no ícone de pesquisa e na caixa de diálogo **Categorias de tipo de observável**, clique em **URL** na lista para preencher o campo.

Tradução automática

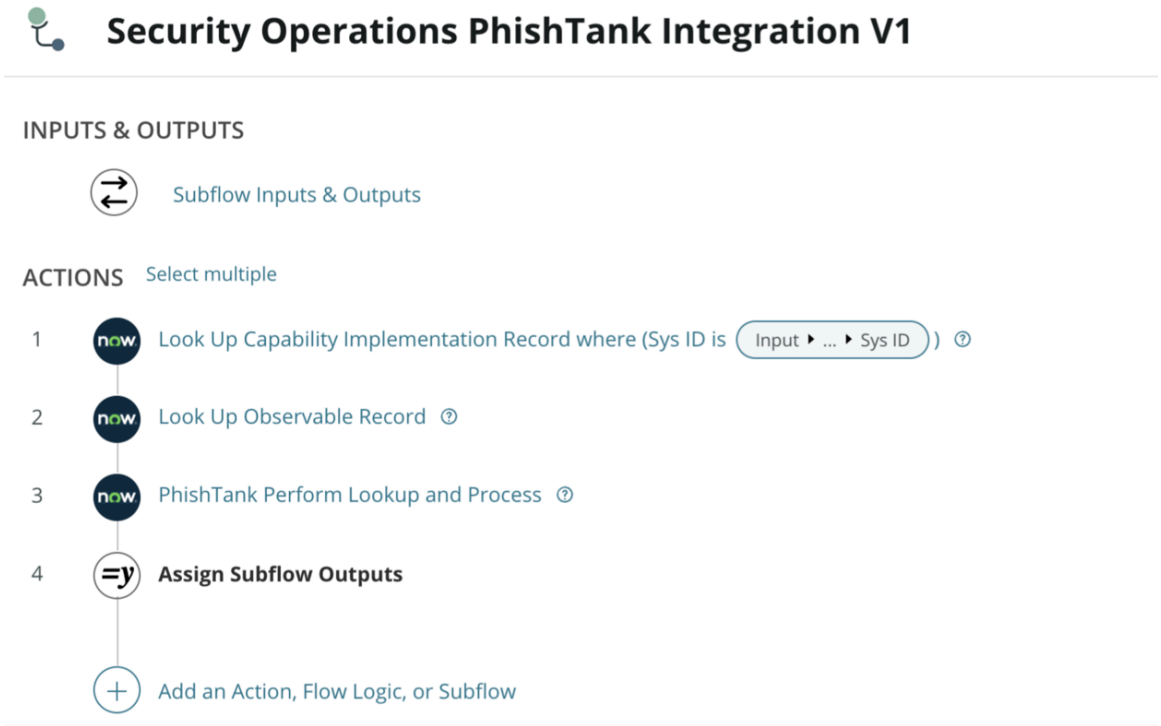
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



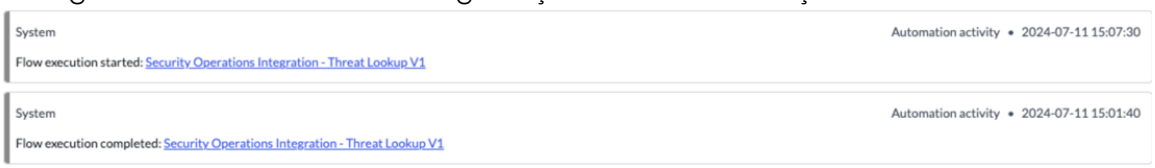
6. Clique em **Enviar**.
   O fluxo é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção de anotações de trabalho no registro de Incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

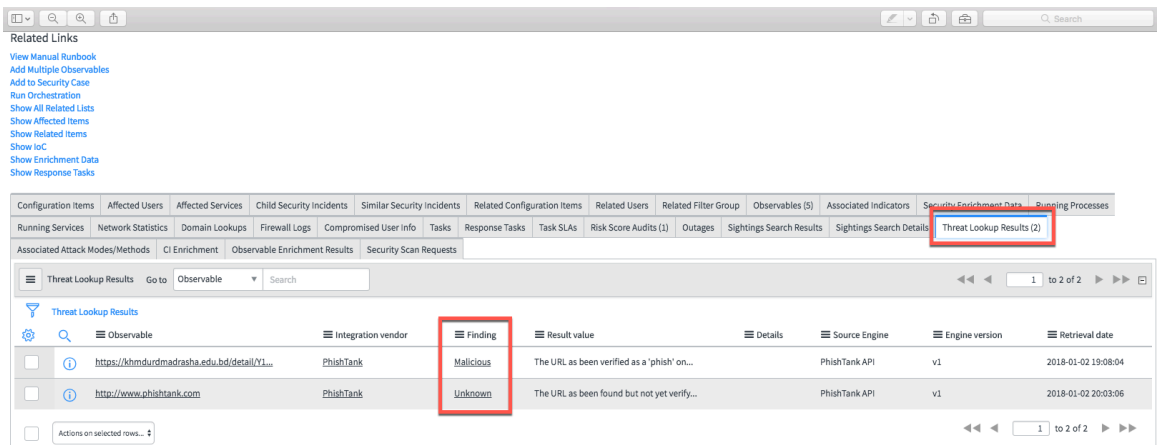


7. Navegue até o seu incidente de segurança e revise as anotações de trabalho.



8. Clique no link relacionado **Mostrar todas as listas** relacionadas na parte inferior do incidente de segurança.

9. Clique na guia **Resultados da pesquisa de ameaças** para exibir os resultados.



10. Na coluna **Observável**, clique no ícone de informações azul ao lado de um determinado observável para obter mais informações e dados brutos.

11. Na caixa de diálogo exibida, clique em **Abrir registro**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trouble?
Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

Integração de Reverse Whois

Reverse Whois é um serviço que realiza pesquisas em nomes de domínio registrados por indivíduos ou organizações.

Execute pesquisas de domínio usando termos de pesquisa em observáveis que você anexa a um incidente de segurança. A API Reverse Whois pesquisa registros de domínio com base nos termos de pesquisa inseridos e retorna todos os registros que correspondem a esses termos.

Às vezes, os analistas usam essa integração junto com a integração Whois para pesquisa de incidentes de segurança. A integração Whois fornece informações de aprimoramento adicionais com base nas pesquisas de domínio da integração Reverse Whois.

Instalar e configurar Reverse Whois

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que a aplicação Reverse Whois se integre corretamente ao produto Operações de segurança.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções obrigatórias da ServiceNow.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o aplicativo e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração. O administrador de incidentes de segurança também atribui a função de Analista de incidentes de segurança (sn_si.analyst). • O Analista de incidentes de segurança (sn_si.analyst) executa pesquisas de domínio com Reverse Whois e analisa e trabalha com incidentes de segurança.
Obtenha uma chave de API.	Visite o site da API WhoisXML para obter informações sobre chaves de API e para criar uma conta: Site da API WhoisXML . A configuração requer que você insira as chaves de API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte	Requisitos da versão Madrid e posterior

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Madrid e as versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .

Função necessária: administrador

Procedimento

1. Se você já instalou e configurou a aplicação Reverse Whois, siga estas etapas:

a. Exclua a configuração existente.

b. Instale e crie uma nova configuração usando a chave de API que você obteve.

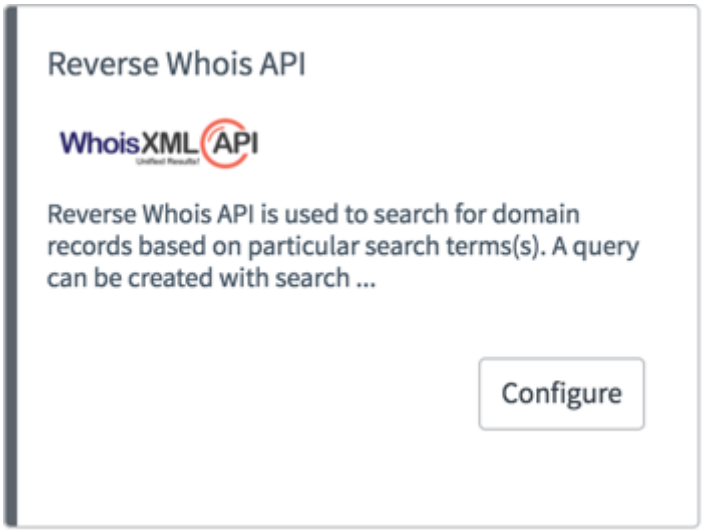
2. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.

3. Depois que a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco de API Reverse Whois.

4. Clique em **Configurar**.

Tradução automática

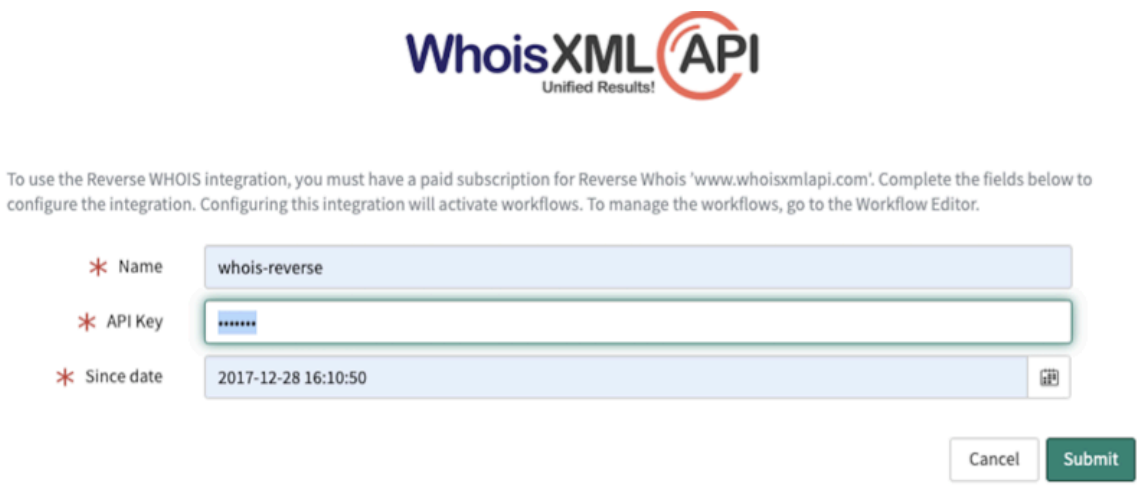
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na caixa de diálogo **Configuração da Reverse Whois API**, insira a chave de API que você obteve no site da Whois XML API.
6. Escolha uma opção na tabela a seguir para filtrar pesquisas de domínio para seus termos de pesquisa.

Descrição	Configuração
Sua pesquisa inclui todos os domínios, ativos e expirados, que foram registrados após a data Desde para os termos de pesquisa inseridos. Esta é a configuração recomendada.	**Desde a data**: data inserida no formato aa-aa-mm-dd. Por exemplo, `1991-06-01` para 1º de junho de 1991.
Sua pesquisa inclui todos os domínios ativos para os termos de pesquisa inseridos.	**Desde a data**: campo limpo.

Essas definições de configuração permanecem salvas até que você as altere e as apliquem a todas as Reverse Whois pesquisas de API.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

Trouble?
Se uma mensagem de erro for exibida, a chave de API pode ser inválida.

Mensagem de erro

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

(Opcional) Instalar e configurar Whois

Instale o plug-in Whois para fornecer informações de enriquecimento adicionais em suas pesquisas de domínio da API Reverse Whois. Esta pesquisa fornece dados de enriquecimento adicionais no domínio, como a data de registro, o nome do registrador e o país de origem.

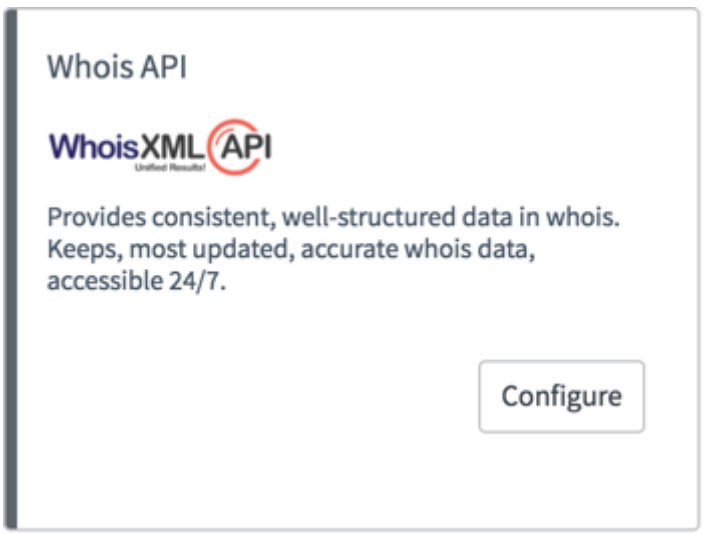
Antes de Iniciar

1. Se você não solicitou o direito da aplicação, consulte para a aplicação Whois na ServiceNow Store.
2. Obtenha credenciais para a chave de API Whois no site do produto: site da API WHOIS .

Função necessária: administrador

Procedimento

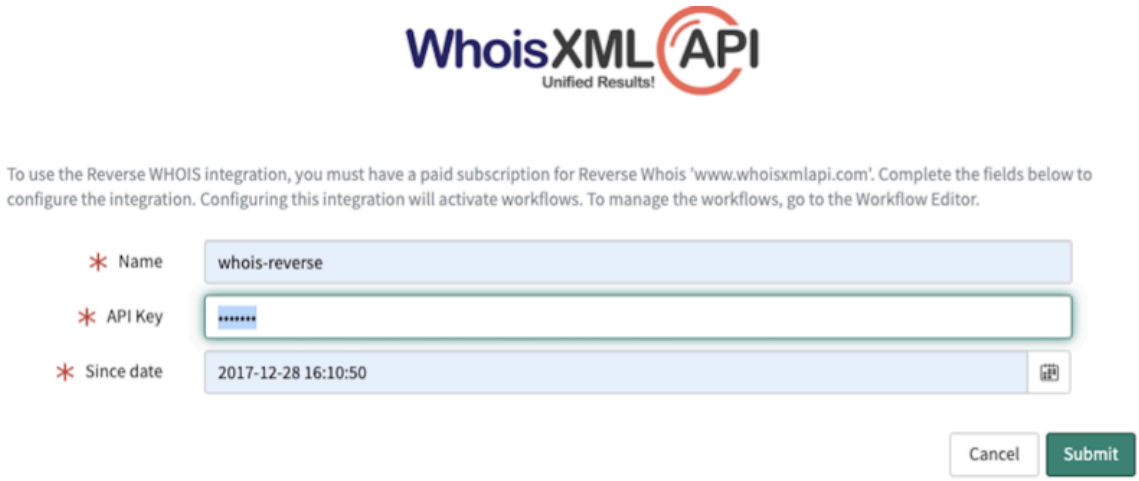
1. Se você não instalou a aplicação, consulte e siga as etapas para instalá-la.
2. Depois que a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco de API Whois.
3. Clique em **Configurar**.



4. Na caixa de diálogo **Configuração da API Whois**, insira a chave de API que você obteve no site do produto.

Tradução automática

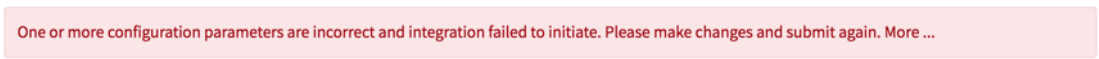
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Agora você pode executar pesquisas de aprimoramento nos domínios retornados da integração Reverse Whois.

Trouble?
Se uma mensagem de erro for exibida, a chave de API pode ser inválida.

Solução de problemas



Iniciar a pesquisa de Reverse Whois

Inicie pesquisas de domínio usando termos de pesquisa em observáveis que você anexa manualmente a um registro de incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

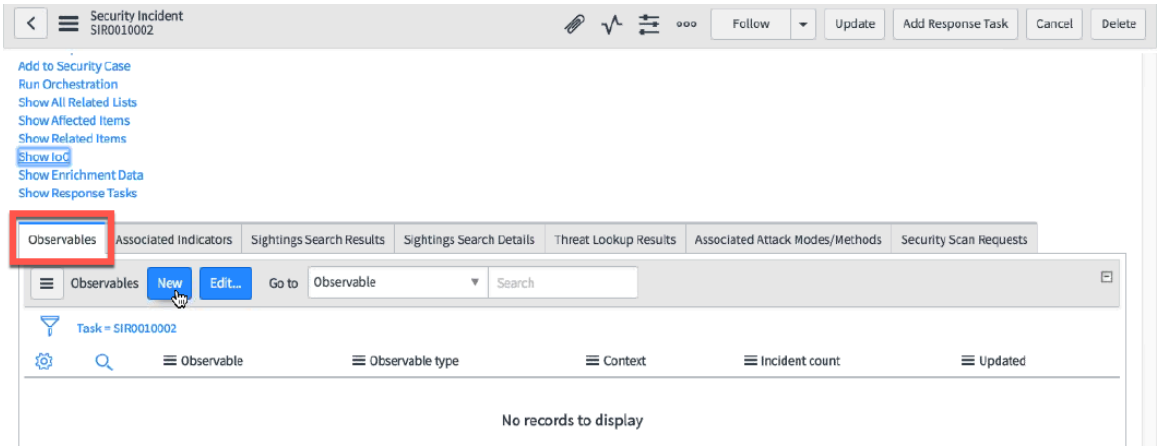
Procedimento

1. Se não estiver aberto, navegue até **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes** e abra o incidente de segurança com o qual você está trabalhando.
2. Na parte inferior do registro, clique no link relacionado **Mostrar IoC** para exibir a guia Observáveis.

> **Nota:** As imagens nas etapas a seguir são mostradas com a configuração **Formulários com guias** ativa nas Configurações do sistema. Se você não vir as guias no incidente de segurança, no canto superior direito da faixa, clique no ícone de engrenagem **Configurações**. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se Formulários **com guias** e **Com o formulário** estão selecionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

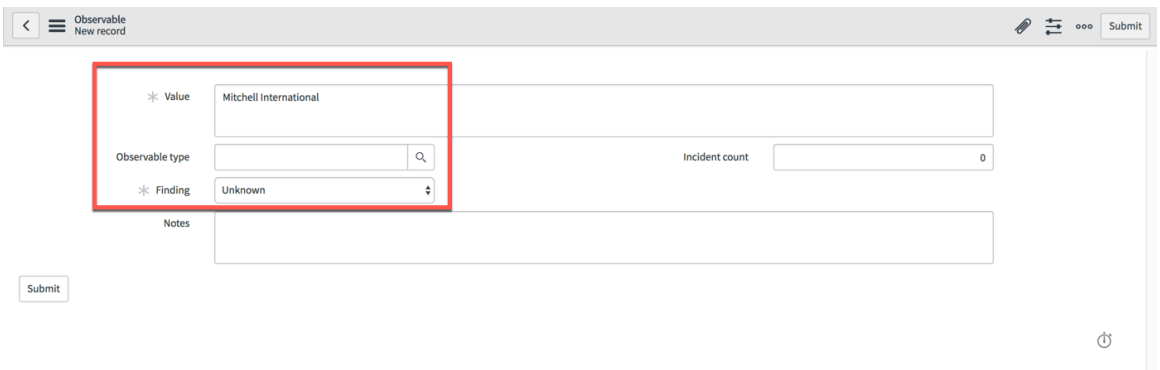


3. Na guia Observáveis, clique em **Novo**.

4. Preencha os campos.

Campos obrigatórios no novo registro

Campo	Descrição
Valor	Termo de pesquisa exclusivo para um domínio.
Tipo de observável	Este campo é limpo automaticamente.
Descoberta	Este campo é definido automaticamente como **Desconhecido**.



5. Clique em **Enviar**.
Você retorna ao registro do incidente de segurança e o fluxo inicia a pesquisa.

O que Fazer Depois

Verifique os resultados da pesquisa sobre o incidente de segurança. Consulte Verificar resultados esperados para Reverse Whois.

Verificar resultados esperados para Reverse Whois

Os resultados de aprimoramento são exibidos na guia **Domínios ReverseWhois** na parte inferior do registro de incidente de segurança. Localize os resultados da pesquisa para verificar se a pesquisa foi executada com sucesso.

Antes de Iniciar

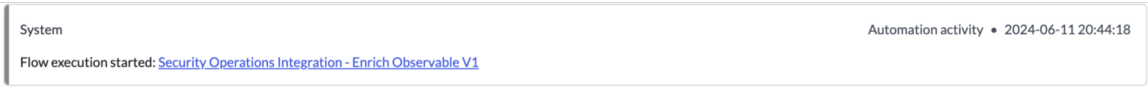
Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ainda não estiver aberto, navegue até **Incidentes de segurança** > **Incidentes** > **Mostrar todos os incidentes** e localize o incidente de segurança com o qual você está trabalhando.

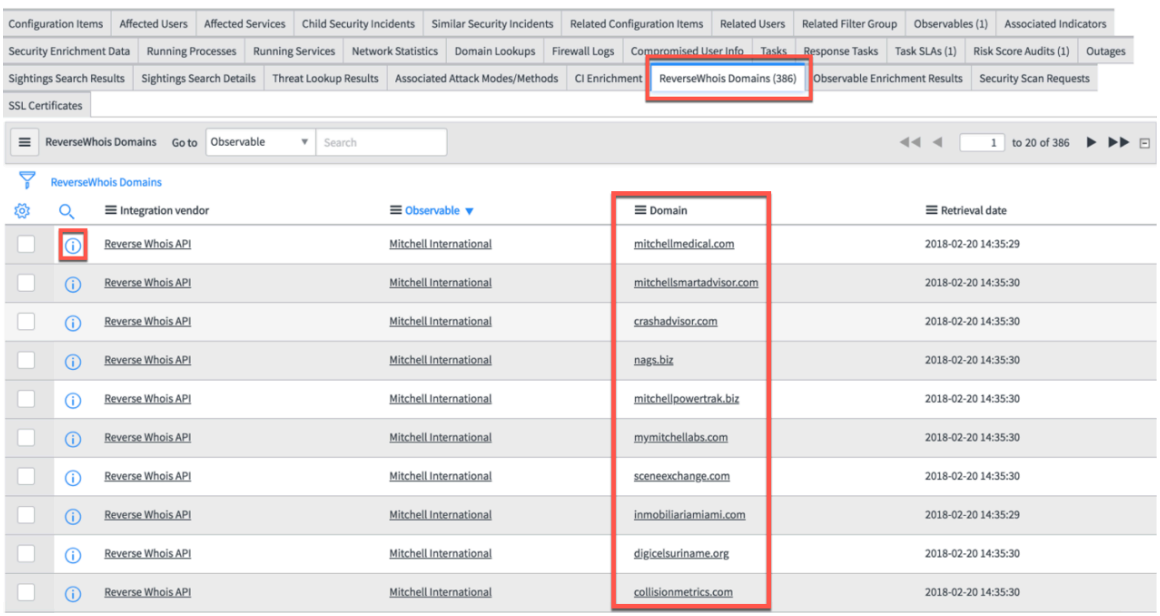
   

   Depois que a aplicação é configurada e você anexa um observável, o fluxo é iniciado automaticamente. As anotações de trabalho no registro do incidente de segurança exibem o status de execução e conclusão da pesquisa.

2. Se você não puder verificar se a pesquisa foi executada com sucesso, revise as anotações de trabalho para obter mais informações sobre como prosseguir.

3. Navegue até a parte inferior do incidente de segurança e clique no link relacionado **Mostrar todas as listas** relacionadas.

   Nota: Para os resultados de pesquisa filtrados mostrados na figura a seguir, as definições de configuração no bloco de configuração da API Reverse Whois foram salvas com **1991-06-01** inserido no campo **Desde a data**.

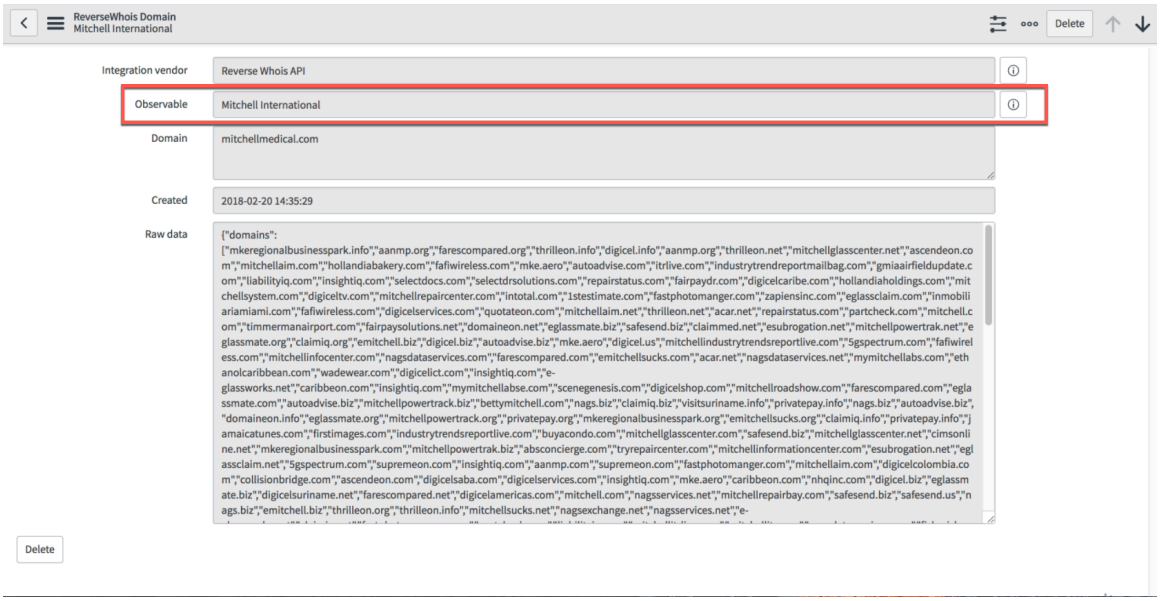
   

   Os resultados de aprimoramento são exibidos na guia **Domínios de ReverseWhois**. Os domínios ativos para este observável são exibidos na coluna **Domínio**.

4. Clique no ícone de informações azul ao lado de um item e clique em **Abrir registro** na caixa de diálogo exibida.

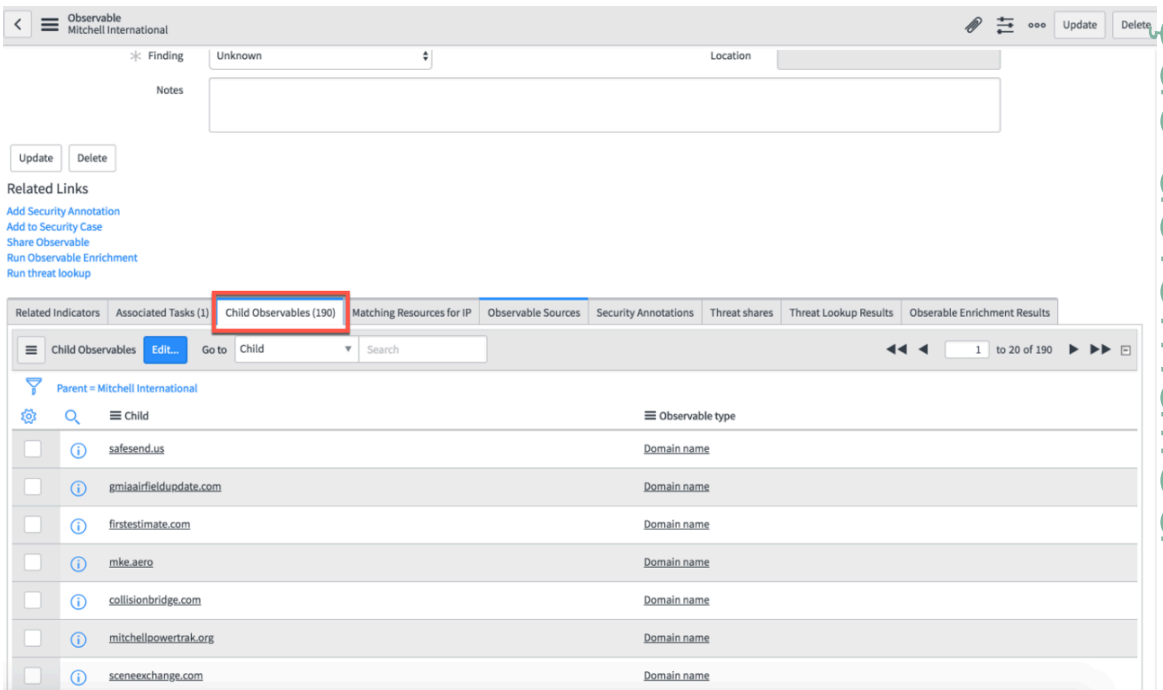
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro é exibido com detalhes de aprimoramento, incluindo os dados brutos.

5. Navegue de volta para o incidente de segurança e, com a guia **ReverseWhois Domains** selecionada, clique em um observável na coluna **Observável** para abrir um registro.



Os observáveis secundários são exibidos na guia **Observáveis** secundários no registro do Observável. Os observáveis secundários serão gerados somente se a aplicação Reverse Whois tiver retornado domínios.

Trouble?
Se a pesquisa não for concluída com sucesso, verifique se os termos de pesquisa inseridos são compatíveis com a integração. Revise as anotações de trabalho para obter mais informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Para obter mais dados de aprimoramento nos resultados da pesquisa de domínio, você pode executar a integração Whois para realizar pesquisas de aprimoramento nos observáveis secundários retornados pela integração Reverse Whois. Esses dados de aprimoramento nos observáveis secundários incluem informações sobre data de registro, nome do registrador e país de origem.

(Opcional) Execute a pesquisa de aprimoramento e verifique os resultados esperados para Whois

Execute a integração Whois para realizar pesquisas de aprimoramento nos domínios retornados da integração Reverse Whois.

Antes de Iniciar

Verifique se você instalou e configurou os plug-ins Reverse Whois e Whois. Execute essas etapas somente depois de executar a pesquisa de domínio com o plug-in Reverse Whois.

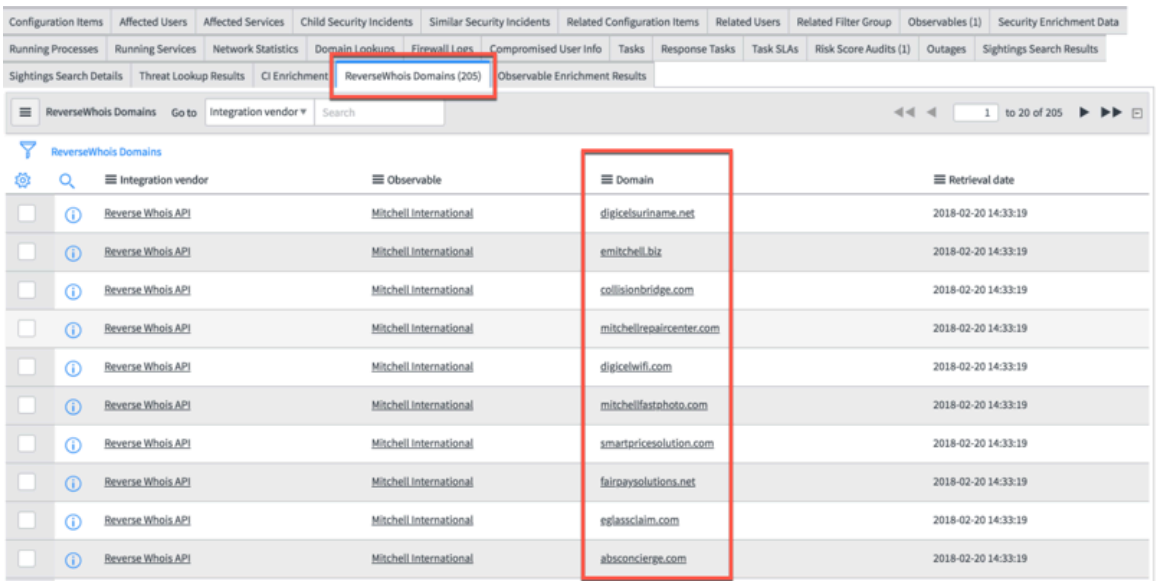
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os resultados são exibidos na guia **Resultados** de aprimoramento do observável no registro do observável.

Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Incidentes** > **Mostrar todos os incidentes** e localize o incidente de segurança com o qual você está trabalhando que executou a pesquisa de domínio com sucesso.
2. Abra o registro e clique no link relacionado **Mostrar todas as listas** relacionadas.
3. Selecione a guia **Reverter domínios Whois** na parte inferior do registro.

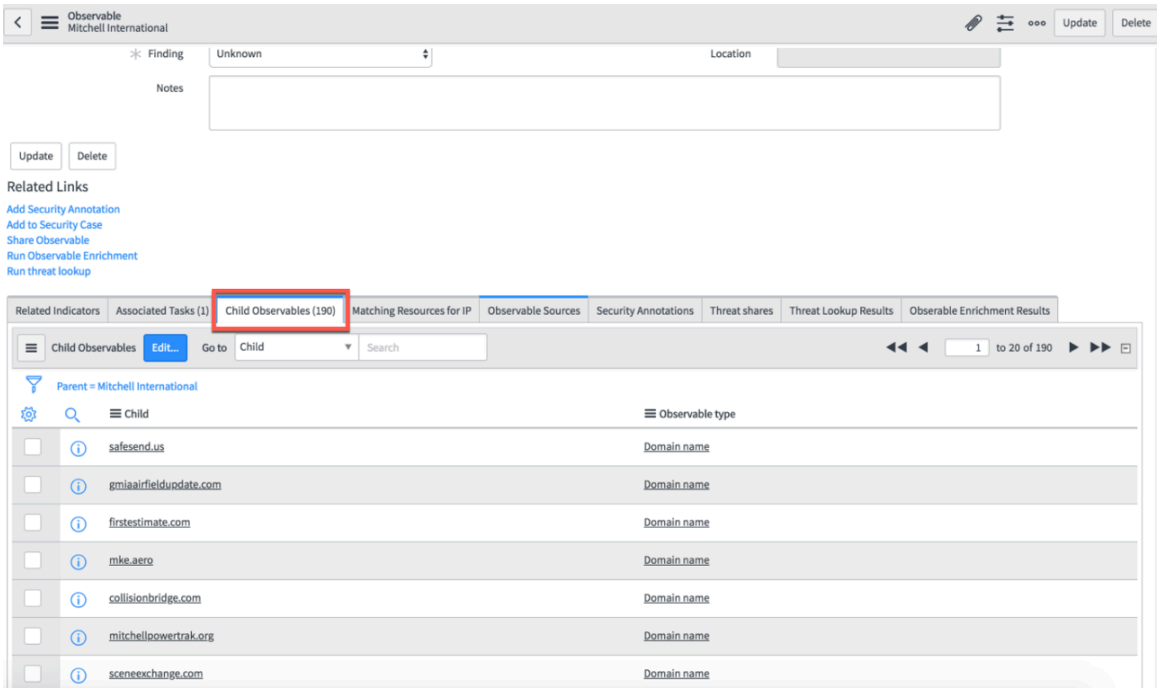


Na coluna **Domínios**, a lista de domínios retornados é exibida.

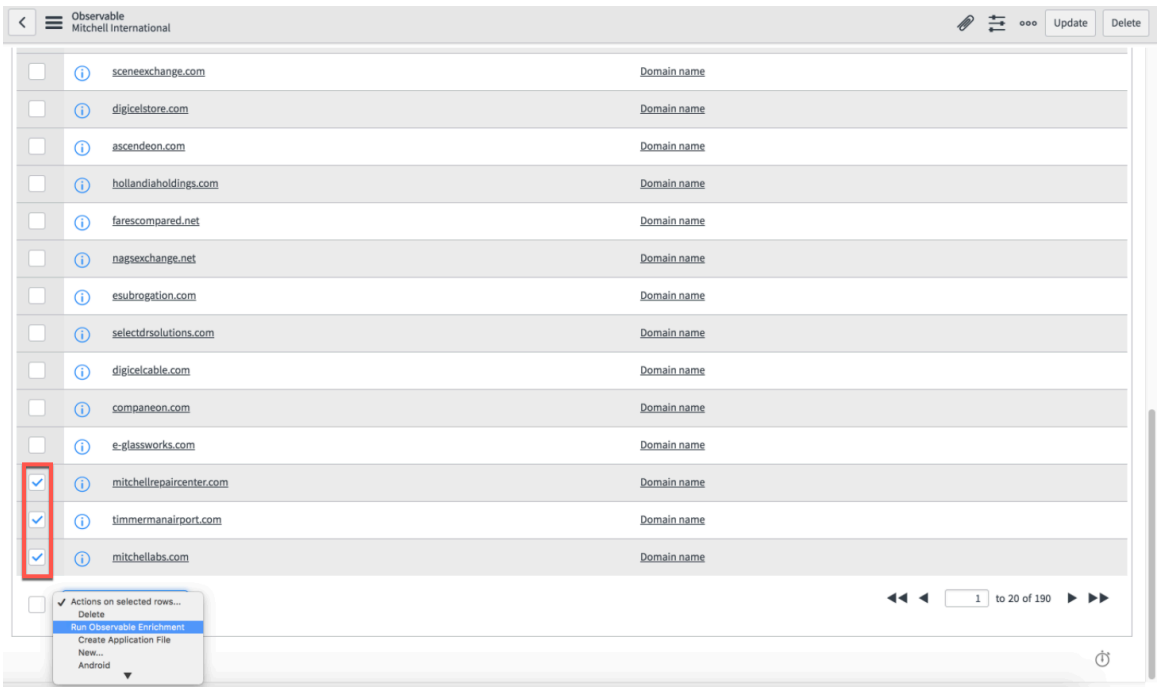
4. Na coluna **Observável**, clique em um observável.
   Na guia **Observáveis secundários**, os observáveis secundários são exibidos. Os observáveis secundários serão gerados somente se a verificação inicial do observável pela aplicação Reverse Whois retornar domínios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Selecione os observáveis secundários nos quais você deseja executar o aprimoramento de observável e, na lista de seleção **Ação em linhas selecionadas**, selecione **Executar aprimoramento de observável**.

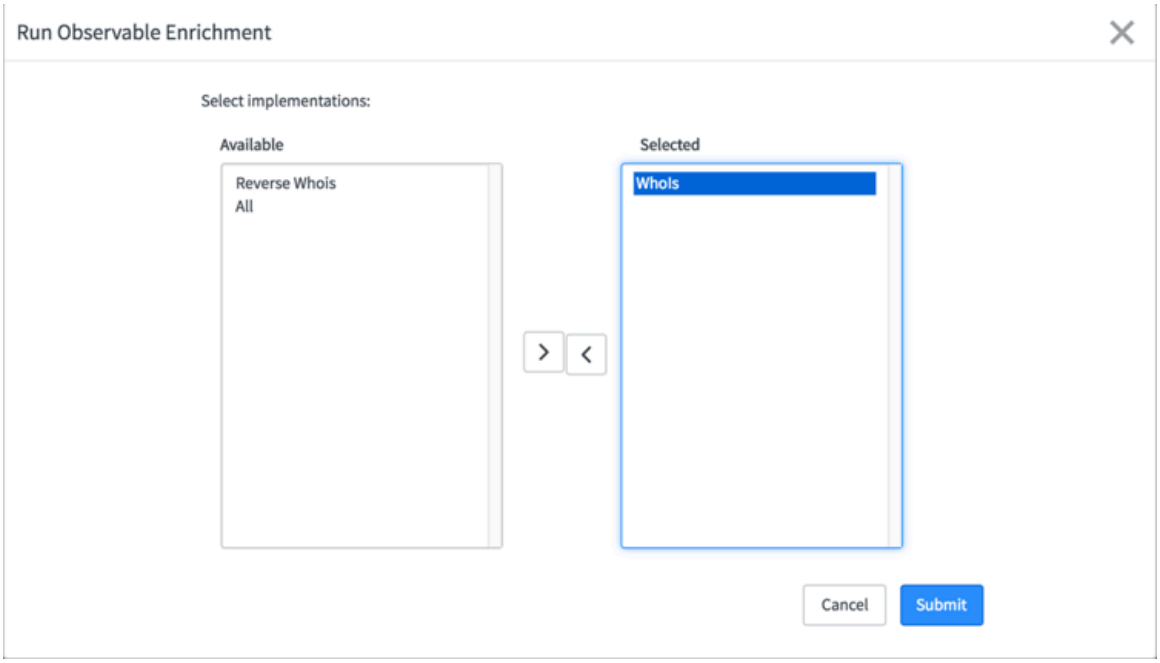


A caixa de diálogo **Executar aprimoramento de observável** é exibida.

6. Mova a integração Whois de **Disponível** para **Selecionada** e clique em **Enviar**.

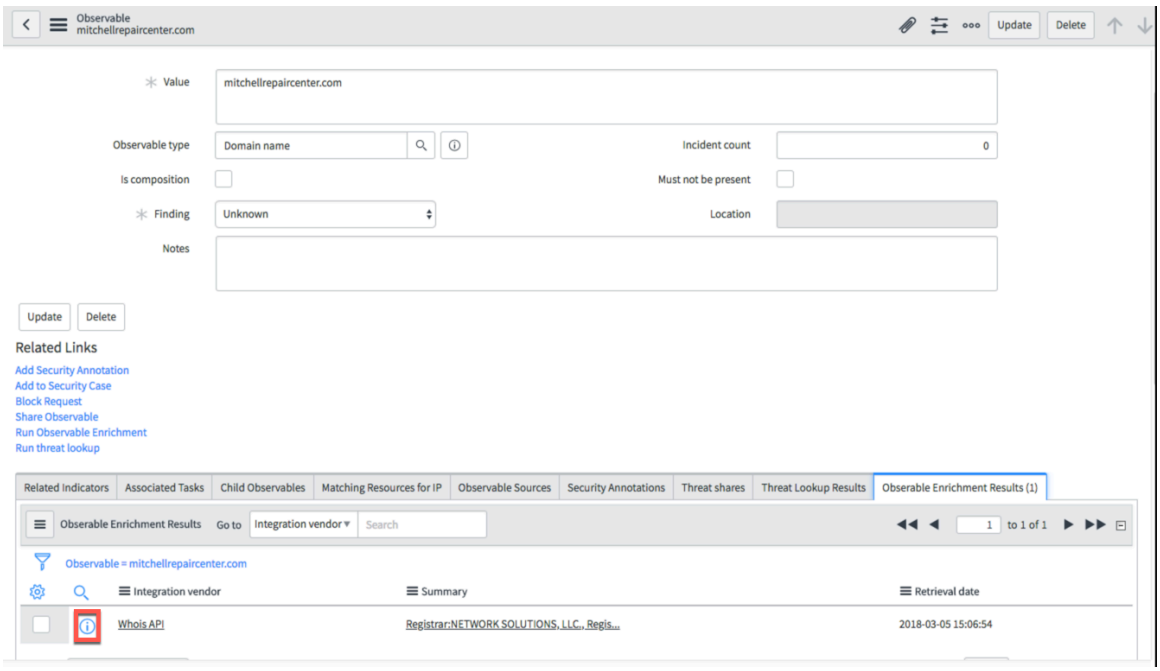
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados são exibidos na guia **Resultados** de aprimoramento do observável do registro do observável.

7. Clique no ícone de informações azul e, em seguida, clique em **Abrir registro** na caixa de diálogo que é exibida.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações e dados brutos relacionados à pesquisa de domínio original são exibidos, como a data de registro, o nome do registrador e o país de origem.

Trouble?
Se você não puder localizar observáveis secundários ou resultados de aprimoramento, verifique se a integração Reverse Whois foi executada com sucesso e retornou domínios. Além disso, consulte as anotações de trabalho no registro para obter mais informações.

Informações relacionadas

- Instalar e configurar Reverse Whois
- Verificar resultados esperados para Reverse Whois

IntegraçãoRISKIQ e WHOISIQ

Com a integração das APIs RISKIQ e WHOISIQ com o produto Now Platform® Operações de segurança, os analistas de segurança recebem dados de enriquecimento adicionais e informações sobre a validade dos sites.

A RISKIQ API de certificados SSL executa pesquisas em certificados SSL, que incluem detalhes sobre a autoridade de certificação de emissão, organizações que solicitam certificados, os certificados de entidade são emitidos para e o domínio. As pesquisas de certificado SSL são realizadas automaticamente quando os incidentes de segurança são criados.

A API RISKIQ WHOISIQ executa pesquisas em outros tipos de observáveis, como domínio, e-mail, nameserver, organização, endereço e número de telefone. Os observáveis de URL e domínio são enriquecidos automaticamente quando os incidentes de segurança são criados.

A integração requer os produtos Security Incident Response e Inteligência contra ameaças.

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

A API RISKIQ oferece suporte a pesquisas automáticas de certificado SSL em observáveis de endereço IP, hash de arquivo, número de série do certificado, domínio e URL. Os observáveis de URL e domínio são enriquecidos automaticamente com a API WHOISIQ. Para enriquecimento observável em outros tipos de observáveis com a API WHOISIQ, crie observáveis e execute pesquisas manualmente na tabela Observáveis.

Observáveis compatíveis

A tabela a seguir lista o tipo de APIs usadas nesta integração e os observáveis compatíveis com cada API. A tabela também indica se uma pesquisa ocorre automaticamente quando

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

os incidentes de segurança são criados ou se a pesquisa é executada manualmente na tabela Observáveis.

Observáveis e pesquisa compatíveis

API	Observáveis compatíveis	Pesquisa (automatizada ou manual)
RISKIQ API do certificado SSL	• Endereço IP • Hash de arquivo (impressão digital do certificado). Consulte a figura a seguir para obter um exemplo de um hash de arquivo. • Número de série do certificado ou número de série. Esta cadeia de caracteres é um ID exclusivo da entidade. Consulte a figura a seguir para obter um exemplo de um número de série de certificado. • Domínio (`www.site.com`ou `site.com`) • URL **Nota:** verificações automáticas são executadas para o formato URL usando o protocolo `https://`, por exemplo, `https://example.com/index.html`	Pesquisa automatizada quando os incidentes são criados. Os resultados são exibidos na guia **Certificados SSL** do registro de incidente de segurança.
RISKIQ WHOISIQ API	• Domínio • URL	Pesquisa automatizada quando os incidentes são criados. Os resultados são exibidos na guia **Resultados de aprimoramento do observável** no registro de incidente de segurança.
RISKIQ WHOISIQ API	• Endereço de e-mail • Nome da organização	A pesquisa manual é executada na tabela Observáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observáveis e pesquisa compatíveis

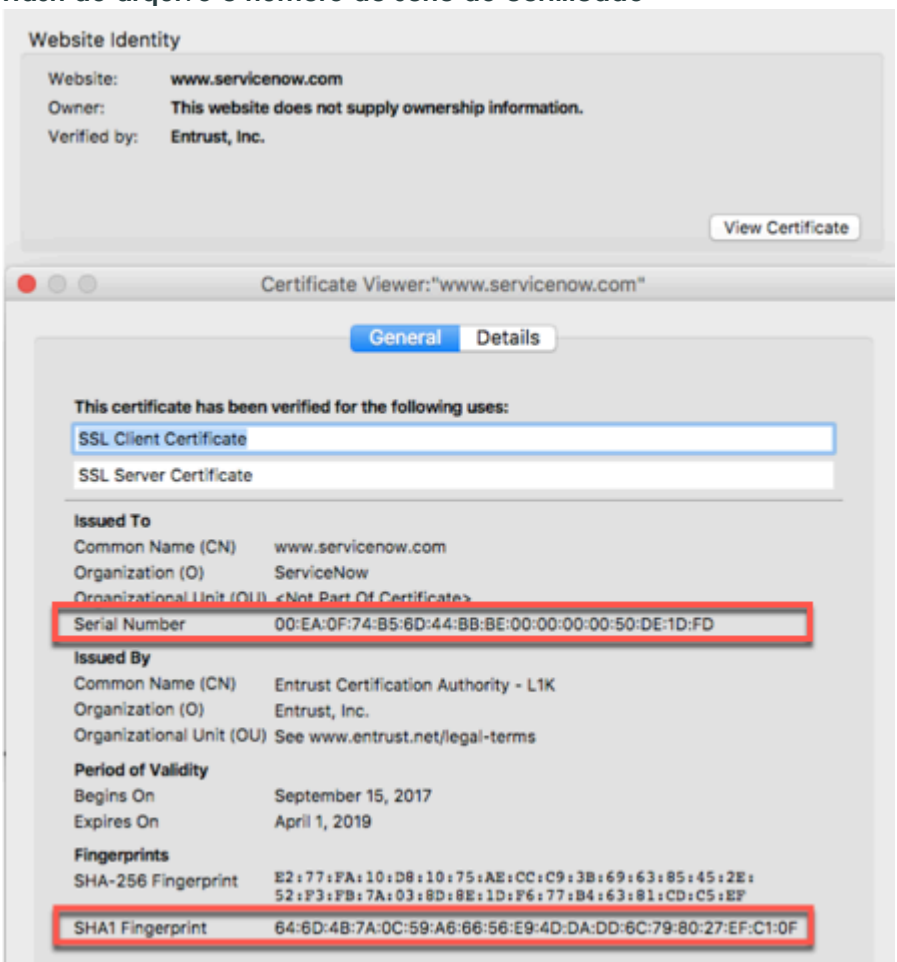
API	Observáveis compatíveis	Pesquisa (automatizada ou manual)
	• Número de telefone • Endereço para correspondência	Os resultados são exibidos na guia **Resultados** de aprimoramento do observável no registro do observável.

Exemplo de hash de arquivo e número de série de certificado

Esta figura mostra um exemplo dos observáveis de hash de arquivo e número de série de certificado usados para as pesquisas de certificado SSL para esta integração. O hash do arquivo se refere a uma impressão digital SHA-1. Este valor é exibido em sua instância Now Platform sem os dois pontos separadores. Por exemplo, `646D4B7A0C59A66656E94DDADD6C798027EFC10F`.

O observável número de série do certificado se refere ao ID exclusivo ou ao número de série da entidade. Este valor também é exibido sem os dois pontos separadores. Por exemplo, `00EA0F74B56D44BBBE0000000050DE1DFD`.

Hash do arquivo e número de série do certificado



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar RISKIQ e WHOISIQ

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que as aplicações RISKIQ e WHOISIQ se integrem corretamente a Now Platform Operações de segurança.

Antes de Iniciar

Função necessária: administrador, RISKIQ e WHOISIQ administrador.

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções necessárias.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o aplicativo e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Operações de segurança e atribui a função de Analista de incidentes de segurança (sn_si.analyst). • O Analista de incidentes de segurança (sn_si.analyst) trabalha com registros de incidentes de segurança.
Obtenha um nome de usuário e uma chave de API.	Visite o site para obter informações sobre a chave de API e como criar uma conta: site do RISKIQ . A configuração requer que você insira a chave de API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posterior Para a versão Madrid e as versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

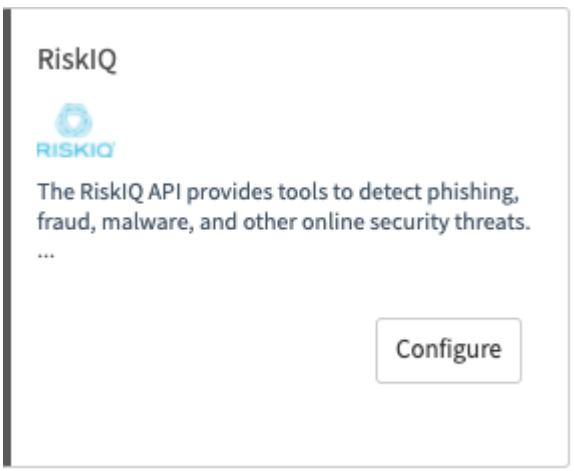
Configuração de tarefa	Descrição
	uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .

Procedimento

1. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.

2. Quando a instalação for concluída, navegue até **Operações de segurança** > **Integrações** > **Configurações de integrações** e localize o bloco da API.

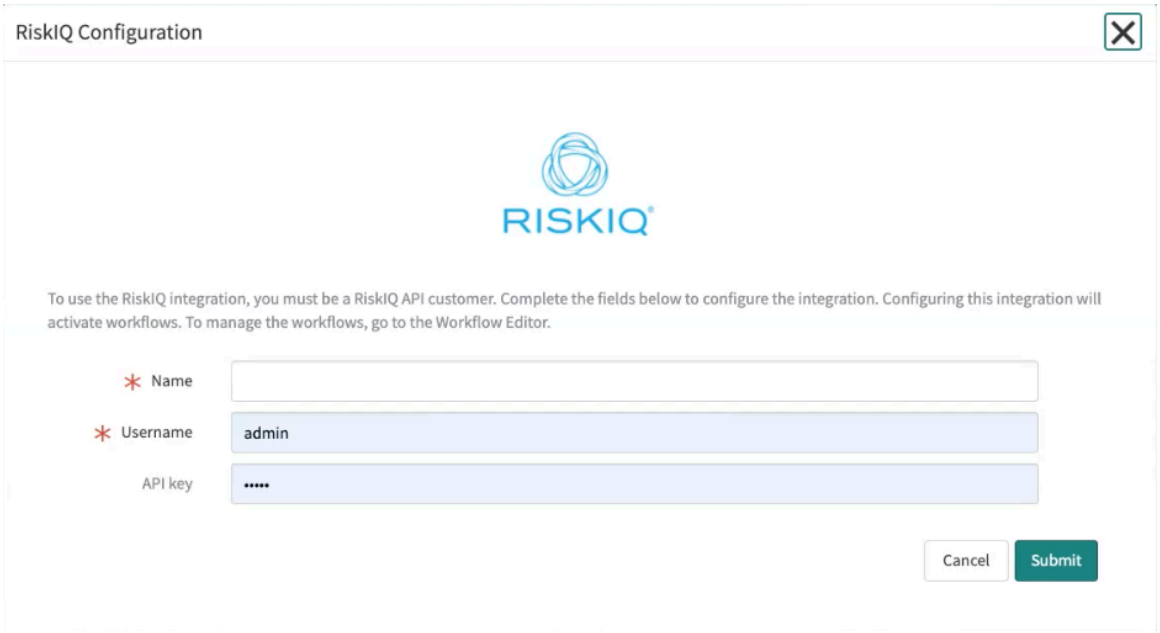
3. Clique em **Configurar**.



4. Na caixa de diálogo Configuração do RiskIQ exibida, insira o nome de **usuário** e **a chave de API**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
6. Verifique a configuração bem-sucedida.
   Quando a configuração for concluída com sucesso, a página Integrações de segurança com os blocos de integração será exibida.

Trouble?
Se uma mensagem de erro for exibida, o nome de usuário ou a chave de API podem ser inválidos. Verifique se o nome de usuário e a chave de API estão corretos:

Solução de problemas

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Verificar os resultados esperados para RISKIQ pesquisas de certificado SSL

Quando um incidente de segurança gera observáveis para URLs, domínios, endereços IP, hashes de arquivo de certificado (impressão digital SHA-1) e números de série de certificados, os analistas de incidentes de segurança usam os resultados da pesquisa de certificado SSL para verificar se os sites têm certificados que foram emitidos por um confiável autoridade de certificação (CA) pública.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Para observáveis compatíveis, o Now Platform verifica a ocorrência mais recente de URLs, domínios, endereços IP, hashes de arquivo de certificado (impressão digital SHA-1) e números de série de certificado. Estes são os resultados possíveis da verificação:

Foi encontrada uma correspondência exata

Um emissor válido de um certificado SSL é listado no registro de incidente de segurança.

Nenhum resultado de certificação encontrado

Nenhum resultado está listado no registro de Incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Foi encontrada uma correspondência exata para um certificado autoassinado ou gerado internamente

Os resultados de um certificado SSL gerado internamente são exibidos no registro de incidente de segurança.

Não foi encontrada uma correspondência exata para um certificado SSL primário

Um valor de pesquisa retorna várias entradas e um certificado primário não pode ser identificado. Uma mensagem de resumo é exibida no registro do Incidente de segurança.

Procedimento

1. Para exibir os observáveis e verificar os resultados da pesquisa, abra o registro de incidente de segurança com o qual você está trabalhando e localize as anotações de trabalho.

Example
Para ilustrar exemplos dos possíveis resultados de pesquisa para esta integração, suponha que um incidente de segurança tenha sido gerado com os seguintes observáveis:

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

Observáveis e local dos resultados da pesquisa

Observável (exemplo)	Resultados da varredura	Descrição e local
comunidade.servicenow.com	Certificado encontrado com um hash SHA1.	Uma correspondência exata foi encontrada e um emissor válido de um certificado SSL está listado. Os resultados da correspondência exata são exibidos na guia **Certificados SSL** no registro de incidente de segurança.
invalidsubdomain.servicenow.com	Nenhum certificado encontrado.	Um resumo que indica que nenhum resultado de certificado foi encontrado é exibido na guia **Resultados de aprimoramento do observável** no registro de incidente de segurança.
mail.dgnetworks.com	Certificado encontrado com hash SHA1.	Uma correspondência exata é listada para um certificado autoassinado ou gerado internamente. Os resultados são exibidos na guia **Certificados SSL** no registro de incidente de segurança.
servicenow.com	A pesquisa retornou 138 certificados e não foi	Não foi encontrada uma correspondência exata

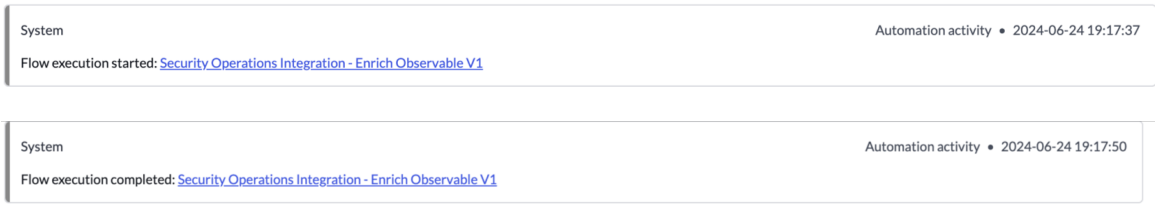
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observável (exemplo)	Resultados da varredura	Descrição e local
	possível identificar um único certificado primário.	para um certificado SSL primário, porque um valor de pesquisa retorna vários certificados. Um resumo que indica que nenhum certificado primário foi encontrado é exibido na guia **Resultados de aprimoramento do observável** no registro de incidente de segurança.

Depois que a aplicação é configurada, o fluxo é iniciado automaticamente. O status da pesquisa e os observáveis são exibidos nas anotações de trabalho.

2. Verifique se a pesquisa foi executada com sucesso.



Trouble?
Se você não puder exibir os resultados esperados, verifique se o observável é compatível com a pesquisa de certificado SSL para a integração.

Informações relacionadas

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

RISKIQ Pesquisas de certificado SSL que retornam uma correspondência exata

RISKIQ Os resultados da pesquisa de certificado SSL para uma correspondência exata são exibidos na guia **Certificados SSL** no registro de incidente de segurança. Uma correspondência exata fornece um nome de autoridade de certificação válido, o que ajuda um analista de incidentes de segurança a determinar a validade de um site.

Example: Correspondência exata para um certificado SSL válido

O exemplo a seguir mostra um emissor válido de um certificado SSL de uma correspondência exata nos resultados da pesquisa. Siga as etapas para exibir os resultados e os dados brutos.

Nota: As imagens nos exemplos a seguir são mostradas com a configuração **Formulários com guias** ativa nas Configurações do sistema. Se sua tela não corresponder à exibição mostrada abaixo, siga as etapas para definir formulários com guias.

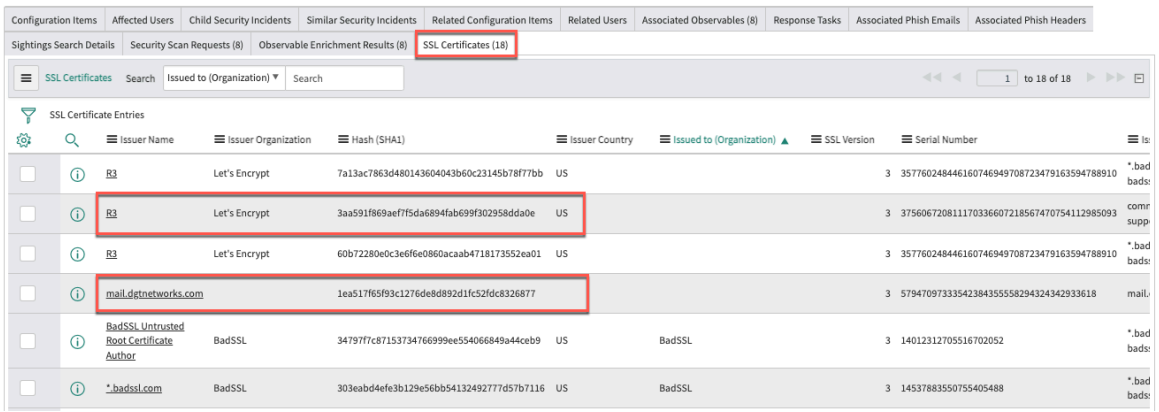
1. No canto superior direito da faixa superior, clique no ícone Configurações.
2. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se Formulários **com guias** e **Com o formulário** estão selecionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. No registro de incidente de segurança, clique na guia **Certificados SSL**.

Guia Certificados SSL



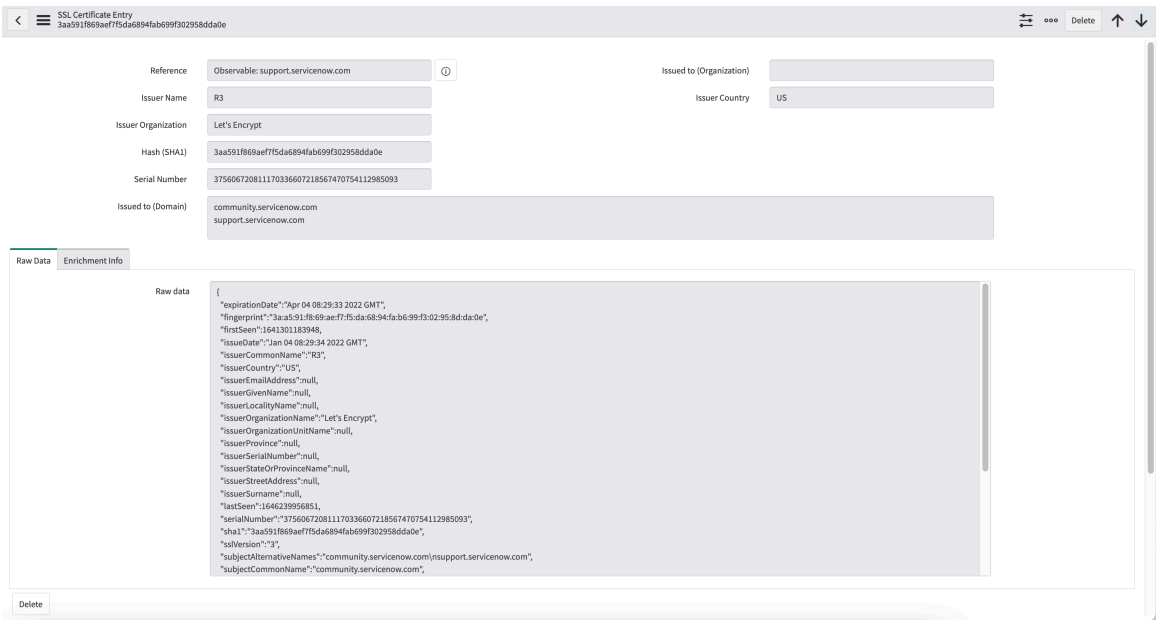
As informações sobre o nome do emissor do certificado, a organização do emissor e para quem o certificado foi emitido (Organização) são exibidas junto com outros dados.

18 itens são exibidos na coluna **Nome do emissor**. O segundo item (`R3`) fornece um nome de autoridade de certificação válido (`Let's Encrypt`) na coluna **Organização do emissor**.

Nenhuma informação nas colunas **Organização do emissor** e **Emitido para** é exibida para o segundo item (`mail.dgtnetworks.com`).

2. Clique no segundo item na coluna **Nome do emissor**, que é (**R3**) para abrir o registro de entrada. Como alternativa, clique no ícone de informações ao lado do item e, em seguida, em **Abrir registro**.
3. Selecione a guia **Dados brutos**.

Guia Dados brutos



O registro de entrada de certificado SSL inclui o observável na guia **Dados brutos** na coluna **Nome da entidade**, bem como outros dados.

Observe que na coluna **Categoria**, o `Assunto`e o `Emissor` correspondem a entidades reconhecíveis na coluna **Nome da entidade**. O emissor deste certificado provavelmente é válido e de uma autoridade de certificação pública confiável. Observe também que

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

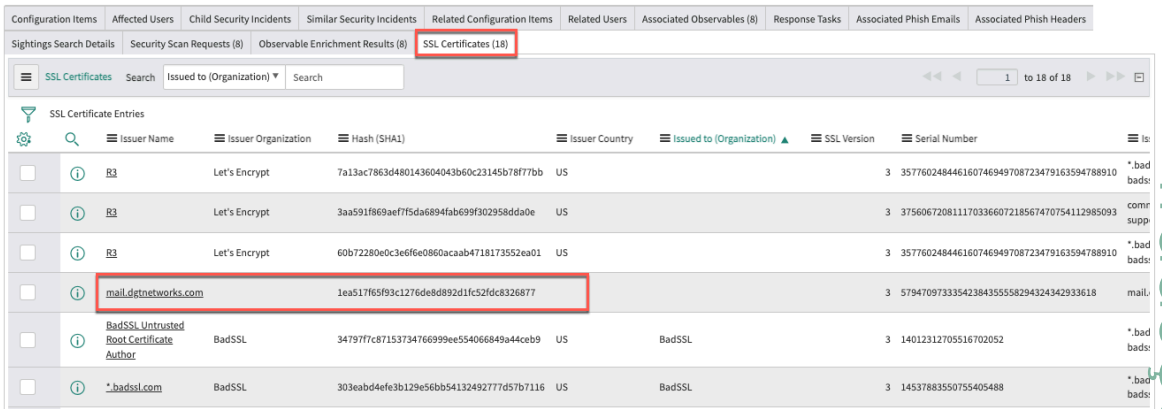
o `Assunto`e o `Emissor` são entidades diferentes. Essas entidades separadas indicam que o certificado não é um certificado assinado internamente de uma autoridade de certificação desconhecida.

Example: Correspondência exata para um certificado SSL autoassinado

O exemplo a seguir mostra os resultados de um certificado SSL autoassinado da pesquisa. Siga as etapas para exibir os resultados e os dados brutos.

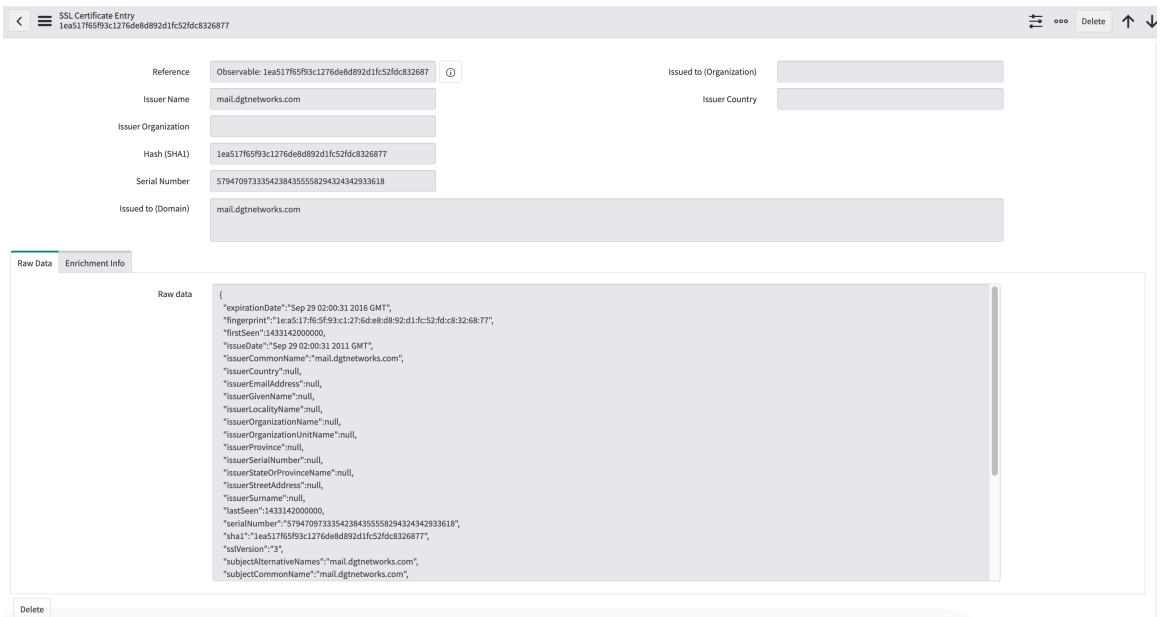
1. Navegue de volta para o registro do incidente de segurança. Na coluna **Nome do emissor**, clique no outro item (**mail.dgtnetworks.com**).

Guia Certificados SSL



2. No registro aberto, selecione a guia **Dados brutos**.

Guia Dados brutos



A coluna **Categoria** indica que o `Emissor` (`mail.dgtnetworks.com` e `dgtsbs.DGTNetworks.local`) não são autoridades de certificação públicas confiáveis. Observe também que o `Emissor` e o `Assunto` são a mesma entidade (`dgtsbs.DGTNetworks.local`) e cada um contém o nome do observável (`dgtsbs`). Este certificado é possivelmente um certificado autoassinado. Certificados autoassinados podem justificar uma investigação mais aprofundada, pois esses certificados não são emitidos por uma autoridade de certificação conhecida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

RISKIQ Pesquisas de certificado SSL que retornam vários certificados ou nenhum certificado

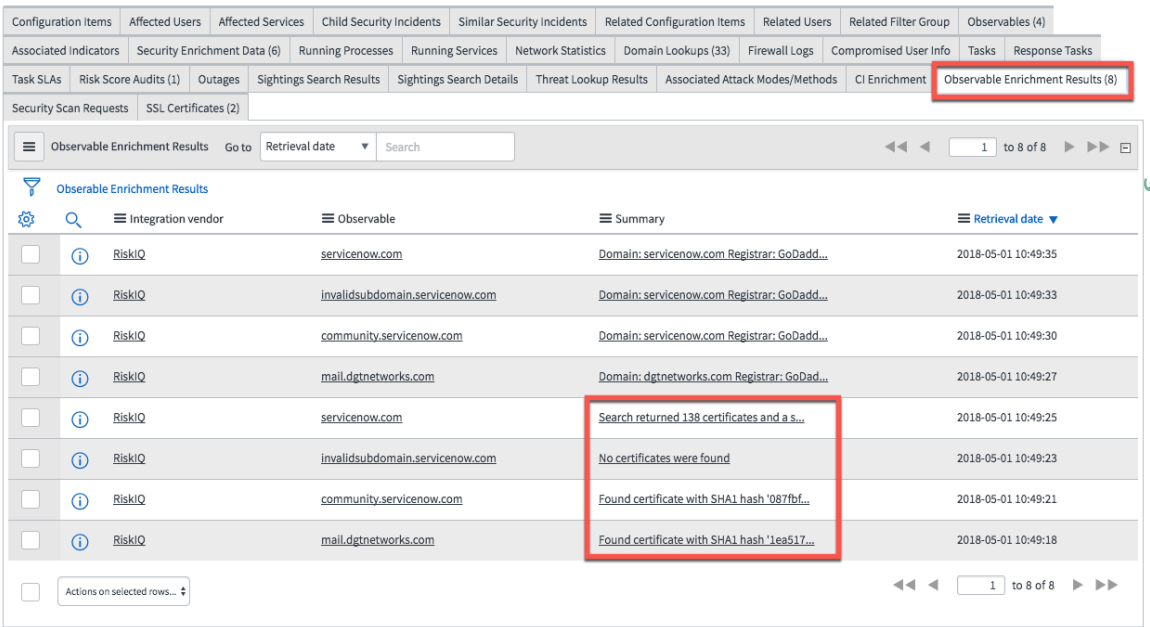
Um analista de incidentes de segurança pode usar vários resultados de certificado SSL para determinar se um site faz parte de uma entidade comum e reconhecível. Nenhum resultado de certificado SSL pode indicar que sites com nomes obscuros ou suspeitos não têm certificados confiáveis. Os resultados da pesquisa de observáveis que não retornam certificados SSL ou que retornam vários certificados SSL são exibidos na guia Resultados de aprimoramento do observável no registro de incidente de segurança.

Example: Nenhum resultado de certificado SSL ou vários resultados de certificado SSL

Siga as etapas para exibir os resultados de observáveis que não retornam certificados SSL ou que retornam vários certificados.

1. No registro de incidente de segurança, clique na guia **Resultados de aprimoramento do observável**.

Guia Resultados de aprimoramento do observável



Os resultados de aprimoramento do observável para a pesquisa RISKIQ e WHOISIQ são exibidos.

Na coluna **Observável**, `servicenow.com` corresponde à mensagem A `pesquisa retornou 138 certificados` na coluna **Resumo**. Da mesma forma, `invalidsubdomain.servicenow.com` corresponde a `Nenhum certificado encontrado` na coluna **Resumo**. Esses resumos indicam que vários certificados SSL foram encontrados e que nenhuma correspondência exata para certificados SSL foi encontrada, respectivamente.

2. Na coluna **Observável**, clique em **servicenow.com**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vários certificados SSL

A mensagem de resumo exibida no registro indica que vários resultados de certificados SSL foram retornados para `servicenow.com`e não foi possível corresponder a um certificado SSL primário. Essa mensagem geralmente é retornada em pesquisas que incluem nomes de domínio comuns, como `servicenow.com`.

Se você precisar de mais informações sobre um domínio comum, poderá executar a pesquisa diretamente com a API RISKIQ.

3. Navegue de volta para a guia **Resultados** de aprimoramento do observável e, na coluna **Observável**, clique em **invalidsubdomain.servicenow.com**.

Sem certificados SSL

Nota:

- Se nenhum certificado SSL for encontrado para o observável atual, o campo Resumo exibirá a mensagem `Nenhum certificado encontrado`.
- Se nenhum certificado SSL ativo for encontrado para o observável atual, o campo Resumo exibirá a mensagem `Nenhum certificado ativo encontrado`.

Verificar resultados esperados para WHOISIQ pesquisas de URL

Quando um incidente de segurança gera observáveis para URLs ou domínios, a API WHOISIQ executa o aprimoramento do observável automaticamente após a criação do incidente de segurança. Os resultados da pesquisa são exibidos nas guias **Resultados de aprimoramento do observável** e **Certificados SSL** no registro de incidente de segurança.

Antes de Iniciar

Nota: As imagens nas etapas a seguir são mostradas com a configuração **Formulários com guias** ativa nas Configurações do sistema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

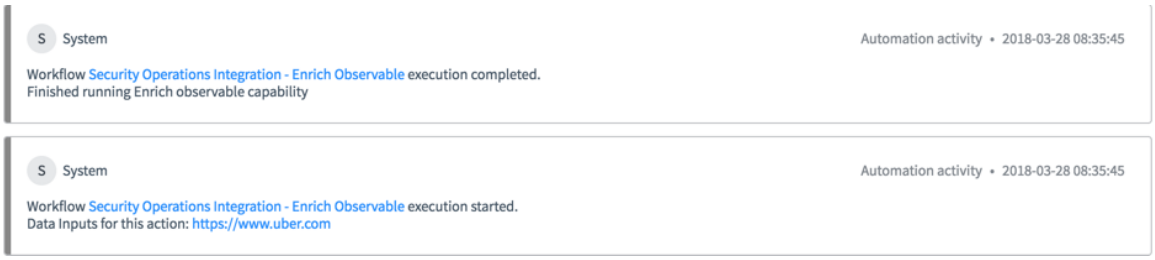
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os resultados de aprimoramento do observável são exibidos na guia **Resultados** de aprimoramento do observável na parte inferior do registro de incidente de segurança. Para observáveis compatíveis, uma pesquisa de certificado SSL também é executada e os resultados são exibidos na **guia Certificados SSL**.

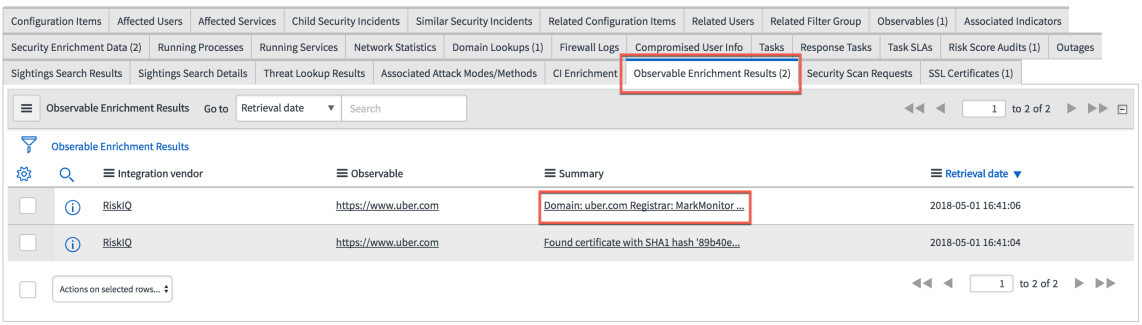
Procedimento

1. Abra o registro de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso nas anotações de trabalho.



   Depois que a aplicação é configurada, o fluxo é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no registro de Incidente de segurança.

2. Se você não puder verificar se a pesquisa foi executada com sucesso, revise as anotações de trabalho para obter mais informações sobre como prosseguir.
3. No incidente de segurança em aberto, clique no link relacionado **Mostrar todas as listas** relacionadas.
4. Clique na guia **Resultados de aprimoramento do observável** para selecioná-la.
5. Na coluna **Resumo**, clique no primeiro item, **Domínio: uber.com Registrador: Markmonitor...**.



   O registro exibido contém informações sobre o domínio.

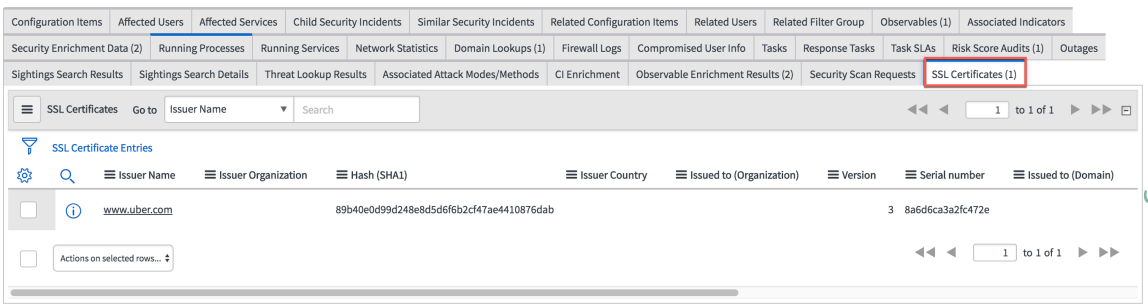
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Navegue de volta para a guia **Resultados de aprimoramento do observável** e, na coluna **Resumo**, clique no segundo item, **Certificado encontrado com hash SHA1...**.

Este registro indica que um certificado SSL foi encontrado com um hash de arquivo.

7. Navegue de volta para o registro do incidente de segurança e clique na guia **Certificados SSL**.



Os resultados do certificado SSL para o hash do arquivo também são exibidos aqui.

Trouble?
Se você não puder exibir os resultados esperados, revise as anotações de trabalho. Além disso, verifique se o observável é compatível com a pesquisa pela integração.

Informações relacionadas

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

Criar um observável para pesquisas manuais WHOISIQ

Os analistas de incidentes de segurança usam informações do enriquecimento observável com a API WHOISIQ para saber mais sobre endereços de e-mail, nomes e números de telefone das organizações.

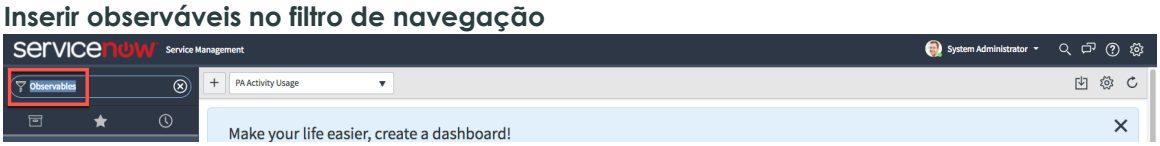
Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Repositório LOC** > **Observáveis**.

Inserir observáveis no filtro de navegação

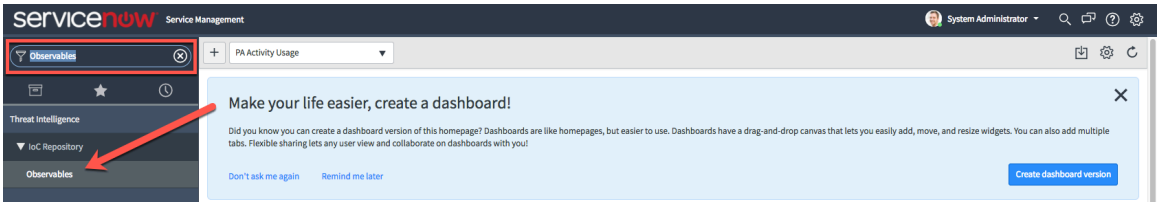


No painel de navegação, o módulo Observáveis é exibido.

Tradução automática

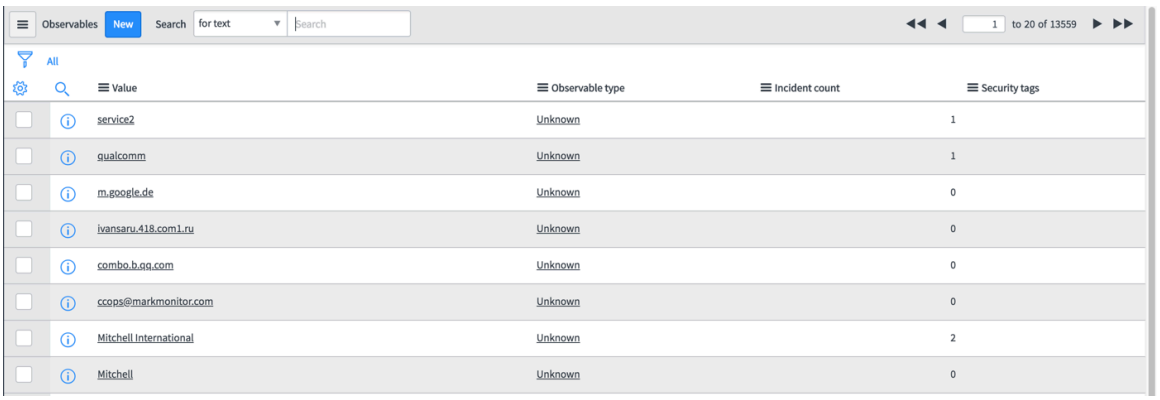
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo de observáveis



2. Clique no módulo **Observáveis** para exibir a lista de Observáveis.

Lista de observáveis

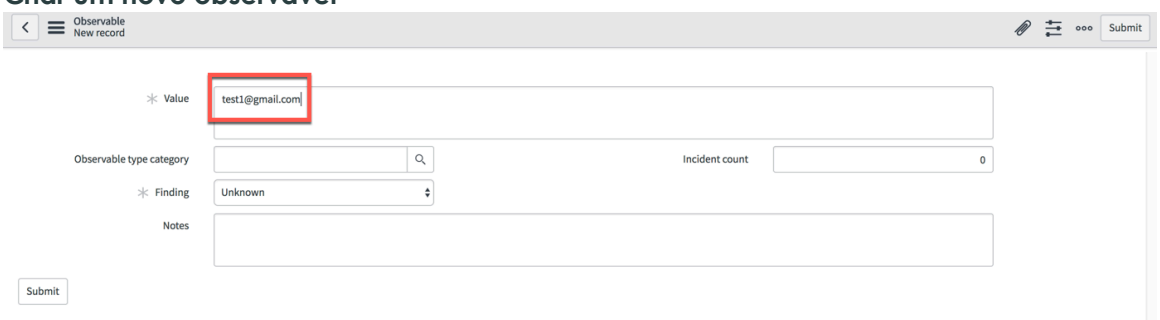


3. Clique em **Novo** para criar um novo observável.

4. No formulário Observável, preencha os campos.

Campo	Descrição
Valor	Endereço de e-mail, nome da organização, número de telefone ou endereço para correspondência. Por exemplo, `test1G-mail.com`
Tipo de observável	O campo é limpo automaticamente.
Descoberta	O campo é definido automaticamente como **Desconhecido**.

Criar um novo observável



5. Clique em **Enviar**.
Você retorna à lista de Observáveis. Na coluna **Valor**, seu novo observável é exibido.

Nota: Se você não conseguir localizar seu observável na parte da lista exibida, use a funcionalidade de pesquisa para localizá-lo.

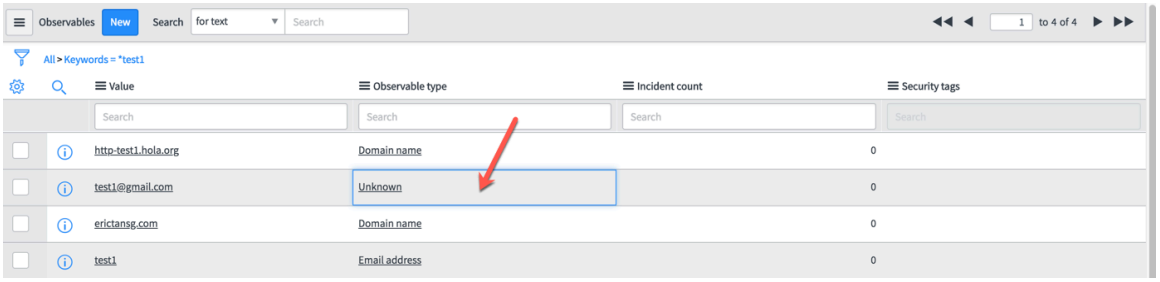
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Edite o campo **Tipo de observável** para mudar o tipo de **Desconhecido** para Endereço de **e-mail** para corresponder ao seu observável.

   a. Na coluna **Tipo de observável**, clique uma vez à direita do texto **Desconhecido** para selecioná-lo.

Selecione o campo Tipo de observável

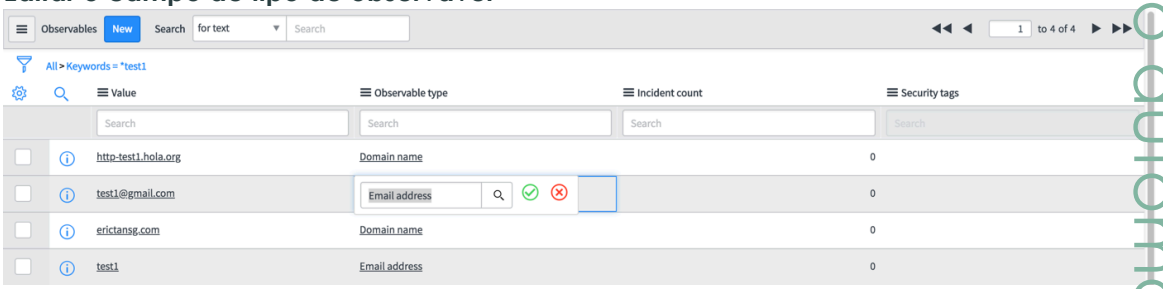


   O campo selecionado é contornado em azul.

   b. Com o campo contornado em azul, clique duas vezes em qualquer lugar dentro do campo realçado para abrir o editor.

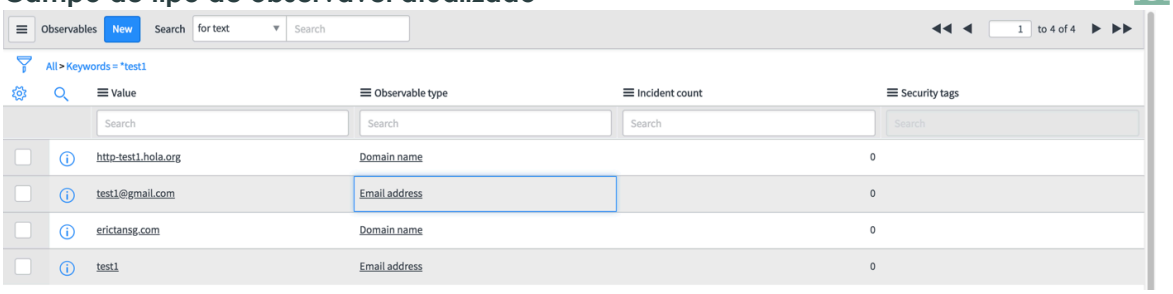
   c. No campo exibido, insira o tipo de observável (Endereço de e-mail) e clique na marca de seleção verde para salvar o valor.

Editar o campo de tipo de observável



   Na coluna **Tipo de observável** na lista, `Endereço` de e-mail é exibido para o novo observável.

Campo de tipo de observável atualizado



O que Fazer Depois

Se você tiver criado e editado um observável para pesquisa, execute a pesquisa de aprimoramento do observável a partir do registro do observável com a API WHOISIQ.

Verificar os resultados esperados para pesquisas manuais WHOISIQ

Execute uma pesquisa manual em um observável quando ele não gerar automaticamente um incidente de segurança. Para pesquisas de aprimoramento de observáveis usando a

Tradução automática

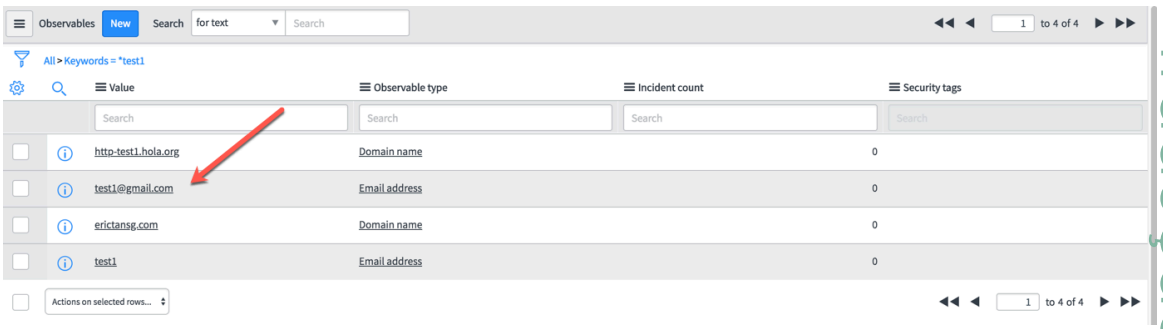
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

API WHOISIQ para endereços de e-mail, nomes de organizações, números de telefone ou endereços de correspondência, inicie a pesquisa manualmente na tabela Observáveis.

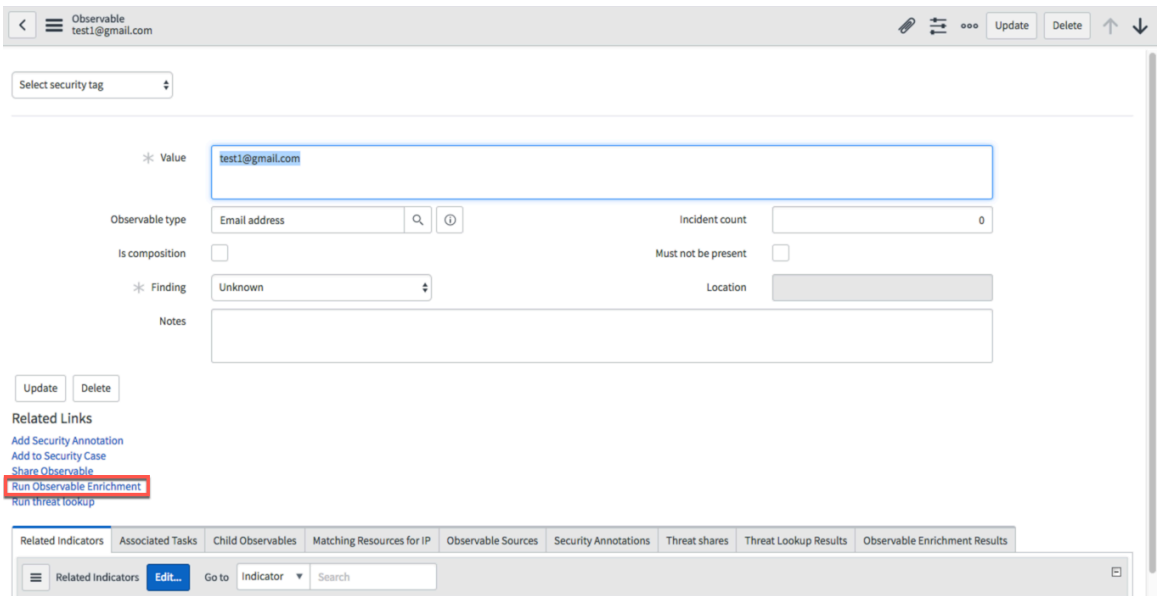
Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Crie um observável para uma pesquisa manual usando a API WHOISIQ. Para obter mais informações sobre como criar e editar um observável, consulte Criar um observável para pesquisas manuais WHOISIQ.

Procedimento
1. Navegar até **Todos** > **Repositório LOC** > **Observáveis** e localize o observável na lista com a qual você está trabalhando.
2. Clique no observável na coluna **Valor** para abrir o registro.



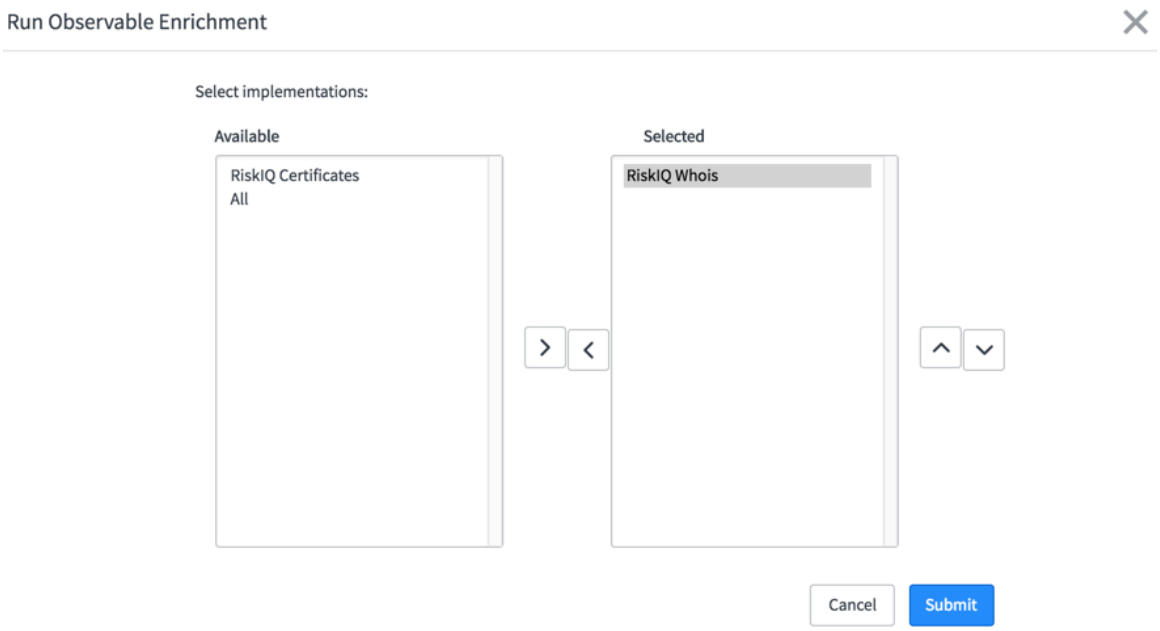
3. Clique no link relacionado **Executar aprimoramento de observável** para executar a pesquisa.



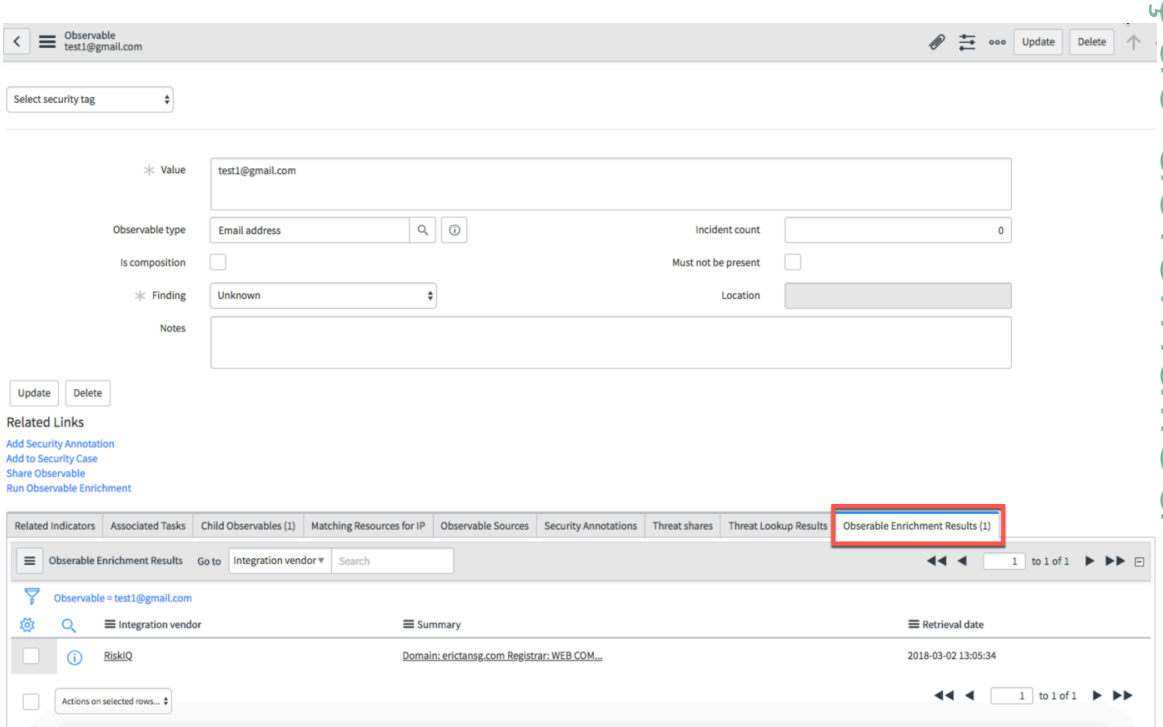
4. Na janela **Executar aprimoramento de observável**, mova **RiskIQ Whois** para a lista Selecionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   Os resultados da pesquisa são exibidos na guia **Resultados** de aprimoramento do observável no registro do observável.



Trouble?
Se nenhum resultado for retornado para o observável, uma mensagem será exibida na coluna **Resumo**. Se você não vir resultados, verifique se o observável é compatível com a API.

Informações relacionadas

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de Shodan

Shodan é um mecanismo de pesquisa que analisa informações da faixa de serviço de dispositivos conectados em todo o mundo. As faixas de serviço incluem informações sobre um sistema de computador, como nome do host, tipo de dispositivo, sistema operacional, localização geográfica e ISP conectado. Quando integradas ao produto Now Platform Operações de segurança, essas informações da faixa de serviço fornecem aos analistas dados de enriquecimento adicionais e informações para incidentes ou investigações de segurança.

A integração requer os plug-ins Security Incident Response e Inteligência contra ameaças.

A integração Shodan executa o enriquecimento nos seguintes observáveis:

- Endereços IP
- URLs

A aplicação verifica se há novos observáveis a cada cinco minutos. Se os observáveis forem de um tipo reconhecido pela integração Shodan, os observáveis serão aprimorados.

Instalar e configurar Shodan

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que a aplicação Shodan se integre corretamente a Now Platform Operações de segurança.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Tarefas de configuração	Descrição
Verifique se você atribuiu as funções Now Platform necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o aplicativo e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Operações de segurança.
Obtenha a chave de API Shodan.	Crie uma conta e obtenha a chave de API do site Shodan : site do Shodan .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Madrid e as versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident

Tradução automática

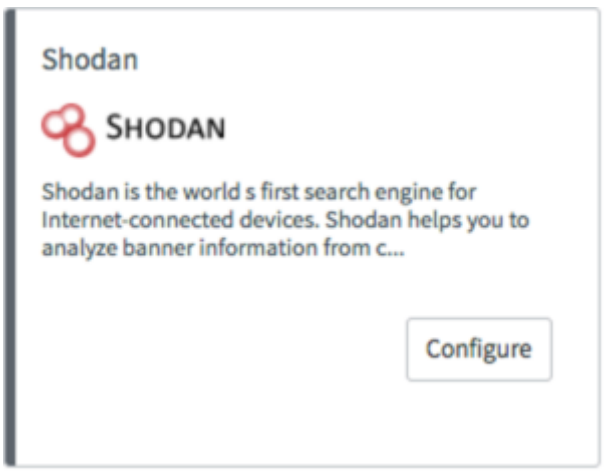
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Resposta a incidentes de segurança **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte e .

Função necessária: administrador

Procedimento

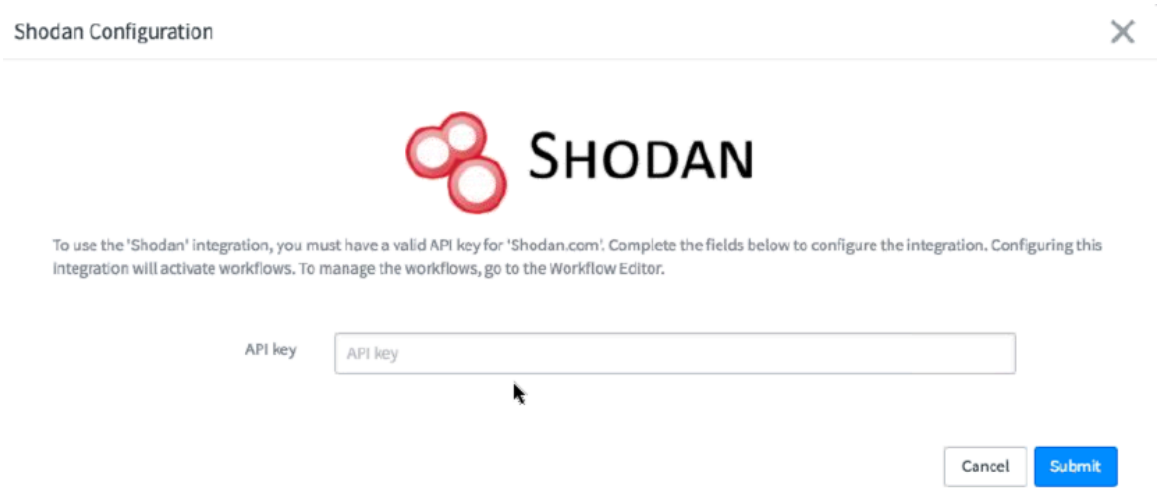
1. Se você não instalou a aplicação para a integração, consulte e siga as etapas para instalá-la.
2. Depois que a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Shodan.



3. Clique em **Configurar**.
4. Na caixa de diálogo **Configuração do Shodan**, insira a chave de API que você obteve no site Shodan e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, a chave de API Shodan pode ser inválida.

Verificar resultados esperados para Shodan

Os observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Os resultados de aprimoramento são exibidos nas guias **Resultados de aprimoramento do observável** e **Faixas de rede**.

Antes de Iniciar

Função necessária: sn_si.analyst.

Procedimento

1. Abra o incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

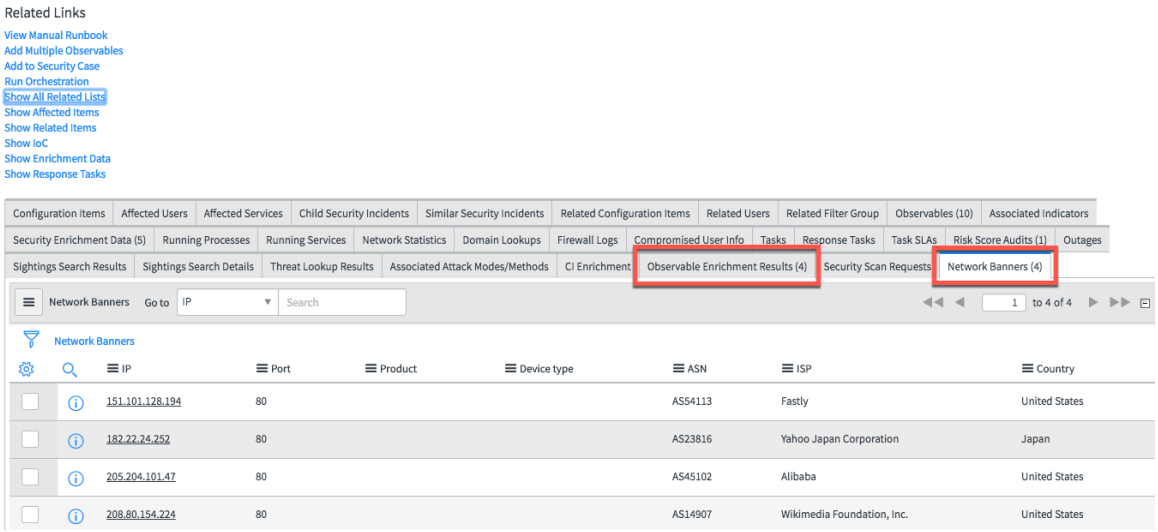
   Depois que a aplicação é configurada, o fluxo de trabalho é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.
3. Navegue até a parte inferior do incidente de segurança e clique no link **Mostrar todas as listas** relacionadas em **Links relacionados**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As imagens nas etapas a seguir são mostradas com a configuração **Formulários com guias** ativa nas Configurações do sistema. Se os formulários com guias não forem exibidos, no canto superior direito da faixa superior, clique no ícone de engrenagem Configurações. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se Formulários **com guias** e **Com o formulário** estão selecionados.



Os resultados são exibidos nas guias **Resultados de aprimoramento do observável** e **Faixas de rede** na parte inferior do incidente de segurança.

4. Com a guia **Faixas de rede** selecionada, clique no ícone de informações azul ao lado de um observável.

5. Na caixa de diálogo exibida, clique em **Abrir registro** para exibir os dados brutos e mais detalhes.

Trouble?
Se você não vir os resultados nas guias **Resultados de aprimoramento do observável** e **Faixas de rede**, verifique se o observável é de um tipo compatível com a pesquisa pela integração.

(Opcional) Anexar manualmente um observável para Shodan

Você pode anexar observáveis manualmente a um incidente de segurança. Você anexa observáveis manualmente quando deseja executar pesquisas de ameaças em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

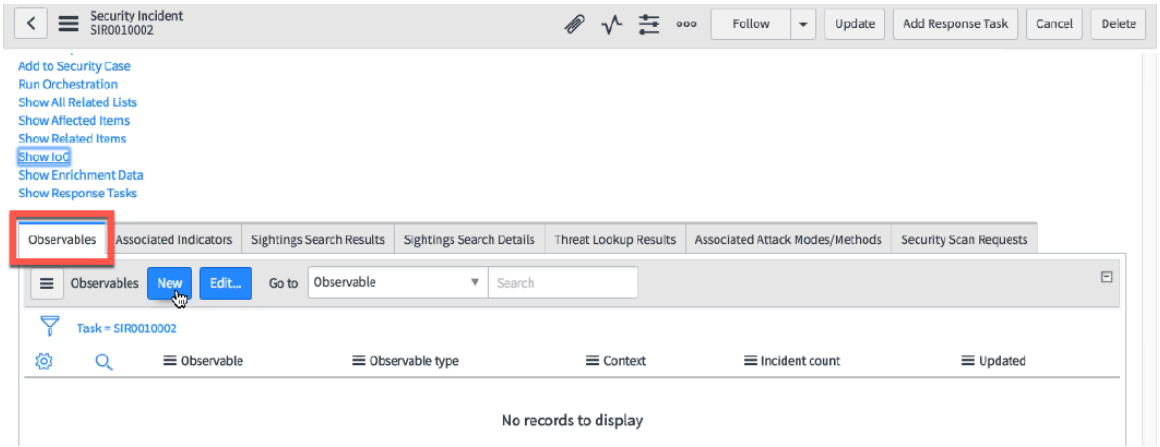
Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

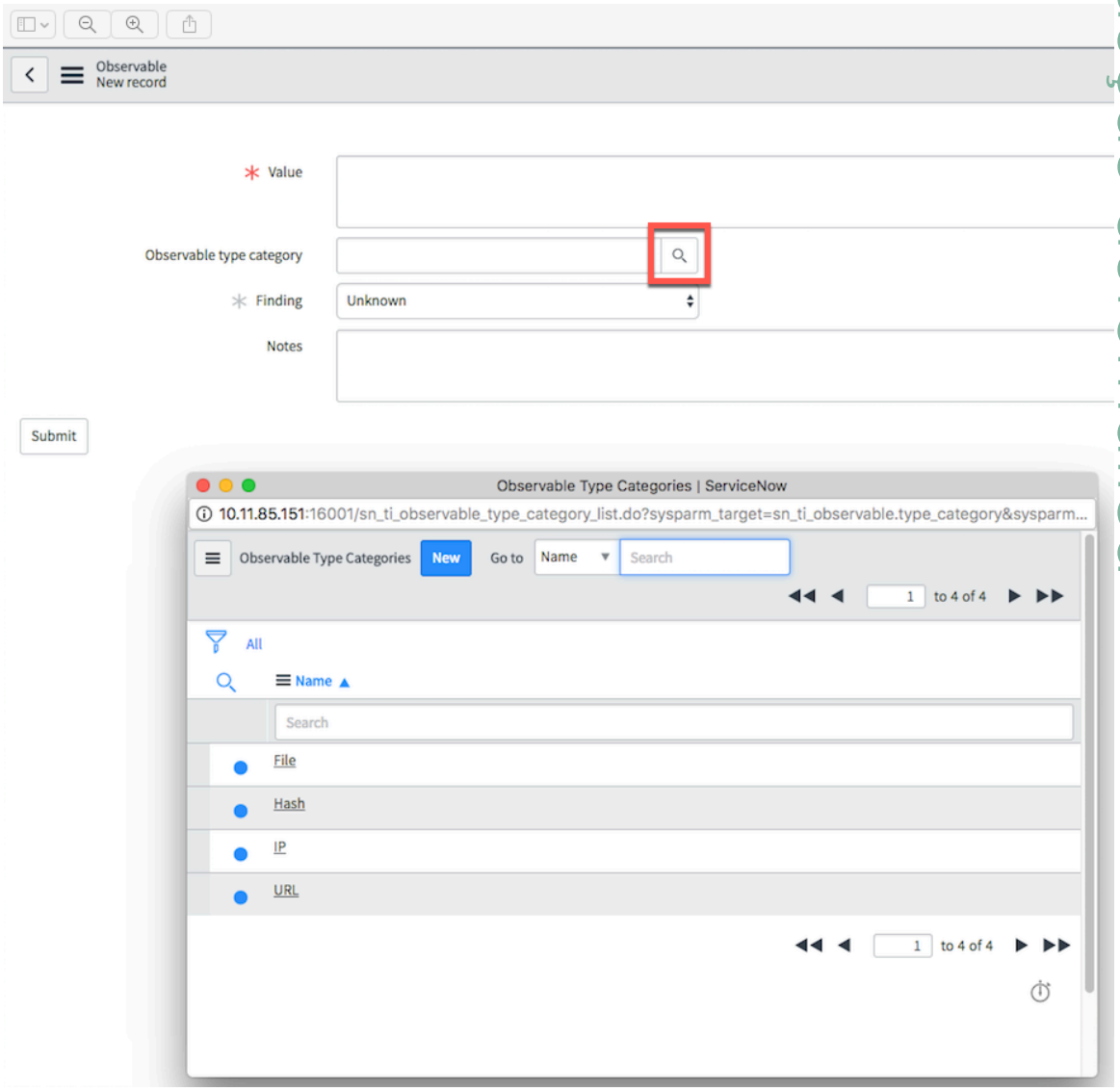
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes** e abra um incidente de segurança ao qual você deseja anexar o observável.
2. Na parte inferior do registro, clique no link **Mostrar IoC**em **Links relacionados**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na guia **Observáveis**, clique em **Novo**.
   O formulário Observável é exibido.
4. No campo **Valor**, insira um observável (endereço IP ou URL).
5. Clique no ícone de pesquisa e, na caixa de diálogo **Categorias de tipo de observável**, clique no tipo de observável desejado na lista para preencher o campo.

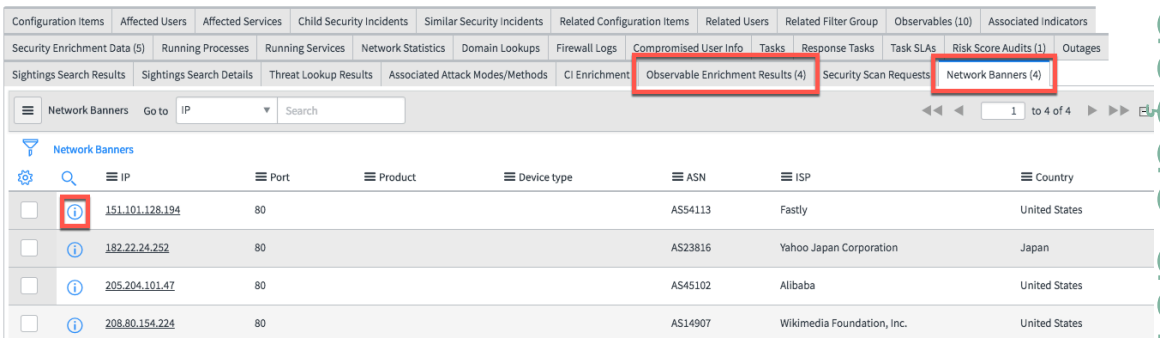


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   O fluxo de trabalho é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção de anotações de trabalho no registro de incidente de segurança.
7. Navegue até o seu incidente de segurança e revise as anotações de trabalho.

8. Na parte inferior do registro, clique no link relacionado **Mostrar todas as listas** relacionadas.
9. Clique nas guias **Resultados de aprimoramento do observável** ou **Faixas de rede** para obter os resultados e clique no ícone de informações azul ao lado de um observável para obter mais informações sobre um item específico.



10. Na caixa de diálogo exibida, clique em **Abrir registro** para exibir os dados brutos e mais detalhes.
11. Opcional: Clique no ícone de configurações azul próximo ao ícone de pesquisa para personalizar a saída e a ordem das colunas.
12. Em **Personalizar colunas de lista**, selecione as configurações disponíveis, mova-as para a coluna **Selecionada** e clique em **OK**.

Trouble?
Revise as **Anotações de trabalho** para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

Secureworks CTP Integração de ingestão de tíquete

A integração de ingestão de Secureworks Counter Threat Platform tíquete permite que você busque automaticamente Secureworks CTP tíquetes, converta-os em incidentes de segurança e execute ações de resposta automatizadas.

Os principais recursos desta integração incluem:

- Ingestão automática de tíquetes selecionados (incluindo anexos) com base em uma programação predefinida.
- Mapeamento de campos de tíquete e evento para campos Security Incident Response.
- Visualização de incidentes de segurança mapeados para os campos de tíquete.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Filtragem e agregação de tíquetes.
- Recuperação sob demanda de eventos associados a um tíquete.
- Acompanhamento periódico das principais atualizações dos tíquetes.
- Automatização de atualizações e fechamentos de tíquetes com base no status do incidente SIR
- Atualização do tíquete mestre.
- Sincronização de logs de trabalho do Secureworks com Security Incident Response anotações de trabalho.

Configure sua instância [Now Platform para a integração de ingestão de tíquetes Secureworks CTP

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform antes de instalar a aplicação a partir do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para a instalação, configuração e uso da integração em sua instância Now Platform. • Um usuário com a função de administrador Now Platform (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador SIR (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform: ◦ Nomeia, cria e edita perfis. ◦ Seleciona e mapeia Secureworks CTP campos de tíquete para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão contínua de tíquetes. ◦ Habilita atualizações de tíquete quando um incidente SIR SIR é criado e encerrado. ◦ Atribui a função de analista de incidentes de segurança (sn_si.analyst). ◦ Usuários com sn_si.analyst trabalham com incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre funções e como atribuir funções a usuários, consulte Gestão de funções
Verifique se você está usando as seguintes versões: • API de tíquete do Secureworks 4.0 • API de eventos do Secureworks 1.0 • API de aprimoramento do Secureworks 1.0	Se você tiver acesso ao portal Secureworks CTP, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Ingestão de eventos e alertas para Operações de segurança (necessário para integrações de SIEM): esta aplicação requer: ◦ com.glide.hub.integration.runtime => Tempo de execução do IntegrationHub da ServiceNow ◦ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in Event and Alert Ingestion. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de tíquete do Secureworks CTP

Antes de executar a integração em sua instância Now Platform, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Operações de segurança em sua instância Now Platform.

Antes de Iniciar

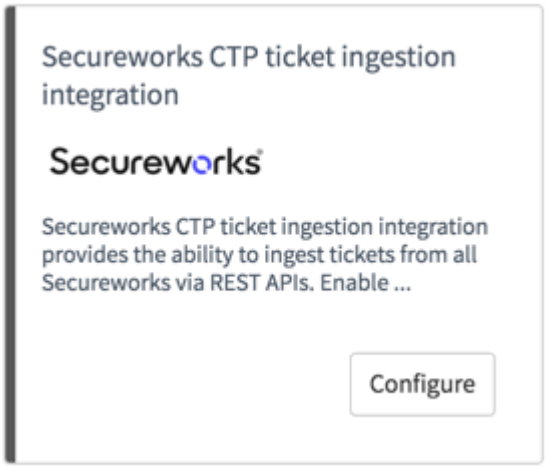
Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não instalou a aplicação de tíquete [Secureworks CTP de ServiceNow Store para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Secureworks CTP de integração de ingestão de tíquete.



3. Para configurar a aplicação, clique em **Novo**.
4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo exibida, preencha os campos.

Campo	Descrição
Nome	Nome da instância Secureworks CTP usada para a integração. Você pode inserir somente valores alfanuméricos e hifens (-) neste campo.
Descrição	Insira uma descrição para a conta do usuário.
Nome de usuário	Insira o nome de usuário da conta da API Secureworks CTP. Observe que o nome de usuário faz distinção entre maiúsculas e minúsculas. Para encontrar o nome de usuário, siga estas etapas: ◦ Faça login no portal Secureworks CTP. ◦ Navegar até **Conta** > **Gestão de contas** > **Credenciais de API**. O nome de usuário é exibido na página Credencial da API.
Senha da API	Insira a Secureworks CTP senha de API. Para encontrar a senha da API, siga estas etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Faça login no portal Secureworks CTP. ◦ Navegar até **Conta** > **Gestão de contas** > **Credenciais de API**. A senha da API é exibida na página Credencial da API. Para obter mais informações sobre como obter o nome de usuário e a senha da API, siga as etapas na seção Geração de uma chave de API persistente do Guia de API de registro de tíquete do Secureworks.

6. Clique em **Enviar**.
   Depois de validadas e enviadas com sucesso, cada configuração é salva na página Integrações de segurança como um bloco.

Resultados
Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança. No canto superior direito da página, na lista de seleção **Mostrar configurações**, clique em **Sim**.

Criar um perfil para integração de ingestão de tíquete do Secureworks CTP

Crie um perfil em sua instância Now Platform e determine quais tíquetes precisam ser ingeridos e quais serão usados para criar incidentes de segurança. Antes que os incidentes de segurança sejam criados a partir de tíquetes ingeridos, os valores de campo dos tíquetes são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será exibido.

A integração permite ingerir tíquetes com base nos perfis que você configura no ambiente Operações de segurança da sua instância. Todos os tíquetes são ingeridos inicialmente para um tipo de tíquete configurado em um perfil. Os tíquetes ingeridos podem ser filtrados para especificar quais tíquetes criam incidentes de segurança.

Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para tíquetes identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de tíquetes ingeridos, os valores de campos individuais nos tíquetes são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização.

Identificar a origem do perfil

Especifique o nome e a origem do perfil.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para um tíquete em sua instância Now Platform, navegue até **Integração de ingestão de tíquete do Secureworks** > **Perfis do Secureworks**.
2. Clique em **Nova**.
3. Preencha os campos.

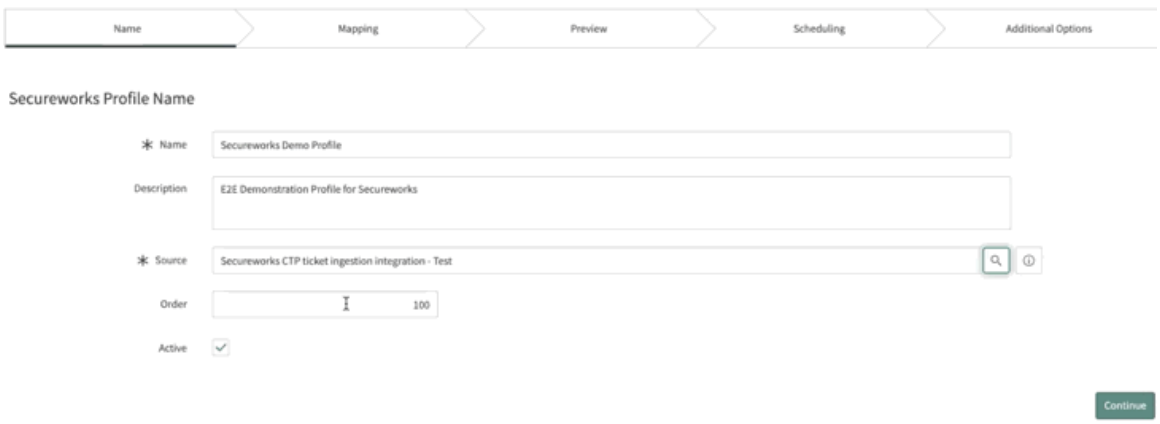
   Um exemplo de um formulário preenchido segue a tabela.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e nomes de perfil duplicados não serão salvos. Os nomes de perfil em sua instância Now Platform devem ser exclusivos.
Origem	Selecione a origem de onde você deseja ingerir os dados.
Ordem	O padrão é 100. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem as mesmas condições de acionamento. Quanto menor o valor do pedido, maior será a prioridade.
Ativo	Esta opção está desmarcada por padrão. Se esta opção estiver desabilitada, o perfil não estará ativo. **Nota:** Você deve concluir todas as seções no perfil antes de torná-lo ativo.

A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

Mapeie os campos de tíquete.

Mapeamento de campos de tíquete para a integração do SecureWorks CTP

Mapeie os campos de tíquete e evento para os campos no formulário de incidente de segurança.

Para a etapa de mapeamento, você deve primeiro ingerir tíquetes de amostra e, em seguida, garantir que todos os campos de tíquete relevantes estejam mapeados para o local apropriado no formulário Security Incident Response e, em seguida, visualizar o incidente de segurança na seção de visualização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O mapeamento dos campos de tíquete de amostra envolve o seguinte:

- Buscando e preenchendo os dados de amostra: consulte Ingestão de tíquetes do Secureworks de amostra
- Mapeamento dos campos de tíquete para o incidente de segurança: consulte Mapeamento de campos de tíquete do Secureworks para campos de resposta a incidentes de segurança

Ingestão de tíquetes do Secureworks de amostra

Selecione os tíquetes de amostra que serão ingeridos.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair os cinco tíquetes de amostra mais recentes ou fornecer os IDs de tíquete exclusivos para os tíquetes específicos que deseja usar para sua experiência de mapeamento.
   Na lista de seleção **Preferência de ingestão**, selecione uma das seguintes opções:
   - Recuperar tíquetes mais recentes: os 5 tíquetes mais recentes são recuperados.
   - Selecionar tíquetes com base no ID do tíquete: especifique o ID do tíquete a ser recuperado. Você pode especificar no máximo 5 IDs de tíquete separadas por vírgulas.
3. Clique em **Buscar dados de amostra** para extrair os dados de tíquete de amostra mais recentes do servidor Secureworks CTP.
   A extração de tíquetes de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela. Os tíquetes recuperados são exibidos como guias individuais. Clique em uma guia para exibir os dados do tíquete. Para cada tíquete, você pode ver os campos de tíquete e seus valores e detalhes do evento de contribuição que acionou o tíquete.

   Nota: Você verá os detalhes dos eventos de contribuição somente se eles tiverem ocorrido nos últimos 7 dias. Eventos com mais de 7 dias não são exibidos.

O que Fazer Depois

Depois de obter os dados de amostra, a próxima etapa é mapear os campos de tíquete para o incidente de segurança.

Mapeamento de campos de tíquete do Secureworks para campos de resposta a incidentes de segurança

Mapeie campos de evento ou tíquete individual para campos em um incidente de segurança Now Platform SIR.

Mapeamento de campo de tíquete

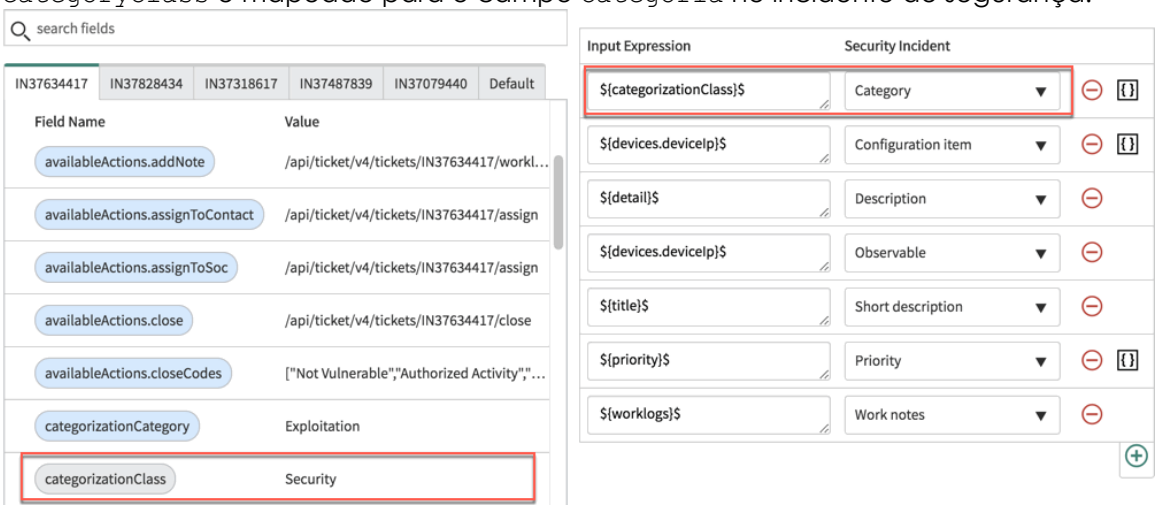
Como um usuário com a função sn_si.admin, use os campos da seção Tíquetes de amostra à esquerda e mapeie-os para os campos de incidente de segurança na coluna **Mapeamento de campo de incidente do SIR**. Edite a configuração de mapeamento arrastando os campos de tíquete ou evento do lado esquerdo e soltando-os na seção Mapeamento de campo de incidente de SIR à direita. O mapeamento à direita associa o campo de tíquete de entrada a um campo de incidente de segurança de saída.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
2. Você pode inserir manualmente o nome do campo na coluna Expressão de entrada ou arrastar e soltar o nome do campo. Por exemplo, `descrição`e solte-o em um campo na coluna **Expressão de entrada** ao lado de um nome de campo na coluna **Incidente de segurança**.

   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, `categoryClass` é mapeado para o campo `Categoria` no incidente de segurança.



   Nota: Se você inserir o nome do campo de evento manualmente na seção **Expressão de entrada**, deverá adicionar um prefixo como *`${Event:eventfield}$`* antes do nome do campo que está sendo mapeado.

   Para garantir que nenhum campo de tíquete ou evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação de cores dos campos de tíquete ajuda a rastrear os valores de tíquete que você já mapeou à medida que eles se tornam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de tíquete importante restante permanece não mapeada.

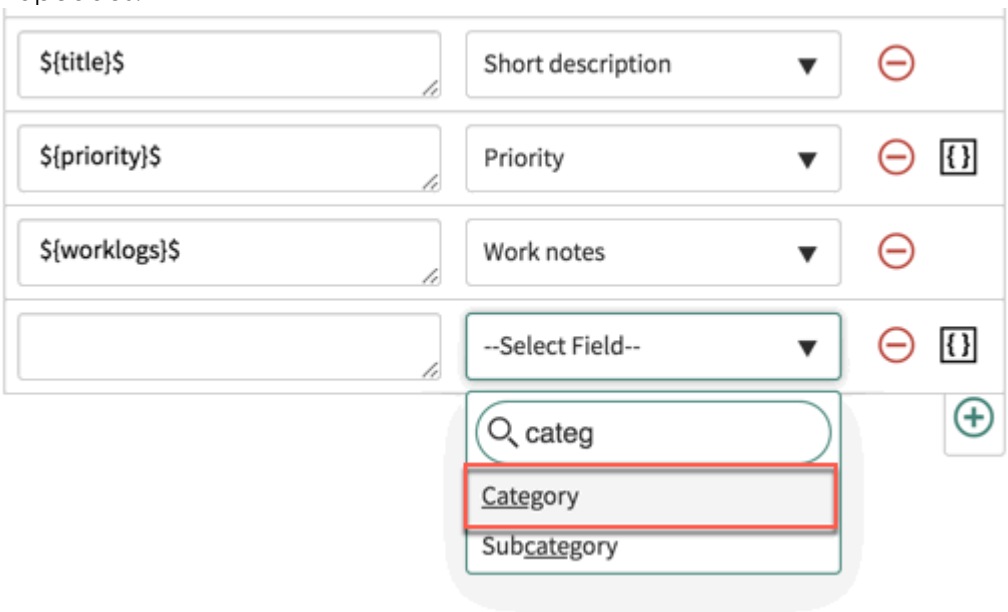
   Os campos em azul claro à esquerda indicam que um campo de tíquete ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um tíquete de entrada ou campo de evento a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas:
   a. À direita do formulário na seção SIR Mapeamento de campo de incidente, na parte inferior da grade, clique no ícone de adição (+). Um novo campo é exibido.
   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

      Na lista de seleção expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, a categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores para os campos de tíquete no lado esquerdo do formulário, essa codificação de cores para os campos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de incidente de segurança à direita ajuda a rastrear os campos de incidentes SIR já mapeados.



Nota: Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, selecione o campo de tíquete e arraste-o e solte-o em um campo de incidente de segurança apropriado à direita.

4. Remova campos usando o ícone - ao lado do nome do campo na seção Mapeamento de campo de incidente SIR.
5. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.

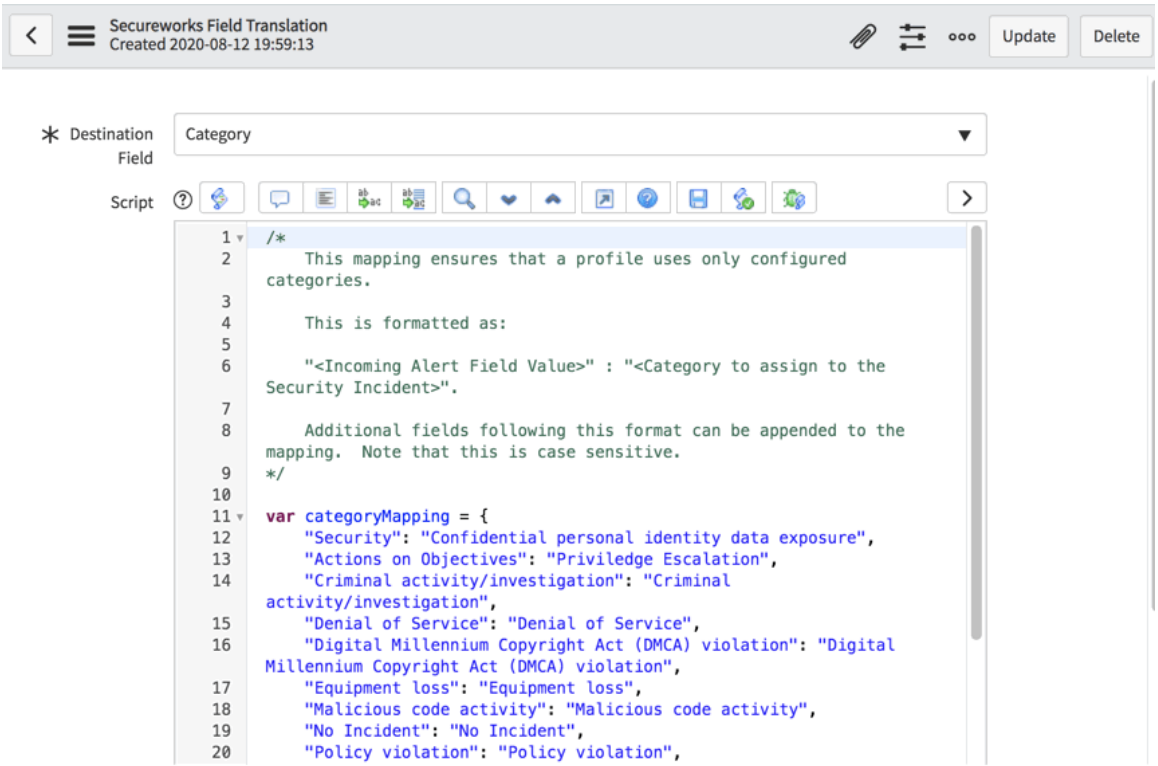
Formatar tradução do campo

Em determinados casos, os campos de tíquete podem não ser convertidos diretamente para os campos no SIR incidente de segurança. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de Malware e Infecção de Vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos para uma Atividade de Código Mal-intencionado comum no campo Categoria no incidente de segurança SIR usando o Funcionalidade Formatar tradução de campo.

Para usar o editor de script, clique no ícone {} ao lado do campo Categoria. O editor de scripts é exibido

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



.

Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças e retornar à página Mapeamento.

Condições de geração de incidentes

Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais tíquetes devem criar incidentes de segurança e quais devem ser filtrados, por exemplo, tíquetes de baixa prioridade. Você pode usar os mesmos valores de campos no construtor Condições de geração de incidentes para definir critérios adicionais que um tíquete de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até a seção **Condições de geração de incidente** no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

   O Construtor de condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção do primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção **Ingestão de tíquete de amostra** dos tíquetes ingeridos. Esses campos são dinâmicos e mudam de acordo com os tíquetes que você ingere. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores do tíquete Secureworks CTP. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console Secureworks CTP e revisar seus tíquetes quanto às palavras-chave.

   Nota: Os *campos worklogs*, *dispositivos*, *anexos*, *observadores*, *availableactions*e tíquete *closeCodes* podem ter vários valores (já que os valores são armazenados em matrizes). Como a condição de filtro pode recuperar somente cadeias de caracteres, você deve usar a condição de filtro " *contém*" para esses campos para garantir que os dados sejam filtrados corretamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   - Se **E** for selecionado, todas as condições deverão ser atendidas.
   - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.
4. (Opcional) Na segunda linha, defina uma segunda condição de filtro.

   Esse tipo de filtragem de condição de geração de incidente ajuda a restringir os tíquetes e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a regra ou os filtros subjacentes. Se critérios de filtragem adicionais forem definidos, somente os tíquetes que corresponderem a todos os critérios serão mapeados para incidentes de segurança.

Critérios de agregação de tíquete para lidar com tíquetes semelhantes e evitar incidentes duplicados

Defina critérios adicionais de agregação de tíquete que agreguem um tíquete de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de tíquete relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

1. Role até a seção **Critérios de agregação de tíquete** no formulário e marque a caixa de seleção **Condições de agregação** para habilitar essa opção.

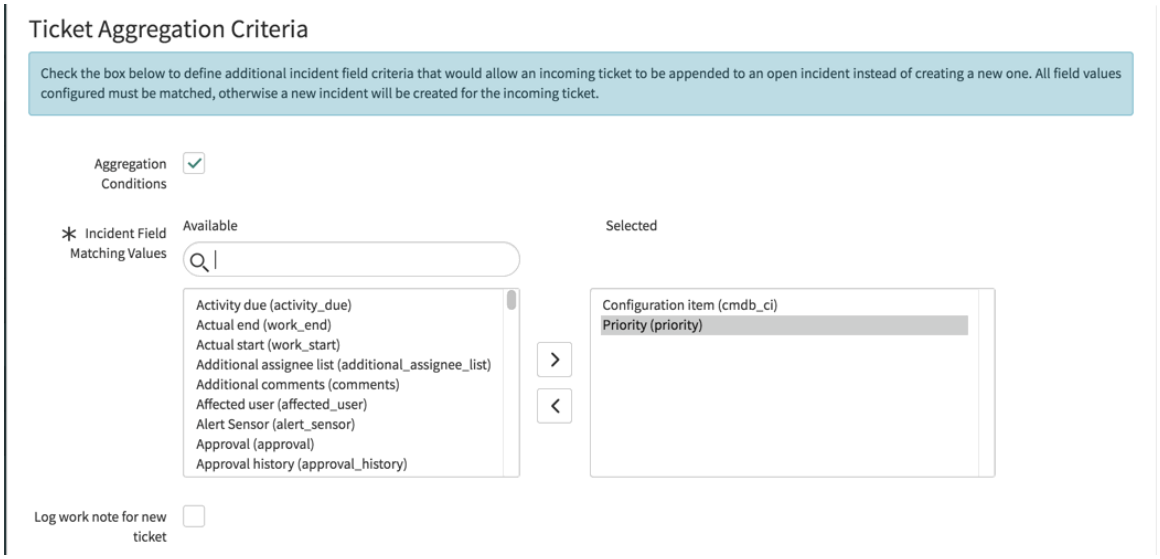
   As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

2. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes na NOW Platform e mova-os para a lista Selecionado.

   Todos os valores de campo selecionados devem ser correspondidos para anexar este tíquete de entrada a um incidente de segurança existente. Isso inclui campos, como Observáveis e Itens de configuração, que podem ter vários valores de campo de tíquete mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de tíquete não serão atendidas e um novo incidente de segurança será criado. Consulte a captura de tela abaixo para mapeamento de campos de vários valores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se um novo tíquete corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o novo tíquete será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os tíquetes agregados adicionados em uma lista relacionada em um incidente de segurança. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que esses tíquetes estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida em um incidente de segurança, role para o lado esquerdo do registro em **Links relacionados** e clique no link **Mostrar todas as listas** relacionadas.

Nota: A lista relacionada de Tíquetes agregados do Secureworks não está disponível com o sistema de base. Você deve configurar o layout da Lista relacionada e incluí-lo explicitamente com as outras listas relacionadas.

3. (Opcional) Para registrar uma anotação de trabalho para um novo tíquete adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar essa opção. A anotação de trabalho registra que um novo tíquete foi adicionado junto com um link para os detalhes do tíquete e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Você mapeou com sucesso valores de um tíquete Secureworks CTP para campos em um incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidente. Você também anexou tíquetes a incidentes de segurança existentes quando os valores do campo de tíquete correspondem aos critérios de agregação configurados.

4. Clique em **Continuar** para continuar com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Visualizar os valores mapeados no incidente de segurança

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um SIR incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de tíquete que deseja exibir no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

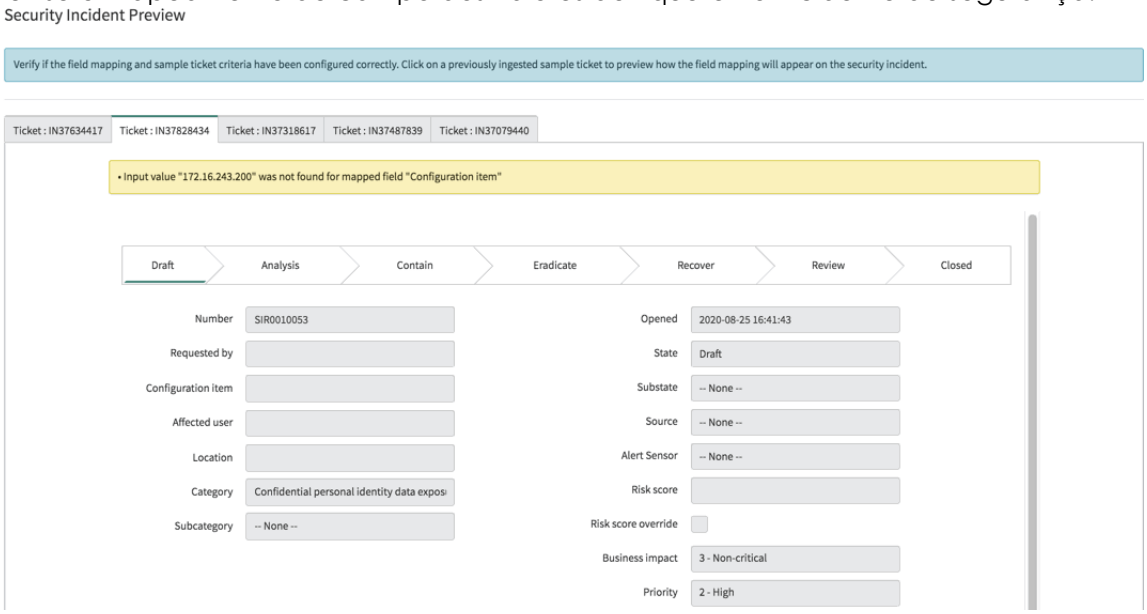
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
   Os tíquetes são exibidos como guias.
2. Clique em uma guia para visualizar o incidente de segurança.
   Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de tíquete no incidente de segurança.



   A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida, e você estiver satisfeito com o mapeamento de campo no incidente de segurança. Defina a programação.

Definir programação para a ingestão do tíquete de CTP do Secureworks

Verifique as configurações padrão para recuperação de tíquete ou modifique a programação conforme necessário. Esta etapa permite filtrar a recuperação do tíquete com base em um intervalo de datas e um intervalo de pesquisa.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você também escolhe com que frequência pesquisará tíquetes futuros que correspondam à configuração do perfil do tíquete. Configure esses intervalos de pesquisa por perfil. Ao programar, você pode preferir equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de um minuto é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

Procedimento

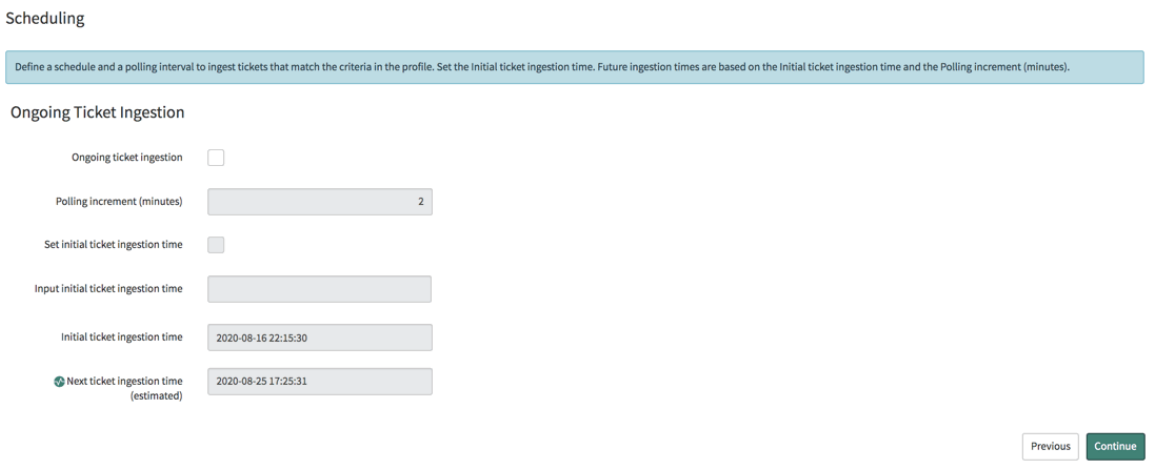
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os tíquetes são extraídos do portal Secureworks CTP.

Opção	Descrição
Ingestão contínua de tíquete selecionada	Com base na configuração padrão, a instância Now Platform extrai do portal Secureworks CTP novos tíquetes a cada cinco minutos. Os incidentes de segurança serão criados se os tíquetes forem encontrados e os critérios de filtragem de geração de incidentes forem correspondidos. Para equilibrar a ingestão de tíquete em relação à carga do servidor e para extrair os dados mais atuais, cinco minutos é a configuração que você pode preferir. No entanto, este valor pode ser modificado conforme necessário.
◦ Ingestão contínua de tíquete selecionada ◦ Definir tempo de ingestão do tíquete inicial	Tempo de ingestão inicial Se você quiser programar a ingestão inicial em um horário específico, siga estas etapas: ◦ Selecione os campos Ingestão contínua de tíquete e Definir tempo de ingestão do tíquete inicial. ◦ Especifique o tempo no campo Tempo de ingestão do tíquete inicial de entrada. A ingestão inicial ocorrerá no horário especificado aqui. As ingestões subsequentes serão baseadas na programação definida no campo Incremento de pesquisa (minutos). Como um exemplo de programação, se você tiver um trabalho de tíquete diário que é executado uma vez por dia às 4h no horário local, poderá configurar o perfil de tíquete correspondente em sua instância da Now Platform para ser executado às 4h05 no horário local para capturar o tíquete imediatamente e crie um incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Insira 04 05 00 no campo Ingestão de tíquete inicial. No campo Incremento de pesquisa (minutos), insira 1440 (24 horas) para programar a próxima ingestão de tíquete por 24 horas a partir da ingestão do tíquete inicial. O tempo de ingestão do tíquete inicial e o tempo de ingestão do próximo tíquete são exibidos nos campos. Para definir as configurações neste exemplo, siga estas etapas: ◦ Selecione a opção **Ingestão contínua de tíquete**. ◦ No campo Incremento de pesquisa (minutos), insira 1440 (24 horas). ◦ Selecione a opção **Definir tempo de ingestão do tíquete inicial**. ◦ No campo Tempo de ingestão do tíquete inicial de entrada, insira 04 05 00. A hora da próxima ingestão de tíquete é exibida no campo Tempo de ingestão do próximo tíquete (estimado).



3. Clique em **Continuar** para navegar até a página Opções adicionais.

Automatizar atualizações e fechamento de tíquetes com base no status do incidente SIR

A integração de ingestão de tíquete Secureworks CTP tem uma interface bidirecional que permite que ambos os tíquetes criem incidentes de segurança, bem como a capacidade de atualizar os tíquetes depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como o número do incidente de segurança , grupo de atribuição, URL do incidente de segurança e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Conclua a configuração para atualizar os tíquetes quando o incidente de segurança for criado.

Opção ou campo	Descrição
Atualizar anotações de trabalho SIR com worklogs do Secureworks	Selecione esta opção para habilitar os logs de trabalho do Secureworks e o recurso de sincronização de anotações de trabalho SIR. Isso permite que você rastreie as atualizações feitas no tíquete em Secureworks CTP após a criação do incidente de segurança. **Nota:** ◦ Se o campo Logs de trabalho do Secureworks tiver sido mapeado para o campo Anotações de trabalho do SIR, os logs de trabalho do Secureworks serão recuperados até que o incidente de segurança seja criado. ◦ Se o recurso de sincronização estiver habilitado, somente os logs de trabalho criados ou atualizados após a criação de um incidente de segurança serão recuperados.
Atualizar tíquetes do Secureworks após a criação do incidente no SIR	Selecione esta opção para atualizar o tíquete Secureworks CTP e adicionar comentários adicionais quando um incidente de segurança for criado a partir do tíquete. Isso pode ocorrer para os tíquetes de acionamento iniciais que criam o incidente de segurança, bem como para os tíquetes agregados.
Comentários iniciais retornados para o tíquete do Secureworks	Quando um incidente de segurança é criado, o tíquete é atualizado automaticamente em Secureworks CTP com comentários. Você pode modificar o texto padrão e usar o formato ${field name}$ para adicionar ou modificar quaisquer campos disponíveis no formulário de incidente de segurança.
Fechar tíquetes do Secureworks após o fechamento do incidente no SIR	Selecione esta opção se quiser usar a opção de fechamento automatizado de tíquete. Isso pode ocorrer para os tíquetes de acionamento iniciais que criam o incidente de segurança, bem como para os tíquetes agregados. Quando um incidente de segurança é encerrado, o tíquete correspondente é encerrado automaticamen-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	te em Secureworks CTP junto com o mesmo código de encerramento do incidente de segurança e os comentários de fechamento padrão especificados no perfil. **Nota:** Você não pode usar esta opção para atualizar o status do Tíquete mestre.
Comentários de fechamento retornados para o tíquete do Secureworks	Os comentários de fechamento padrão são exibidos aqui. Você pode editar o texto padrão e usar o formato ${field name}$ para adicionar ou modificar quaisquer campos disponíveis no formulário de incidente de segurança.

3. Clique em **Concluir** para concluir a configuração e mover o perfil para o estado **Aguardando**.
   Uma caixa de diálogo de confirmação é exibida. Você configurou o perfil com sucesso. Ative este perfil para extrair tíquetes do portal Secureworks CTP com base em sua programação.

Opcional: copiar um perfil CTP do Secureworks

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar os perfis para economizar tempo.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Todos** > **Integração de ingestão de tíquete do Secureworks** > **Perfil do Secureworks**.
2. Na lista Perfis do Secureworks exibida, selecione um perfil que você deseja copiar e, na lista de seleção **Ações nas linhas selecionadas**, clique em **Copiar**.
   O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém (cópia). Embora o perfil original esteja habilitado (`verdadeiro`), a cópia está desabilitada neste ponto (`falso`). Você pode preferir editar valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.

   Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativo** está definido como falso, pois o perfil precisa ser ativado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

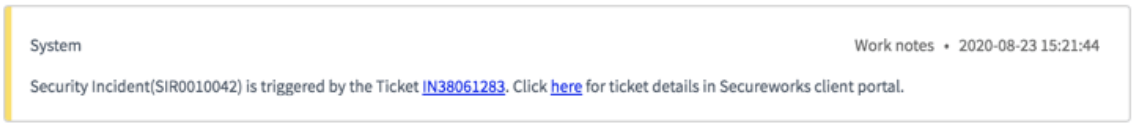
Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

O formulário do Security Incident Response muda após a ingestão do tíquete

Depois que um tíquete Secureworks CTP é ingerido, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro do incidente de segurança.

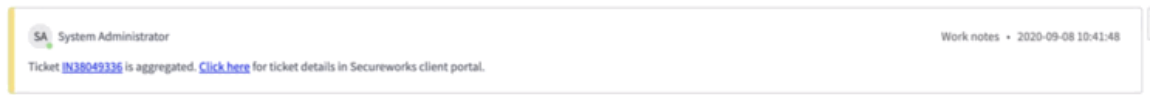
Anotações de trabalho

Uma anotação de trabalho é publicada com detalhes do tíquete que acionou o incidente de segurança.



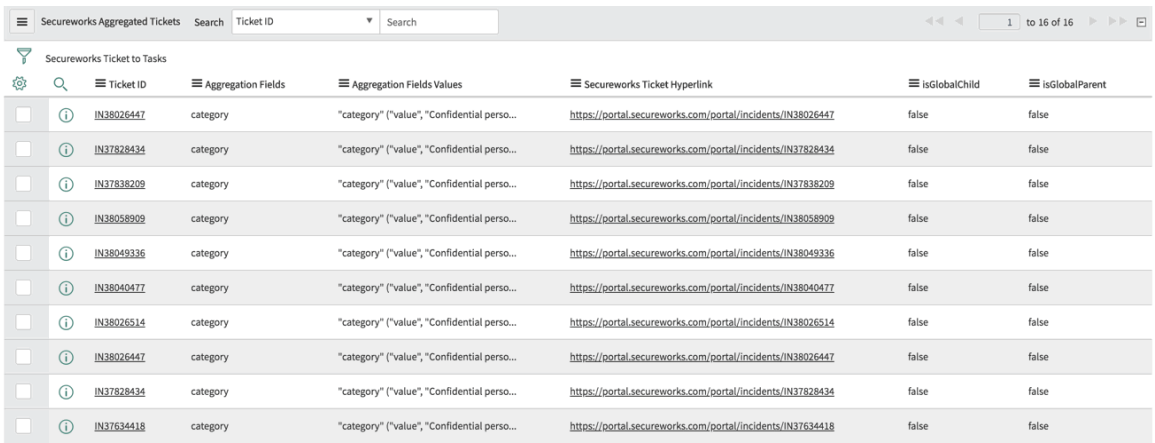
Clique no link do tíquete para navegar até o registro interno Tíquete para tarefa do Secureworks. O hiperlink **Clique aqui** leva você para o painel Secureworks CTP, onde você pode exibir os detalhes do tíquete.

Se você selecionou a opção **Registrar anotação de trabalho para novo tíquete** nos Critérios de agregação de tíquete conforme descrito na página Criar perfil: mapeamento, uma anotação de trabalho será publicada quando o tíquete for agregado.



Tíquetes agregados

Clicar **Listas relacionadas** > **Tíquetes agregados do Secureworks** para exibir o tíquete agregado ao incidente de segurança. Clique no hiperlink do tíquete para exibir o tíquete no painel Secureworks CTP.



Criar incidente de segurança: selecione um tíquete na lista, clique no menu **Ações** e clique em **Criar incidente de segurança**. Esta opção cria um novo incidente de segurança para o tíquete e este tíquete é desagregado do incidente de segurança primário.

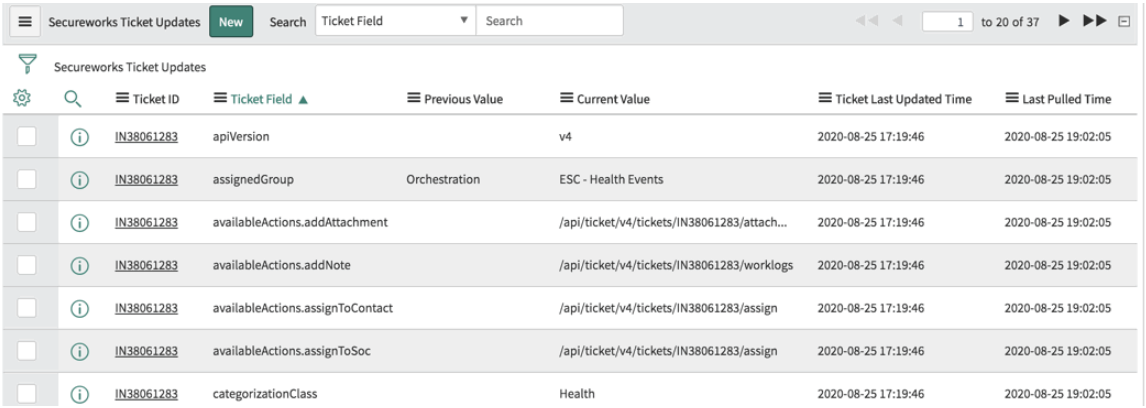
Excluir registro de tíquete: selecione um tíquete na lista, clique no menu **Ações** e clique em **Excluir**. Esta opção exclui o registro do tíquete.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

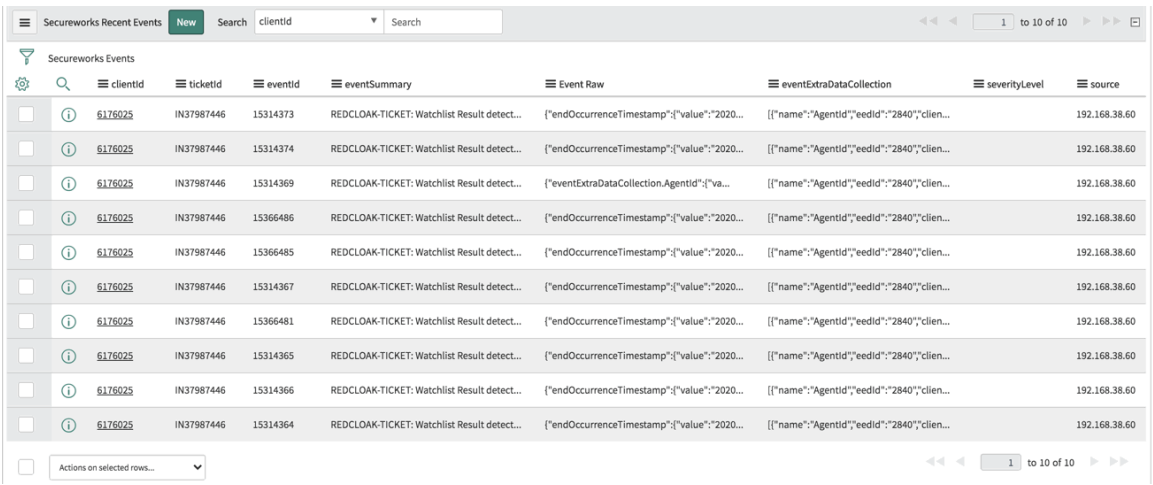
Atualizações de tíquete do Secureworks

Mostra os campos de tíquete padrão e rastreia as mudanças nos tíquetes durante cada intervalo de pesquisa. Isso é útil, pois você pode exibir todas as atualizações de tíquete diretamente sem navegar até o painel Secureworks CTP. Todas as mudanças nos valores são exibidas nos campos Valor anterior e Valor atual.



Eventos recentes do Secureworks

Clique na opção **Buscar eventos recentes do Secureworks** em **Links relacionados** para exibir os eventos mais recentes do Secureworks.



Por padrão, um número máximo de 50 eventos será exibido. Você pode modificar esta configuração padrão nas Configurações de integração do Secureworks.

Exibir os tíquetes do Secureworks e os incidentes de segurança correspondentes

Os Secureworks CTP tíquetes importados são armazenados inicialmente na tabela Importação de tíquete. Exiba todos os Secureworks CTP tíquetes que foram importados antes que qualquer condição de filtro seja aplicada.

Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração de ingestão de tíquete do Secureworks** > **Importação de tíquete seguro**.
2. Você pode exibir todos os Secureworks CTP tíquetes que foram importados antes de serem agregados ou de qualquer condição de filtro ser aplicada.
3. Clique em um ID de tíquete para ver os dados brutos do tíquete.
4. Navegar até **Ingestão de tíquete do Secureworks** > **Tíquetes do Secureworks para a tarefa**.
   Os Secureworks CTP tíquetes com seus incidentes de segurança correspondentes são exibidos.

Aviso de fechamento do tíquete mestre do CTP do Secureworks

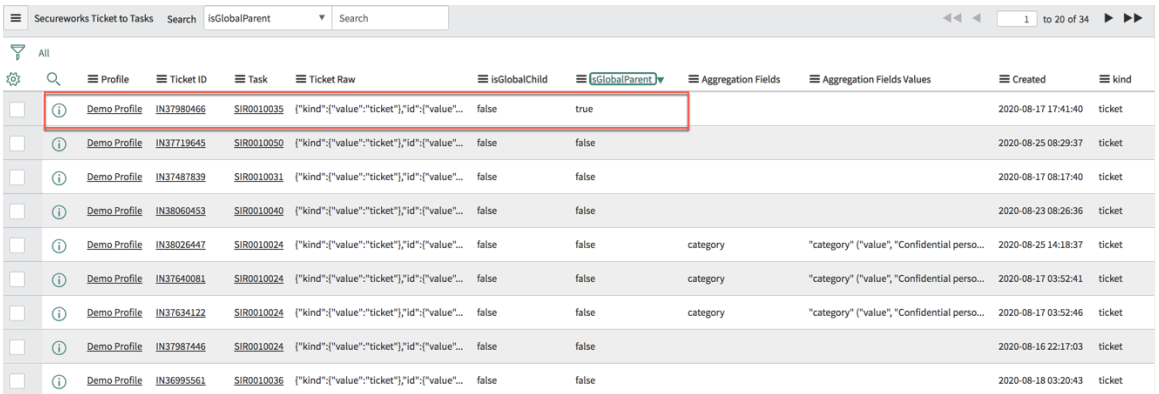
Antes de fechar um incidente de segurança criado por um tíquete mestre Secureworks CTP, você deve verificar se todos os tíquetes secundários associados ao tíquete mestre estão fechados.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

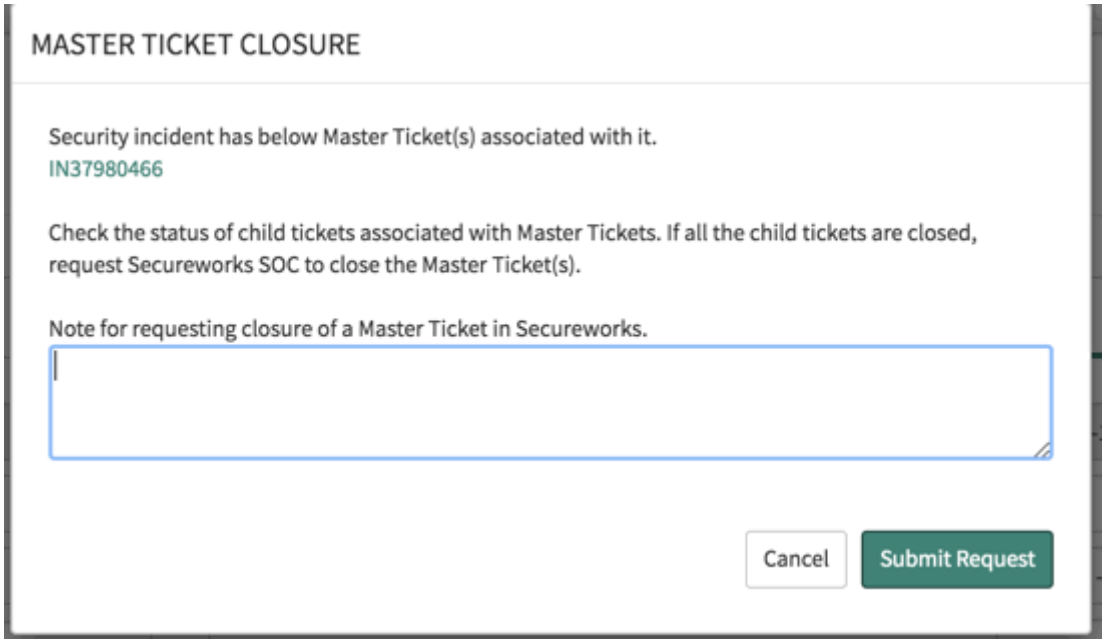
1. Navegar até **Todos** > **Ingestão de tíquete do Secureworks** > **Tíquetes do Secureworks para a tarefa**.
   Os Secureworks CTP tíquetes com seus incidentes de segurança correspondentes são exibidos.



2. Clique no incidente de segurança com o campo **isGlobalParent** definido como **verdadeiro.**
3. Altere o Estado do incidente de segurança para **Encerrado**, especifique os códigos de encerramento e clique em **Salvar**.
   A caixa de diálogo a seguir é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este incidente de segurança está associado a um tíquete mestre do Secureworks. Um tíquete mestre pode ter um ou mais tíquetes secundários associados a ele. Antes que o tíquete mestre possa ser encerrado, você deve verificar se todos os tíquetes secundários associados a este tíquete mestre estão encerrados.

4. Adicione uma nota solicitando o fechamento do tíquete mestre no Secureworks e clique em **Enviar solicitação**.
   O tíquete mestre agora foi reatribuído à equipe de SOC do Secureworks.
5. Depois que a solicitação for enviada, você poderá fechar o incidente de segurança.
6. Navegar até **Aplicação** > **Módulo**.

Definições de configuração da integração do CTP do Secureworks

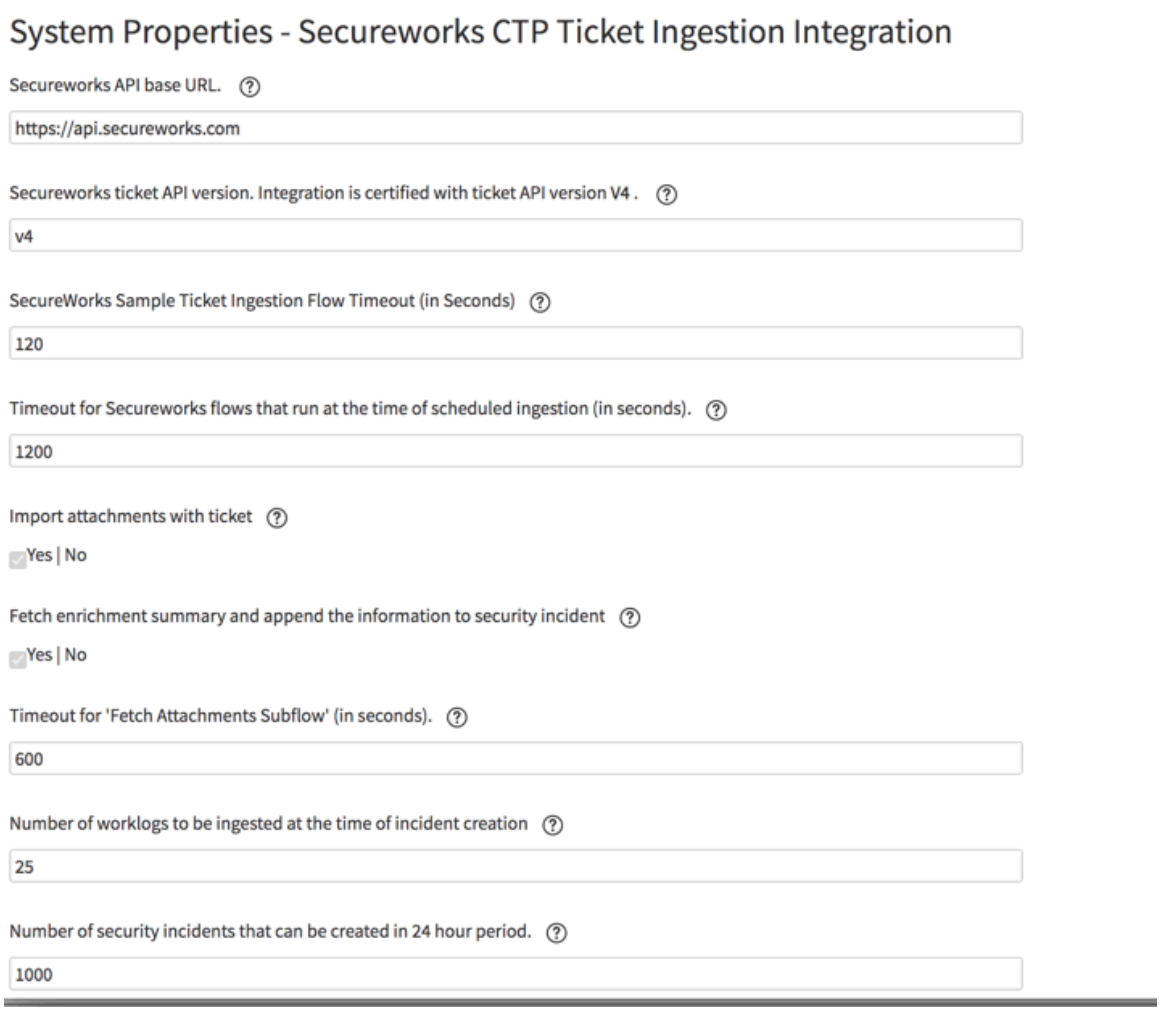
Use esta opção para modificar as Secureworks CTP propriedades do sistema padrão de integração de ingestão de tíquete.

Para modificar as propriedades do sistema, faça login como um usuário com a função `sn_si.admin` e navegue até **Integração de ingestão de tíquete do Secureworks** > **Configurações de integração do Secureworks**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Integração de Resposta a incidente de segurança com Zscaler

Você pode usar o produto Integração de Resposta a incidente de segurança com Zscaler para conectar os logs do servidor Zscaler Internet Access (ZIA) com o Now Platform. Essa integração permite que você exiba painéis, crie alertas personalizados e ajude a investigar incidentes de segurança.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

O Zscaler produto de gateway de internet e web é entregue a partir da nuvem. Ele fornece os principais pontos de dados e informações sobre o ambiente de segurança da sua empresa. Integração de Resposta a incidente de segurança com Zscaler conecta o produto Zscaler Internet Access à sua instância Now Platform. Ao usar o produto Zscaler no Now Platform, você obtém mais informações sobre o uso da internet pela sua organização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos da integração

Esta integração inclui os seguintes recursos principais:

- Pesquisa de reputação de observáveis em relação à biblioteca de ameaças globais que o produto Zscaler mantém.

  Nota: A Zscaler biblioteca de ameaças globais lista as ameaças por tendências, país de origem, destino, volume e várias categorias de ameaças. Esta biblioteca de ameaças globais permite que você investigue seus observáveis em relação ao cenário de ameaças globais.

- Manutenção de observáveis em uma lista de bloqueios ou lista de permissões no produto Zscaler.
- Capacidade de buscar e revisar relatórios de área restrita do produto Zscaler para um hash MD5. O recurso Sandbox de nuvem no produto Zscaler é executado e analisa arquivos em um ambiente virtual para detectar comportamento mal-intencionado.
- Alertas de segurança de eventos do paciente 0 que são gerados no produto Zscaler quando um usuário baixa um arquivo mal-intencionado desconhecido.
- Várias listas de categorias de URL que atuam como listas de bloqueios ou listas de permissões, conforme definido no produto Zscaler.
- Now Platform incidentes de segurança que podem ser marcados para identificar a categoria de URL à qual os observáveis são adicionados.
- Períodos de expiração que mantêm o tamanho das entradas da lista de categorias de URL expirando ou removendo automaticamente as entradas mais antigas.
- Fluxo de trabalho de aprovação para adicionar e remover observáveis das listas de categorias de URL.
- Entradas de categoria de URL que podem ser vinculadas a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Conheça esta integração

Identificador do documento	Título do documento
Zscaler site de documentação do produto	Site de documentação do produto ZScaler
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Comece com Integração de Resposta a incidente de segurança com Zscaler

Ative e configure o produto Zscaler Internet Access para interagir com sua instância [Now Platform e o produto Security Incident Response.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique as funções Now Platform e Security Incident Response.	Essas funções são necessárias para configuração e verificação dos resultados esperados:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria, ativa e remove as listas de categorias de URL. ◦ Atribui a função sn_si.analyst. • A função sn_si.analyst cria entradas e trabalha com incidentes de segurança.
Verifique se as ServiceNow aplicações principais estão instaladas e ativadas antes de configurar esta integração.	O plug-in ServiceNow Integration Hub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] é necessário. O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências do produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações para a integração. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, instale e ative cada aplicação, uma de cada vez, na seguinte ordem: **1.** Security Incident Response Dependência (com.snc.si_dep) **2.** Estrutura de integração de segurança **3.** Security Support Common **4.** Orquestração de suporte de segurança **5.** Inteligência contra ameaças Suporte comum **6.** Trusted Security Circles **7.** Operações de segurança Assistente de configuração **8.** Security Incident Response

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique as Zscaler versões.	• Esta integração é compatível com Zscaler Internet Access versão 1.0 ou posterior. • Esta integração foi testada com as seguintes Zscaler versões: ◦ Conector de cliente Zscaler para Windows - 3.0 ◦ Conector de cliente Zscaler para macOS - 3.0 ◦ Conector de cliente Zscaler para Linux - Beta ◦ Conector de nuvem Zscaler - 6.1
Verifique se você tem as Zscaler permissões necessárias e configurou acesso ao Zscaler Internet Access APIs.	• Você deve ter as credenciais de administrador para Zscaler Internet Access. • Você deve ter uma assinatura de API de serviço em nuvem válida. Zscaler O suporte deve fornecer sua chave. • Você deve ter Zscaler Internet Access credenciais de administrador (nome de usuário e senha). A autenticação de API é baseada em uma combinação da chave de API e Zscaler Internet Access credenciais de administrador. **Nota:** Para obter mais informações sobre como gerenciar as chaves de API Zscaler Internet Access, consulte a documentação do Zscaler .

Tradução automática

Configurar acesso a Zscaler Internet Access APIs

Configure o acesso ao servidor Zscaler Internet Access para autenticar a conexão segura entre a instância Now Platform e o servidor Zscaler.

Antes de Iniciar

Função necessária: administrador do Zscaler Internet Access

Por Que e Quando Desempenhar Esta Tarefa

Depois que Zscaler habilita sua assinatura de API para o serviço em nuvem da sua organização, ela fica disponível na página de gerenciamento de chaves de API Zscaler Internet Access com o URL base. Sua organização só pode ter uma chave de API ou token. Exclua a chave ou o token existente antes de adicionar um novo.

O URL base da API é `${Cloud_Name}/api/v1`. Verifique o nome da nuvem Zscaler que foi provisionado para sua organização e use-o para substituir `{Cloud_Name}` no URI de base. Alguns exemplos da URL base são:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Nota: Para obter mais informações sobre o portal de administração Zscaler Internet Access, consulte a documentação de gerenciamento de chaves da API Zscaler e a documentação do Portal Zscaler .

Procedimento

1. Faça login como administrador no portal de administração Zscaler Internet Access.
2. Navegar até **Administração** > **Gestão de chaves de API**.
3. Clique **em Adicionar chave de API**.
   Se você não vir a opção **Adicionar chave de API**, exclua a chave existente.
   A nova chave de API é válida imediatamente e é exibida na guia.

Resultados

Você recuperou o URL base e a chave de API para configurar o acesso a Zscaler da instância Now Platform.

Instalar e configurar Integração de Resposta a incidente de segurança com Zscaler

Instale e configure o produto Integração de Resposta a incidente de segurança com Zscaler de acesso à Internet do ServiceNow Store para começar a usar a integração em sua instância Now Platform.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe o produto Integração de Resposta a incidente de segurança com Zscaler do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco Integração de Resposta a incidente de segurança com Zscaler e clique em **Configurar** > **Criar nova configuração**.
4. No formulário, preencha os campos.

Zscaler Formulário de configuração

Campo	Descrição
Nome do Servidor	Zscaler nome do servidor. Por exemplo, ZSserver.
Ativo	Indicador de que o perfil está ativo.
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem dos fluxos de trabalho quando dois ou mais perfis compartilham condições de acionamento.

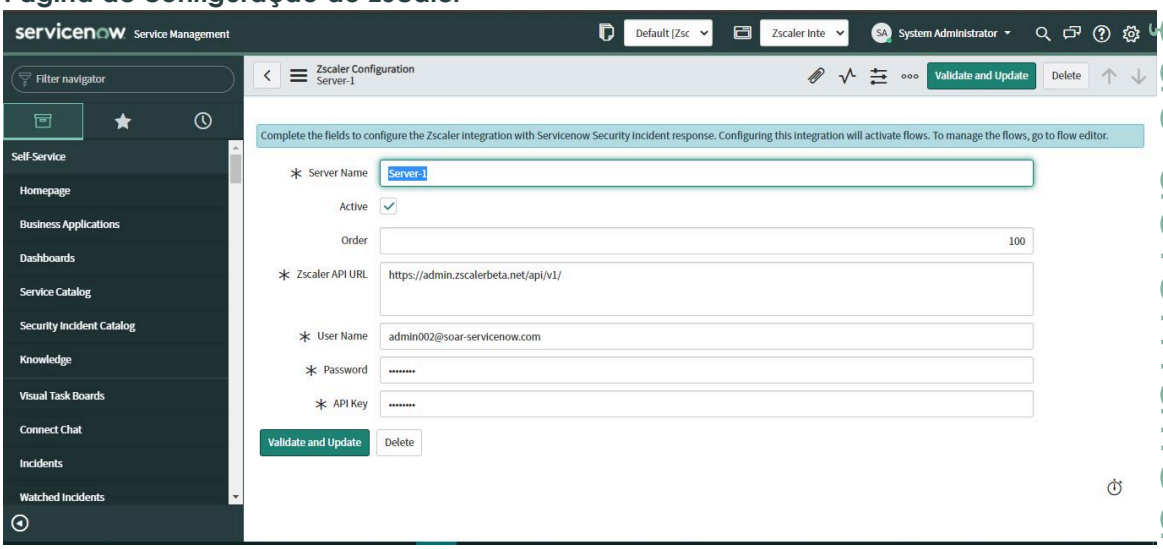
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Zscaler URL da API	URL base que hospeda a Zscaler API. Por exemplo, https://example.zscalerbeta.net
Nome do usuário	Nome de usuário da conta de administrador Zscaler Internet Access.
Senha	Senha da conta de administrador Zscaler Internet Access.
Chave de API	Chave de API que você obteve do Zscaler Internet Access portal de administração.

O exemplo a seguir mostra a página de configuração do Zscaler.

Página de configuração do ZScaler



5. Clique **em Validar e atualizar**.

Resultados

Depois de validar e salvar esta configuração, retorne à página Zscaler Configurações.

Adicionar Zscaler Internet Access listas de categorias de URL

Adicione as categorias de URL que estão disponíveis no produto Zscaler de acesso à Internet à instância Now Platform para especificar uma ação para cada URL para que você tenha acesso fácil para filtragem granular e criação de políticas.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O Integração de Resposta a incidente de segurança com Zscaler fornece uma lista de categorias de URL de lista de permissões e de proibições padrão para ajudar a filtrar o conteúdo.

As categorias de URL adicionadas na instância Now Platform já devem estar no ambiente Zscaler Internet Access. Você não pode usar Integração de Resposta a incidente de segurança com Zscaler para criar categorias de URL em Zscaler.

Nota: Para obter mais informações sobre listas de categorias de URL no produto Zscaler, consulte a documentação do Zscaler em Categorias de URL .

Procedimento

1. Navegar até **Todos** > **Integração com ZScaler** > **Listas de categorias de URL do ZScaler**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Zscaler Formulário Listas de categorias de URL

Campo	Descrição
Origem	Nome do servidor. Você pode exibir somente os servidores Zscaler Internet Access configurados anteriormente na lista de categorias de URL.
Ativo	Indicador de que a lista de categorias de URL está ativa.
Categoria de URL	Campo que é habilitado depois que você seleciona a origem. Você pode exibir a lista de categorias de URL criadas em Zscaler.
Período de Expiração (dias)	Período de expiração da lista de categorias de URL. 0 (por padrão) indica que a entrada da lista de categorias de URL nunca expira. Ao alterar este valor, qualquer observável que foi adicionado a esta categoria de URL fica ativo pelo número de dias que você inserir. Você pode inserir um valor mínimo de 1. Por exemplo, se você definir o período de expiração como 30 dias, as entradas serão removidas da lista de categorias após 30 dias.
Marcador de exibição	Marcador de segurança que aparece no incidente de segurança SIR. Quando você habilita a opção **Exibir marcador**, o campo Zscaler Marcador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	para observáveis fica disponível no formulário.
Criar solicitação de mudança	Solicitação de mudança e tarefas de mudança em sua instância Now Platform para os registros que estão anexados à lista de categorias de URL. Quando você habilita a opção **Criar solicitação de mudança**, o campo **Solicitação** de mudança fica disponível no formulário.
Requer Aprovação	Lista de grupos de aprovadores. Depois de enviar uma solicitação, é necessária uma aprovação do grupo para concluir a solicitação. Quando você habilita a opção **Exigir aprovação**, os campos **Aprovadores para adicionar observáveis** e **Aprovadores para remover observáveis** ficam disponíveis no formulário. ◦ **Aprovadores para adicionar observáveis**: selecione os aprovadores usando a pesquisa para adicionar os observáveis na página **Lista de categorias de URL do Zscaler**. Esta opção permitirá que você adicione os grupos de usuários para aprovações. ◦ **Aprovadores para remover observáveis**: selecione os aprovadores para remover os observáveis usando a pesquisa na página **Lista de categorias de URL do Zscaler**. Esta opção permitirá que você remova os grupos de usuários da lista de aprovação.
Descrição	Descrição da lista de categorias de URL Zscaler. Use este campo para adicionar mais detalhes sobre o registro da categoria de URL.

Tradução automática

4. Clique em **Enviar**.
   Um envio bem-sucedido aciona uma notificação por e-mail para o grupo de aprovação.

Enviar observáveis de um registro de incidente de segurança para uma lista de categorias de URL

Envie observáveis que estão anexados a um registro de incidente de segurança para uma lista de categoria de URL configurada usando a solicitação de permissão ou bloqueio. Adicionar observáveis à lista de permissões ou bloqueios para verificações de segurança permite que os usuários revisem o conteúdo desses URLs e obtenham acesso a conteúdo confiável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

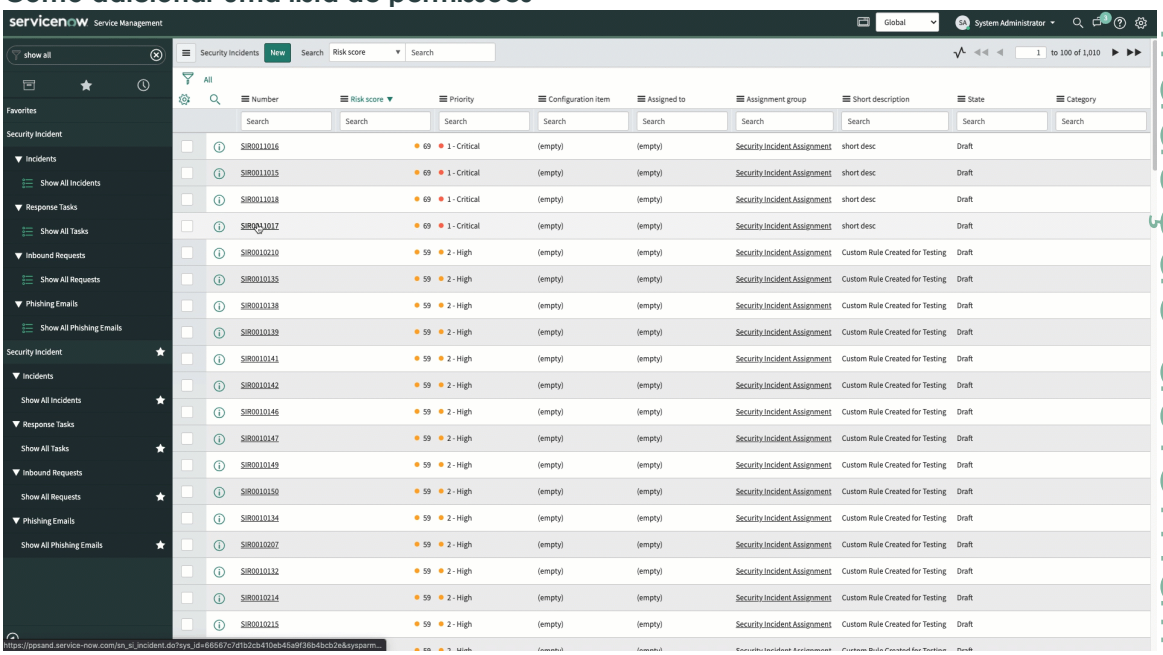
Por Que e Quando Desempenhar Esta Tarefa

Você envia entradas de observável usando a ação de solicitação de permissão ou bloqueio da lista relacionada Observáveis associados. Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicam uma invasão. Use a lista de Categorias de URL configuradas anteriormente para selecionar o observável que você deseja enviar. Depois de enviar a solicitação, uma solicitação de aprovação será enviada ao seu grupo de aprovação.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**.
   Neste exemplo, você vê como selecionar um incidente de segurança e um observável e como adicionar uma lista de permissões.

Como adicionar uma lista de permissões



2. Selecione o incidente de segurança que você deseja associar à Zscaler solicitação de permissão ou bloqueio.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
   Se você não encontrar nenhum observável, clique em **Novo**.
4. Selecione um observável e, no menu de ações, clique em **Permitir/Bloquear solicitação**.
5. Na caixa de diálogo Solicitação de permissão/bloqueio, selecione se deseja executar a solicitação de permissão ou bloqueio no observável.
6. Clique em **Enviar**.
7. Exiba as Anotações de trabalho para ver o status do envio e os marcadores de segurança.
   Clique nos links nas Anotações de trabalho para obter mais informações sobre o status ou para analisar os detalhes no Flow Designer. Os marcadores de segurança são metadados no registro de resposta e definem quem deve ter acesso a tipos específicos de conteúdo de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Para exibir o status do observável selecionado, navegue até **Integração com Zscaler** > **Entradas da Lista de Categorias de URL do Zscaler**.
9. Na página Entradas da lista de categorias de URL do Zscaler, clique no observável para exibir o registro.

Aprovar observáveis para listas de categorias de URL

Aprove observáveis que são adicionados a uma lista de categorias de URL para que as entradas de observáveis estejam nas listas de permissões ou proibições apropriadas.

Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Integração com Zscaler** > **Aprovações do Zscaler**.
2. Selecione o registro a ser aprovado.
3. Clique em **Aprovar**.
   O grupo de aprovadores recebe uma notificação por e-mail da solicitação de aprovação. Depois que os aprovadores clicam no link **Aprovar/Rejeitar** no e-mail, o status muda para aprovado.

Enviar o incidente de segurança para a lista de categorias de URL Zscaler

Envie entradas diretamente para observáveis que não estão associados a um registro de incidente de segurança Now Platform específico para que as entradas de observáveis estejam nas listas de permissões ou proibições apropriadas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você também pode adicionar observáveis à lista de categorias de URL diretamente do registro do Observável.

Procedimento

1. Navegar até **Todos** > **Integração com Zscaler** > **Entradas da Lista de Categorias de URL do Zscaler**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Zscaler Formulário de Entradas de Listas de Categorias de URL

Campo	Descrição
Valor de Entrada	Nome do observável. Se um observável correspondente for encontrado, o restante do formulário será preenchido automaticamente. Se nenhum observável correspondente for encontrado, você deverá preencher o restante das informações manualmente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Observável	Valor (por exemplo, endereço IP ou hash) que está associado ao observável.
Tipo de Observável	Classificação de observável, como um endereço IP ou hash de arquivo.
Lista de categorias de URL	Categoria de URL. Por exemplo, se uma organização usar example.com para serviços do Office 365, Zscaler categorizará example.com como Serviços profissionais e Office 365.
Origem	Nome do servidor. Você pode exibir somente os servidores Zscaler configurados anteriormente na lista de categorias de URL.
Contagem de incidentes	Número de incidentes em que este observável aparece. Este valor é atualizado automaticamente quando o observável é adicionado a outro incidente manualmente ou por meio de um fluxo de trabalho.
Ativo	Indicador de que a lista de categorias de URL está ativa.
Status	Status se o observável for aprovado ou rejeitado.
Período de Expiração (dias)	Período de expiração da lista de categorias de URL. 0 (por padrão) indica que a entrada da lista de categorias de URL nunca expira. Ao alterar este valor, qualquer observável que você adicionar a esta categoria de URL ficará ativo pelo número de dias que você inserir. Você pode inserir um valor mínimo de 1. Por exemplo, se você definir o período de expiração como 30 dias, as entradas serão removidas da lista de categorias após 30 dias. **Nota:** Se você alterar o período de expiração padrão da entrada da lista de categorias de URL, verá um aviso de que o período é diferente do período configurado na lista de categorias de URL selecionada.
Informações adicionais	Campo onde você pode adicionar mais detalhes sobre o observável.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar uma pesquisa de ameaças usando a biblioteca de ameaças globais Zscaler

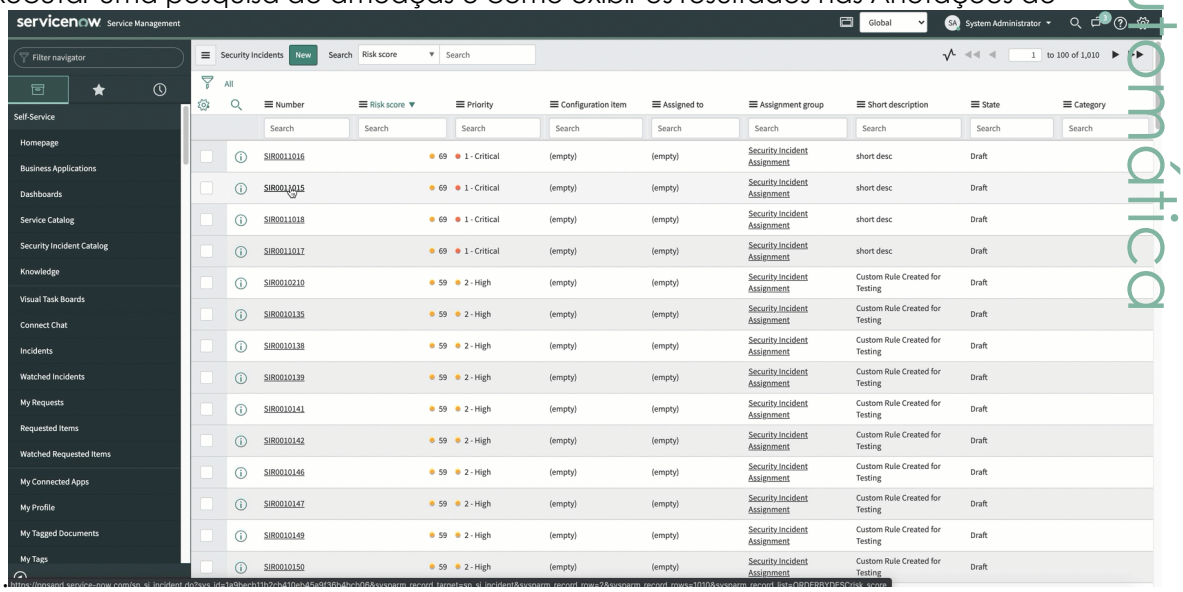
Execute uma pesquisa de ameaças em um observável usando a biblioteca de ameaças globais do produto Zscaler Internet Access. Zscaler oferece suporte a pesquisas em relação a IPs, URLs e domínios do tipo de observável.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode executar pesquisas de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. Quando um observável é associado a um incidente de segurança pela primeira vez, todas as implementações de pesquisa de ameaças ativas no Now Platform executam uma pesquisa automática de ameaças. Você pode exibir os resultados em relação à lista relacionada de resultados de pesquisa de ameaças.

Por padrão, a configuração com a menor ordem é selecionada para executar a pesquisa de ameaças em relação à Zscaler Internet Access biblioteca de ameaças globais do produto. Você também pode executar a pesquisa de ameaças manualmente.

Procedimento
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar a pesquisa de ameaças.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione o observável e, no menu Ações, clique em **Executar pesquisa de ameaças**. Neste exemplo, você vê como selecionar um incidente de segurança e um observável, como executar uma pesquisa de ameaças e como exibir os resultados nas Anotações de trabalho.



Resultados
Depois de iniciar a pesquisa de ameaças, você pode exibir as Anotações de trabalho para ver o status do seu envio.

Enviar para Zscaler análise da área restrita

Use o serviço de área restrita de produtos Zscaler Internet Access para analisar arquivos em um ambiente virtual para detectar comportamento mal-intencionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

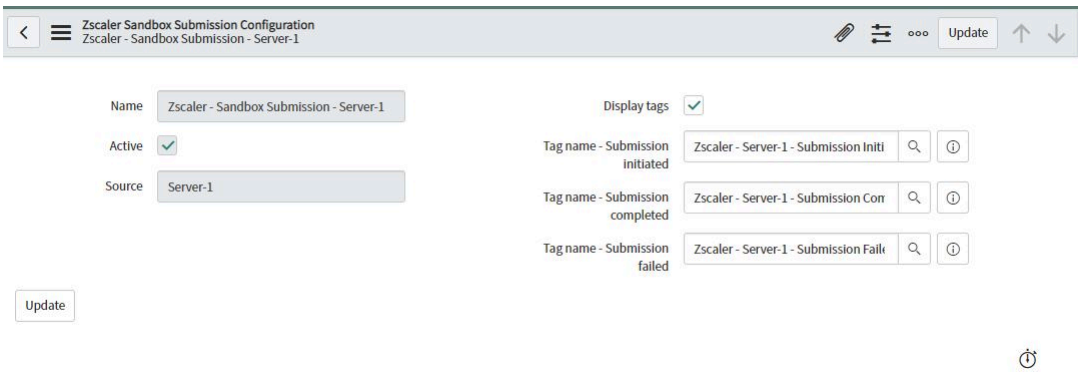
Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Quando você cria uma configuração Zscaler, um envio de área restrita Zscaler é criado por padrão no módulo Configuração de área restrita do Zscaler.

Os campos de nome e origem são preenchidos automaticamente e a configuração está habilitada por padrão. Você pode editar somente o marcador de exibição e as opções ativas. O produto Zscaler Internet Access permite que você busque somente o relatório de área restrita para os observáveis do tipo hash MD5.

A análise do arquivo associado ao hash MD5 deve ser concluída e o relatório correspondente deve estar na área restrita Zscaler. Se o hash MD5 enviado não tiver um relatório em Zscaler, você receberá uma mensagem de erro.

Envio da área restrita do Zscaler



Procedimento
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar a análise da área restrita.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione um observável de tipo de hash MD5 e, no menu Ações, selecione **Enviar para área restrita**.
   Crie um observável de tipo de hash MD5 se você não encontrar um observável de tipo de hash MD5 existente.
5. Na caixa de diálogo Envio de arquivo, selecione a opção **Zscaler - Envio de área restrita - Servidor** em Configuração de envio e clique em **Enviar para área restrita**.
   Depois de iniciar o envio da área restrita, você pode exibir as Anotações de trabalho para ver o status do envio. Um marcador também é anexado ao incidente de segurança.
6. Nas Anotações de trabalho, clique no link na publicação Resultado de envio da área restrita.

Resultados
Você também pode exibir os resultados na guia Mostrar todas as listas relacionadas e resultados de envio da área restrita.

Configurar alertas de e-mail para eventos de paciente 0

Configure o produto Zscaler Internet Access para identificar e verificar arquivos desconhecidos e potencialmente mal-intencionados, como eventos do paciente 0, para que você possa proteger sua rede contra arquivos mal-intencionados.

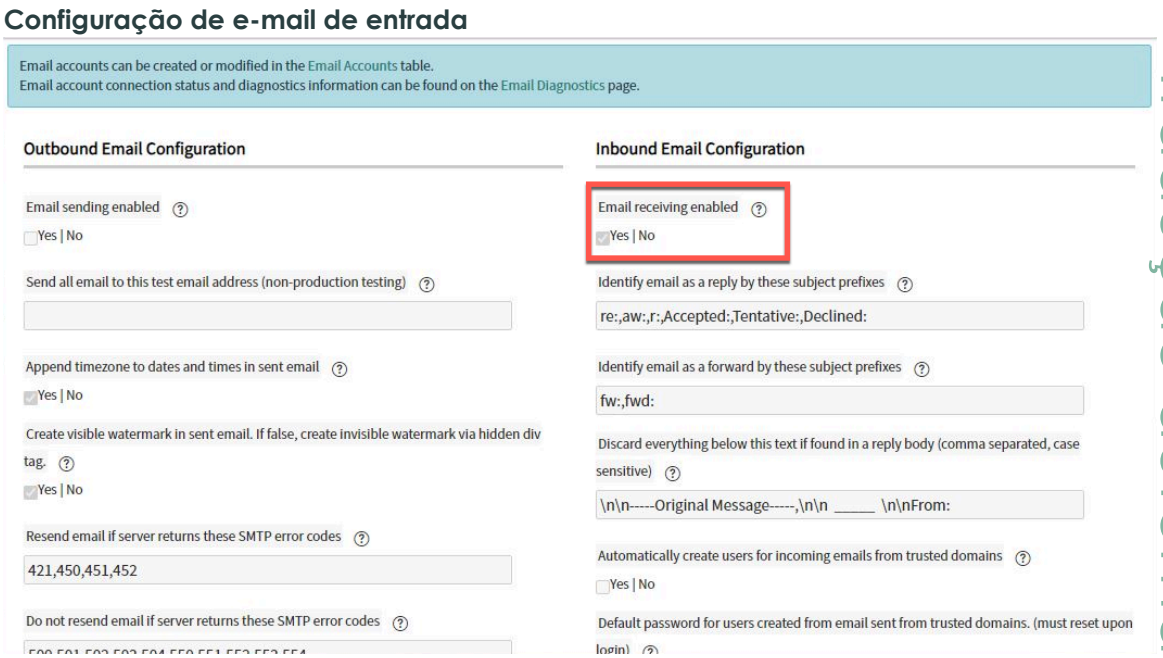
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

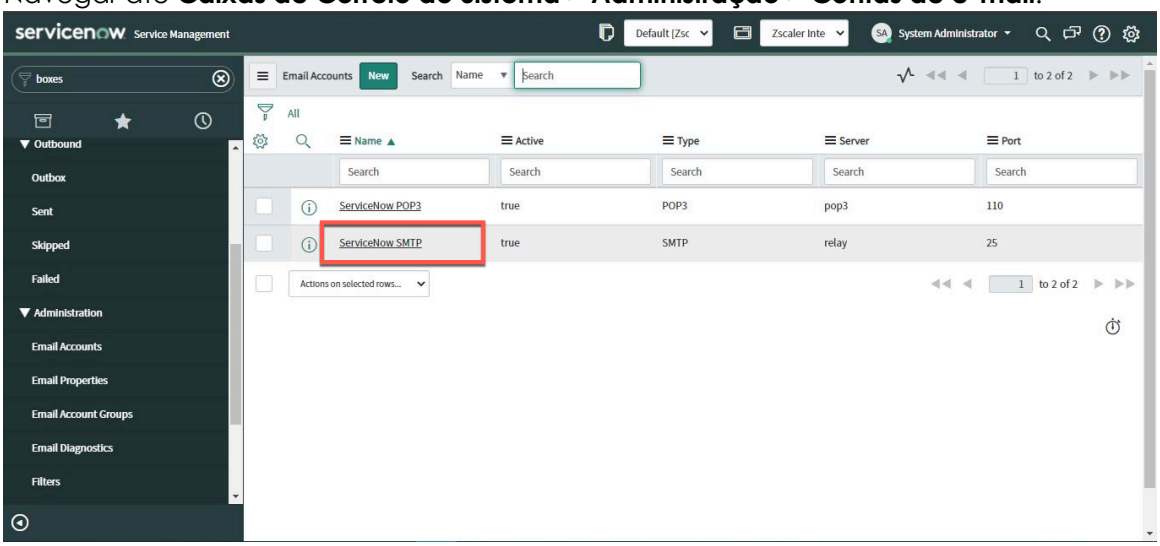
Antes de Iniciar
Função necessária: sn_si.admin, Zscaler Internet Access admin

Por Que e Quando Desempenhar Esta Tarefa
O paciente O é uma classe de alerta que inclui um arquivo desconhecido cujo download foi permitido, mas é considerado mal-intencionado. O evento do paciente 0 é classificado como crítico. Você pode configurar o Now Platform para receber alertas por e-mail em intervalos regulares para eventos do paciente 0.

Procedimento
1. Navegar até **Todos** > **Caixas de Correio do Sistema** > **Administração** > **Propriedades do E-mail**.
2. Na seção Configuração de e-mail de entrada, selecione a opção Recepção de e- **mail habilitada**.



3. Clique em **Salvar**.
4. Navegar até **Caixas de Correio do Sistema** > **Administração** > **Contas de e-mail**.



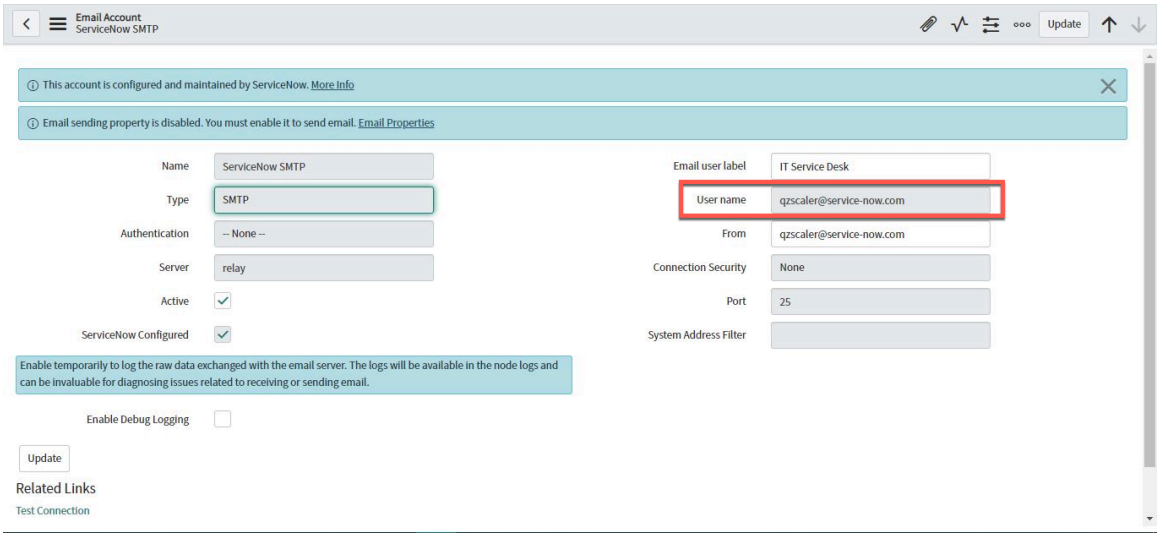
5. Selecione a conta de e-mail **SMTP da ServiceNow**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anote o nome de usuário. O nome de usuário identificado aqui é o endereço de e-mail Now Platform que você usa para configurar em Zscaler para alertas do paciente 0.

Nome de usuário da conta SMTP da Now Platform



6. Faça login no portal de administração Zscaler Internet Access.

> **Nota:** Para obter mais informações sobre o portal de administração Zscaler Internet Access, consulte a documentação do Zscaler .

7. Navegar até **Administração** > **Alertas** > **Publicar alertas**.
8. Clique **em Adicionar assinatura de alerta**.
9. No formulário, preencha os campos.

Formulário Adicionar assinatura de alerta

Campo	Descrição
E-mail	Now Platform Endereço de e-mail da conta SMTP.
Descrição	Campo para adicionar mais detalhes sobre os alertas do paciente 0.

10. Clique em **Salvar**.

ServiceNow Operações de segurança Visão geral do complemento para Splunk

O complemento ServiceNow Operações de segurança para Splunk permite que um administrador de software Splunk colete dados e crie incidentes e eventos no Now Platform.

O complemento é instalado a partir do Splunkbase.

> **Importante:** Splunk também é compatível com o ambiente do provedor de serviços gerenciados (MSP).

Configuração da integração do Splunk

Os procedimentos de configuração do complemento ServiceNow Operações de segurança para Splunk incluem o download do arquivo do complemento no Splunk,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a instalação do complemento e a configuração da instância ServiceNow em que os incidentes e eventos de segurança são criados.

Função necessária

Antes de executar os procedimentos de configuração de integração do Splunk, certifique-se de definir um usuário de integração com as funções sn_si.integration_user e sn_si.analyst em sua instância da ServiceNow. Além disso, para executar importações, você precisa da função import_transformer para obter permissão de leitura e gravação nas tabelas de segurança. A função sn_si.integration_user deve ser definida com a parte import_transformer da função.

Baixar a aplicação Operações de segurança da ServiceNow

A primeira etapa na configuração da integração ServiceNow-to-Splunk é baixar a aplicação ServiceNow Operações de segurança do Splunkbase.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Abra o Splunkbase.
2. Pesquise Integração de Operações de segurança da ServiceNow .
3. Baixe a aplicação.

Instalar o complemento Operações de segurança da ServiceNow para Splunk

Instale o **complemento Operações de segurança da ServiceNow para Splunk** para vincular o Splunk a ServiceNow.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Abra o Splunk.
2. Clique no ícone de engrenagem **Aplicações** ou no item do menu de atalho **Gerenciar aplicações**.
3. Clique **em Instalar app a partir do arquivo**.
4. Clique em **Escolher arquivo**, selecione sn_sec_ops.spl e clique em **Carregar**.
5. Se solicitado, reinicie Splunk.
   O complemento ServiceNow Operações de segurança do Splunk está instalado e pronto para ser configurado.

Configurar ou alterar a instância em que os incidentes ou eventos são criados

Para configurar ou alterar a instância ServiceNow em que novos incidentes e eventos de segurança são criados, use a ação Configurar na lista de aplicações.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o **Splunk**.
2. Clique no ícone de engrenagem **Aplicações** ou no item do menu de atalho **Gerenciar aplicações**.
3. Na lista de aplicações, pesquise apps da **ServiceNow** usando o filtro.
4. Procure a **Integração de Operações de segurança da ServiceNow**e clique na ação **Configurar** correspondente.
5. No formulário, preencha os campos.

Campo	Descrição
Especificar servidor da ServiceNow	
URL	URL do console [Splunk Enterprise Security ou instância Splunk Cloud. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Tipo de autenticação	Opção para selecionar o tipo de autenticação. Você pode selecionar **Autenticação básica ou AutenticaçãoOAuth 2.0**. ◦ Se você estiver usando o Nome de usuário e a Senha da conta de API para configuração, habilite a caixa de seleção **Autenticação básica**. O padrão é desabilitado. ◦ Se você estiver usando a autenticação OAuth 2.0 para a configuração, marque a caixa de seleção **Autenticação OAuth 2.0**. O padrão é desabilitado.
Autenticação básica	
Nome de usuário	Nome de usuário que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Senha	Senha que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Confirmar senha	Alugue a senha para confirmá-la.
Autenticação OAuth 2.0	
ID de cliente	ID de cliente do aplicativo criado no servidor da ServiceNow.
Segredo do cliente	Segredo do cliente do app criado no servidor da ServiceNow.
URL de redirecionamento	A URL para a qual será redirecionado. Você pode copiar e colar este URL no URL de

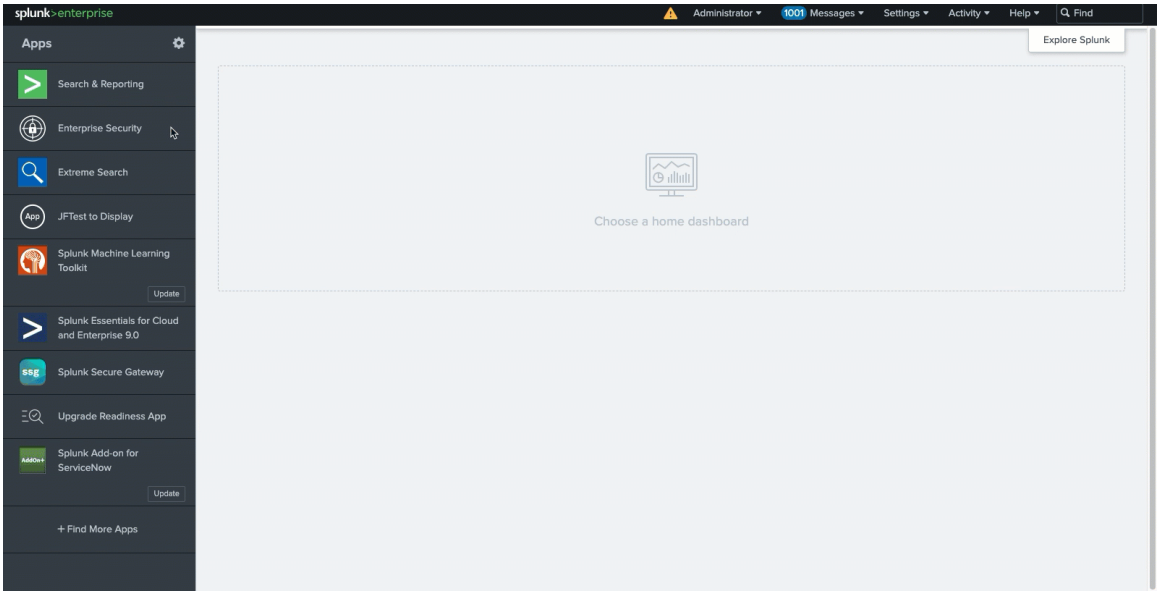
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	redirecionamento do registro da Service-Now.
Proxy opcional	
URL do proxy	URL do proxy para o console [Splunk Enterprise Security ou a instância Splunk Cloud.
Porta	Endereço da porta.
Nome de usuário	Nome de usuário que você criou para a conta de proxy no console Splunk Enterprise Security.
Senha	Senha que você criou para a conta de proxy no console Splunk Enterprise Security.
Confirmar senha	Alugue a senha para confirmá-la.
Configuração do nível de registro em log	
Nível de registro em log	O nível de logs de emissão de relatórios gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ◦ **informações** ◦ **error** ◦ **aviso** ◦ **depurar** Por padrão, o valor é **info**.
Seleção de API	
Seleção de API	Selecione uma das seguintes APIs: ◦ API da tabela ◦ API do Import Set

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique em **Salvar**.
7. Como alternativa, procure a **Integração de ingestão de eventos da ServiceNow**e clique na ação **Configurar** correspondente.

   A integração de ingestão de eventos da ServiceNow está configurada em três guias diferentes.

   - **Splunk primário**: a configuração padrão ou primária do Splunk.
   - **Splunk secundário**: (opcional) o backup ou a segunda configuração do Splunk.
   - **Nível de registro**em log : o nível de logs de emissão de relatórios gerados pela integração, ou seja, o nome do tipo de informação.
8. Selecione a guia **Splunk primário**.
9. No formulário, preencha os campos.

Campo	Descrição
Rótulo de ação de fluxo de trabalho	Nome do console primário Splunk Enterprise Security ou da instância primária Splunk Cloud usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `SplunkES2`.
URL	URL do console primário Splunk Enterprise Security ou da instância primária Splunk Cloud. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Endpoint	Endpoint para o console primário Splunk Enterprise Security ou a instância primária Splunk Cloud.

Tradução automática

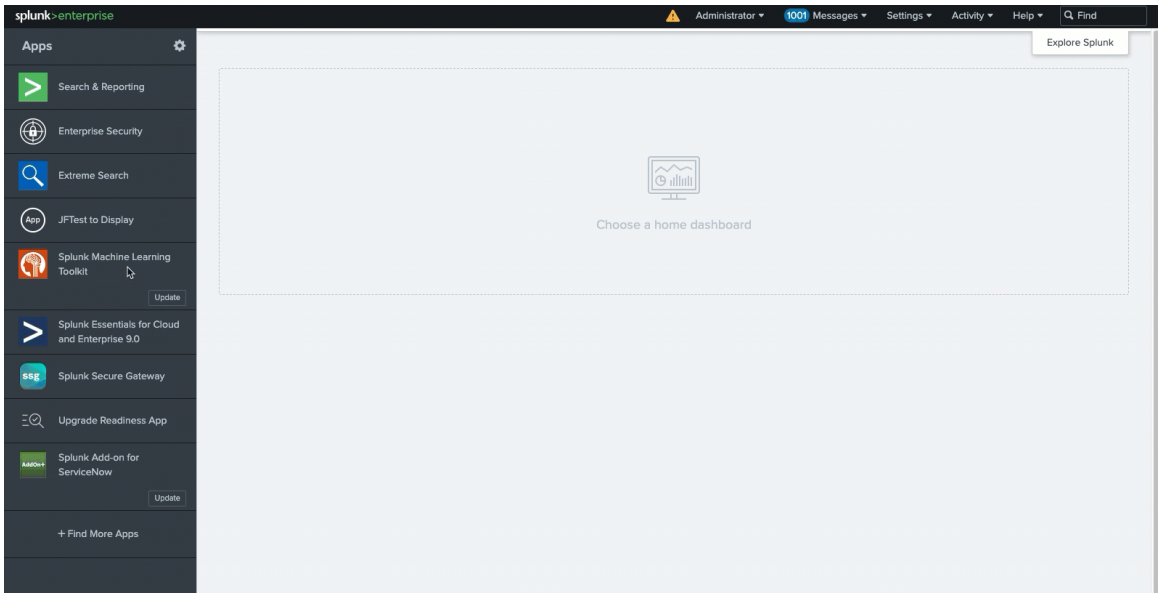
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de autenticação	Opção para selecionar o tipo de autenticação. Você pode selecionar **Autenticação básica ou AutenticaçãoOAuth 2.0**. ◦ Se você estiver usando o Nome de usuário e a Senha da conta de API para configuração, habilite a caixa de seleção **Autenticação básica**. O padrão é desabilitado. ◦ Se você estiver usando a autenticação OAuth 2.0 para a configuração, marque a caixa de seleção **Autenticação OAuth 2.0**. O padrão é desabilitado.
Autenticação básica	
Nome de usuário	Nome de usuário que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Senha	Senha que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Confirmar senha	Alugue a senha para confirmá-la.
Autenticação OAuth 2.0	
ID de cliente	ID de cliente do aplicativo criado no servidor da ServiceNow. Para obter informações sobre como obter o ID de cliente, consulte Configurar o Registro de aplicações na instância da ServiceNow
Segredo do cliente	Segredo do cliente do app criado no servidor. Para obter informações sobre como obter o segredo do cliente, consulte Configurar o Registro de aplicações na instância da ServiceNow
URL de redirecionamento	A URL para a qual será redirecionado. Você pode copiar e colar este URL no URL de redirecionamento do registro da ServiceNow. Para obter informações, consulte Configurar o Registro de aplicações na instância da ServiceNow
Configuração de proxy opcional	
URL do proxy	URL do proxy para seu console secundário [Splunk Enterprise Security ou instância secundária Splunk Cloud.
Porta	Endereço da porta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de usuário	Nome de usuário que você criou para a conta de proxy no console secundário Splunk Enterprise Security.
Senha	Senha que você criou para a conta de proxy no console secundário Splunk Enterprise Security.
Confirmar senha	Alugue a senha para confirmá-la.



10. Opcional: Selecione a guia **Splunk secundário**.
11. Opcional: No formulário, preencha os campos.

Campo	Descrição
Rótulo de ação de fluxo de trabalho	(Optional) Nome do console secundário Splunk Enterprise Security ou da instância secundária Splunk Cloud usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `SplunkES2`.
URL	URL do console secundário Splunk Enterprise Security ou da instância secundária Splunk Cloud. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Endpoint	Endpoint para o console secundário Splunk Enterprise Security ou a instância secundária Splunk Cloud.
Tipo de autenticação	Opção para selecionar o tipo de autenticação. Você pode selecionar **Autenticação básica ou AutenticaçãoOAuth 2.0**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Se você estiver usando o Nome de usuário e a Senha da conta de API para configuração, habilite a caixa de seleção **Autenticação básica**. O padrão é desabilitado. ◦ Se você estiver usando a autenticação OAuth 2.0 para a configuração, marque a caixa de seleção **Autenticação OAuth 2.0**. O padrão é desabilitado.
Autenticação básica	
Nome de usuário	Nome de usuário que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Senha	Senha que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Confirmar senha	Alugue a senha para confirmá-la.
Autenticação OAuth 2.0	
ID de cliente	ID de cliente do aplicativo criado no servidor da ServiceNow.
Segredo do cliente	Segredo do cliente do app criado no servidor da ServiceNow.
URL de redirecionamento	A URL para a qual será redirecionado. Você pode copiar e colar este URL no URL de redirecionamento do registro da ServiceNow.
Configuração de proxy opcional	
URL do proxy	URL do proxy para seu console secundário [Splunk Enterprise Security ou instância secundária Splunk Cloud.
Porta	Endereço da porta.
Nome de usuário	Nome de usuário que você criou para a conta de proxy no console secundário Splunk Enterprise Security.
Senha	Senha que você criou para a conta de proxy no console secundário Splunk Enterprise Security.
Confirmar senha	Alugue a senha para confirmá-la.

12. Selecione a guia **Nível de registro em log**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

13. No formulário, preencha os campos.

Campo	Descrição
Nível de log	O nível de logs de emissão de relatórios gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ◦ **informações** ◦ **error** ◦ **aviso** ◦ **depurar** Por padrão, o valor é **info**.

14. Clique em **Salvar**.
    Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, os botões **Atualizar** e **Excluir** são exibidos, conforme mostrado na figura a seguir.

    Nota: Você precisa usar somente a Autenticação básica ou a Autenticação OAuth 2.0. Habilite uma das autenticações e insira os detalhes de autenticação correspondentes. Habilitar ambos exibirá um erro.

    Depois de validada e enviada com sucesso, cada configuração de servidor de Ingestões de eventos Splunk é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista Mostrar configurações, clique em **Sim**.

Configurar o Registro de aplicações na instância da ServiceNow

Registre a aplicação com a instância para usar a autorização do OAuth.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **OAuth de Sistema** > **Registro de aplicações**.
2. Clique em **Nova**.
3. Clique em **Criar um endpoint da API do OAuth para clientes externos**.
4. No formulário, preencha os campos.

Campo	Descrição
Nome	Um nome exclusivo que identifica a aplicação para o qual você solicitou acesso ao OAuth.
ID de cliente	(Somente leitura) O ID exclusivo gerado automaticamente da aplicação. A instância usa o ID de cliente ao solicitar um token de acesso.

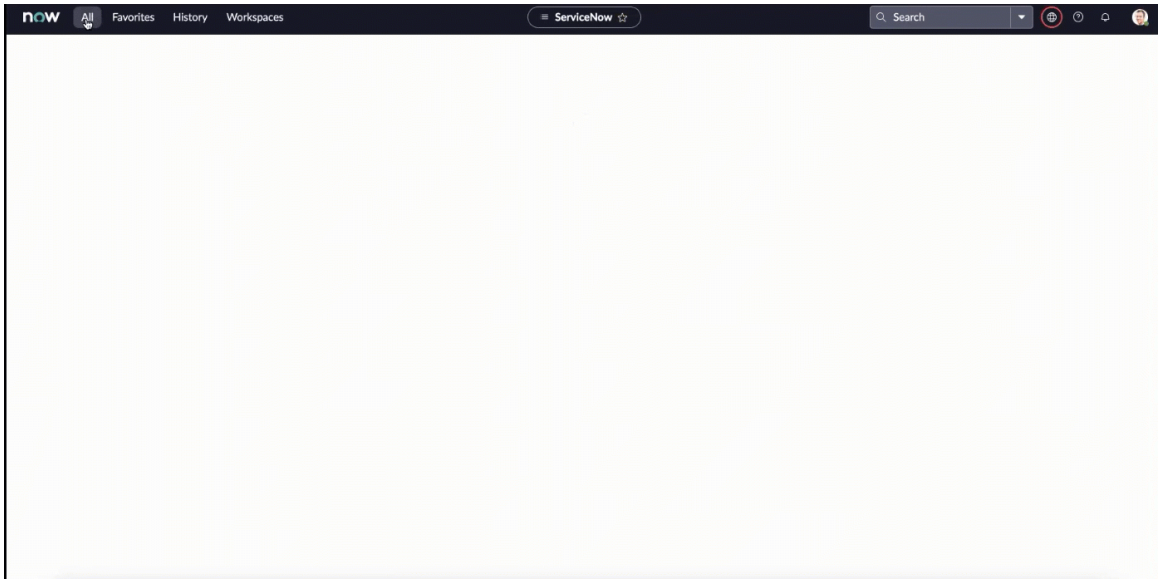
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Segredo do cliente	A cadeia de caracteres do segredo compartilhado que a instância e a aplicação cliente ou site usam para autorizar as comunicações entre si. A instância usa o segredo do cliente ao solicitar um token de acesso. Deixe este campo em branco para que a instância gere automaticamente um segredo do cliente. Para exibir segredos de cliente existentes, clique no ícone do cadeado.
URL de redirecionamento	O URL de retorno de chamada para o qual o servidor de autorização é redirecionado. Insira quantos URLs forem necessários para todos os consumidores de token possíveis. A instância corresponde ao URL da solicitação de entrada para um dos URLs de redirecionamento. Se nenhuma correspondência for feita, a instância usará o primeiro URL de redirecionamento.
URL do logotipo	O URL que contém uma imagem a ser usada como logotipo da aplicação. O logotipo aparece na página de aprovação quando o usuário recebe uma solicitação para conceder acesso a uma aplicação cliente a um recurso restrito na instância.
Aplicação	O nome da aplicação.
Acessível de	Defina o escopo da aplicação. Selecione uma das seguintes propriedades: ◦ **Todos os escopos da aplicação** ◦ **Somente este escopo da aplicação**
Ativo	Marque a caixa de seleção para ativar o registro da aplicação.
Tempo de vida do token de atualização	O número de segundos que um token de atualização é válido. A instância usa o valor de tempo de vida ao solicitar um token de atualização. Por padrão, os tokens de atualização expiram em 100 dias (8.640.000 segundos).
Tempo de vida do token de acesso	O número de segundos que um token de acesso é válido. A instância usa o valor de tempo de vida ao solicitar um token de acesso. Por padrão, os tokens de acesso expiram em 30 minutos (1800 segundos).
Comentários	Informações adicionais a serem associadas à aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
6. Clique em **Enviar**.

Comandos de pesquisa manual

Os comandos de pesquisa manual são inseridos em qualquer janela de pesquisa. Você pode criar um incidente ou evento de segurança. Após o comando, há pares de nomes de campo e valores usados para criar o registro desejado.

Evento de segurança

O comando de evento de segurança, **snsecevent**, cria um evento em ServiceNow com a classificação de segurança.

Esses eventos podem ser revisados por conta própria ou as regras de alerta em ServiceNow ou ações manuais podem transformar um evento ou coleção de eventos em um incidente de segurança.

Se o evento se tornar um incidente de segurança e cada parâmetro for enviado para o evento, esses dados serão usados para preencher o incidente de segurança da seguinte forma:

Evento de segurança

Nome do Parâmetro	Obrigatório	Uso	Usar no incidente de segurança
node	Sim	O nó representa o servidor ou o item de configuração do evento. O ideal é que este nó seja mapeado para um IC existente em ServiceNow.	Usar no incidente de segurança
tipo	Sim	A categoria do evento.	Descrição resumida

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Evento de segurança

Nome do Parâmetro	Obrigatório	Uso	Usar no incidente de segurança
recurso	Sim	O item de configuração.	Descrição resumida
origem	Não	A origem desses dados. Por padrão, o servidor Splunk gera os dados.	Log de atividades
external_url	Não	O URL de detalhamento a ser usado em ServiceNow para retornar aos dados do Splunk sobre este evento. Por padrão, este URL contém o link de resultado de qualquer alerta ou um link para a página de pesquisa padrão do Splunk.	URL externo acessado por meio do botão **Detalhamento** no formulário de Incidente de segurança
time_of_event	Não	A hora em que o evento foi registrado no Splunk.	N/D
Todos os outros valores (categoria, subcategoria no exemplo)	Não	Qualquer campo que não faça parte do campo de informações no evento. Se um incidente de segurança for criado, ele será usado.	Se o campo existir e não estiver preenchido, o incidente de segurança usará esse valor. Por exemplo, a categoria aprovada pelo Evento se torna a categoria do novo incidente de segurança. Se não existir um campo com este nome, o valor será colocado no log de atividades.

Incidente de segurança

O comando Incidente de segurança, **snsecincident**, cria um incidente de segurança em sua instância ServiceNow.

Incidente de segurança

Parâmetro	Obrigatório	Uso
short_description	Sim	Uma descrição resumida de uma linha do incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança

Parâmetro	Obrigatório	Uso
categoria	Não	A categoria do incidente de segurança. Se esta categoria não existir, ela será criada.
subcategoria	Não	A subcategoria. Se esta subcategoria não existir, ela será criada.
cmdb_ci	Não	O item de configuração do incidente de segurança. O ideal é que este item seja mapeado para um IC existente em ServiceNow.
descrição	Não	A descrição mais longa e detalhada do incidente.

Existem muitas colunas úteis possíveis - qualquer coisa no mapa de transformação de Incidente de segurança pode ser usada. Se novas colunas forem adicionadas ao incidente de segurança, elas também serão usadas, desde que estejam no mapa de transformação. Algumas colunas úteis: local, prioridade, assign_group, assigned_to, afetado_user, ataque_vetor e watch_list.

Ações de evento do Splunk

Ao revisar os logs do Splunk, você pode criar rapidamente eventos e incidentes de segurança a partir de qualquer item no log usando as Ações de evento.

Clicar em uma dessas ações cria um comando de pesquisa manual preenchido com os dados na entrada de log e o executa para gerar o novo registro.

Essas ações são facilmente configuradas para adicionar campos em seus dados normalizados. No Splunk, usando **Configurações** > **Campos** > **Ações de Fluxo de Trabalho**, você pode selecionar e editar qualquer uma dessas ações usando os campos de pesquisa manual.

Você pode escolher onde a ação é mostrada, para quais campos e modificar a cadeia de caracteres de pesquisa que contém um comando de pesquisa para criar seu registro.

Alertas do Splunk de registro único

Em qualquer alerta, você pode especificar eventos de segurança ou incidentes de segurança a serem criados quando o alerta for disparado.

Abra ou crie seu alerta e, ao editar ações, selecione o tipo de registro desejado e preencha a caixa de diálogo do alerta.

Alertas do Splunk de campo personalizado com vários registros

Os alertas de vários registros (definidos usando as ações de gatilho **Criar vários incidentes de segurança da ServiceNow** e **Criar vários eventos de segurança da ServiceNow**) podem criar automaticamente registros com qualquer conjunto de campos compatível.

Eles agem de forma diferente das outras ações de alerta, pois os valores padrão são fornecidos. No entanto, a maioria dos dados vem do resultado da pesquisa desse alerta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Nas versões anteriores do complemento e nesta documentação, os alertas com script eram compatíveis. Esse recurso foi descontinuado e substituído por estas instruções.

Criar um alerta do Splunk de vários registros e de campo personalizado

Para criar um alerta do Splunk de vários registros com campos personalizados, você deve criar uma pesquisa projetada para corresponder às colunas da ServiceNow que deseja preencher.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegue até **Pesquisar**.
2. Na caixa **Pesquisar**, crie uma pesquisa que gere seus dados de registro. Consulte os exemplos para obter os critérios de pesquisa recomendados.
3. Clique **em Salvar como** e selecione **Alerta**.
4. Defina o nome, as permissões e a programação, conforme necessário.
5. Clique **em Adicionar ações**.
6. Faça uma das seguintes seleções.
   - Para criar um evento por resultado da pesquisa, selecione **Criar vários eventos de segurança da ServiceNow**.
   - Para criar um incidente por resultado da pesquisa, selecione **Criar vários incidentes de segurança da ServiceNow**.
7. Defina quaisquer padrões, conforme necessário. Se o campo no resultado da pesquisa estiver em branco ou ausente, os padrões serão usados. Se houver um valor no resultado, os padrões serão substituídos.

Exemplos de alertas do Splunk de vários registros e de campo personalizado

Ao criar vários alertas do Splunk de registro com campos personalizados, você precisa definir critérios de pesquisa para gerar dados de alerta. São mostrados exemplos de critérios de pesquisa para incidentes e eventos de segurança.

Pesquisa de incidentes de segurança

Para um incidente de segurança, esses critérios criam uma pesquisa para preencher colunas na tabela de incidentes de segurança.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Pesquisa de eventos de segurança

Para um evento de segurança, esta é a mesma pesquisa, mas preenche os campos de Evento. Se este evento for transformado em um incidente de segurança e todos os campos que não existirem no evento forem preenchidos, eles serão transferidos para o incidente de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

segurança. Caso contrário, eles permanecerão no campo de informações adicionais do evento e do alerta.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Nota: Os critérios de pesquisa usados adicionarão o mesmo número de registros encontrados na pesquisa. Pode adicionar 5 ou 10.000.000.000 de registros. Portanto, este NÃO é um método recomendado para a transferência em massa de dados. A intenção deste método é adicionar um registro por chamada REST à instância da ServiceNow.

Relatório de erros do Splunk

Sempre que ocorre um problema de conectividade com sua instância da ServiceNow, um erro é registrado no Splunk com informações que descrevem o problema.

As mensagens de erro são armazenadas em um novo índice chamado **servicenow** com o tipo de origem **servicenow**.

Para pesquisar logs de erro, certifique-se de especificar o índice da **ServiceNow** em sua pesquisa. Como alternativa, consulte a documentação atual do Splunk para saber como adicionar o novo índice da **ServiceNow** aos índices de pesquisa padrão.

Splunk Enterprise Event Ingestion integração para Operações de segurança por ServiceNow

A integração de dados de alerta e evento Splunk Enterprise com o produto Security Incident Response (SIR) permite que os analistas de incidentes de segurança coletem e processem logs de segurança e dados de eventos relacionados.

Visão geral

Os dados são coletados em tempo real e usados por analistas para identificar e relatar possíveis ameaças cibernéticas. Os eventos de segurança coletados podem ser processados em alertas acionados que são ingeridos automaticamente com esta integração. Além disso, os eventos de segurança individuais podem ser encaminhados manualmente sob demanda da interface de pesquisa e emissão de relatórios Splunk EnterpriseSecurity Incident Response] para o produto do Now Platform para criar incidentes de segurança. Você pode recuperar eventos notáveis da pesquisa Splunk Enterprise com a configuração de cluster de cabeçalho de pesquisa. Você pode fazer isso usando a URL e a porta de API de qualquer cabeçalho de pesquisa que faça parte do cluster.

Esta integração fornece a um analista do centro de operações de segurança (SOC) visibilidade para eventos e dados de alerta relacionados. Esses dados podem ser integrados a Now Platform Security Incident Response (SIR) incidentes de segurança para investigação e correção adicionais. Perfis para Splunk alertas ingeridos em andamento e eventos encaminhados são criados em sua instância Now Platform. Esses perfis personalizam como diferentes Splunk campos de alerta e evento são exibidos em SIR incidentes de segurança. É fornecido um mapeamento padrão de campos de alerta que pode ser editado e aumentado para atender às necessidades específicas do cliente.

Principais recursos

Esta integração inclui os seguintes recursos principais:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Crie vários perfis de ingestão de alertas para criar incidentes de segurança SIR para tipos específicos de ameaças, como phishing e malware.
- Crie vários perfis de evento para encaminhamento de eventos sob demanda a partir do console Splunk para criar incidentes de segurança SIR.
- Mapeamento de arrastar e soltar de Splunk valores de campo de alerta e evento para campos de incidente de segurança SIR associados.
- Uma visualização do layout de incidente de segurança SIR com base em exemplos de alertas ou eventos para validar a configuração do perfil.
- Ingerir alertas históricos, bem como alertas futuros em andamento em intervalos configuráveis.
- Agregue eventos ou alertas a incidentes de segurança SIR existentes com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.

Versões da Now Platform compatíveis

O plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações.

As Operações de segurança aplicações a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Estrutura de integração de segurança
2. Security Support Common
3. Orquestração de suporte de segurança
4. Resposta a incidentes de segurança

Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

ServiceNow Complementos

O ServiceNow Complemento de ingestão de eventos das Operações de segurança para Splunk Enterprise será necessário somente se você preferir encaminhar eventos manualmente do console [Splunk Enterprise para a instância Now Platform. Este ServiceNow addon está disponível em splunkbase .

Este ServiceNow Complemento de ingestão de eventos das Operações de segurança para a aplicação Splunk Enterprise no splunkbase não é necessário para a ingestão automatizada de alertas compatível com a integração.

Versões compatíveis com Splunk

Esta integração é compatível com a versão 6.0 ou posterior do Splunk Enterprise. A integração também oferece suporte ao serviço Splunk Enterprise Cloud.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao serviço Splunk se o servidor Splunk estiver implantado em sua

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

rede corporativa. Se você estiver usando o serviço Splunk Cloud, um MID Server não será necessário. Para obter mais informações sobre MID Servers, consulte MID Server .

Arquitetura de integração e conexão de sistemas

Para obter mais informações sobre a arquitetura da integração, incluindo termos-chave e detalhes da conexão de sistemas externos, consulte Arquitetura de integração e conexão de sistemas externos para a integração Splunk Enterprise Event Ingestion.

Check-list

Para obter uma check-list imprimível desses tópicos, consulte Check-list para a integração de ingestão de eventos notáveis Splunk Enterprise Security. Você pode usar essa lista para monitorar o andamento enquanto trabalha nas tarefas da integração.

As imagens usadas nos tópicos a seguir foram geradas para a versão Kingston do Now Platform. Para obter informações sobre a interface do usuário do San Diego, consulte Gerenciar ameaças à segurança usando o Espaço do analista de segurança.

Os tópicos a seguir estão numerados. Siga os tópicos listados abaixo na ordem em que são apresentados para uma instalação e configuração tranquilas da aplicação.

Configure sua instância Now Platform® para a integração Splunk Enterprise Event Ingestion

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação a partir do ServiceNow Store.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Procedimento

1. Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.

   As funções a seguir são necessárias para a instalação, configuração e uso da integração em sua instância Now Platform®.

   - Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin).
   - Se você quiser encaminhar eventos manualmente de Splunk Enterprise para esta integração, um usuário com a função de administrador Now Platform® atribuirá um usuário com a função (sn_sec_splunk_v2.api_account_access) no Now Platform®. Esta função permite que um usuário com a função de administrador Splunk Enterprise acesse a API no Now Platform® que é necessária para o encaminhamento manual de eventos para esta integração.

     A função (sn_sec_splunk_v2.api_account_access) não será necessária para a integração se você estiver ingerindo alertas automaticamente de Splunk Enterprise para sua instância Now Platform®.

   - Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Nomeia, cria e edita perfis de alerta e evento.
- Seleciona e mapeia valores de alertas e eventos para Now Platform® incidentes de segurança.
- Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração.
- Programa a ingestão de alertas contínuos.
- Atribui a função de analista de incidentes de segurança (sn_si.analyst).
- Usuários com sn_si.analyst trabalham com incidentes de segurança.

Para obter mais informações sobre funções e como atribuir funções a usuários, consulte Gestão de funções .

2. Verifique se você está usando a versão 6.0 ou posterior da API Splunk.

   Se você tiver acesso ao console Splunk Enterprise, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.

3. Verifique se você instalou e configurou um MID Server.

   Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço Splunk se o servidor Splunk estiver implantado em sua rede corporativa. Para obter mais informações sobre MID servers, consulte MID Server

   Se você estiver usando o serviço Splunk Cloud, um MID Server não será necessário.

4. Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas.

   O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração.

   Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas.

   a. Resposta a incidentes de segurança

   b. Estrutura de integração de segurança

   c. Security Support Common

   d. Orquestração de suporte de segurança

   Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação Splunk Enterprise Event Ingestion da ServiceNow Store para a integração. Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion.

Se você não salvou pesquisas no console Splunk Enterprise para ingestão ou se estiver executando a configuração inicial desta integração no console Splunk Enterprise e no produto Operações de segurança da sua instância Now Platform®, consulte Salvar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion para obter mais informações.

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para a integração, consulte Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos Splunk Enterprise para obter mais informações.

Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion

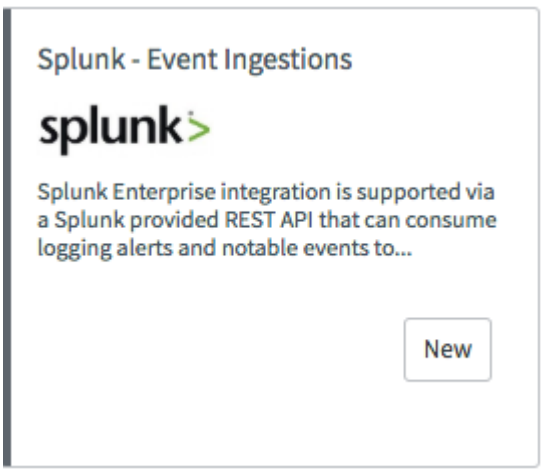
Antes de executar a integração em sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Operações de segurança em sua instância Now Platform®.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Se você não instalou a aplicação [Splunk Enterprise Event Ingestion de ServiceNow Store para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Splunk Ingestões de eventos.
3. Para configurar a aplicação, clique em **Novo**.



4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo Configuração de ingestões de eventos exibida, preencha os campos.

Campo	Descrição
Nome	Nome do console [Splunk Enterprise ou instância Splunk Cloud usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `HQ-EUA`ou `HQ EUA`.

Tradução automática

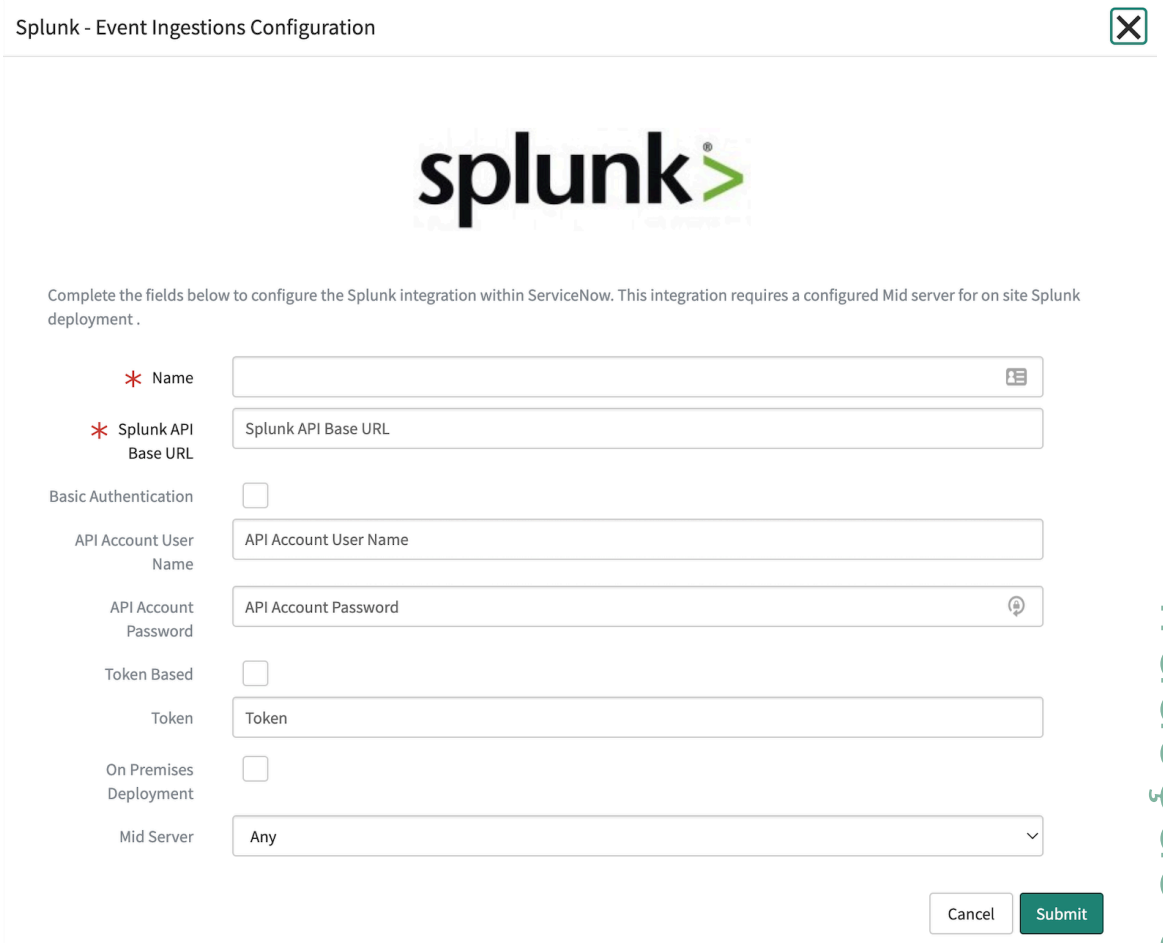
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL base da API Splunk	URL do console [Splunk Enterprise ou instância Splunk Cloud.
Autenticação básica	O padrão é desabilitado. Se você estiver usando o nome de usuário da conta da API e a senha da API para configuração, marque a caixa de seleção.
Nome de usuário da conta da API	Nome de usuário que você criou para sua conta de usuário individual no console do Splunk Enterprise.
Senha da API	Senha que você criou para sua conta de usuário individual no console Splunk Enterprise.
Baseado em token (disponível a partir da versão 12.0.0)	Autenticação baseada em token que você criou para sua conta de usuário de API no console Splunk Enterprise.
Token	Token que você criou para sua conta de usuário de API no console Splunk Enterprise.
MID Server	MID Server específico que está configurado em seu ambiente. Somente MID Servers ativos e validados estão disponíveis nesta lista de seleção.
Implantação no Local	O padrão é desabilitado. Se você estiver usando a versão baseada em nuvem do Splunk Enterprise, verifique se a caixa de seleção está desmarcada. Se esta opção estiver habilitada, a lista de seleção do MID Server será exibida. Se você estiver usando uma versão local do Splunk Enterprise, siga estas etapas para selecionar um MID Server. **a.** Marque a caixa de seleção. Uma lista de seleção é exibida. O padrão é **Qualquer**. **b.** Selecione **Qualquer** somente se este MID Server estiver configurado para a integração Splunk Enterprise Event Ingestion. **c.** Na lista de seleção, selecione o Now Platform® MID Server que você configurou em sua instância para esta integração específica.

A figura a seguir é um exemplo de um formulário preenchido para uma configuração de uma versão local do Splunk Enterprise com um MID Server.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cada alerta Splunk Enterprise que você ingere do console Splunk Enterprise requer um perfil de evento exclusivo em sua instância Now Platform®. No entanto, a origem que você configura no formulário Configuração de ingestões de eventos pode ser reutilizada para vários perfis Now Platform®, desde que cada perfil ingere alertas acionados Splunk exclusivos.

6. Clique em **Enviar**.
   Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, os botões **Configurar** e **Excluir** são exibidos, conforme mostrado na figura a seguir.

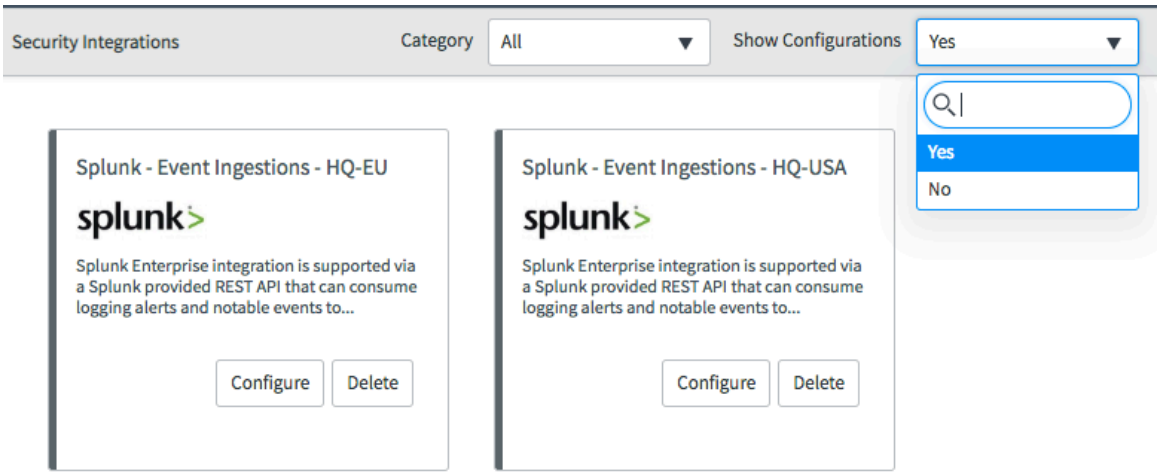
   Nota: Você precisa usar somente a Autenticação básica ou a Autenticação baseada em token. Habilite uma das autenticações e insira os detalhes de autenticação correspondentes. Habilitar ambos exibirá um erro.

   Depois de validada e enviada com sucesso, cada configuração de servidor de Ingestões de eventos Splunk é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.



Trouble?

Se uma mensagem de erro for exibida após você clicar em **Enviar**, insira suas informações novamente e clique em **Enviar**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Definir configurações de ingestão de eventos do Splunk Enterprise

Use as configurações de ingestão de eventos do Splunk Enterprise para modificar as configurações predefinidas e seus valores de acordo com seus requisitos.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Splunk Integration** > **Configurações de integração do Splunk**.
2. No formulário, preencha os campos.

Configurações de integração do Splunk

Campo	Descrição
Número máximo de alertas a serem exibidos na criação do perfil	Opção para definir o número máximo de alertas que você deseja exibir ao criar um perfil de evento. Por padrão, o valor é definido como 500.
Número máximo de incidentes de segurança a serem criados em um dia	Opção para definir o número máximo de incidentes de segurança que podem ser criados em um dia. Por padrão, o valor é definido como 1000.

Tradução automática

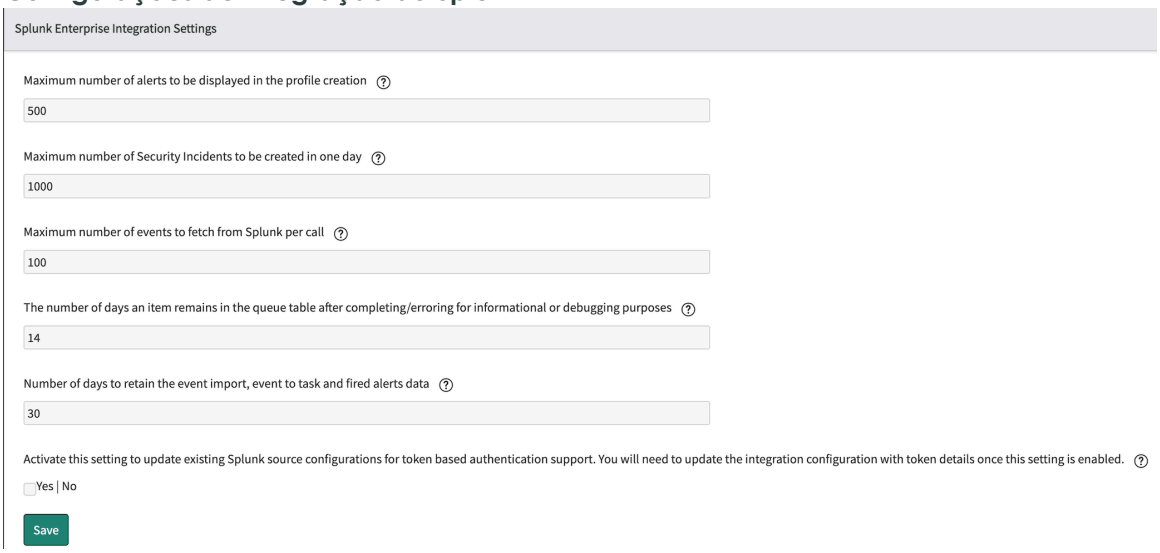
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Número máximo de eventos a serem buscados do Splunk por chamada	Opção para definir o número máximo de eventos a serem recuperados do Splunk para cada chamada. Por padrão, o valor é definido como 100.
O número de dias que um item permanece na tabela da fila após a conclusão/erro para fins de informação ou depuração	Opção para definir o número de dias para um item permanecer na tabela de fila após a conclusão ou a ocorrência de erro devido a informações ou fins de depuração. Por padrão, o valor é definido como 14.
Número de dias para reter os dados de importação de eventos, eventos para tarefas e alertas disparados	Opção para determinar o número de dias em que você deseja reter a importação de eventos, o evento para tarefa e os dados de alertas disparados. Por padrão, o valor é definido como 30.
Ative esta configuração para atualizar as configurações de origem do Splunk existentes para suporte à autenticação baseada em token. Você precisará atualizar a configuração de integração com detalhes do token quando essa configuração estiver habilitada.	Opção para atualizar a configuração de origem do Splunk existente para suporte à autenticação baseada em token de uma versão existente. **Nota:** Depois de fazer upgrade para a nova versão, o campo de token ficará indisponível. Você precisa habilitar esta configuração para obter a autenticação baseada em token e, em seguida, atualizar a configuração de integração com os detalhes do token. Por padrão, o valor é definido como Não.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de integração do Splunk



3. Clique em **Salvar**.

Criar e nomear um perfil de evento para a integração Splunk Enterprise Event Ingestion

Crie um perfil de evento em sua instância Now Platform e determine quais alertas Splunk criam incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Antes que Now Platform Security Incident Response (SIR) incidentes de segurança sejam criados a partir de alertas ingeridos, os valores de campos de alertas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será exibido.

De uma perspectiva de integração usando as APIs disponíveis, os eventos Splunk são encaminhados individual e manualmente como eventos discretos ou são combinados em alertas acionados que são ingeridos automaticamente no ambiente Operações de segurança da sua instância Now Platform. Os fluxos de trabalho de integração ingerem diferentes tipos de alertas, como tentativas de acesso não autorizado e malware, por exemplo.

Esses alertas são ingeridos com base nos perfis que você configura no ambiente Operações de segurança da sua instância. Todos os alertas são ingeridos inicialmente para um tipo de alerta configurado em um perfil. Os alertas ingeridos podem ser filtrados para especificar quais alertas criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para alertas identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de alertas ingeridos, os valores de campos individuais nos alertas filtrados são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização.

Os nomes de alerta para perfis de evento em sua instância Now Platform devem ser exclusivos e só podem ser mapeados para um perfil de evento ativo por vez. Estes são os nomes de alertas acionados que você configurou no serviço Splunk como parte da configuração da integração. Para obter mais informações sobre como configurar alertas no ambiente Splunk Enterprise, consulte Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Now Platform ingere alertas específicos usando os fluxos de trabalho da integração. Todos os alertas que atendem aos critérios de seleção no console empresarial Splunk são ingeridos inicialmente na instância Now Platform.

Um perfil em seu Now Platform é um encapsulamento de um alerta [Splunk no console empresarial Splunk. Há um relacionamento de um para um entre alertas que são ingeridos com um perfil e conexões com o console do Enterprise Splunk : um alerta para uma conexão. Há uma única conexão https para um cabeçalho de pesquisa no console Splunk Enterprise. Vários alertas podem vir de um único cabeçalho de pesquisa. Se você se conectar a vários cabeçalhos de pesquisa no console Splunk Enterprise, deverá criar vários perfis na instância Now Platform para ingerir esses alertas.

Etapas para criar perfis para ingestão de alertas programada

Procedimento

1. Para criar um perfil de evento para um alerta, na sua instância Now Platform, navegue até **Splunk Integration** > **Perfil de eventos do Splunk**.
2. Se o formulário Splunk de perfil de evento não for exibido, clique em **Nome** na barra de andamento.
3. Clique em **Nova**.
4. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

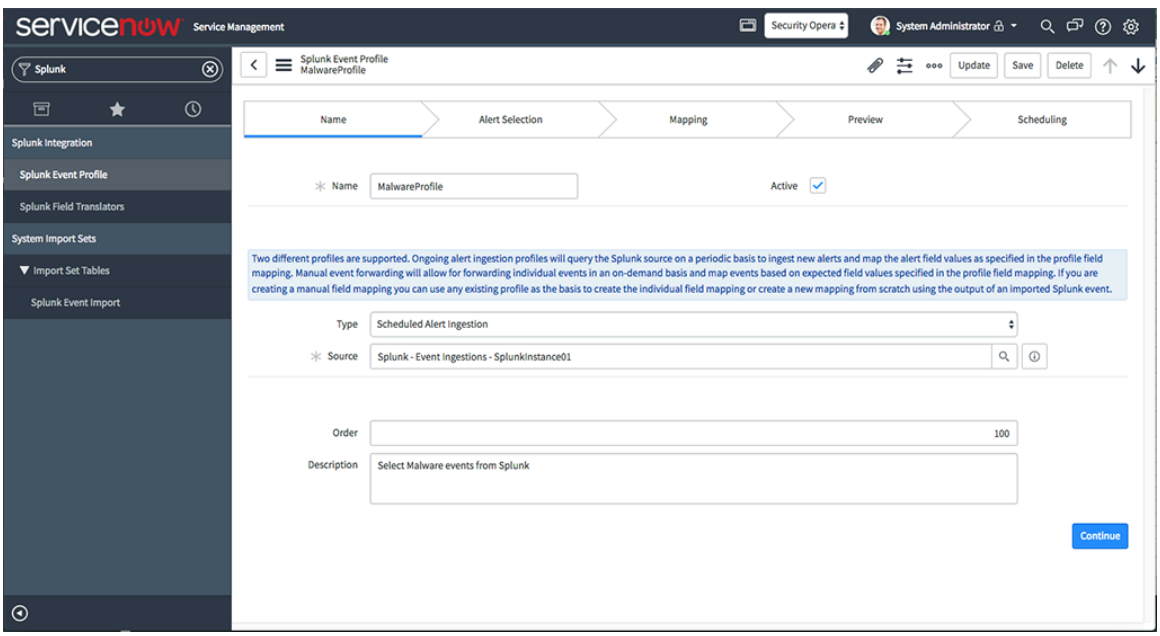
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, os nomes de perfil duplicados não serão salvos. Os nomes de perfil em sua instância Now Platform devem ser exclusivos.
Ativo	A caixa de seleção está desmarcada por padrão. A opção Ativa está desabilitada e não está disponível para seleção até que você conclua todas as etapas de configuração do perfil e clique em **Concluir**.
Tipo	Selecione o tipo de perfil na lista de seleção. ◦ Ingestão de alertas programada - Este tipo de perfil oferece suporte a alertas acionados que são ingeridos em uma programação que você configura. Preencha os campos e clique em **Continuar** para prosseguir para a etapa de Seleção de alerta do perfil. ◦ Encaminhamento manual de eventos - Este tipo de perfil oferece suporte a eventos individuais que são encaminhados manualmente do console Splunk En-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	terprise sob demanda. Consulte as etapas a seguir para preencher o formulário para esses tipos de perfis.
Tipo de Origem	Splunk servidor ou extremidade da pesquisa que você configurou para ingerir alertas. Se você tiver vários servidores Splunk configurados, selecione o servidor apropriado para os tipos de alerta que você planeja ingerir para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração no padrão. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem as mesmas condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido para um alerta programado.



5. Para um perfil com um alerta programado, escolha uma opção para continuar com a configuração do perfil.

Opção	Descrição
Continuar	Salve o perfil e avance para a etapa de Seleção de alerta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Atualizar	Salve atualizações neste perfil e retorne à lista Splunk de Perfis de eventos.
Salvar	Salve este perfil e permaneça na página.
Excluir	Exclua este registro de perfil e retorne à lista Splunk de Perfis de eventos.

Etapas para criar perfis para encaminhamento manual de eventos

6. Para criar um perfil que ofereça suporte ao encaminhamento manual de eventos, siga estas etapas.

   Para eventos que você encaminha sob demanda do console empresarial Splunk, você pode basear o mapeamento de campo individual em qualquer perfil existente. Como alternativa, você pode criar uma nova grade de mapeamento para dados de anexo exportados. Os eventos encaminhados manualmente não são programados no perfil de eventos.

   a. Se ainda não estiver selecionado, na lista de seleção do campo Tipo, selecione **Encaminhamento manual de eventos**.

   b. No campo Opção de mapeamento exibido, na lista de seleção, escolha uma opção de mapeamento para continuar.

      Consulte as imagens e tabelas a seguir para obter mais informações sobre as opções de mapeamento disponíveis na lista de seleção Opções de mapeamento.

Criar nova opção de mapeamento de campo

Opção ou campo	Descrição
Criar nova opção de mapeamento de campo	Novo mapeamento de campo para seu evento. Se você não tiver um mapeamento de campo existente semelhante ao perfil que

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	está criando, selecione esta opção para criar um novo mapa.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos os eventos Splunk. O padrão é limpo (desabilitado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. Este é o único perfil ativo e usado para cada mapeamento de campo de evento Splunk para um incidente de segurança SIR. Um perfil se ajusta a todos os eventos encaminhados. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Tipo de origem	Splunk servidor. Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, a opção Tipo de origem permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base no tipo de origem Splunk. Se você quiser gerenciar eventos de log do firewall de forma diferente dos eventos de detecção de endpoint, e eles tiverem diferentes tipos de origem Splunk, você poderá criar perfis de evento diferentes com base nos tipos de origem para atender a esse requisito.
Ordem	O padrão é 100. Deixe esta configuração no padrão. Se você criou um grande número de perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para um perfil com um novo mapeamento de campo, verifique se você inseriu um valor no campo Tipo de origem e clique em **Continuar** para prosseguir para a etapa de mapeamento da configuração.

Para um perfil com um mapeamento de campo existente, consulte a figura e a tabela a seguir para obter mais informações.

Selecione o perfil existente para a opção de mapeamento de campo

Selecione o perfil existente para a opção de mapeamento de campo

Opção ou campo	Descrição
Selecionar perfil existente para mapeamento de campo	Um mapeamento de campo existente para o seu evento. O campo Copiar do perfil é exibido. Siga estas etapas para copiar um mapeamento de campo existente para este perfil. **i.** À esquerda do campo Copiar do perfil exibido, clique no ícone de pesquisa. **ii.** Na lista Splunk Perfis de eventos exibida, clique no nome do perfil que tem o mapa que você deseja copiar. O nome do perfil é exibido no campo Copiar do perfil.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos os eventos Splunk. O padrão é limpo (desabilitado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. Este perfil é o único que está ativo. Ele é usado para cada mapeamento de campo de evento Splunk para um incidente de segurança SIR. Um perfil se ajusta a todos os eventos encaminhados. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Tipo de origem	Splunk servidor. Este campo não estará disponível se a opção de perfil padrão estiver selecionada. Se disponível, a opção Tipo de origem permite o mapeamento de campo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	de evento exclusivo para campos de incidente de segurança com base no tipo de origem Splunk. Se você quiser gerenciar eventos de log do firewall de forma diferente dos eventos de detecção de endpoint, e eles tiverem diferentes tipos de origem Splunk, você poderá criar perfis de evento diferentes com base nos tipos de origem para atender a esse requisito.
Ordem	O padrão é 100. Deixe esta configuração no padrão. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Na parte inferior do formulário para selecionar um mapeamento existente para o seu perfil, clique em **Concluir** para concluir a configuração do perfil.

O que Fazer Depois

Você concluiu com sucesso as etapas para criar perfis para alertas programados e encaminhamento manual de eventos. Para perfis de encaminhamento manual de eventos, você concluiu a configuração do perfil. A próxima etapa é carregar os dados do anexo na etapa de mapeamento.
Para perfis de alertas programados, a próxima etapa é selecionar alertas para ingestão automática.

Selecione alertas programados para a integração Splunk Enterprise Event Ingestion

Depois de criar um perfil para um alerta programado, selecione um alerta Splunk para este perfil que você deseja mapear para um incidente de segurança Now Platform Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba os alertas disponíveis em sua instância Now Platform para que você saiba quais valores de campo estão disponíveis para mapeamento. Selecione um alerta para verificar se você recebe os resultados esperados no layout de formulário básico antes de mapear os valores para campos em SIR incidentes de segurança. Você só pode selecionar um alerta da lista neste formulário.

Tradução automática

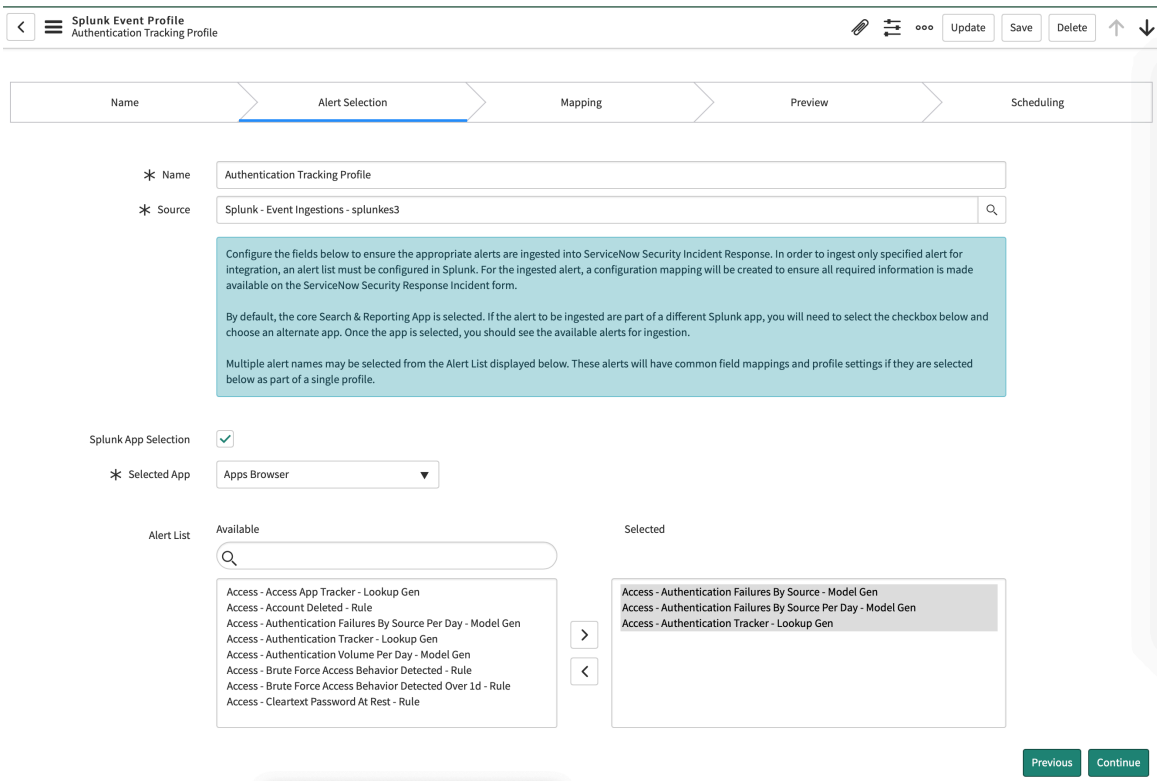
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a página Seleção de alerta não for exibida, selecione-a na barra de andamento para exibi-la.
   Por padrão, o aplicativo principal de pesquisa e emissão de relatórios está selecionado.
2. Se o alerta a ser ingerido fizer parte de um app Splunk diferente, selecione **Seleção de app Splunk** e escolha seu app Splunk na lista **App selecionada**.
3. Na **Lista de alertas**, escolha um alerta e mova-o para da coluna **Disponível** para a coluna **Selecionado**.
   Você também pode escolher vários alertas. Se os alertas forem selecionados como parte de um único perfil, eles terão mapeamentos de campo e configurações de perfil comuns.

   A lista de alertas neste formulário corresponde à lista de alertas no console do Splunk. Até 500 alertas são exibidos neste formulário. Se houver mais de 500 alertas listados no console do Splunk na página Alertas, somente os primeiros 500 alertas serão exibidos neste formulário na instância Now Platform.

Opção	Descrição
No campo de pesquisa Lista de alertas, insira o texto.	A coluna abaixo do campo de pesquisa é filtrada com as opções disponíveis com base no texto inserido. Selecione um alerta e, com as teclas de seta, mova o alarme selecionado de **Disponível** para **Selecionado**.
Na Lista de Alertas, clique duas vezes em um Alerta.	A coluna **Selecionada** é preenchida com sua seleção.
Na Lista de alertas, clique uma vez em uma regra de alarme.	O alarme está selecionado. Com as teclas de seta, mova o alerta selecionado de **Disponível** para **Selecionado**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Escolha uma opção para continuar.

Opção	Descrição
Continue ou, como alternativa, clique em Mapeamento na barra de andamento	O formulário Mapeamento é exibido. O**mapeamento** é selecionado na barra de andamento. A próxima etapa é mapear campos de alerta para um SIR incidente de segurança.
Atualizar	Seus dados são salvos e a lista Perfis de eventos do Splunk é exibida.
Anterior	A etapa **Nome** é exibida.
Excluir	Exclua este perfil de evento e a lista Perfis de eventos do Splunk será exibida.

O que Fazer Depois

Você selecionou com sucesso um alerta para um perfil de alerta programado. A próxima etapa é mapear valores de alerta para campos em um incidente de segurança.

Mapeamento de alertas e eventos para a integração Splunk Enterprise Event Ingestion

Depois de identificar as origens para ingestão de alertas programada ou encaminhamento manual de eventos, a próxima etapa é mapear campos de evento individuais para os campos em um Now Platform Security Incident Response (SIR) incidente de segurança.

Visão geral

Para a etapa de mapeamento, como um usuário com a função sn_si.admin, você ingere alertas de amostra do console Splunk Enterprise ou exporta dados de evento para um evento Splunk Enterprise.

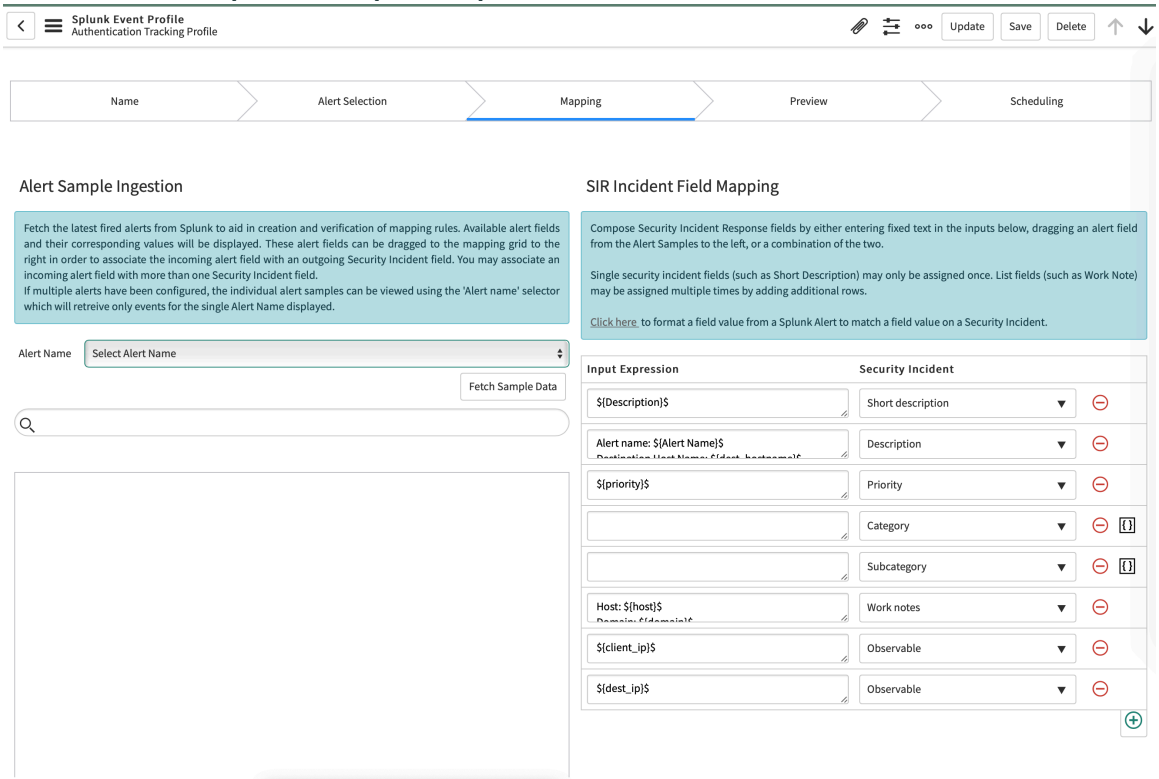
As imagens a seguir são exemplos das grades de mapeamento padrão fornecidas para cada tipo de perfil de evento. Este mapeamento padrão pode ser editado. Esta modificação permite que você personalize os campos que preenchem o incidente de segurança. Com a etapa de mapeamento, você pode visualizar como a adição ou remoção de campos de evento afeta os valores do campo de incidente de segurança SIR.

Selecione o **Nome do Alerta**e, depois de clicar para **Buscar Dados de Amostra**, os valores do campo de alerta Splunk serão preenchidos no lado esquerdo do formulário quando os alertas de amostra forem ingeridos pelo perfil. Estes são os campos de alerta Splunk que você mapeia para os campos de incidente de segurança SIR.

Tradução automática

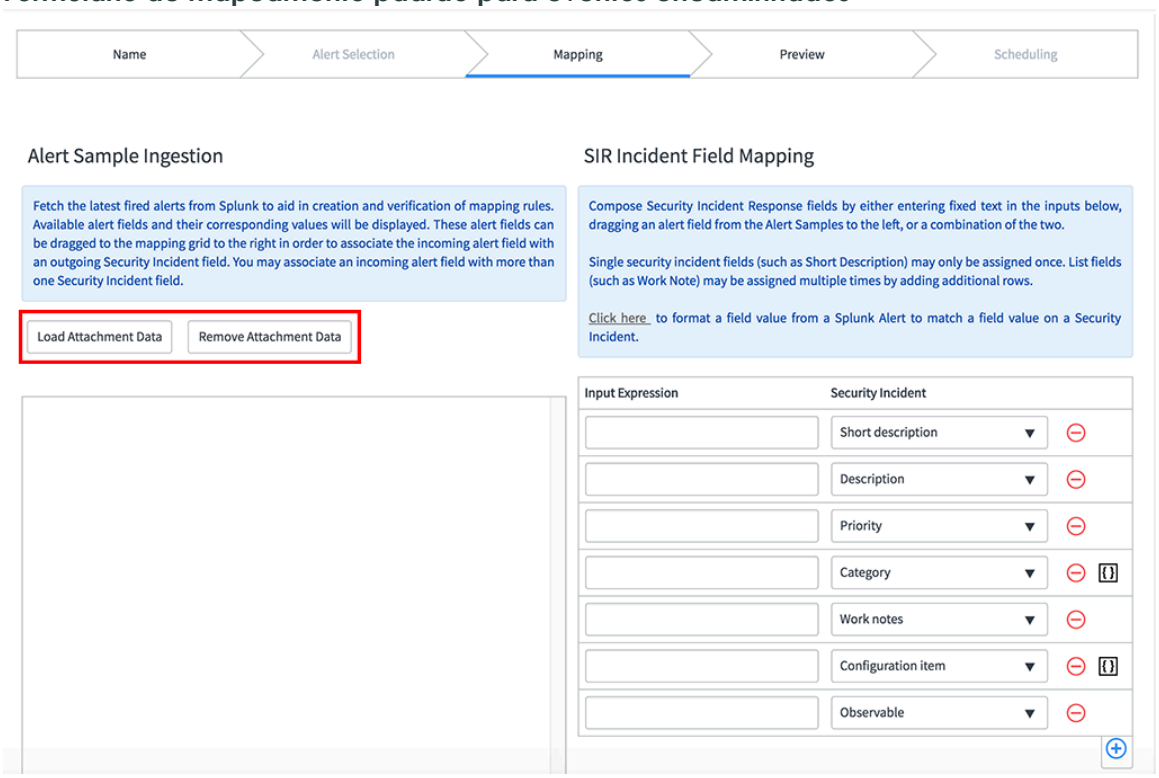
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de mapeamento padrão para alertas



Depois de clicar para carregar dados de anexo para eventos encaminhados, os campos de evento Splunk são preenchidos no lado esquerdo do formulário. Estes são os campos de dados Splunk que são mapeados para os campos de incidente de segurança SIR.

Formulário de mapeamento padrão para eventos encaminhados



Você pode preferir revisar alguns alertas de amostra no console Splunk para ingerir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada como

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento.

O mapeamento de alertas e a exportação de eventos sob demanda do console empresarial Splunk incluem os seguintes conceitos e tarefas:

- Buscar dados de amostra para perfis de alerta ingeridos automaticamente. Depois que os dados são obtidos (extraídos) de um alerta disparado no console Splunk Enterprise, os campos de alerta disponíveis e seus valores correspondentes são exibidos em um layout de mapeamento padrão no lado esquerdo do formulário de mapeamento. As guias são exibidas para você exibir os valores de um ID de alerta que você extraiu. Verifique se todos os campos críticos da seção Ingestão de amostra de alerta à esquerda do formulário estão mapeados para a grade à direita do formulário.
- Se necessário, carregue dados de amostra de evento para todos os perfis de evento encaminhados manualmente. Os dados de amostra desses eventos são exportados em um arquivo `.xml` do console Splunk Enterprise e carregados na instância Now Platform®. Os dados importados são exibidos na seção Ingestão de amostra de alerta à esquerda do formulário.
- Edite a configuração de mapeamento arrastando alertas do lado esquerdo e soltando-os na grade de mapeamento à direita. A grade de mapeamento à direita associa o campo de alerta de entrada a um campo de incidente de segurança de saída.
- Personalize a grade de mapeamento adicionando ou removendo campos. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida.
- Defina condições de filtro para que você possa especificar quais alertas são ingeridos na aplicação SIR e quais alertas são filtrados.
- Defina critérios de campo de incidente adicionais que agregam um alerta de entrada a um incidente de segurança SIR existente para evitar incidentes duplicados. Essa filtragem adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de eventos de segurança relacionados em um único incidente de segurança.
- Em determinados casos, os valores do campo de evento no console do Enterprise Splunk podem não ser convertidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, os valores de campo Alerta de malware e Infecção de vírus no console Splunk são convertidos em Atividade de código malicioso no campo Categoria no incidente de segurança SIR.

Tradução automática

Perfis de alertas programados

Depois de criar um perfil de alerta programado, o fluxo do processo para a configuração é mostrado na figura a seguir.

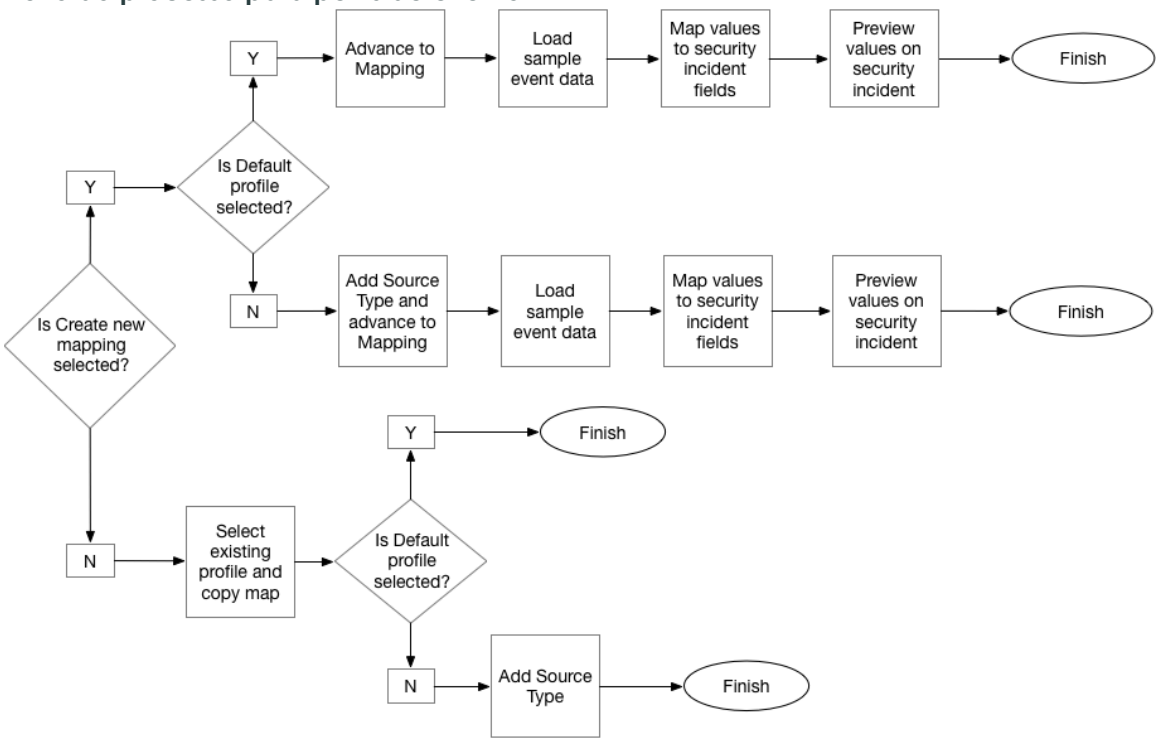
Fluxo do processo para perfis de alertas programados

Perfis de encaminhamento de eventos manuais

Depois de criar um perfil para um evento, o fluxo do processo para a configuração é mostrado na figura a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo do processo para perfis de evento



A próxima etapa é ingerir alertas acionados ou exportar dados e mapear valores para os campos de incidente de segurança SIR.

Mapear alertas para a integração Splunk Enterprise Event Ingestion

Durante a etapa de mapeamento de campo de evento, você mapeia campos de evento individuais de alertas acionados ou dados de eventos importados para campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

A grade de mapeamento pré-configurada dos campos de incidente de segurança padrão pode ser editada. A codificação de cores dos campos de evento ajuda a monitorar os valores de campo que você já mapeou. Esta etapa ajuda a visualizar como suas edições afetam os campos no incidente de segurança.

Mapeie até cinco alertas da coluna Ingestão de amostra de alerta à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente de SIR à direita.

Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. A personalização dos campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no incidente de segurança SIR.

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Para um perfil com um alerta programado, abaixo de Ingestão de amostra de alarme, selecione o alerta no **Nome** do alerta e clique em **Buscar dados de amostra** para extrair a instância mais recente de um alerta disparado do console Splunk Enterprise.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

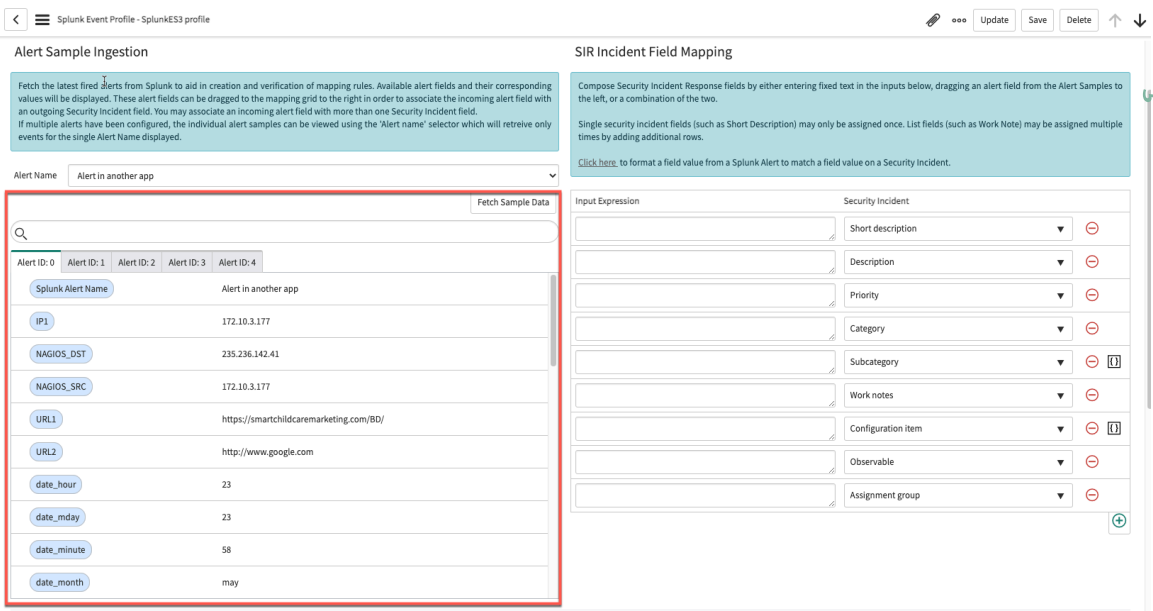
Os alertas são exibidos como guias. Você pode ingerir até cinco dos alertas mais recentes.

A extração de eventos de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

Nota: Um campo de mapeamento adicional, **Splunk Alert Name**, é adicionado pela integração para permitir o rastreamento de um evento para a regra de alerta de origem em Splunk. Isso pode ser útil em cenários em que vários Splunk alertas são combinados em um único perfil.

Quando um único campo contém vários valores, esses valores são analisados e mapeados para entradas de campo individuais na seção de mapeamento de campo de incidente SIR. Por exemplo, os endereços IP de origem, nomes de ativos ou URLs podem ter várias entradas de campo observável ou vários ICs, que são analisados e mapeados para entradas de campo individuais na seção de mapeamento de campo de incidente SIR.

Na figura a seguir, os pares de valores de nome de campo para o alerta ingerido ou o evento de amostra importado são exibidos no lado esquerdo deste formulário após a conclusão da extração. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.



3. Para perfis de alerta programados, prossiga para a etapa cinco para mapear os valores.
4. Como alternativa, para um perfil de um tipo de evento que você deseja exportar do console Splunk Enterprise, siga estas etapas para carregar dados de anexo na instância Now Platform®.

   a. Se ainda não estiver conectado, faça login no console do Splunk Enterprise.

   b. Navegue até a guia Pesquisar e insira um nome para uma pesquisa que tenha os dados de evento que você deseja exportar.

      Por exemplo, malware é um termo de pesquisa usado para todos os eventos de malware que você pode encaminhar com o fluxo de trabalho desta integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Expanda o evento e, na coluna Campo, selecione os campos que você deseja importar.

Esses campos são os pares de campo-valor que são exportados e exibidos na página Mapeamento em sua instância Now Platform®.

d. No console Splunk Enterprise, no canto superior direito da página Pesquisar, clique no ícone **Exportar**.

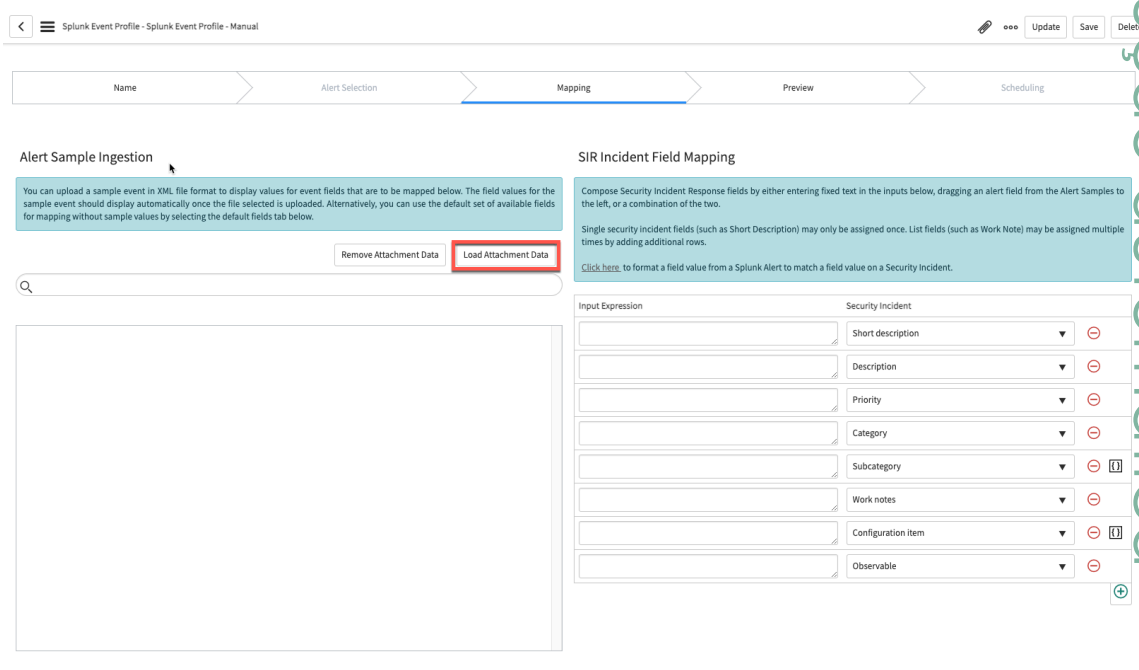
e. Na lista do campo Formato na caixa de diálogo exibida, clique em **Formato XML**.

f. Opcional: Insira um novo nome de arquivo.

g. Clique em **Exportar**.
O arquivo foi baixado para sua instância Now Platform®.

h. Se a página Mapeamento ainda não estiver exibida na sua instância Now Platform®, clique em **Mapeamento** na barra de andamento.

i. Na coluna Ingestão de amostra de alerta, clique em **Carregar dados de anexo**.



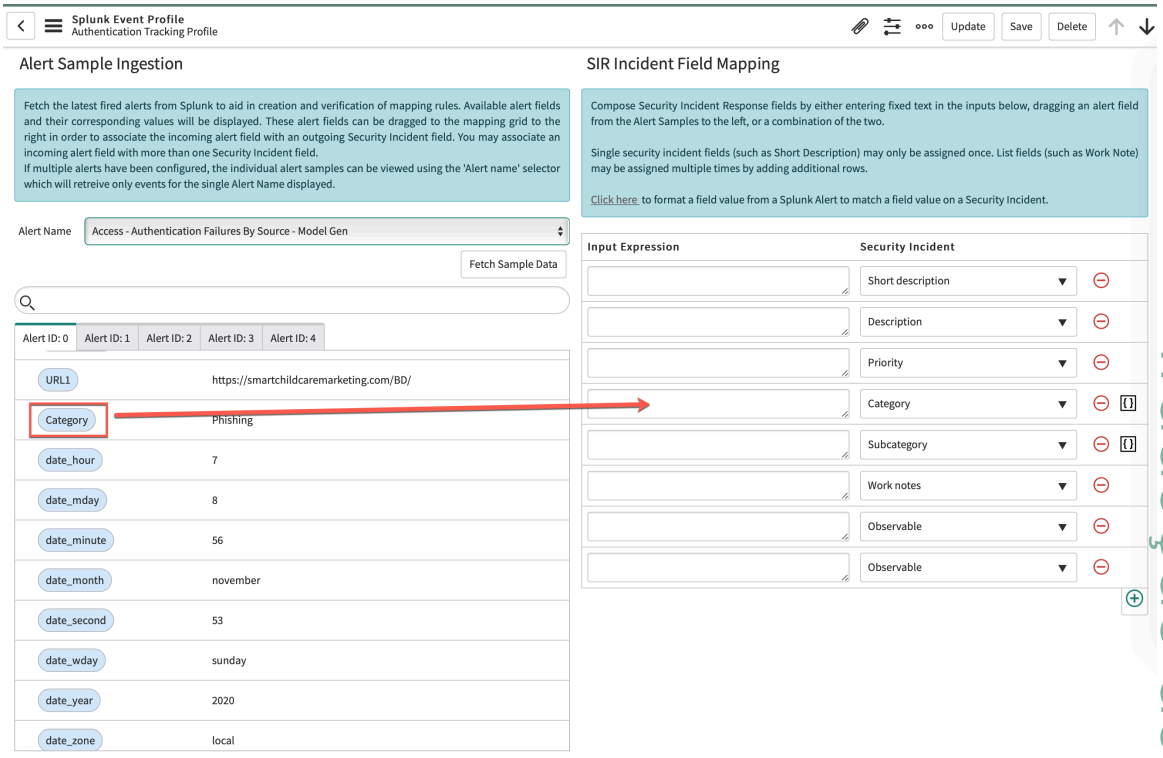
j. Na caixa de diálogo exibida, clique em **Escolher arquivos**, navegue até o arquivo `.xml` que você exportou e clique em **Abrir**.
Os pares de valores dos campos que você exportou para o evento são exibidos no lado esquerdo do formulário de mapeamento.

Na figura a seguir, os pares de dados de um alerta programado ingerido são exibidos no lado esquerdo deste formulário. Os pares de valores para eventos importados também são exibidos neste lado do formulário. Esses valores são os valores de campo que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente de Sir do formulário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
6. Arraste o nome do campo, por exemplo, `categoria`e solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.



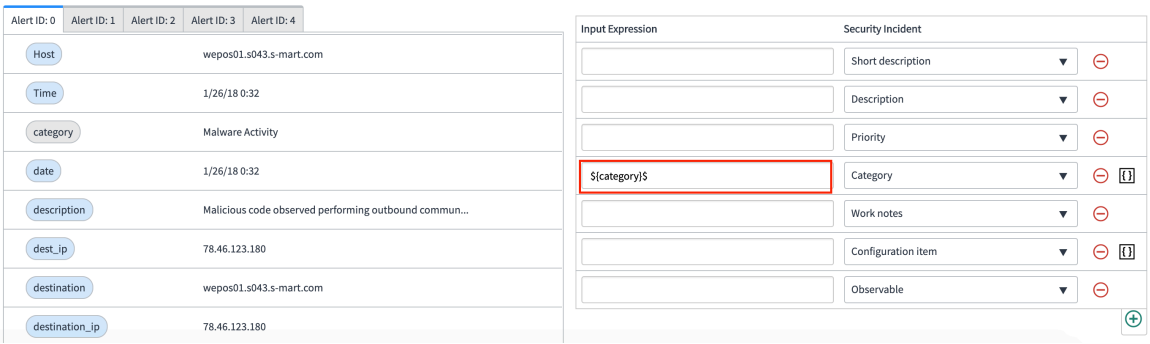
O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, a `categoria` é mapeada para o campo de `categoria` no incidente de segurança. No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo à direita. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudá-lo a garantir que nenhum evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Os campos em azul claro à esquerda indicam que um campo ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de alerta de entrada a mais de um campo em um incidente de segurança.

Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento porque, em determinados casos, os campos de evento de alerta só podem ser atribuídos uma vez. Por exemplo, você só pode atribuir valores a campos como Descrição resumida uma vez. No entanto, você pode atribuir campos de lista, como Anotação de trabalho, várias vezes adicionando linhas adicionais à grade de mapeamento.

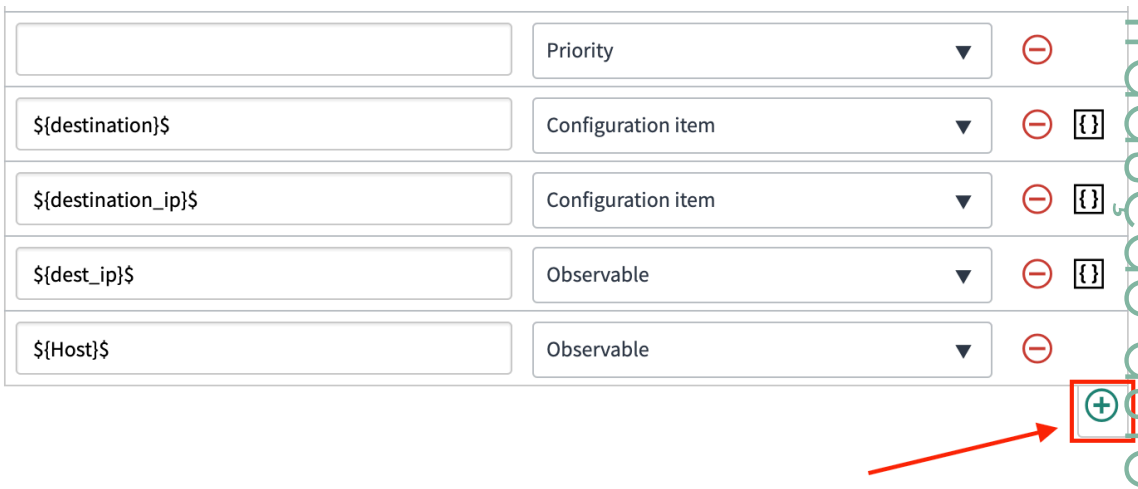
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Para adicionar campos ao mapeamento padrão do incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de mais.



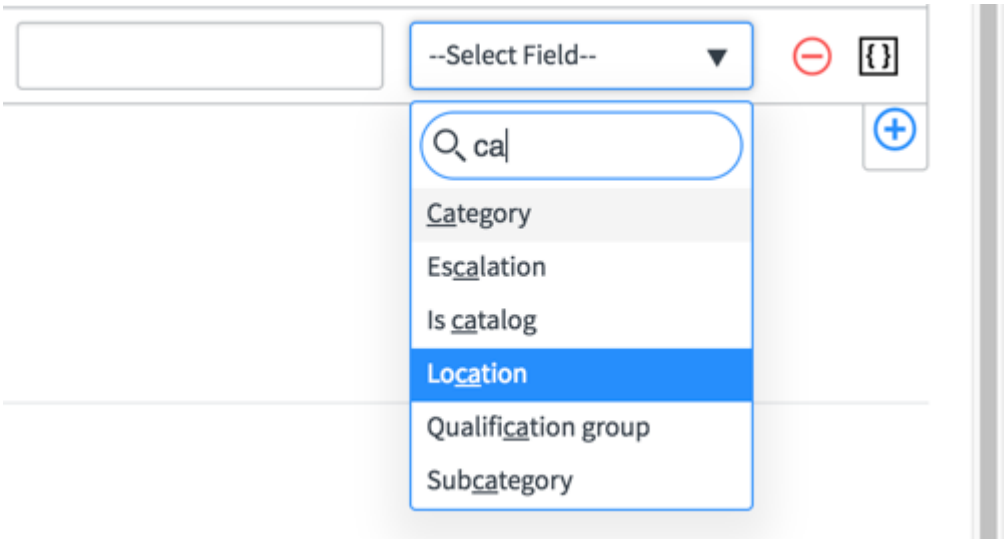
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Na lista expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, a `categoria` tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores para campos de alerta no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear o mapeamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

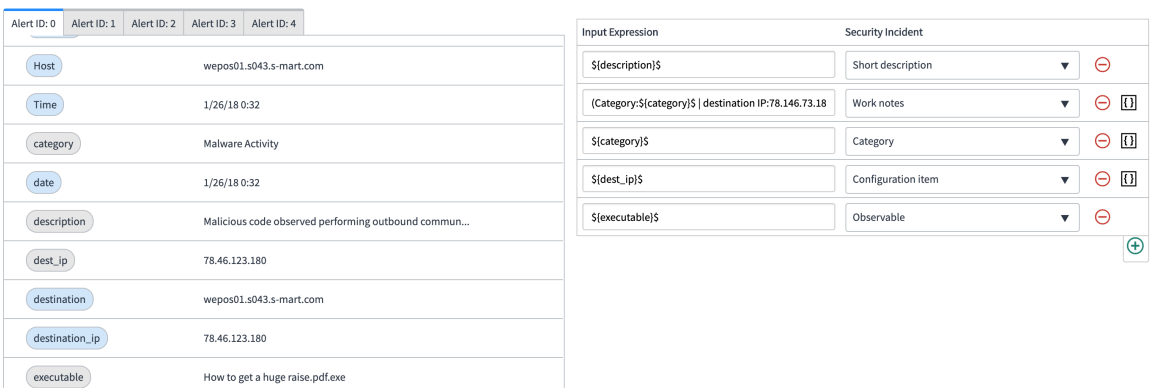


Nota: Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o **ID de alerta** desejado no campo Expressão de entrada.
Com o recurso de arrastar, mapeie-o ao lado do novo campo.

8. Continue mapeando adicionando ou removendo campos e adicionando valores ao mapa.
A figura a seguir é um exemplo de uma grade de mapeamento editada. No campo inferior à direita, o campo Anotações de trabalho é adicionado e tem mais de um valor. Os valores são separados por espaços e sinais de pontuação (`Category:${category} | IP de destino:78.146.73.180`).



Na visualização, esses valores são exibidos nas Anotações de trabalho no incidente de segurança. Como o valor é para um campo que você adicionou à grade e há

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vários valores mapeados para o campo Anotações de trabalho, os valores são exibidos conforme inseridos. Neste exemplo, os espaços e sinais de pontuação que você inseriu no campo são exibidos na seção Itens relacionados como uma anotação de trabalho na visualização do incidente de segurança.

A imagem a seguir é um exemplo de como os valores na imagem anterior são exibidos no incidente de segurança.

Related Items

Field Name	Field Value
Work Note	Category: Malware Activity | destination IP: 78.46.123.180
Work Note	Source: MalwareDemoData Top 100 events with 15 host machines

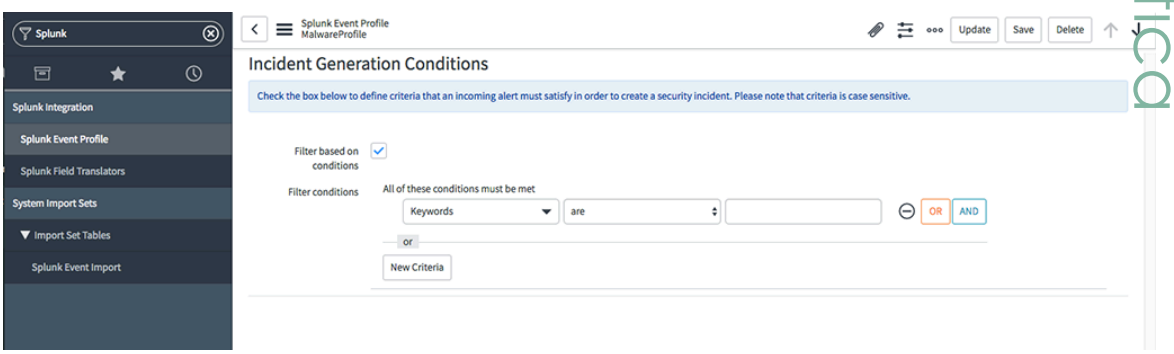
Condições de filtragem de geração de incidente

9. Opcional: Depois de concluir as etapas anteriores de mapeamento em nível de campo, você pode usar os mesmos valores de campos no construtor de Condições de filtro para definir critérios adicionais que um alerta de entrada deve satisfazer para criar um incidente de segurança SIR.
Para definir as condições de filtragem, siga estas etapas.

   a. Role até a seção Condições de geração de incidente no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

      (Optional) O Construtor de condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

      As opções nas listas do primeiro campo no construtor de Condições de filtro correspondem aos campos que são exibidos na seção Ingestão de amostra de alerta para o alerta que você ingeriu. Esses campos são dinâmicos e mudam dependendo do alerta Splunk que você ingere ou do evento que você encaminha manualmente. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores do alerta ou evento Splunk Enterprise. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console Splunk Enterprise e revisar seus alertas e eventos para as palavras-chave.



   b. Usando as listas e os campos do construtor de condições, defina filtros para a primeira linha.

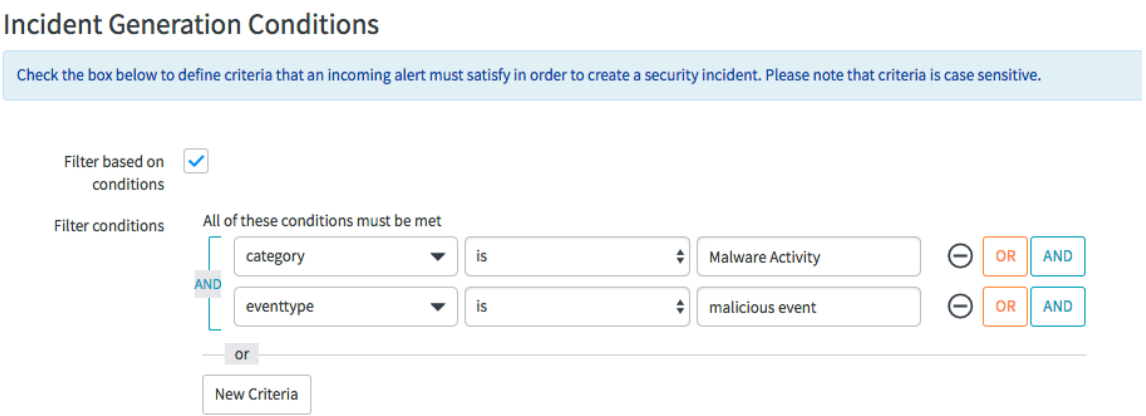
   c. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   Se **E** for selecionado, todas as condições deverão ser atendidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

   d. Opcional: Na segunda linha, defina uma segunda condição de filtro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser atendidas antes que os incidentes de segurança sejam criados.



(Optional) Você definiu as condições de acionamento para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

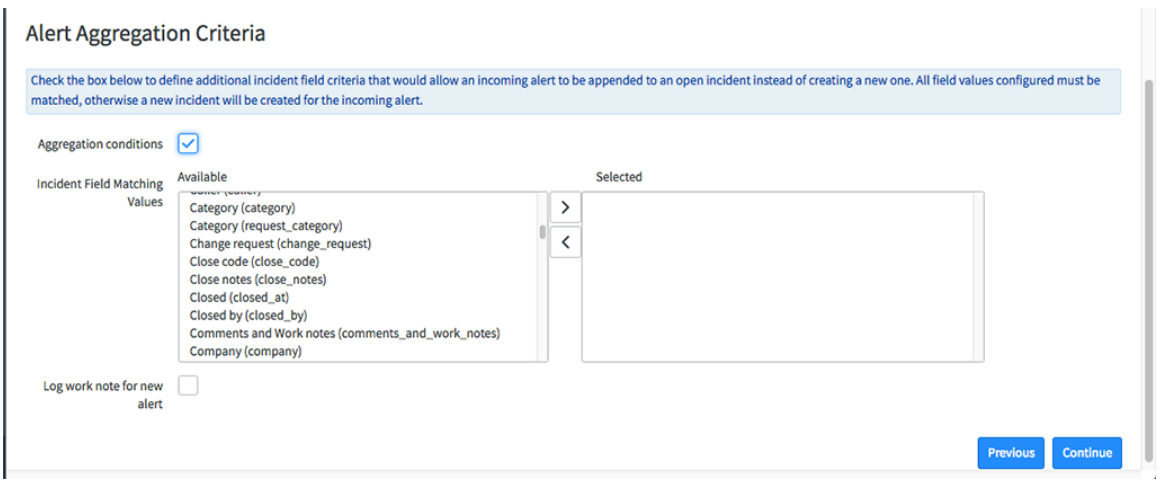
Esse tipo de filtragem ajuda a isolar eventos de segurança e limita o número de incidentes de segurança que você cria. Se critérios de filtragem adicionais forem definidos, somente os alertas necessários serão ingeridos sem a necessidade de alterar a consulta Splunk ou a configuração do alerta acionado.

Alertas de agregação para evitar incidentes duplicados

10. Opcional: Para evitar a criação de incidentes de segurança duplicados, defina critérios de campo de incidente adicionais para que os alertas de entrada sejam agregados a um incidente de segurança aberto.
Para definir esses critérios, siga estas etapas.

a. Role até a seção Critérios de agregação de alertas no formulário e marque a caixa de seleção Condições agregadas para habilitar essa opção.

(Optional) As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.



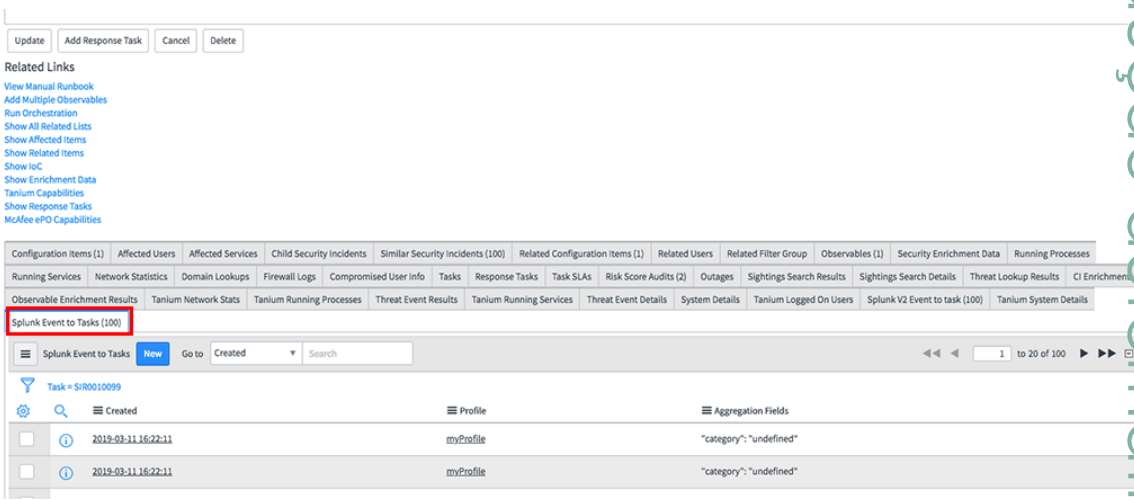
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes em seu Now Platform e mova-os para a lista Selecionada.

(Optional) Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Se você preferir revisar os valores de campo em incidentes de segurança a serem usados para esses critérios, navegue até **Incidentes** > **Mostrar todos os incidentes**.

Se um novo alerta corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o alerta será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os alertas agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os alertas agregados em um incidente de segurança são exibidos na lista relacionada Splunk de eventos para tarefas. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que os alertas são adicionados aos incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.



c. Opcional: Para registrar uma anotação de trabalho para um novo alerta adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra que um novo alerta foi adicionado junto com um link para os detalhes do alerta.

Você mapeou com sucesso valores de um alerta ou evento Splunk para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem. Você também anexou alertas ou eventos a incidentes de segurança SIR existentes.

11. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de scripts, consulte Use o editor de script para formatar valores de alerta para a integração Splunk Enterprise Event Ingestion.

12. Escolha um para continuar com a configuração do perfil.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Continuar	O formulário Mapeamento é exibido. A**visualização** está selecionada na barra de andamento. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR.
Atualizar	Seus dados são salvos e a lista Splunk de Perfis de eventos é exibida.
Anterior	O formulário Seleção de alertas é exibido.
Excluir	Exclua este perfil de evento e a lista Splunk de Perfis de Evento será exibida.

O que Fazer Depois

A próxima etapa é visualizar os valores que você mapeou no incidente de segurança.

Visualizar o incidente de segurança da integração Splunk Enterprise Event Ingestion

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um Now Platform® Security Incident Response (SIR) incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de alerta que deseja exibir no incidente de segurança.

Antes de Iniciar

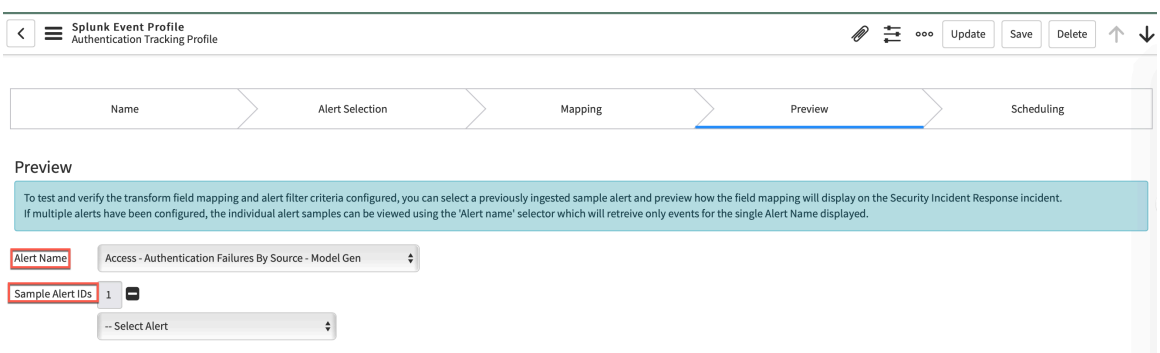
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto SIR.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Selecione o **Nome do Alerta** e um item na lista de **IDs de Alerta de Amostra**.

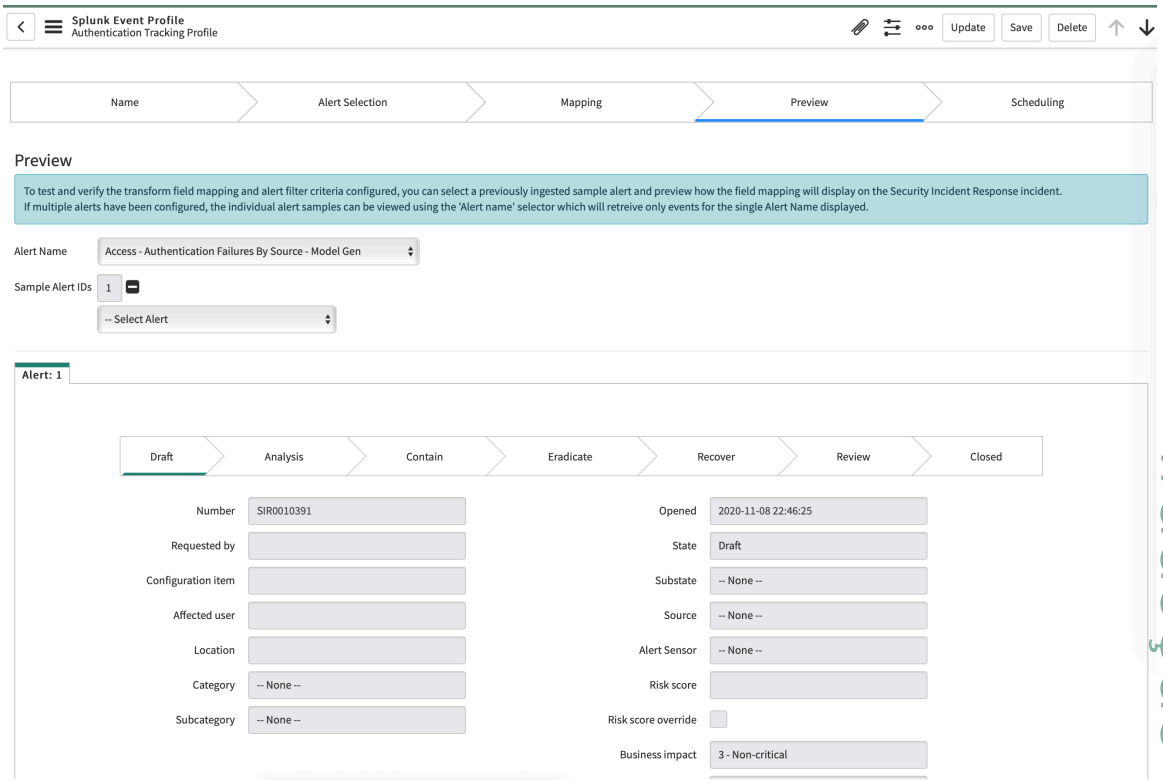


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.

3. Revise o mapeamento de campo dos valores de alerta no incidente de segurança.



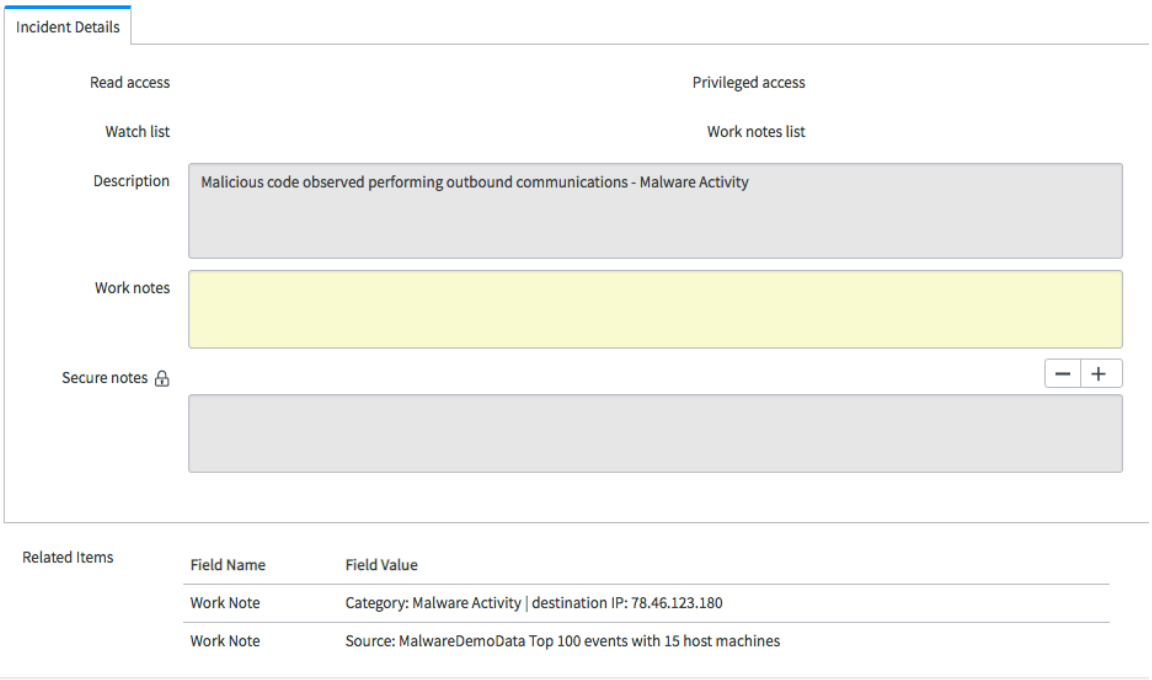
A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um campo no incidente de segurança não existe para um valor ou o campo não é compatível com o valor que você mapeou. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para o campo `Item de configuração`.

4. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

   A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança SIR depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos do console Splunk Enterprise. O primeiro campo Anotações de trabalho não tem valor. Este campo foi deixado em branco na grade de mapeamento durante a etapa de mapeamento. Os campos de anotação de trabalho adicionais que têm valores foram adicionados à grade de mapeamento durante a etapa de mapeamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Depois de corrigir todos os erros e verificar se os campos estão como você deseja, escolha uma opção para continuar.

Opção	Descrição
Continuar	O formulário Programação é exibido para perfis com alertas programados. A**programação** é selecionada na barra de andamento.
Concluir	Para perfis configurados para encaminhamento manual de eventos, clique em **Concluir**. Não há etapa de programação para perfis com dados de evento que são exportados sob demanda diretamente do console Splunk Enterprise.
Atualizar	Seus dados são salvos e você retorna à lista Splunk de Perfis de eventos.
Anterior	A etapa Mapeamento na barra de andamento é exibida.
Excluir	Exclua este perfil de evento e a lista Splunk de Perfis de Evento será exibida.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campos no incidente de segurança, a próxima etapa é Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion.

Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion

Para perfis de ingestão de alertas automatizados, esta etapa é a etapa final da configuração do perfil de evento. Durante esta etapa, você pode verificar as

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configurações padrão para recuperação de alertas ou modificar a programação conforme necessário. Esta etapa permite filtrar a recuperação do alerta com base em um intervalo de datas.

Antes de Iniciar
Função necessária: função sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Depois de concluir todas as etapas na barra de andamento da configuração do perfil, conforme mostrado na figura a seguir, você concluiu a configuração dos perfis para encaminhamento manual de eventos. Não há programação disponível para eventos encaminhados manualmente do console Splunk Enterprise. Para perfis de ingestão de alertas automatizados, você escolhe se deseja ingerir alertas históricos durante a etapa de Programação. Você também escolhe com que frequência pesquisará alertas futuros que correspondam à configuração do perfil de alerta.

Barra de andamento

Para perfis de ingestão de alertas automatizados, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação do alerta. Esta etapa é a etapa final do processo de configuração do perfil de evento para perfis de alertas programados.

Configure esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de eventos Splunk é afetado pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga prevista em seu sistema.

No console Splunk Enterprise, você define um alerta a ser acionado com base em incrementos ou em um horário específico. Use esta configuração para ajudá-lo a configurar a programação em sua instância Now Platform para que os incrementos de tempo no console Splunk Enterprise sejam sincronizados com a programação que você configurou em sua instância Now Platform.

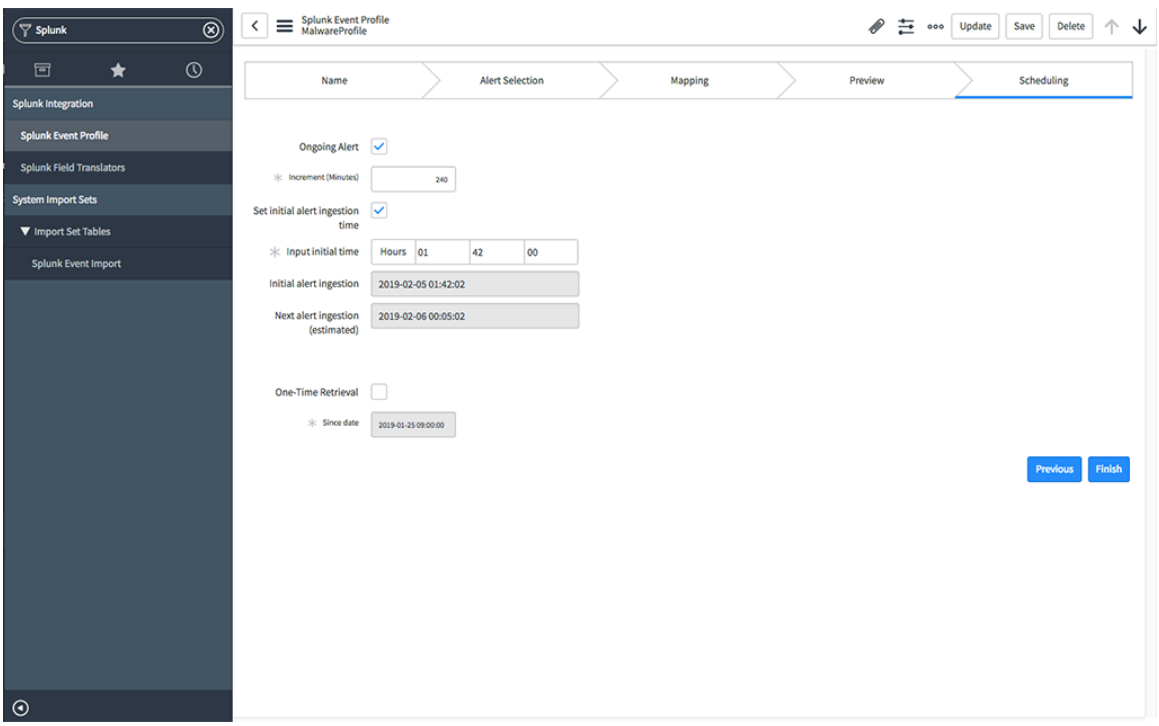
Procedimento
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os alertas são extraídos do console Splunk Enterprise.

Opção	Descrição
◦ Campo de alerta contínuo selecionado ◦ Campo de recuperação única limpo	Alerta contínuo Com base na configuração padrão, a instância Now Platform extrai do servidor Splunk Enterprise novos alertas a cada cinco minutos. Os incidentes de segurança serão criados se os alertas acionados forem encontrados e os critérios de filtragem forem correspondidos. Para equilibrar a ingestão de alertas em relação à carga do servidor e para extrair os dados mais atuais, cinco minutos é a configuração que você po-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	de preferir. No entanto, este valor pode ser modificado conforme necessário.
◦ Campo de alerta contínuo limpo ◦ Campo de recuperação única selecionado	Recuperação única Use esta configuração se quiser uma extração única para ingerir alertas com base em eventos históricos. Quando configurado, um perfil é usado uma vez para recuperar alertas acionados, incluindo alertas de eventos históricos que são baseados em um intervalo de datas. À direita do campo **Data desde**, clique no ícone de calendário. No calendário exibido, selecione a data em que deseja começar a extrair alertas. Começando com o valor de **data Desde**, os alertas acionados são recuperados até a data atual. Depois que os alertas forem extraídos, esta configuração não recuperará alertas acionados para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todos os alertas encontrados para o intervalo inserido.



Como um exemplo de programação, se você tiver um alerta Splunk diário que é executado uma vez por dia às 4h no horário local, você pode configurar o perfil de alerta correspondente em sua instância Now Platform para ser executado às 4h05 no horário local para capturar o alerte imediatamente e crie um incidente de segurança. Insira `04 05 00` no campo **Ingestão de alerta inicial**. No campo **Incrementar (minutos)**, insira `1440` (24 horas) para programar a próxima ingestão de alertas por 24 horas a partir da ingestão

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de alertas inicial. O tempo de ingestão do alerta inicial e o tempo de ingestão do próximo alerta são exibidos nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

   a. Com a página Programação exibida, marque a caixa de seleção **Alerta contínuo** para habilitar essa opção.

   b. No campo **Incrementar (minutos)**, insira `1440` (24 horas).

   c. Clique na caixa de seleção **Selecionar ingestão de alerta inicial** para habilitar a edição dos campos Ingestão de alerta inicial e Próxima ingestão de alerta.

   d. No campo Ingestão de alerta inicial, insira `04 05 00`.
   No campo **A próxima ingestão de alertas (estimada)**, a hora da próxima ingestão de alertas é exibida.

4. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Este perfil está ativado e extrai alertas do console Splunk Enterprise com base na sua programação. Há um limite de 1.000 incidentes de segurança que podem ser criados em um período de 24 horas. Até 100 eventos são por alerta acionado. Os eventos subsequentes serão ignorados depois que os limites forem atingidos.

Arquitetura de integração e conexão de sistemas externos para a integração Splunk Enterprise Event Ingestion

O tópico a seguir descreve a arquitetura de integração desenvolvida para oferecer suporte à ingestão de alertas acionados do console Splunk Enterprise. Essas informações esclarecem, em alto nível, a operação conceitual da integração. Ele também explica por que há etapas de configuração necessárias antes de instalar a aplicação do ServiceNow Store.

Termos-chave usados para esta integração

Os termos-chave a seguir são usados durante a instalação e a configuração do. Para obter mais informações sobre esses termos, consulte o site de documentação do produto da ServiceNow e o site e recursos do Splunk na página Recursos do Splunk.

Now Platform

> Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

ServiceNow Complemento Splunkbase

> Uma aplicação ServiceNow instalada no console Splunk Enterprise que oferece suporte à opção de encaminhamento manual de eventos da integração. O encaminhamento manual de eventos é um recurso opcional da integração. Este ServiceNow complemento Splunkbase não é necessário para a ingestão automatizada de alertas fornecida pela integração.

Security Incident Response (SIR)

> Uma aplicação Now Platform que rastreia o andamento de incidentes de segurança desde a descoberta e análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk Enterprise

Um produto ou serviço em nuvem automatizado de gestão de eventos de incidentes de segurança (SIEM) que coleta dados usados para análise e gestão de incidentes. Este serviço está em um host que às vezes também é chamado de console Splunk neste guia.

Splunk alerta

Uma pesquisa que você configura e salva em Splunk para verificar dados específicos com base nos parâmetros configurados no serviço Splunk Enterprise. Ao extrair alertas de Splunk, você também extrai todos os eventos associados a esse alerta.

Splunk alerta acionado

Uma pesquisa configurada no console Splunk Enterprise que retorna resultados e sinaliza esses resultados como alertas acionados. Os alertas acionados são ingeridos do console Splunk para sua instância Now Platform para esta integração. Os alertas acionados têm um ou mais eventos Splunk.

Splunk evento

Um ou mais elementos de dados que resultam nos alertas acionados do serviço Splunk. Na sua instância Now Platform, você pode pesquisar quais eventos [Splunk acionaram Now Platform incidentes de segurança.

MID Server

Esta aplicação facilita a comunicação e a movimentação de dados entre Now Platform e aplicações, fontes de dados e serviços externos. Esta aplicação é normalmente necessária para integração com tecnologias no local e, para esta integração Splunk Enterprise Event Ingestion, o MID Server facilita a comunicação entre o Now Platform e a instância no local de Splunk Enterprise. Um MID Server não é necessário se você estiver integrando sua instância Now Platform com uma instância Splunk Cloud.

Administrador de incidentes de segurança (sn_si.admin)

O usuário com esta função supervisiona a configuração da integração com o produto SIR em sua instância Now Platform.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com esta função interage e analisa incidentes de segurança no produto ServiceNow Security Incident Response.

Conexão de sistemas externos

Um perfil de evento é um contêiner que você cria, nomeia e configura para uma conexão única e chama o serviço Splunk para extrair os alertas acionados mais atuais que correspondem a critérios específicos. Depois que os alertas acionados que correspondem ao seu perfil forem extraídos de Splunk, você seleciona qual desses alertas deseja exibir como um incidente de segurança Now Platform Security Incident Response SIR. Uma exibição padrão dos campos de alerta Splunk Enterprise está disponível e você edita este mapeamento de campos de alerta para os campos em um incidente de segurança SIR para atender às suas necessidades. Visualize seu mapeamento para verificar se todos os valores de campo de alerta necessários estão preenchidos no SIR incidente de segurança. Para concluir a configuração do perfil de alerta, programe a recuperação de alertas e ative o perfil. Depois de ativar o perfil no Now Platform, você está pronto para ingerir alertas históricos e contínuos Splunk automaticamente.

Como um usuário com a função sn_si.admin, se você determinar que um novo alerta acionado é semelhante aos alertas ingeridos anteriormente, poderá agregar novos alertas acionados a incidentes de segurança SIR existentes. Você define critérios para especificar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

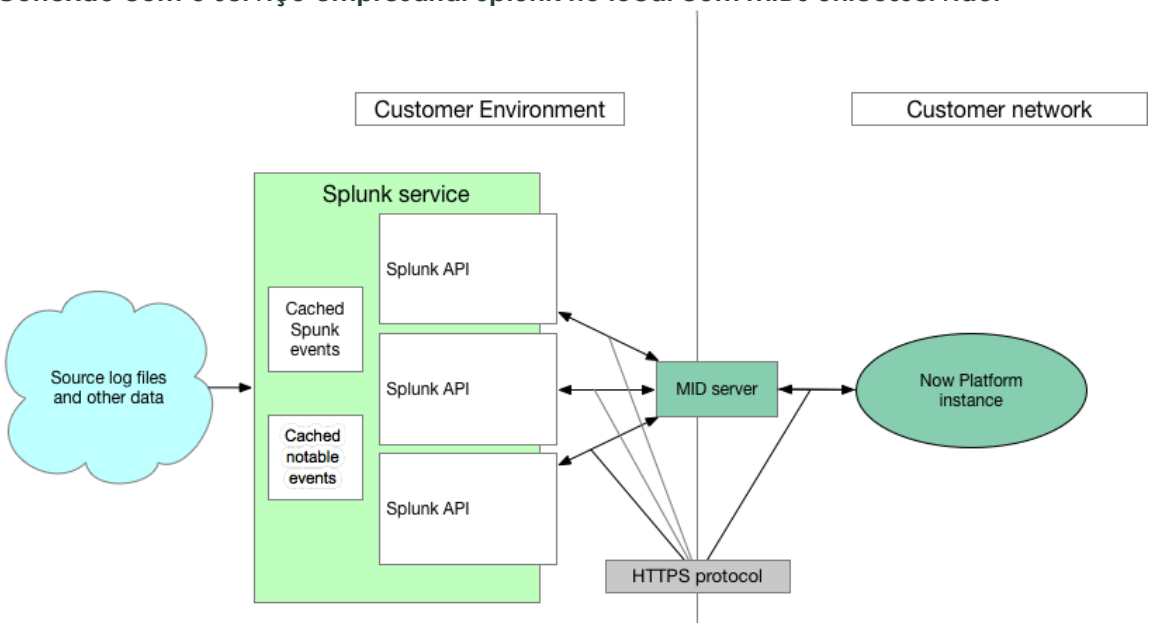
valores de campo de destino correspondentes no perfil de alerta Splunk Enterprise que definem quando um incidente de segurança existente é atualizado e quando um novo incidente de segurança é criado. Se o recurso de agregação estiver habilitado em seu perfil de evento, quando o conjunto para importação for transformado, sua instância Now Platform verificará se há um registro existente na tabela de destino que tenha o mesmo valor nos campos de destino e de origem. Se um registro existente com um valor correspondente na tabela de destino for encontrado, esse registro será atualizado. Se nenhum registro correspondente for encontrado, um novo registro será criado na tabela de destino. Se habilitada, a opção de agregação atualizará os incidentes de segurança existentes com novos alertas acionados e você evitará a criação de vários incidentes de segurança. Para obter mais informações sobre como atualizar registros usando opções de agregação, consulte Atualização de registros usando aglutinação .

Esta aplicação usa o serviço de API Splunk para recuperar informações do serviço Splunk. Uma conexão HTTPS de saída do MID Server com este ambiente é necessária para que a integração funcione corretamente.

Depois de conectada ao serviço Splunk, a integração oferece suporte à extração e ingestão de alertas e eventos acionados que acionam incidentes de segurança.

O fluxo de dados básico é ilustrado nas imagens a seguir. Em cada figura, seu Now Platform está extraindo (ingerindo) dados. Splunk não está enviando dados para alertas programados.

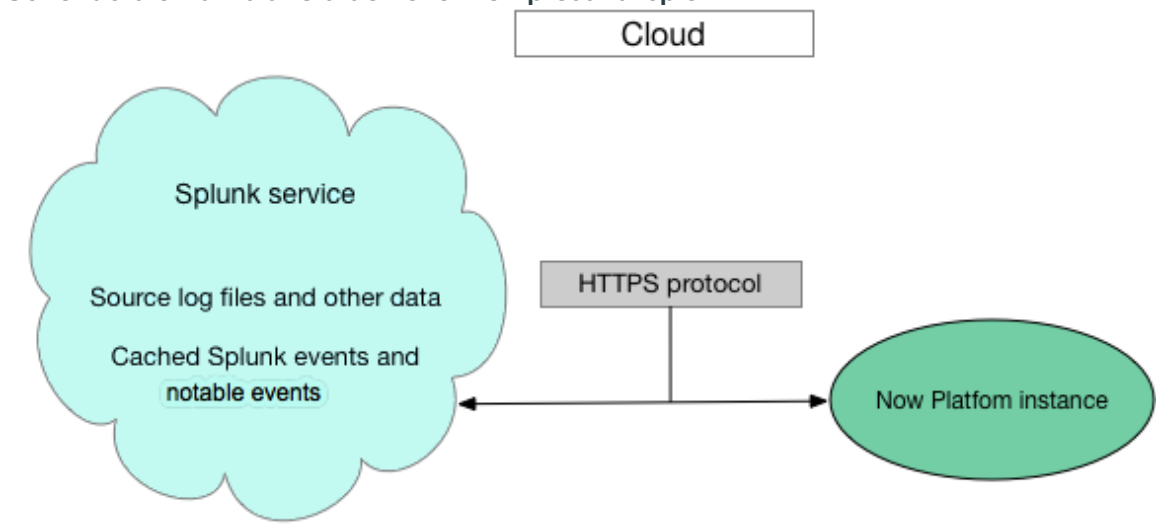
Conexão com o serviço empresarial Splunk no local com MIDs únicosservidor



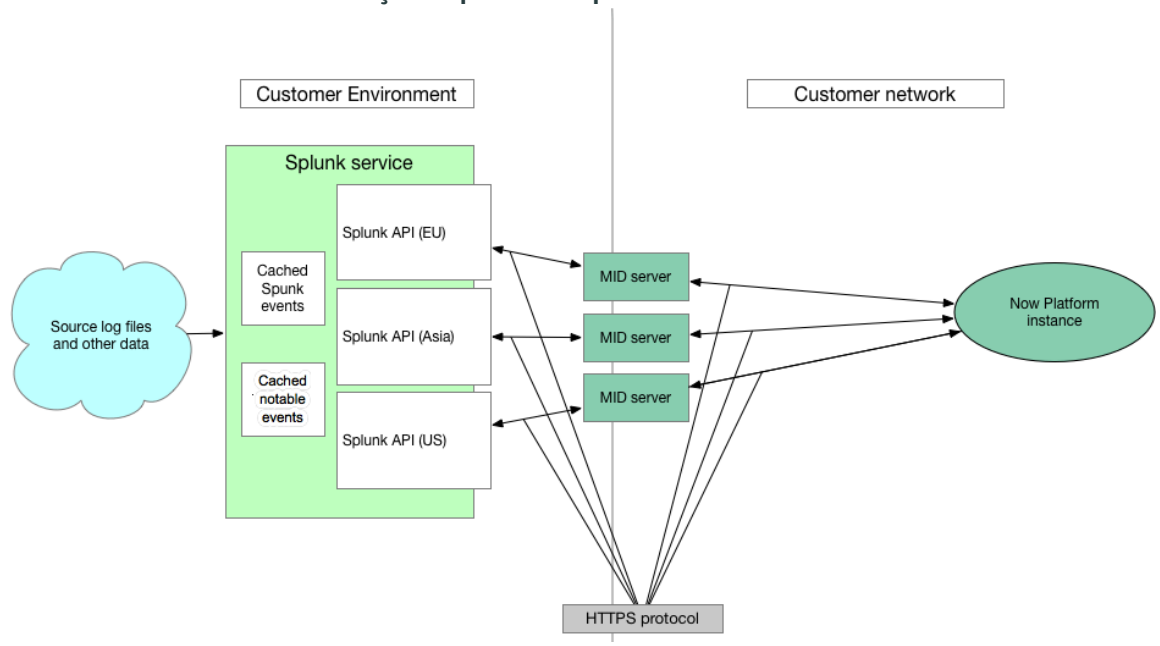
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conexão a uma instância de nuvem empresarial Splunk



Várias conexões com o serviço empresarial Splunk usando vários MID Servers



Tradução automática

Copiar Splunk Enterprise Event Ingestion perfis de uma instância para outra usando a funcionalidade de exportação/importação

Você pode exportar e importar Splunk Enterprise Event Ingestion configurações de perfis de uma instância Now Platform para uma instância Now Platform diferente.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

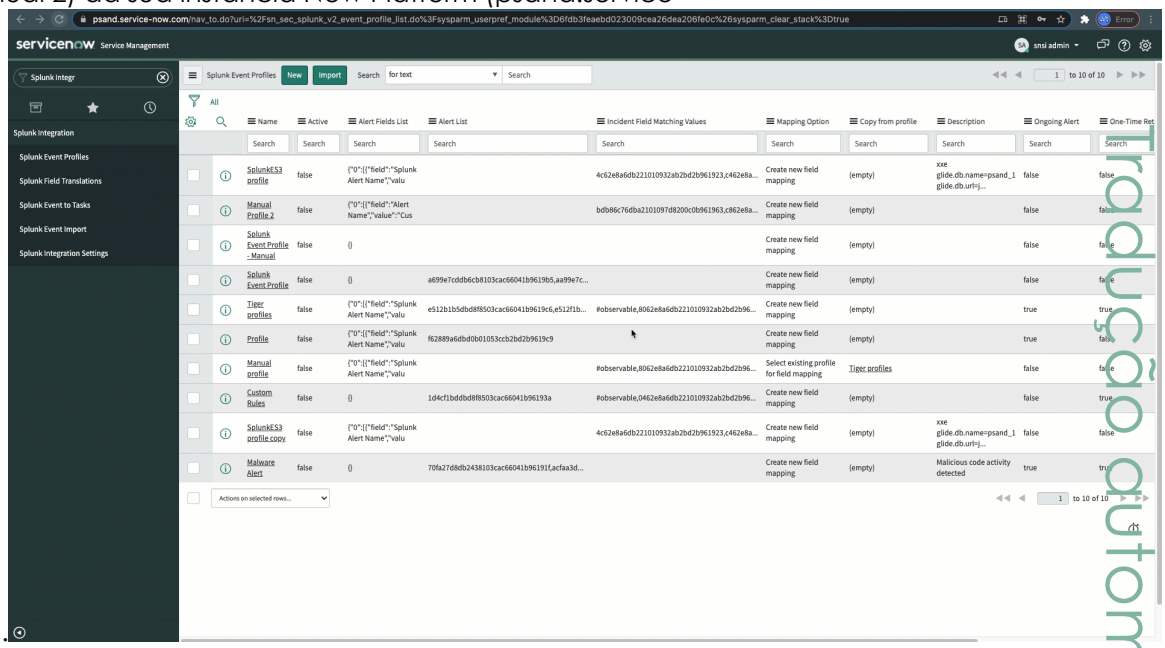
Essa funcionalidade permite que o administrador de segurança copie perfis que foram testados e verificados em uma instância Now Platform, por exemplo, em não produção, para outra instância Now Platform, por exemplo, produção, sem a necessidade de refazer todas as definições de configuração. As configurações que são exportadas e importadas incluem nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando você exporta um tipo de perfil de encaminhamento de eventos manual, os dados de anexo usados para o mapeamento do campo de amostra são copiados, no entanto, o arquivo de anexo em si não é exportado.

Procedimento

1. Navegar até **Todos** > **Splunk Integration** > **Perfis de eventos do Splunk**.
2. Selecione um perfil que você deseja exportar para outra instância Now Platform. Você pode selecionar vários perfis para exportação.
3. No menu Ações, clique em **Exportar**.
4. Quando a mensagem de exportação concluída for exibida, clique em **Download**. A ilustração a seguir mostra a exportação de um perfil Splunk (Perfil Manual 2) da sua instância Now Platform (psand.service-now.com).



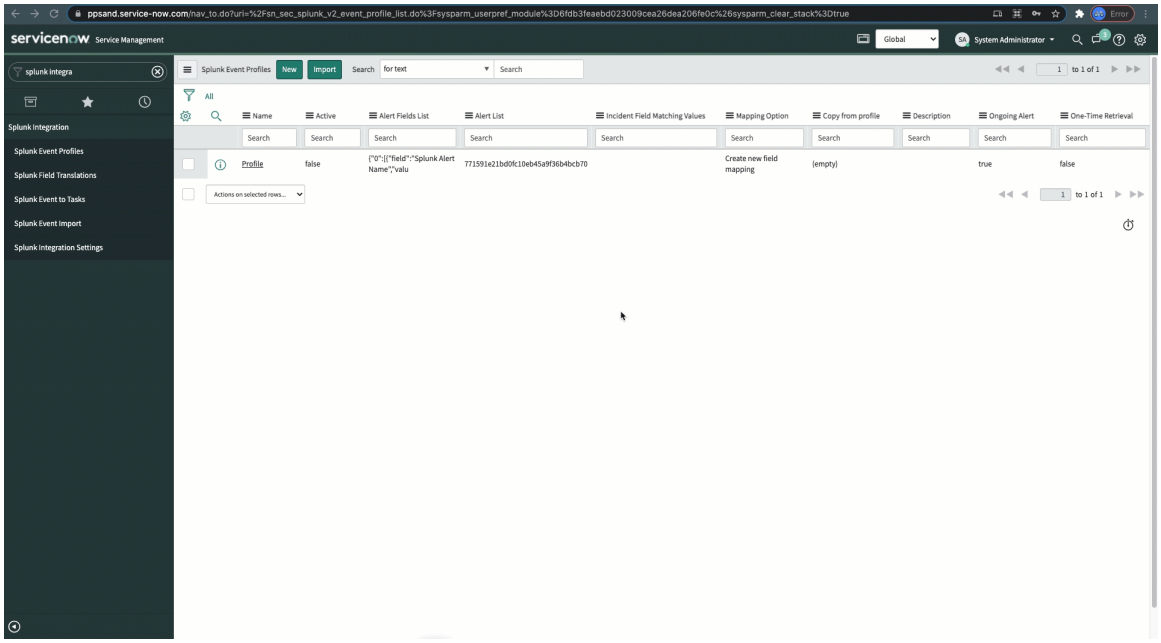
O arquivo payload.xml exportado é baixado no seu computador. O arquivo contém o nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração. Quando você seleciona e baixa vários perfis, eles aparecem no mesmo arquivo payload.xml.

Agora você pode prosseguir para importar o perfil em outra instância Now Platform.

5. Navegar até **Splunk Integration** > **Perfis de eventos do Splunk**.
6. Clique em **Importar**.
7. Clique **em Escolher arquivo** e selecione o arquivo xml no seu computador.
8. Clique em **Carregar**.
9. Clique **em Fechar e recarregar perfis**. A ilustração a seguir mostra a importação de um perfil Splunk (Perfil Manual 2) da instância Now Platform (psand.service-now.com) para outra instância Now Platform (ppsand.service-now.com).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você importou com sucesso o perfil de outra instância Now Platform.

Verifique se a origem exportada (Splunk conta de API e Splunk URL do servidor) e as definições de configuração do MID Server são válidas e estão disponíveis na instância Now Platform importada. Atualize sua configuração Splunk Enterprise Event Ingestion, se necessário.

10. Opcional: Verifique as configurações do MID Server após importar um perfil.
11. Opcional: Navegar até **Operações de segurança** > **Configurações de Integração**.
12. Opcional: Selecione o bloco de configuração Splunk Enterprise Event Ingestion e clique em **Atualizar**.
13. Opcional: Revise e atualize os detalhes de origem e do MID Server conforme necessário.

Copiar um perfil de evento para a integração Splunk Enterprise Event Ingestion

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar os perfis de alarme para economizar tempo.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Copiar um perfil existente e suas configurações associadas é opcional.

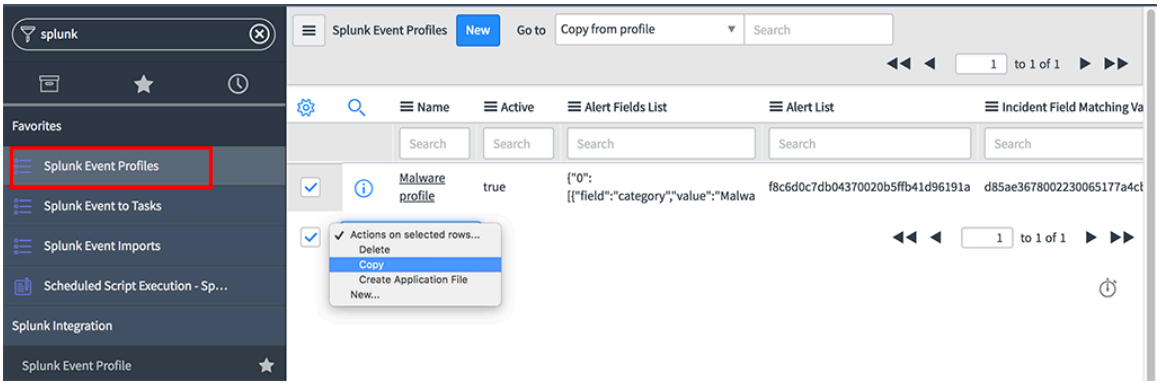
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

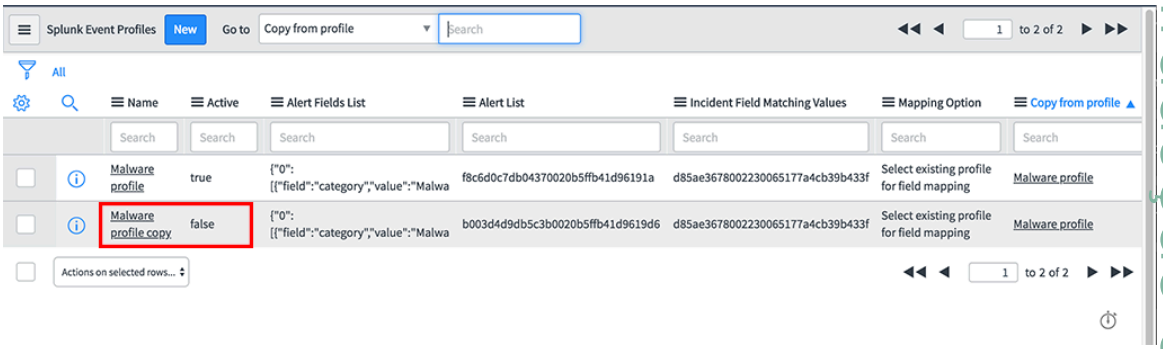
1. Navegar até **Todos** > **Splunk Integration** > **Perfil de eventos do Splunk**.
2. Na lista Splunk Perfis de eventos exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (`verdadeiro`), a cópia está desabilitada neste ponto (`falso`). Você pode preferir editar valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos Splunk Enterprise

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para esta integração, instale e configure o complemento ServiceNow Security Operations Event Ingestion para a aplicação SplunkSplunk Enterprise no console empresarial [] ou na instância do Splunk Cloud.

Antes de Iniciar

Verifique se você instalou a aplicação para esta integração do ServiceNow Store antes de instalar o plug-in de complemento do splunkbase que é necessário para a ingestão manual de eventos. Se você não instalou a aplicação para a integração de ServiceNow Store, consulte Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion e siga as instruções para instalá-la.

Função necessária: Now Platform administrador (admin)

Por Que e Quando Desempenhar Esta Tarefa

A instalação e a configuração do ServiceNow Security Operations Event Ingestion Addon são opcionais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para a integração, baixe, instale e configure o ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise do splunkbase no console Splunk Enterprise.

Este ServiceNow complemento de extensão é necessário para que incidentes de segurança possam ser criados a partir de eventos exportados manualmente em sua instância Now Platform. Este ServiceNow Complemento de ingestão de eventos das Operações de segurança para a aplicação Splunk Enterprise está disponível em splunkbase .

Para o encaminhamento manual de eventos, você pode identificar até dois Now Platform endpoints (instâncias) diferentes no console Splunk Enterprise. Você encaminha os eventos para o endpoint ou endpoints manualmente para criar incidentes de segurança. Por exemplo, você pode especificar uma instância de preparação (desenvolvimento) e uma instância de produção. Ao especificar instâncias separadas e nomear fluxos de trabalho primários e secundários para cada instância, você pode escolher para onde deseja encaminhar eventos diferentes.

Procedimento

1. Se você ainda não instalou o ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise, siga estas etapas para instalá-lo e configurá-lo.

   a. Navegue até splunkbase .

   b. Pesquise o ServiceNow Operações de segurança Complemento de ingestão de eventos das Operações de segurança para Splunk Enterprise.

      Nota: Verifique se você selecionou ServiceNow Operações de segurança Complemento de ingestão de eventos para Splunk Enterprise. Há complementos ServiceNow adicionais que são exibidos nesta lista. Esses complementos são para diferentes ServiceNow Splunk integrações e não são necessários para esta integração.

   c. Baixe a aplicação.

   d. Abra sua conta Splunk Enterprise.

   e. Na página Aplicações, clique no ícone de engrenagem ou no atalho **Gerenciar aplicações** na lista suspensa do menu.

   f. No canto superior esquerdo da página Aplicações exibida, clique em **Instalar app a partir do arquivo**.

   g. Clique em **Escolher arquivo**, selecione ServiceNow Complemento de ingestão de eventos das Operações de segurança para Splunk Enterprisee clique em **Carregar**.

   h. Se solicitado, reinicie Splunk Enterprise.
   O ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise está instalado no console do Enterprise Splunk Enterprise. A próxima etapa para configurar o complemento.

2. Para configurar o complemento, siga estas etapas.

Tradução automática

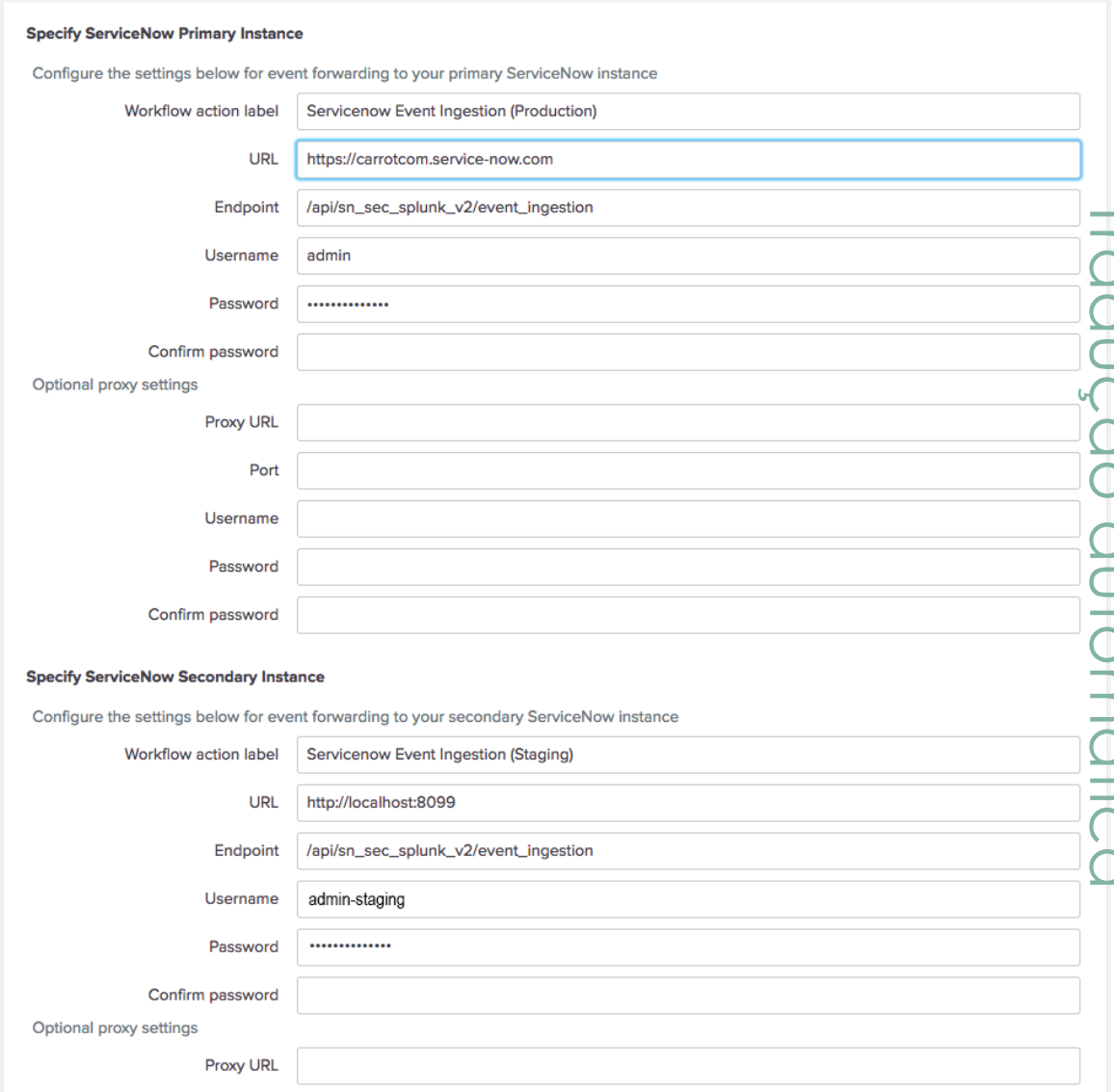
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Em Splunk Enterprise, clique no ícone de engrenagem de **aplicações** ou em **Gerenciar aplicações** na lista suspensa do menu.

b. Na lista de aplicações exibida, na coluna **Ações**, clique em **Configurar** para ServiceNow Operações de segurança Complemento de ingestão de eventos para Splunk Enterprise.

c. Preencha o formulário.

A figura a seguir é um exemplo de um formulário preenchido no console do Splunk Enterprise.



Campo na seção Especificar instância primária da ServiceNow	Descrição
Rótulo de ação de fluxo de trabalho	Nome do fluxo de trabalho Now Platform para sua instância de produção (primária). Este nome é o nome de uma instância Now Platform que os usuários que estão monitorando eventos Splunk identificam como

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	uma instância primária, por exemplo, ingestão de eventos da ServiceNow (produção). O padrão para este campo é Ingestão de eventos da ServiceNow (produção). No console Splunk Enterprise, este nome de fluxo de trabalho é exibido para a instância de produção (primária) na lista suspensa `Ações de evento` expandidas de uma pesquisa. Este nome é o nome da sua instância de produção. Você pode editar o nome.
URL	O URL da instância Now Platform que você inseriu no campo de rótulo de ação de fluxo de trabalho anterior. Copie o URL no navegador e cole-o neste campo do formulário.
Endpoint	Caminho da API base. Para obter mais informações, consulte a figura que segue a tabela. Se você não tiver um valor para o endpoint da sua instância de produção Now Platform, siga estas etapas. **a.** Faça login na sua instância de produção Now Platform como um usuário com a função de administrador do sistema (admin). **b.** Insira `Scripted REST APIs` no painel de navegação. **c.** Depois que o painel de navegação for atualizado, selecione o módulo **Scripted REST APIs** que será exibido. **d.** Se a Ingestão de eventos não estiver listada na coluna Nome da lista de `Scripted REST APIs` exibida, no campo de pesquisa na parte superior, insira `Ingestão de eventos`. **e.** Na coluna Caminho da API base na página atualizada, copie este valor e cole-o no campo Endpoint do formulário. Um exemplo de caminho de API base é `/api/sn_sec_splunk_v2/event_ingestion`.
Nome de usuário	Nome de usuário para sua instância Now Platform. Este nome é o nome de usuário da instância Now Platform na qual você atribuiu um usuário com a função (sn_sec_-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	splunk_v2.api_account_access) para encaminhamento manual de eventos. Para obter mais informações sobre como atribuir essa função, consulte Configure sua instância Now Platform para a integração Splunk Enterprise Event Ingestion.
Senha	Senha para sua instância Now Platform. Esta senha é a senha para a instância Now Platform na qual você atribuiu um usuário com a função (sn_sec_splunk_v2.api_account_access) para encaminhamento manual de eventos.
(Opcional) Campos na seção Especificar instância secundária da ServiceNow	Descrição Esses campos são opcionais. Você não é obrigado a especificar uma instância secundária.
Rótulo de ação de fluxo de trabalho	Nome do fluxo de trabalho Now Platform para sua instância secundária (preparação). Este nome é o nome de uma instância Now Platform que os usuários que estão monitorando eventos Splunk identificam como uma instância secundária, por exemplo, ServiceNow ingestão de eventos (preparação). No console Splunk Enterprise, este nome de fluxo de trabalho é exibido para a instância de preparação (secundária) na lista suspensa Ações de evento expandidas de uma pesquisa. Esta instância Now Platform é sua instância de preparação. Você pode editar o nome.
URL	O URL da instância Now Platform que você inseriu no campo de rótulo de ação de fluxo de trabalho anterior para a instância Now Platform secundária. Copie o URL no navegador e cole-o neste campo do formulário.
Endpoint	Caminho da API base. Este valor para o caminho da API de base para sua instância secundária é o mesmo valor que o caminho da API de base para sua instância primária. Consulte a figura anterior do formulário para obter mais informações.
Nome de usuário	Nome de usuário da sua instância de preparação Now Platform. O usuário deve ter

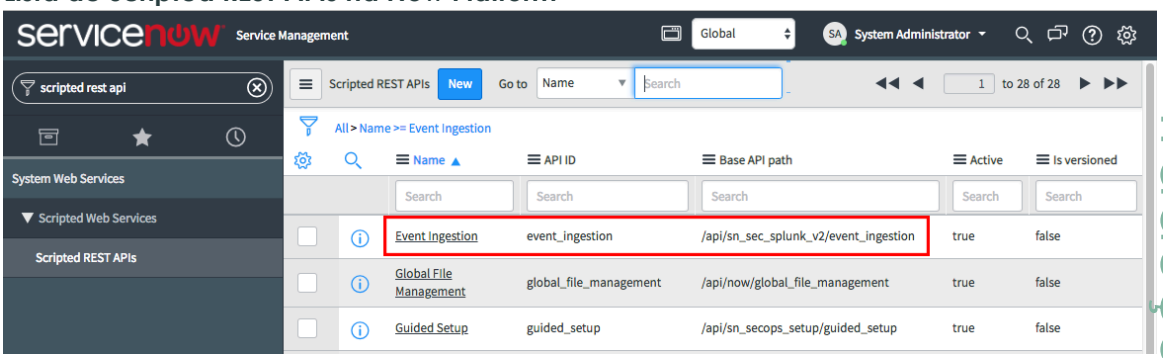
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	a função (sn_sec_splunk_v2.api_account_-access).
Senha	Senha para sua instância de preparação Now Platform. O usuário deve ter a função (sn_sec_splunk_v2.api_account_access).

A figura a seguir é um exemplo da lista de Scripted REST APIs em seu Now Platform. A lista exibe o local do valor do endpoint de uma instância Now Platform que você insere no formulário como parte da configuração da extensão ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise no console Splunk Enterprise.

Lista de Scripted REST APIs na Now Platform



3. No formulário de configuração do console Splunk Enterprise, clique em **Salvar** para salvar suas edições.

   Depois de alguns momentos, na parte superior esquerda do formulário no console Splunk Enterprise, será exibida uma mensagem informando que o registro foi atualizado com sucesso.

   Depois de salvar o formulário, os nomes (rótulos de ação de fluxo de trabalho) das instâncias Now Platform que você criou no formulário ficam disponíveis na lista de seleção Ações de evento em um evento selecionado de uma pesquisa no console Splunk Enterprise.

O que Fazer Depois

Se você ainda não salvou as pesquisas no console Splunk Enterprise, a próxima etapa é salvar pesquisas como alertas no console Splunk Enterprise.

Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion

As etapas a seguir para salvar pesquisas no console Splunk Enterprise são fornecidas para um usuário com a função de administrador Splunk Enterprise.

Antes de Iniciar

Se você já tiver pesquisas salvas e alertas acionados no console Splunk Enterprise, não será necessário modificar essas pesquisas para esta integração.

A integração do produto Now Platform® Operações de segurança com o serviço de notificação de eventos Splunk extrai informações de eventos e alertas de Splunk.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de ingerir alertas em seu ambiente Operações de segurança, configure pesquisas no console Splunk Enterprise para que você extraia automaticamente os eventos de segurança relevantes em Splunk Enterprise que deseja salvar como alertas.

Se você não tiver pesquisas salvas e alertas acionados estabelecidos para notificação quando ocorrerem eventos de segurança importantes no console do Splunk Enterprise, siga estas etapas para salvar pesquisas.

Função necessária: Splunk Enterprise administrador

Procedimento

1. Faça login na sua conta Splunk Enterprise.
2. Clique na guia **Pesquisar**.
3. No campo Nova pesquisa exibido, insira um valor para o alerta, por exemplo, Malware.
4. Para exibir os eventos relacionados à sua pesquisa, à direita do campo Nova pesquisa, clique no ícone de pesquisa ou pressione Enter.
   Os resultados da pesquisa com eventos são exibidos.
5. Para salvar a pesquisa como um alerta, no canto superior direito da página, expanda a lista de seleção Salvar como e selecione **Alerta**.
6. No formulário exibido, preencha os campos.

Campo	Descrição
Título	Nome descritivo do alerta, por exemplo, Eventos de malware. Depois de salvar esta pesquisa como um alerta, os eventos de um alerta disparado no serviço Splunk são processados automaticamente em alertas acionados usando esses dados de pesquisa. Este título de alerta acionado é usado no perfil de evento que você cria em sua instância Now Platform para identificar quais eventos são ingeridos em sua instância para a criação de incidentes de segurança Now Platform® Security Incident Response SIR.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este alerta de outros.
Tipo de alerta	Nos campos exibidos, selecione **Programado** para pesquisar este alerta em uma programação ou **Tempo real** para pesquisar continuamente este alerta.
Resultados do gatilho	Você pode preferir definir uma das seguintes condições de filtro: ◦ O número de resultados é maior ou menor que ◦ Uma vez (uma vez) para cada resultado
Ações de gatilho	Adicione ações para acionar este alerta. Expanda a lista de seleção Adicionar e clique em **Adicionar aos alertas acionados** para que ela seja exibida no formulário. Vo-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	cê pode preferir esta configuração para os alertas que ingere em sua instância Now Platform.

7. Clique em **Salvar**.
   Seu alerta é salvo e exibido na guia Alertas na página Pesquisar.
   O serviço Splunk extrai os eventos correspondendo aos critérios que você configurou no alerta. Ele armazena em cache os eventos e você solicita esses eventos a partir dos perfis que configurou na instância Now Platform. Como a extração de ingestão de eventos ocorre a partir de um cache no serviço Splunk, essa ingestão do Now Platform não afeta o desempenho na plataforma Splunk.

O que Fazer Depois

Você concluiu com sucesso a configuração necessária para a integração no console do Splunk Enterprise. Se você ainda não instalou a aplicação para a integração do ServiceNow Store, a próxima etapa é instalar a aplicação para a integração e configurá-la.

Use o editor de script para formatar valores de alerta para a integração Splunk Enterprise Event Ingestion

Use o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Além dos campos mapeados diretamente dos valores de alerta extraídos e dos valores de alerta inseridos manualmente, você pode, opcionalmente, usar o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. O editor de script muda os valores de um alerta Splunk para que os valores compatíveis com o incidente de segurança Now Platform® Security Incident Response sejam mapeados para os campos Categoria, Item de configuração (IC) e Observável.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

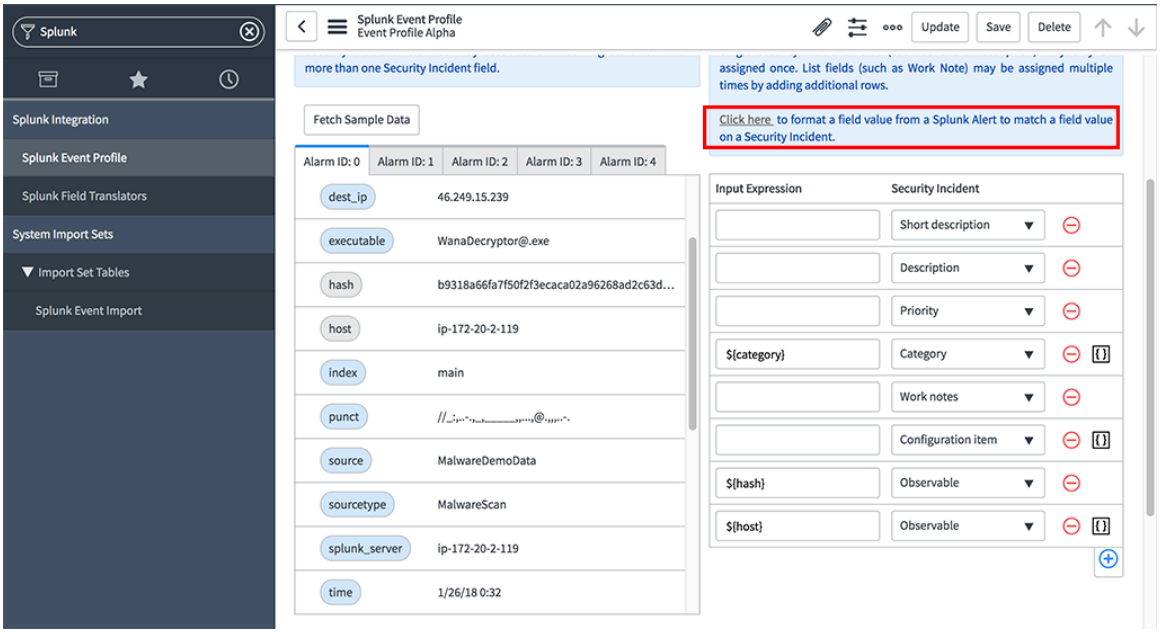
Em determinados casos, os valores de alerta Splunk Enterprise são mapeados para os campos Categoria, Item de configuração (IC) e Observável no incidente SIR e não são compatíveis. Você pode preferir editar os valores mapeados. Se você quiser converter o valor de um alerta Splunk Enterprise para um valor compatível com esses campos no incidente de segurança SIR, use o editor de script.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de script.

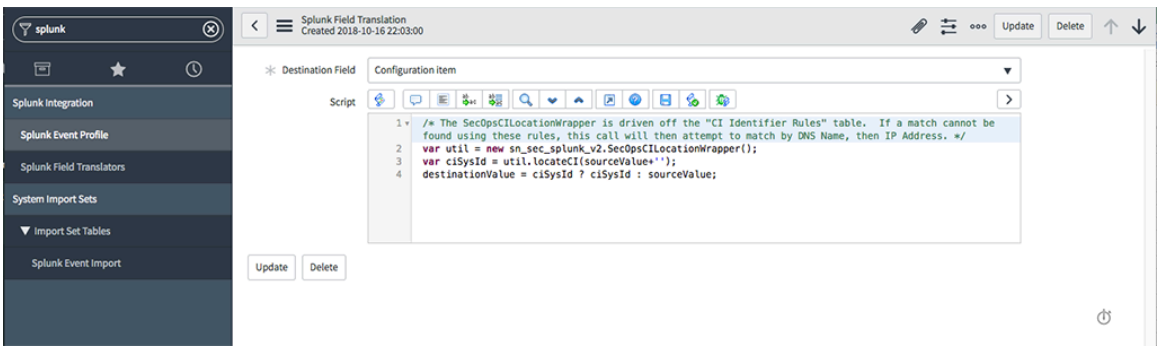


2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete `[{}]` ao lado de um campo para abrir o editor de script desse campo.

   Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um alerta, por exemplo, um valor para o item de configuração pode não ser correspondido.

   Conforme mostrado na figura a seguir, se uma correspondência para um nome de host não puder ser encontrada no Now Platform® CMBD para o campo Item de configuração, você poderá editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

   O editor é aberto com o campo exibido em Campo de destino. A imagem a seguir mostra o editor com o campo `Item de configuração` como o Campo de destino.



4. Insira todas as mudanças no script e clique em **Atualizar** para salvar suas mudanças. A tabela Splunk Traduções de Campo é exibida.
5. Feche a tabela para retornar ao formulário Mapeamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para a integração Splunk Enterprise Event Ingestion

Use esta check-list para se orientar em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem os resultados esperados para a integração.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe o andamento da configuração, instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada linha da tabela lista as tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

Funções necessárias: as funções estão listadas para cada etapa abaixo.

Procedimento

1. Como um usuário com a função de administrador Now Platform, configure sua instância Now Platform.
   - Atribua usuários com as funções sn_si.admin e sn_si.analyst conforme necessário.
   - Instale e configure um MID Server se o servidor Splunk estiver implantado em sua rede corporativa.
   - Verifique se os plug-ins ServiceNow Security Incident Response estão ativados para a versão do Now Platform.
   - Se você quiser encaminhar eventos manualmente do console [Splunk Enterprise para a instância Now Platform, verifique se atribuiu a função (sn_sec_splunk_v2.api_account_access) a um usuário com a permissão de administrador empresarial Splunk Enterprise.

   Para obter mais informações, consulte Configure sua instância Now Platform para a integração Splunk Enterprise Event Ingestion.

   Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.
2. Como um usuário com a função de administrador Now Platform, instale e configure a aplicação Splunk Enterprise Event Ingestion a partir do ServiceNow Store.
   a. Baixe e instale a aplicação em sua instância Now Platform.
   b. Configure a aplicação e conecte-se ao console Splunk Enterprise.

   Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion.
3. Opcional: Se você pretende exportar eventos manualmente do console [Splunk Enterprise para a instância Now Platform, execute as seguintes tarefas:
   a. Como um administrador Splunk Enterprise, instale, configure e habilite o ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise do splunkbase no console Splunk Enterprise.
   b. Como um administrador Splunk Enterprise, se ainda não estiver configurado, salve as pesquisas como alertas no console do Splunk Enterprise.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Para obter mais informações, consulte Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos Splunk Enterprise e Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion.

4. Como um usuário com a função Now Platform sn_si.admin, crie e nomeie um perfil de evento.

   Selecione o tipo de perfil na lista de seleção. As opções são um perfil de alerta programado que você usa para ingerir dados de amostra ou um perfil de evento que você usa para exportar dados de anexo manualmente do console Splunk Enterprise.

   - Para um alerta programado, selecione um alerta disponível.
   - Para o perfil de dados exportados manualmente, crie um novo mapa ou copie um mapa existente.

   Para obter mais informações, consulte Criar e nomear um perfil de evento para a integração Splunk Enterprise Event Ingestion.

5. Como um usuário com a função Now Platform sn_si.admin, mapeie valores ingeridos ou dados de anexo que são exportados de Splunk Enterprise para Now Platform incidentes de segurança.
   a. Buscar dados de amostra para um alerta programado.
   b. Exporte dados de anexo manualmente de Splunk Enterprise para um evento.
   c. Edite a configuração de mapeamento padrão.
   d. Opcionalmente, adicione critérios de filtragem, anexe um alerta a um incidente de segurança existente e use o editor de script.

   Para obter mais informações, consulteMapeamento de alertas e eventos para a integração Splunk Enterprise Event Ingestion e Mapear alertas para a integração Splunk Enterprise Event Ingestion.

6. Como um usuário com a função Now Platform sn_si.admin, visualize os dados de Splunk Enterprise que são exibidos em um incidente de segurança Now Platform.

   Corrija quaisquer erros ou adicione dados ausentes para que nenhuma mensagem de erro seja exibida.

   Para obter mais informações, consulte Visualizar o incidente de segurança da integração Splunk Enterprise Event Ingestion.

7. Como um usuário com a função Now Platform sn_si.admin, programe a recuperação de alertas para um perfil com um alerta programado.

   Para obter mais informações, consulte Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion.

Splunk Enterprise Security integração de ingestão de eventos para Operações de segurança por ServiceNow

A integração de ingestão de eventos notáveis Splunk Enterprise Security com o produto Security Incident Response (SIR) permite que os analistas de incidentes de segurança coletem e processem dados de eventos notáveis (chamados de notáveis).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Os dados são ingeridos continuamente com base em uma programação de pesquisa configurada e são usados por analistas para identificar e responder a possíveis ameaças cibernéticas. Os eventos de segurança coletados podem ser correlacionados a eventos notáveis em Splunk Enterprise Security e ingeridos automaticamente com esta integração. Além disso, eventos notáveis individuais podem ser encaminhados manualmente sob demanda do Splunk Enterprise Security console de análise de incidentes e da interface de emissão de relatórios para o produto Security Incident Response do Now Platform para criar incidentes de segurança.

Esta integração fornece a um analista do centro de operações de segurança (SOC) visibilidade para eventos notáveis e dados de eventos de contribuição relacionados. Esses dados podem ser integrados a Now Platform Security Incident Response (SIR) incidentes de segurança para investigação e correção adicionais. Os perfis são criados em sua instância Now Platform para lidar com diferentes tipos de eventos notáveis que são criados por meio de pesquisas de correlação em Splunk Enterprise Security. Esses perfis personalizam como diferentes Splunk campos de evento são exibidos em SIR incidentes de segurança.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Crie vários perfis de ingestão de eventos notáveis para criar incidentes de segurança SIR para tipos específicos de ameaças, como phishing e malware e tentativas de acesso não autorizado.
- Crie vários perfis de evento para encaminhamento de eventos sob demanda a partir do seu Splunk ES console de análise de incidentes para criar incidentes de segurança SIR.
- Mapeamento de arrastar e soltar de Splunk valores de campos de eventos notáveis para campos de incidentes de segurança SIR associados.
- Uma visualização do layout do incidente de segurança SIR com base em eventos notáveis de amostra para validar os detalhes do mapeamento de eventos.
- Ingerir eventos notáveis históricos, bem como eventos notáveis contínuos, novos e atualizados em intervalos configuráveis.
- Filtrar eventos notáveis que não atendem aos critérios de geração de incidente SIR, por exemplo, eventos de baixa prioridade, eventos que ainda não atingiram um status específico e assim por diante.
- Agregue eventos ou alertas a incidentes de segurança SIR existentes com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.
- Atualize eventos notáveis com base na criação de incidentes SIR e/ou condições de fechamento por meio de uma interface bidirecional para manter Splunk ES atualizações de eventos notáveis em sincronia com o status do incidente ServiceNow SIR.

Versões da Now Platform compatíveis

O plug-in com.snc.si_dep é necessário para esta integração. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações.

As Operações de segurança aplicações a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative uma aplicação de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Estrutura de integração de segurança
2. Security Support Common
3. Resposta a incidentes de segurança

Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

ServiceNow Complementos

O ServiceNow Complemento de ingestão de eventos das Operações de segurança para Splunk ES será necessário somente se você preferir encaminhar eventos manualmente do console de Revisão de incidentes Splunk Enterprise Security] para a instância Now Platform. Este ServiceNow addon está disponível em splunkbase .

Este ServiceNow Complemento de ingestão de eventos das Operações de segurança para a aplicação Splunk Enterprise no splunkbase não é necessário para a ingestão automatizada de alertas compatível com a integração.

Versões compatíveis com Splunk

Esta integração foi testada com a Splunk Enterprise versão 8.0.1 e com a aplicação Splunk Enterprise Security versão 6.2.1.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao serviço Splunk quando o servidor Splunk estiver implantado em sua rede corporativa. Se você estiver usando o serviço Splunk Cloud, um MID Server não será necessário. Consulte MID Server para obter mais informações sobre MID Servers.

Referências

Referência	Identificador de documento	Título do Documento
1	Splunk site do produto	Site do produto Splunk Enterprise Security .

Check-list

Para obter uma check-list imprimível desses tópicos, consulte Check-list para a integração de ingestão de eventos notáveis Splunk Enterprise Security. Você pode usar essa lista para monitorar o andamento enquanto trabalha nas tarefas da integração.

Termos-chave usados nesta integração

Esta seção descreve alguns dos principais termos usados nesta integração.

Os termos-chave a seguir são usados durante a instalação e a configuração do. Para obter mais informações sobre esses termos, consulte o site de documentação do produto da ServiceNow e o site e recursos do Splunk na página Recursos do Splunk.

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ServiceNow Complemento Splunkbase

Uma aplicação ServiceNow instalada no console Splunk Enterprise Security que oferece suporte à opção de encaminhamento manual de eventos da integração. O encaminhamento manual de eventos é um recurso opcional da integração. Este ServiceNow complemento Splunkbase não é necessário para a ingestão automatizada de eventos notáveis fornecida pela integração que extrai eventos de Splunk.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento de incidentes de segurança desde a descoberta e análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Splunk Enterprise Security

Splunk Enterprise Security ajuda as equipes a obter visibilidade e inteligência de segurança em toda a organização para monitoramento contínuo, resposta a incidentes, operações de SOC e fornecer aos executivos uma janela para o risco do negócio. Splunk Enterprise Security é uma solução de segurança premium que requer uma licença paga. Este serviço está em um host ou em uma oferta de nuvem Splunk que é chamada de console Splunk neste guia.

Splunk Enterprise Security evento notável

Quando uma pesquisa de correlação identifica um evento ou um padrão de eventos, ela cria um evento notável. As pesquisas de correlação filtram os dados de segurança e correlacionam eventos para identificar um tipo específico de incidente (ou padrão de eventos) e, em seguida, criar eventos notáveis.

Splunk evento

Um ou mais elementos de dados que resultam nos eventos notáveis do serviço Splunk. Na sua instância Now Platform, você pode pesquisar quais eventos [Splunk acionaram Now Platform incidentes de segurança.

MID Server

Esta aplicação facilita a comunicação e a movimentação de dados entre Now Platform e aplicações, fontes de dados e serviços externos. Esta aplicação é normalmente necessária para integração com tecnologias no local e, para esta Splunk Enterprise Security integração de ingestão de eventos, o MID Server facilita a comunicação entre o Now Platform e a instância no local de Splunk Enterprise Security. Um MID Server não é necessário se você estiver integrando sua instância Now Platform com uma instância Splunk Cloud.

Administrador de incidentes de segurança (sn_si.admin)

O usuário com esta função supervisiona a configuração da integração com o produto SIR em sua instância Now Platform.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com esta função interage e analisa incidentes de segurança no produto ServiceNow Security Incident Response.

Configure sua instância Now Platform® para a integração Splunk Enterprise Security

A seção a seguir lista as tarefas de configuração que você deve concluir na instância Now Platform® antes de instalar a aplicação a partir do ServiceNow Store.

Função necessária: administrador

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR).

   As funções a seguir são necessárias para a instalação, configuração e uso da integração em sua instância Now Platform®.

   - Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidentes de segurança (sn_si.admin).
   - Se você quiser encaminhar eventos notáveis manualmente de Splunk Enterprise Security para esta integração, um usuário com a função de administrador Now Platform® atribuirá um usuário com a função (sn_sec_splunkes.api_account_access) no Now Platform®. Esta função permite que um usuário com a função de administrador Splunk Enterprise Security acesse a API no Now Platform® que é necessária para o encaminhamento manual de eventos para esta integração.

     A função (sn_sec_splunkes.api_account_access) não será necessária para a integração se você estiver ingerindo eventos notáveis automaticamente de Splunk Enterprise Security para sua instância Now Platform®.

   - Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®:
     - Nomeia, cria e edita perfis de evento.
     - Seleciona e mapeia valores de Splunk Enterprise Security para Now Platform® incidentes de segurança.
     - Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração.
     - Programa a ingestão contínua de eventos notáveis.
     - Habilita atualizações de eventos notáveis quando um incidente SIR é criado e encerrado.
     - Atribui a função de analista de incidentes de segurança (sn_si.analyst).
     - Usuários com sn_si.analyst trabalham com incidentes de segurança.

   Para obter mais informações, consulte Gestão de funções .

2. Atribua a função de usuário Splunk.

   Atribua uma função de usuário de Analista de segurança (ess_analyst) no Splunk ES para executar todas as atividades relacionadas à integração no servidor Splunk.

3. Verifique se você está usando a versão 7.2.6 ou posterior da API Splunk. Versões anteriores não são compatíveis.

   Se você tiver acesso ao console Splunk Enterprise Security, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.

4. Verifique se você instalou e configurou um MID Server.

   Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço Splunk se o servidor Splunk estiver implantado em sua rede corporativa. Para obter informações, consulte MID Server .

   Se você estiver usando o serviço em nuvem Splunk Enterprise Security, um MID Server não será necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas.

   O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Operações de segurança aplicações necessárias para a integração.

   Verifique se as seguintes Operações de segurança aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas.

   a. Security Incident Response
   b. Security Integration Framework
   c. Suporte de segurança comum

   Para obter mais informações sobre como instalar as aplicações principais Operações de segurança, consulte e .

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação Splunk Enterprise Security de ingestão de eventos notáveis a partir do ServiceNow Store para a integração. Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security.

Se você quiser exportar eventos notáveis manualmente e sob demanda do console Splunk Enterprise Security para a integração, consulte Configure o ambiente Splunk para ingestão manual de eventos para a integração Splunk Enterprise Security de ingestão de eventos notáveis para obter mais informações.

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security

Antes de executar a integração em sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Operações de segurança em sua instância Now Platform®.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Se você não instalou a aplicação Splunk Enterprise Security de ingestão de eventos de ServiceNow Store para a integração, consulte e siga as etapas para instalá-la.
2. Depois de instalar a aplicação com sucesso, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Splunk Ingestões de eventos.
3. Para configurar a aplicação, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo Configuração de ingestões de eventos exibida, preencha os campos.

Campo	Descrição
Nome	Nome do console [Splunk Enterprise Security ou instância Splunk Cloud usada para a integração. Espaços são compatíveis com nomes, mas parênteses não são compatíveis. Por exemplo, insira `SplunkES2`.
URL base da API Splunk	URL do console [Splunk Enterprise Security ou instância Splunk Cloud. O URL deve incluir a porta da API, por exemplo: `https://mysplunkserver.com:8089`
Autenticação básica	O padrão é desabilitado. Se você estiver usando o nome de usuário da conta da API e a senha da API para configuração, marque a caixa de seleção.
Nome de usuário da conta da API	Nome de usuário que você criou para sua conta de usuário de API no console Splunk Enterprise Security.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Senha da API	Senha que você criou para sua conta de usuário de API no console Splunk Enterprise Security.
Baseado em token (disponível a partir da versão 12.0.0)	Token que você criou para sua conta de usuário de API no console do Splunk Enterprise Security.
Token	Token que você criou para sua conta de usuário de API no Splunk console de segurança empresarial.
Implantação no Local	O padrão é desabilitado. Se você estiver usando uma versão baseada no local do Splunk Enterprise Security, verifique se esta caixa de seleção está marcada.
MID Server	Opção para escolher um MID Server específico para configurar em seu ambiente, que será usado por esta integração para extrair eventos notáveis para ServiceNow. Você pode selecionar um MID Server específico na lista ou selecionar **Qualquer** para habilitar uma seleção automática de um MID Server válido na lista para esta integração. **Nota:** ◦ O MID Server selecionado durante este tempo de configuração se aplica a toda esta integração. ◦ Somente os MID Servers ativos e validados são exibidos nesta lista. Por padrão, o valor é definido como **Qualquer**. Por exemplo, há três MID Servers A, B e C. Se você selecionar **Qualquer**, um desses MID Servers será selecionado automaticamente e se aplicará a toda esta integração. Se você selecionar um MID Server específico, digamos C, o MID Server C selecionado se aplicará a toda esta integração. Se você quiser mudar o MID Server, será necessário reconfigurá-lo no bloco Configuração da aplicação.

A figura a seguir é um exemplo de um formulário preenchido para uma configuração de uma versão local do Splunk Enterprise Security com um MID Server.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada tipo de evento notável Splunk Enterprise Security que você ingere do console de análise de incidentes Splunk Enterprise Security requer um perfil de evento exclusivo em sua instância Now Platform®. No entanto, a origem que você configura no formulário Configuração de ingestões de eventos pode ser reutilizada para vários perfis Now Platform®, desde que cada perfil ingere tipos de eventos notáveis exclusivos.

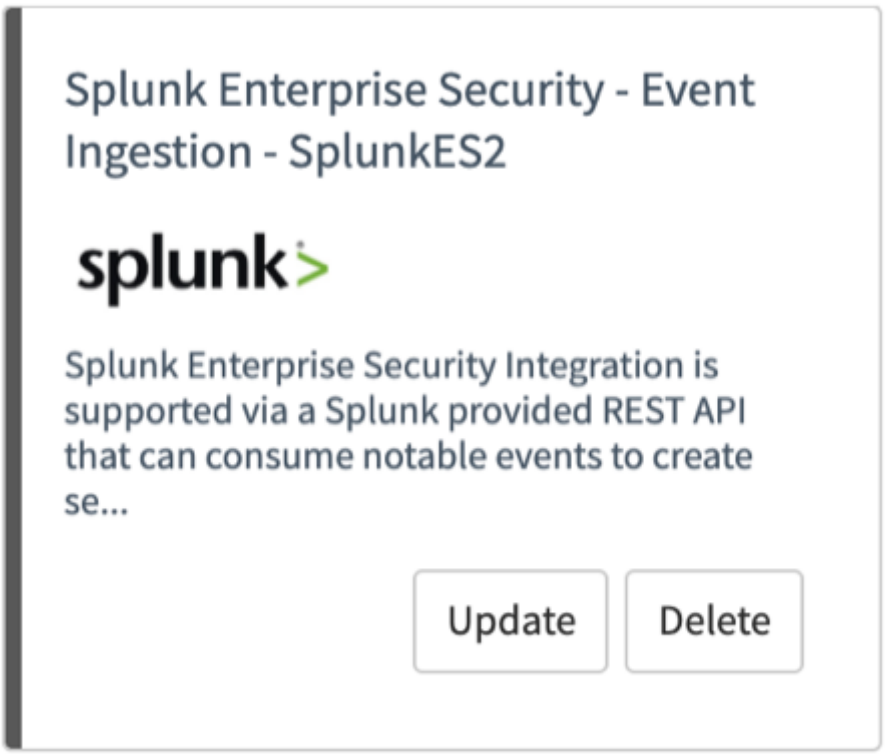
6. Clique em **Enviar**.
   Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, os botões **Atualizar** e **Excluir** são exibidos, conforme mostrado na figura a seguir.

Nota: Os usuários precisam usar a Autenticação básica ou a Autenticação baseada em token. Habilitar ambos gerará o seguinte erro.

Nota: Se os usuários preferirem atualizar os blocos de configuração existentes para baseados em token, eles precisarão habilitar Ativar esta configuração para atualizar as configurações de origem Splunk existentes para a configuração de suporte à autenticação baseada em token no módulo Splunk Configurações do Enterprise.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois de validada e enviada com sucesso, cada configuração de servidor de Ingestões de eventos Splunk é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista Mostrar configurações, selecione **Sim**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Definir Splunk configurações de segurança empresarial

Use as configurações Splunk Enterprise Security (ES) para modificar as configurações predefinidas e seus valores de acordo com seus requisitos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Splunk ES Integration** > **Configurações do Splunk ES**.
2. No formulário, preencha os campos.

Configurações do Splunk ES

Campo	Descrição
Impor um limite ao número de eventos notáveis que podem ser agregados a um único incidente.	Opção para impor um limite ao número de eventos notáveis que você deseja agregar a um único incidente. Por padrão, o valor é definido como 100.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Impor um limite ao número de incidentes de segurança que podem ser criados em um período de 24 horas.	Opção para impor um limite ao número de incidentes de segurança que podem ser criados em um período de 24 horas. Por padrão, o valor é definido como 1000.
Impor um limite ao número de valores a serem analisados em cada campo recebido de Splunk.	Opção para impor um limite ao número de valores que você deseja analisar para cada campo recebido de Splunk. Por padrão, o valor é definido como 1000.
Número de regras de correlação a serem extraídas de Splunk.	Opção para definir o número de regras de correlação a serem recuperadas de Splunk. Por padrão, o valor é definido como 500.
O parâmetro de tempo de vida útil do trabalho de pesquisa Splunk em segundos.	Opção para definir o parâmetro de tempo de vida para a pesquisa Splunk na forma de segundos. Por padrão, o valor é definido como 600.
Número de tipos notáveis para lote em uma pesquisa.	Opção para definir o número total de tipos notáveis que você deseja agrupar em uma única pesquisa. Por padrão, o valor é definido como 20.
Número de dias para reter os metadados de trabalho de pesquisa [Splunk em ServiceNow	Opção para definir o número de dias que você deseja reter os metadados do trabalho de pesquisa do Splunk em ServiceNow. Por padrão, o valor é definido como 30.
O caractere delimitador para dividir os valores em mapeamentos de campo.	Opção para definir o caractere delimitador para dividir os valores em mapeamentos de campo. Por padrão, o valor é definido como (,).
Número de minutos de sobreposição a serem adicionados ao buscar os eventos de Splunk (para superar o atraso de indexação do Splunk)	Opção para definir o número de minutos de sobreposição a serem adicionados ao recuperar os eventos de Splunk para superar o atraso de indexação de Splunk. Por padrão, o valor é definido como 30.
Extrair eventos notáveis atualizados	Opção para recuperar eventos notáveis atualizados. Por padrão, o valor é definido como Não.
Ative esta configuração para atualizar as configurações de origem Splunk	Opção para atualizar a configuração de origem Splunk existente para suporte à

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
existentes para suporte à autenticação baseada em token. Você deve atualizar a configuração de integração com detalhes do token depois que essa configuração for habilitada.	autenticação baseada em token de uma versão existente. **Nota:** Depois de fazer upgrade para a nova versão, o campo de token ficará indisponível. Você deve habilitar esta configuração para obter a autenticação baseada em token e, em seguida, atualizar a configuração de integração com detalhes do token. Por padrão, o valor é definido como Não.

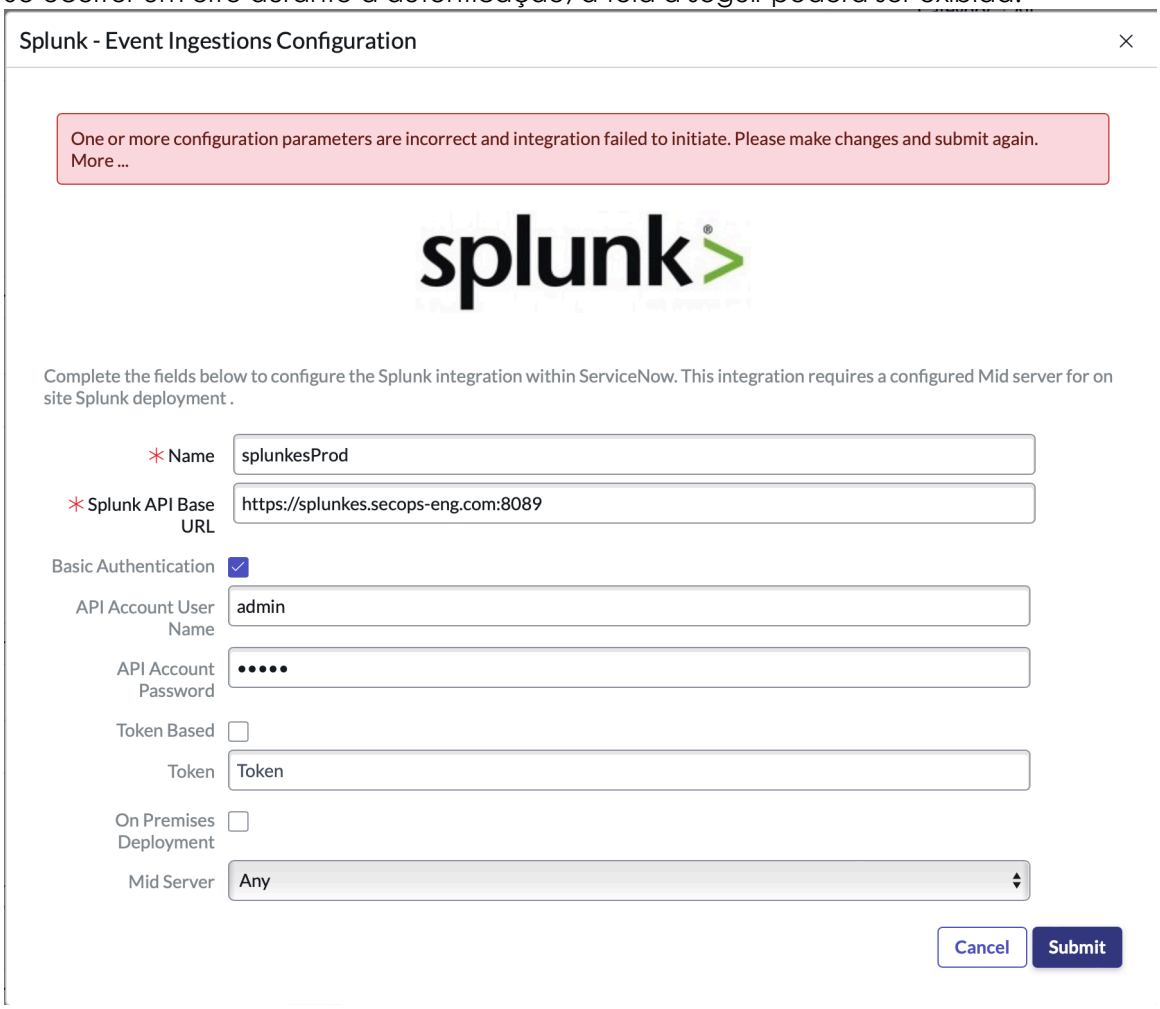
3. Clique em **Salvar**.

Erros de autenticação

Esta seção descreve alguns erros comuns de autenticação e como eles podem ser resolvidos.

Problema de validação de certificado

Se ocorrer um erro durante a autenticação, a tela a seguir poderá ser exibida:

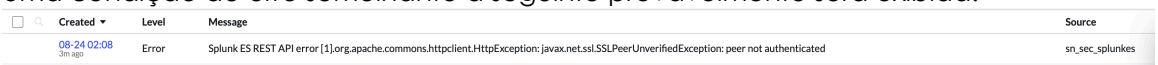


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você verificou que as credenciais da conta da API e as informações da URL base do Splunk estão corretas, esse erro pode ser devido a um problema com o certificado Splunk para a comunicação da porta 8089. A instância ServiceNow® requer um certificado válido com um nome comum que corresponda ao nome do host do servidor para estabelecer conexões seguras. Para obter mais informações, consulte Certificados . Se você vir este erro, poderá verificar se o problema se deve a um problema de certificação exibindo os logs do sistema.

Uma condição de erro semelhante à seguinte provavelmente será exibida:



Para prosseguir com a autenticação, você deve substituir o certificado padrão do Splunk que é fornecido para acesso à API na porta 8089. Para obter instruções detalhadas sobre como substituir o certificado SSL, consulte KB0778285 .

Criar e nomear um perfil de evento para a integração de ingestão de eventos Splunk Enterprise Security

Você cria um perfil de evento em sua instância Now Platform e determina quais eventos notáveis Splunk criam incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Antes que Now Platform Security Incident Response (SIR) incidentes de segurança sejam criados a partir de eventos notáveis ingeridos, os valores de campos de alertas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será criado.

De uma perspectiva de integração usando as APIs disponíveis, Splunk ES eventos notáveis são encaminhados individual e manualmente como eventos discretos notáveis ou são ingeridos automaticamente no ambiente Operações de segurança da sua instância Now Platform, dependendo do tipo de perfil definido.

Os fluxos de trabalho de integração ingerem diferentes tipos de eventos notáveis, como tentativas de acesso não autorizado e malware, por exemplo. Esses eventos notáveis são ingeridos com base nos perfis que você configura no ambiente Operações de segurança da sua instância.

Todos os notáveis são ingeridos inicialmente para um tipo de pesquisa de correlação configurado em um perfil. Os notáveis ingeridos podem ser filtrados para especificar quais notáveis criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para eventos notáveis que são identificados como de alto risco. Antes que um perfil seja ativado e ele crie incidentes de segurança a partir de eventos notáveis ingeridos, os valores de campos individuais nos eventos notáveis são mapeados para os campos correspondentes em um layout do incidente de segurança para uma visualização.

Procedimento

1. Os nomes dos perfis de evento em sua instância Now Platform devem ser exclusivos e só podem ser mapeados para um perfil de evento ativo por vez.
2. O Now Platform ingere notáveis específicos usando os fluxos de trabalho da integração. Todos os eventos notáveis que atendem aos critérios de seleção no console Splunk ES são ingeridos inicialmente na instância Now Platform.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Um perfil no seu Now Platform é um encapsulamento de um evento notável no seu console Splunk ES.
   Há um relacionamento de um para um entre eventos notáveis que são ingeridos com um perfil e conexões com o console Splunk ES : um tipo de evento notável para uma conexão.
4. Para criar perfis para eventos notáveis programados, consulte Configurar um perfil para ingestão de eventos notáveis programados.
5. Para criar perfis para encaminhamento manual de eventos, consulte Configurar um perfil para encaminhamento manual de eventos.

Configurar um perfil para ingestão de eventos notáveis programados

Dependendo do perfil definido, Splunk ES eventos notáveis são ingeridos automaticamente no ambiente Operações de segurança da sua instância Now Platform.

A tabela a seguir mostra a lista de tarefas que você precisa seguir para configurar um perfil para ingestão programada de eventos notáveis:

Etapas para configurar um perfil para ingestão de eventos notáveis programados

Tarefa	Seção
Criar um perfil de evento	Veja Criar perfis para ingestão de eventos notáveis programados
Selecionar eventos notáveis com base no nome da pesquisa de correlação	Veja Selecione eventos notáveis com base no nome da regra de correlação para o perfil para Splunk ES integração de ingestão de eventos
Mapear campos de eventos notáveis	Veja Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security
Criar mapeamentos personalizados	Veja Criar mapeamentos para Splunk ES revisão de incidentes de eventos notáveis e detalhes do evento de contribuição (ingestão programada)
Visualizar o incidente de segurança	Veja Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security
Programar e recuperar eventos notáveis novos e atualizados	Veja Programar e recuperar eventos notáveis novos e atualizados para a integração de ingestão de eventos Splunk Enterprise Security
Automatizar atualizações e fechamento de eventos notáveis com base no status do incidente SIR	Veja Automatizar atualizações e fechamento de eventos notáveis com base no status do incidente SIR

Criar perfis para ingestão de eventos notáveis programados

Você pode configurar um perfil para que eventos notáveis sejam ingeridos automaticamente.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Para criar um perfil de evento para um evento notável ou tipo de regra de correlação em sua instância Now Platform, navegue até **Splunk Integration** > **Perfil de eventos do Splunk**.
2. Se o formulário Splunk de perfil de evento não for exibido, clique em **Nome** na barra de andamento.
3. Clique em **Nova**.
4. Preencha os campos.

   Um exemplo de um formulário preenchido segue a tabela.

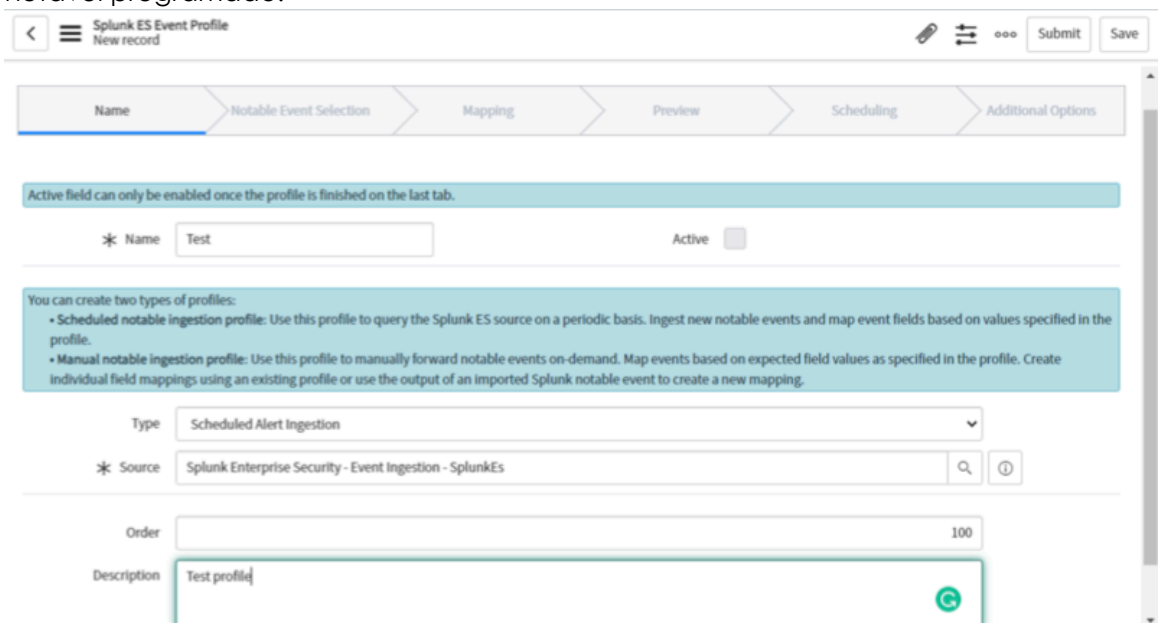
Campo	Descrição
Nome	Nome exclusivo do perfil. Se os nomes não forem exclusivos, um erro será exibido e nomes de perfil duplicados não serão salvos. Os nomes de perfil em sua instância Now Platform devem ser exclusivos.
Ativo	A caixa de seleção está desmarcada e desabilitada por padrão. Você deve concluir todas as seções no perfil antes de torná-lo ativo.
Tipo	Selecione o tipo de perfil na lista de seleção. ◦ Ingestão de eventos programados: este tipo de perfil oferece suporte a eventos notáveis que são ingeridos em uma programação configurada. Preencha os campos. ◦ Encaminhamento manual de eventos: este tipo de perfil oferece suporte a eventos notáveis que são encaminhados manualmente do seu Splunk Enterprise Security console de análise de incidentes sob demanda. Consulte as etapas a seguir para preencher o formulário para esses tipos de perfis.
Origem	Splunk servidor ou extremidade da pesquisa que você configurou para ingerir eventos notáveis. Se você tiver vários servidores Splunk configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão ingeridos para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem as mesmas condições de acionamento. O fluxo de traba-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	lho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto adicional para ajudá-lo a distinguir este perfil de outros perfis.

A figura a seguir é um exemplo de um formulário preenchido para um tipo de evento notável programado.



5. Para um perfil com um evento notável programado, escolha uma opção para continuar com a configuração do perfil.

Opção	Descrição
Continuar	Salve o perfil e avance para a etapa de Seleção de eventos.
Atualizar	Salve atualizações neste perfil e retorne à lista Splunk de Perfis de eventos.
Salvar	Salve este perfil e permaneça na página.
Excluir	Exclua este registro de perfil e retorne à lista Splunk de Perfis de eventos.

O que Fazer Depois

A próxima etapa é selecionar eventos notáveis para ingestão automática.

Selecione eventos notáveis com base no nome da regra de correlação para o perfil para Splunk ES integração de ingestão de eventos

Depois de criar um perfil para uma ingestão de tipo de evento notável programado, selecione um nome de regra de correlação Splunk Enterprise Security para este perfil para o qual você deseja mapear eventos notáveis correspondentes para um incidente de segurança Now Platform Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

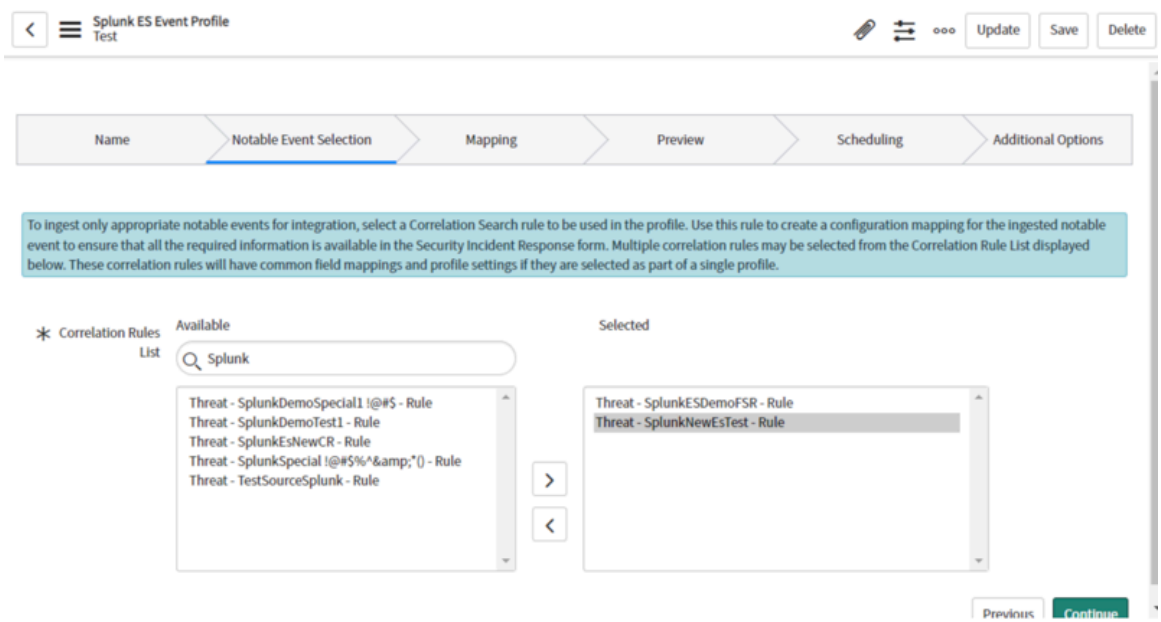
Exiba as regras de correlação disponíveis em sua instância Now Platform para que você saiba os tipos de evento notáveis para os quais deseja ingerir e criar incidentes de segurança. Selecione uma regra de correlação. Você pode selecionar um ou mais eventos notáveis na lista neste formulário.

Procedimento

1. Se a página Seleção de eventos notáveis não for exibida, selecione-a na barra de andamento para exibi-la.
2. Na lista Regra de correlação, escolha uma das seguintes opções para selecionar uma única regra de correlação ou várias regras de correlação e movê-las e movê-las para da coluna Disponível para a coluna Selecionada.

   A lista de regras de correlação neste formulário corresponde à lista de regras de correlação no seu Splunk ES console de Revisão de incidentes. Até 500 regras de correlação são exibidas neste formulário. Se houver mais de 500 regras de correlação listadas em sua Splunk ES, somente os primeiros 500 eventos notáveis serão exibidos neste formulário em sua instância Now Platform.

Opção	Descrição
No campo de pesquisa Lista de regras de correlação, insira o texto.	A coluna abaixo do campo de pesquisa é filtrada com as opções disponíveis com base no texto inserido. Selecione uma regra de correlação e, com as teclas de seta, mova o alarme selecionado de **Disponível** para **Selecionado**.
Na lista Regra de correlação, clique duas vezes em uma Regra de correlação.	A coluna **Selecionada** é preenchida com sua seleção.
Na Lista de Regras de Correlação, clique uma vez em uma Regra de Correlação.	A regra de correlação está selecionada. Com as teclas de seta, mova a regra de correlação selecionada de **Disponível** para **Selecionada**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Escolha uma opção para continuar.

Opção	Descrição
Continue ou, como alternativa, clique em Mapeamento na barra de andamento	O formulário Mapeamento é exibido. O**mapeamento** é selecionado na barra de andamento. A próxima etapa é mapear campos de eventos notáveis para um SIR incidente de segurança.
Atualizar	Seus dados são salvos e a lista Perfis de eventos notáveis do Splunk é exibida.
Anterior	A etapa **Nome** é exibida.
Excluir	Exclua este perfil de evento e a lista Perfis de eventos notáveis do Splunk será exibida.

O que Fazer Depois

Você selecionou com sucesso uma regra de correlação para um perfil programado Splunk Enterprise Security. A próxima etapa é mapear valores de eventos notáveis para campos em um incidente de segurança.

Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security

Depois de identificar a regra de correlação específica e o tipo de evento notável para o perfil, a próxima etapa é mapear campos de eventos notáveis individuais para os campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Visão geral

Para a etapa de mapeamento, você pode ingerir eventos notáveis de amostra para a regra de correlação selecionada ou exportar dados de eventos notáveis para eventos notáveis encaminhados manualmente. O processo de mapeamento de eventos é idêntico, independentemente do tipo de perfil que você está criando.

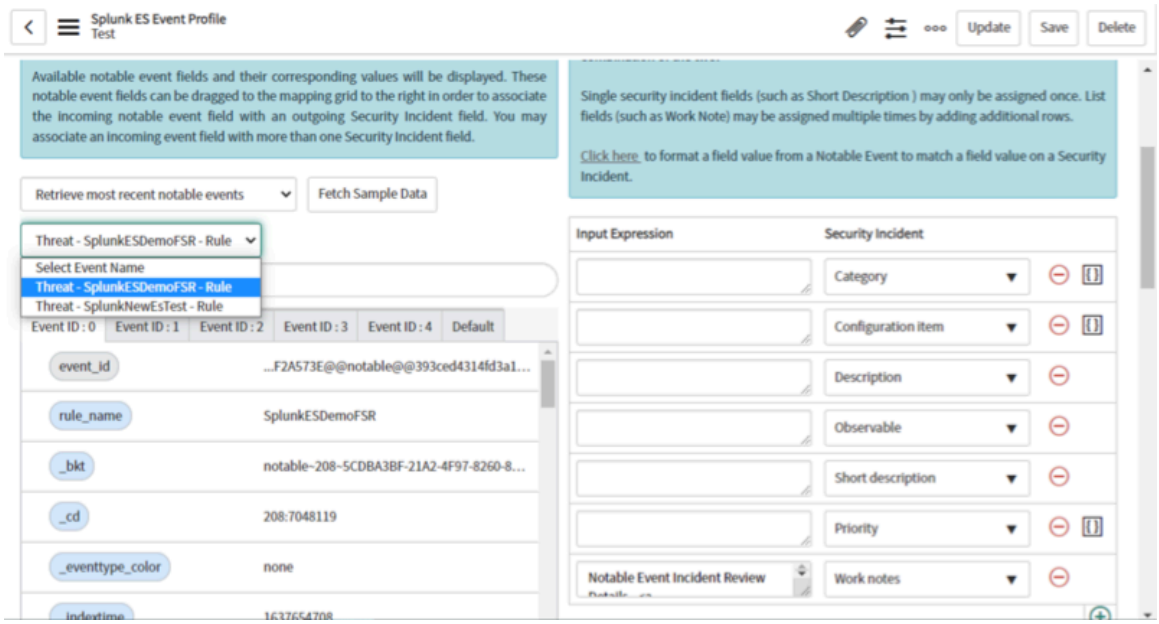
As imagens a seguir são exemplos das configurações de mapeamento padrão fornecidas para cada tipo de perfil de evento. Você pode personalizar os campos que preenchem o incidente de segurança. Durante esta fase de mapeamento, você pode garantir que todos os dados de campo de evento relevantes relevantes sejam mapeados para o local apropriado no formulário de incidente SIR e, em seguida, visualizar o incidente SIR na seção de visualização.

Se várias correlações forem usadas, os eventos notáveis poderão ser obtidos selecionando o evento necessário. Use o **Nome do Alerta** para escolher seu alerta se você tiver configurado vários alertas para ingestão.

Depois de clicar para buscar dados, os Splunk nomes de campo de evento notáveis e os valores correspondentes são preenchidos no lado esquerdo do formulário. Estes são os Splunk campos de eventos notáveis que estão disponíveis para mapear para os SIR campos de incidentes de segurança. Alguns campos podem ser mapeados várias vezes para os campos de incidente de segurança SIR.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode preferir revisar alguns eventos notáveis de amostra no console Splunk para ingerir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada como Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento. Você pode ingerir até cinco eventos notáveis de amostra de Splunk Enterprise Security para ajudar no processo de mapeamento de campo de evento notável. Há opções para ingerir os cinco eventos notáveis mais recentes para a regra de correlação selecionada ou ingerir até cinco eventos notáveis específicos com base nos IDs de eventos notáveis.

Abaixo está um resumo das etapas necessárias para mapear eventos notáveis:

- Ingestão de dados de amostra de eventos notáveis programados: para dados de amostra que são usados para perfis de eventos notáveis ingeridos automaticamente, os campos de eventos notáveis disponíveis e seus valores correspondentes são exibidos em um layout de mapeamento padrão no lado esquerdo do formulário de mapeamento depois que os dados de amostra são recuperados. As guias são exibidas para você exibir os valores de um ID de evento específico específico que você extraiu. Verifique se todos os campos críticos da seção de ingestão de amostra de evento notável à esquerda do formulário estão mapeados para ServiceNow campos de incidente de segurança à direita do formulário.
- Mapeamento de campo: edite a configuração de mapeamento arrastando campos de evento notáveis do lado esquerdo e soltando-os na seção de mapeamento de incidentes ServiceNow SIR à direita. O mapeamento à direita associa o campo de evento notável de entrada a um campo de incidente de segurança de saída.
- Experiência de mapeamento: personalize a grade de mapeamento adicionando ou removendo campos usando o ícone + na parte inferior da seção de mapeamento de campo de incidente SIR. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida (os campos mapeados estão esmaecidos e os campos azuis não estão mapeados).
- Condições de geração de incidentes: quando a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais eventos notáveis devem criar incidentes de segurança e quais eventos notáveis devem ser filtrados, por exemplo, eventos notáveis de baixa prioridade. Isso é feito na seção Condições de geração de incidentes localizada abaixo da seção Mapeamento de eventos notáveis.
- Critérios de agregação de eventos: defina critérios adicionais de agregação de eventos que agregam um evento notável de entrada a um incidente de segurança SIR existente,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em vez de criar incidentes semelhantes e potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de eventos notáveis de segurança relacionados em um único incidente de segurança.

- Conversão de campo de formato: em determinados casos, os valores de campo de evento nos eventos notáveis Splunk do Enterprise podem não ser convertidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de Malware e Infecção de Vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos para uma Atividade de Código Mal-intencionado comum no campo Categoria no incidente de segurança SIR usando o Funcionalidade Formatar tradução de campo.

A próxima etapa é ingerir eventos notáveis e mapear valores para os campos de incidente de segurança SIR.

Criar mapeamentos para Splunk ES revisão de incidentes de eventos notáveis e detalhes do evento de contribuição (ingestão programada)

Durante a etapa de mapeamento de campo de eventos notáveis, você mapeia campos de eventos individuais de eventos notáveis para campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A grade de mapeamento pode ser personalizada para o tipo de evento notável selecionado na seleção da regra de correlação. A codificação de cores dos campos de evento ajuda a rastrear os valores de evento que você já mapeou, pois eles ficam esmaecidos e todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de evento importante restante permanece não mapeada.

Mapeie até cinco eventos notáveis da coluna Ingestão de amostra de eventos notáveis à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos padrão que são normalmente campos importantes a serem preenchidos no formulário de resposta a incidentes de segurança são exibidos. No entanto, esses campos podem ser removidos e quaisquer campos adicionais podem ser exibidos usando os botões + e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. A personalização dos campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no incidente de segurança SIR.

Procedimento
1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Para um perfil com uma ingestão programada, abaixo de Ingestão de amostra de eventos notáveis, clique em **Buscar dados de amostra** para extrair os eventos notáveis

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

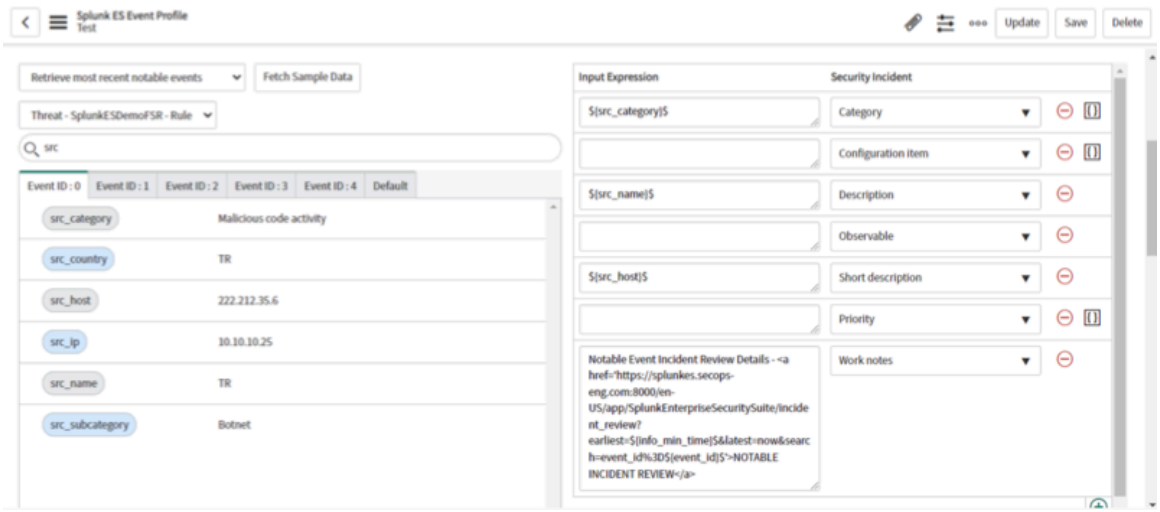
de amostra mais recentes do console Splunk Enterprise para a regra de correlação selecionada.

Nota: Você pode extrair os eventos notáveis de amostra mais recentes ou fornecer os IDs de evento notáveis exclusivos para os eventos notáveis específicos que deseja usar para sua experiência de mapeamento de eventos notáveis.

Os campos de eventos notáveis e resultados de valores são exibidos como guias individuais. Você pode ingerir até cinco eventos notáveis.

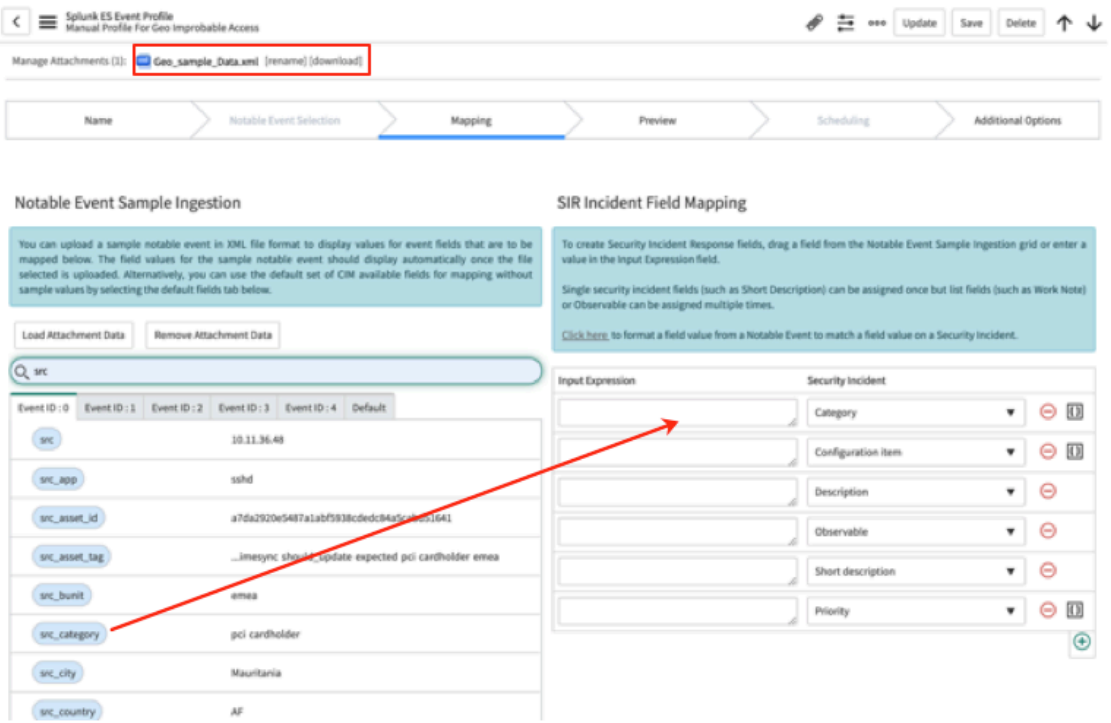
A extração de eventos notáveis de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

Na figura a seguir, os pares de valores de nome de campo do evento notável ingerido ou os eventos de amostra importados são exibidos no lado esquerdo deste formulário após a conclusão da extração de ingestão. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente SIR do formulário.



3. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
4. Arraste o nome do campo, por exemplo, `src_category`e solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



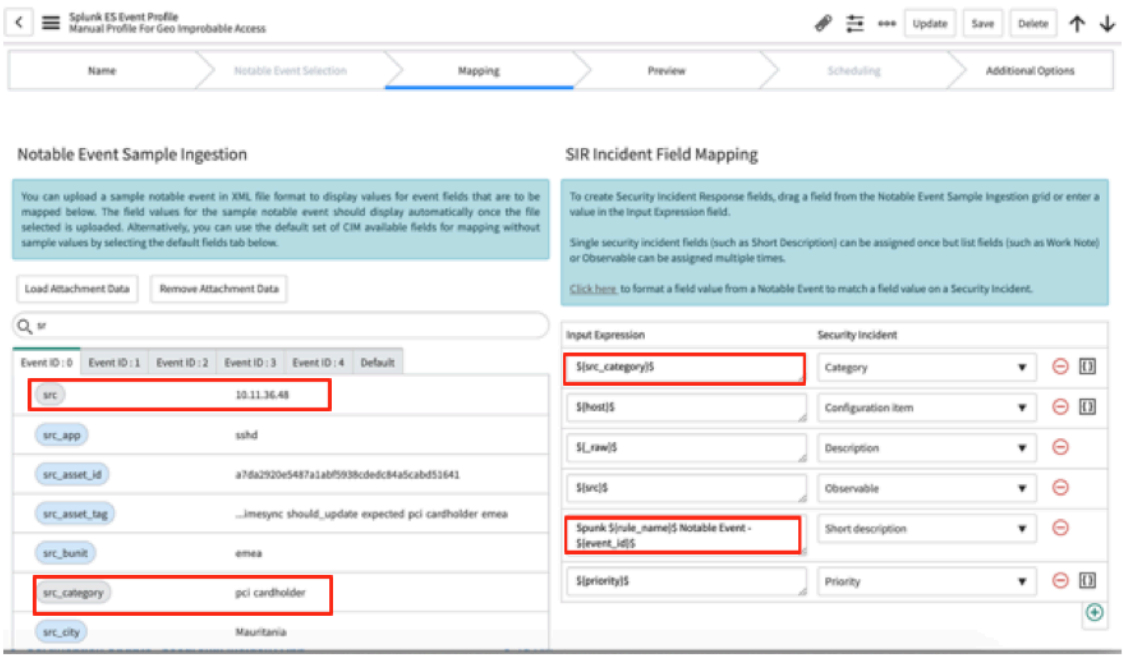
O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, `src_category` é mapeado para o campo de `categoria` no incidente de segurança. No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo à direita. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudá-lo a garantir que nenhum campo de evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Os campos em azul claro à esquerda indicam que um campo de evento notável ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo notável de entrada a mais de um campo em um incidente de segurança.

Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

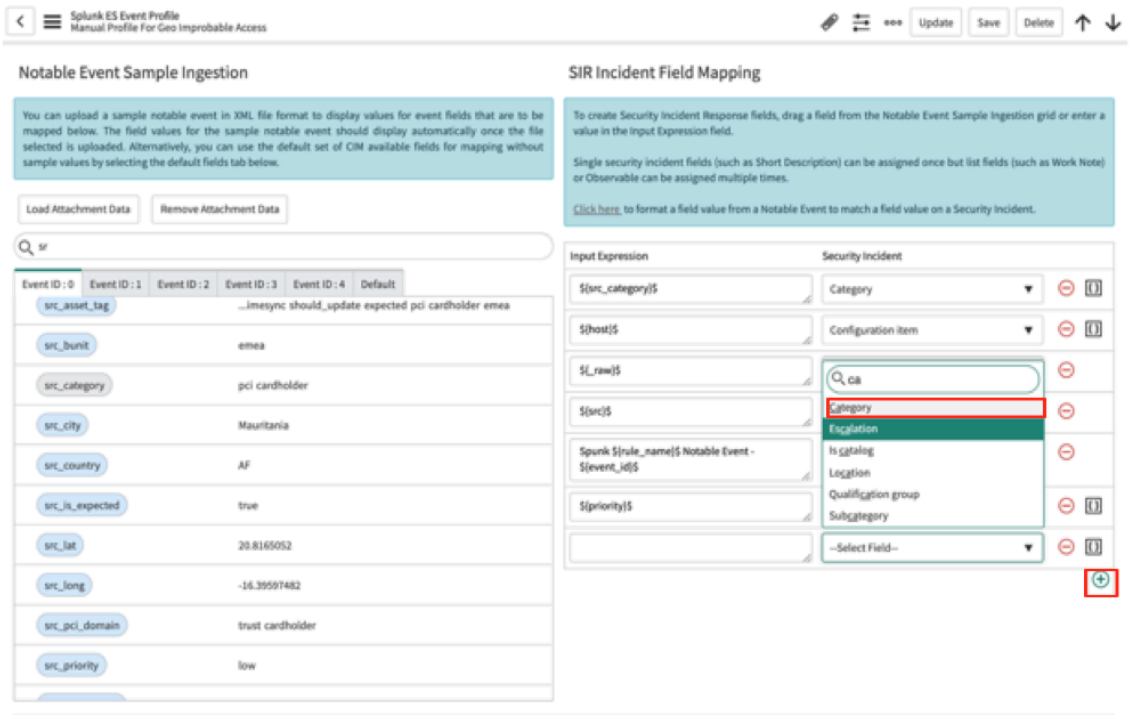
a. À direita do formulário na seção Mapeamento de campo de incidente SIR, na parte inferior da grade, clique no ícone de mais.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Na lista expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, a `categoria` tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores para os campos de eventos notáveis no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidentes SIR já mapeados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista na qual você pode escolher várias opções e tentar mapear uma opção para esse campo que não está exibido na lista, o campo não será preenchido no incidente de segurança.

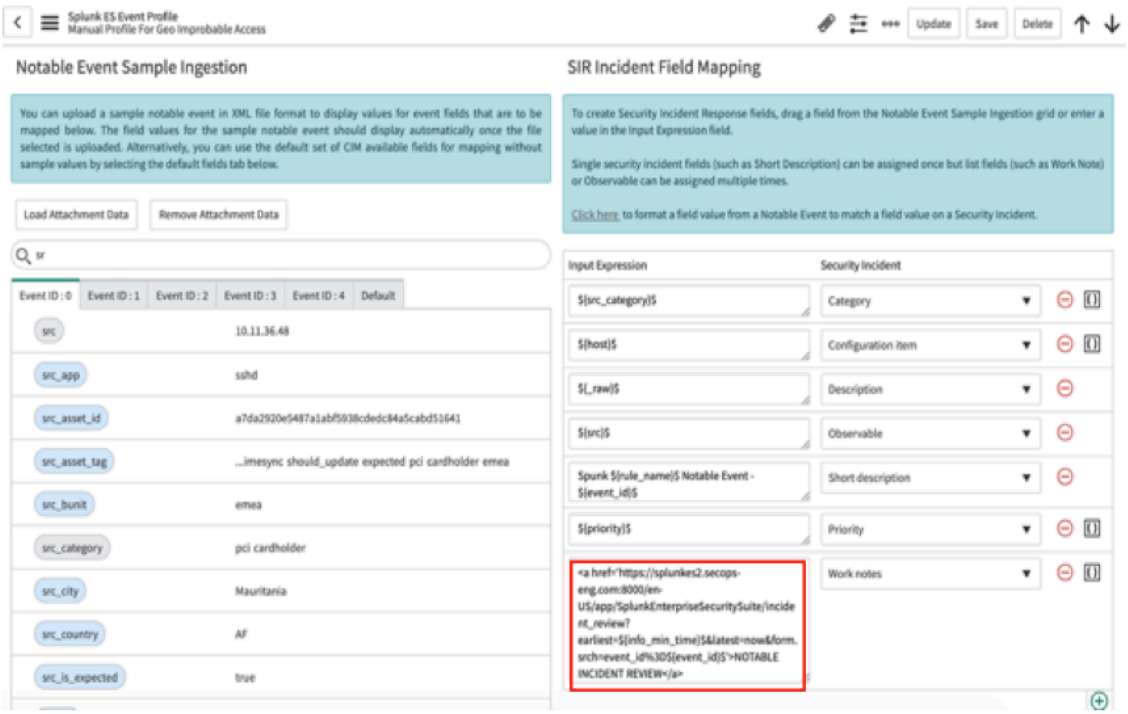
c. Como alternativa, digite um valor no campo Pesquisar para a nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o **ID do evento** desejado no campo Expressão de entrada.

6. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.
A figura a seguir é um exemplo de um mapeamento editado. No campo inferior à direita, o campo Anotações de trabalho é adicionado e tem mais de um valor. Observe que, para o campo de cadeia de caracteres de texto longo, você pode expandir o campo de mapeamento para ver a cadeia de caracteres completa e redimensionar conforme necessário, puxando o canto inferior direito do campo, conforme indicado na captura de tela abaixo com o campo Anotações de trabalho adicionado:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Aviso: Observe que na seção **Mapeamento de campo de incidente SIR**, o URL e o número da porta mencionados no campo **Expressão de entrada** são apenas um exemplo e não o URL ou o número da porta fornecidos prontos para uso.

Na visualização, esses valores são exibidos nas Anotações de trabalho no incidente de segurança. Como o valor é para um campo que você adicionou à seção de mapeamento e há vários valores mapeados para o campo Anotações de trabalho, os valores são exibidos conforme inseridos. Neste exemplo, os espaços e sinais de pontuação que você inseriu no campo são exibidos na seção Itens relacionados como uma anotação de trabalho na visualização do incidente de segurança.

A imagem a seguir é um exemplo de como os valores na imagem anterior são exibidos no incidente de segurança.

Related Items

Field Name	Field Value
Work Note	Category: Malware Activity | destination IP: 78.46.123.180
Work Note	Source: MalwareDemoData Top 100 events with 15 host machines

7. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de scripts, consulte Use o editor de script para formatar valores de alerta para a integração Splunk Enterprise Event Ingestion.

Incluindo hiperlinks para revisão de incidentes de eventos notáveis e eventos de contribuição

Além de campos de mapeamento, o *sn_si.admin* pode mapear um valor de cadeia de caracteres que permite ao analista de segurança que está trabalhando em um incidente vincular de volta à revisão de incidentes de eventos notáveis no console Splunk

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enterprise Security, bem como aos eventos de contribuição subjacentes que fazem parte da pesquisa de detalhamento.

Os seguintes valores de cadeia de caracteres contêm o nome do servidor Splunk Enterprise Security e as variáveis apropriadas que podem ser usadas para hipervincular esses detalhes:

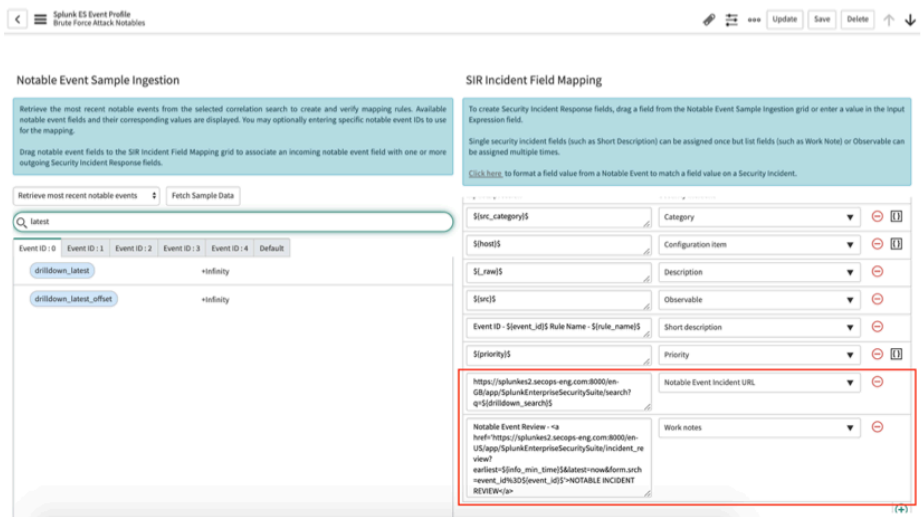
- **Hiperlink de revisão de incidentes de eventos notáveis**: `https://splunkes2.secops-eng.com:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earlist=${info_min_time}$&latest=now&form.srch=event_id%3D${event_id} $`

  em que `splunkes2.secops-eng.com:8000` é a origem do servidor Splunk e `info_min_time` e `event_id` são valores de campo de evento extraídos dos eventos notáveis.

- **Eventos de contribuição de eventos notáveis (pesquisa de detalhamento) Hiperlink**: `https://splunkes2.secops-eng.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/search?q=${drilldown_search}$`

  em que `splunkes2.secops-eng.com:8000` é a origem do servidor Splunk e " `dirdown_search` " é um valor de campo de evento extraído dos eventos notáveis.

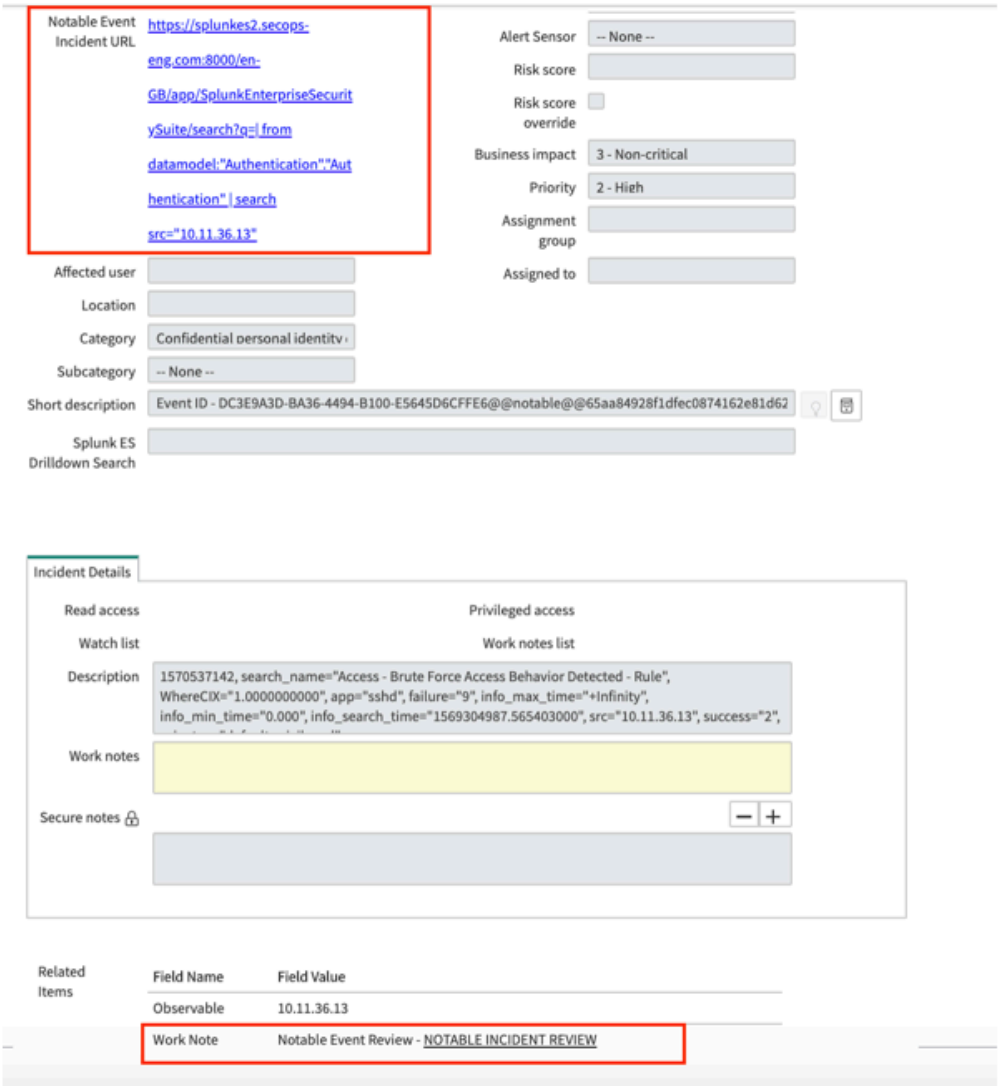
A imagem a seguir mostra a URL de revisão de incidentes de eventos notáveis mapeada para o campo de anotação de trabalho e o hiperlink de eventos contribuintes de eventos notáveis (pesquisa de detalhamento) mapeada para um campo personalizado chamado URL de incidentes de eventos notáveis:



A imagem a seguir é a visualização de incidentes de SIR com o hiperlink de revisão de incidentes de eventos notáveis e a URL

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Condições de filtragem de geração de incidente

8. Opcional: Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um evento notável de entrada deve satisfazer para criar um incidente de segurança SIR.
   Para definir condições de geração de incidentes, siga estas etapas.

   a. Role até a seção Condições de geração de incidente no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

      (Optional) O Construtor de condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

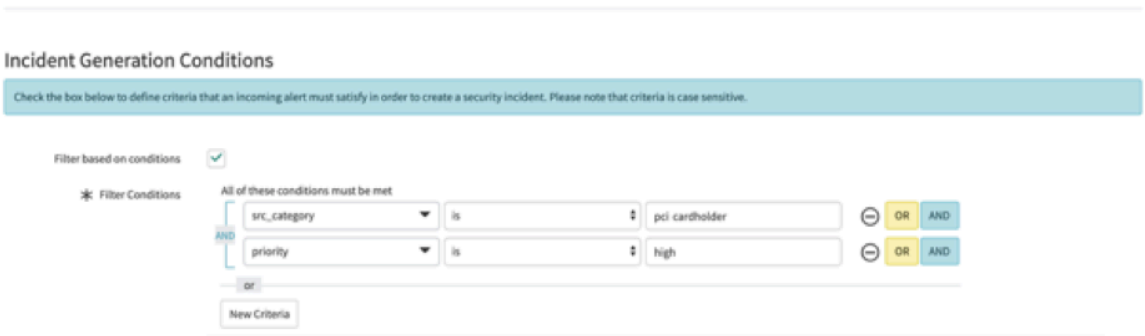
As opções nas listas do primeiro campo no construtor de Condições de filtro correspondem aos campos que são exibidos na seção Ingestão de amostra de evento notável para os eventos que você ingeriu. Esses campos são dinâmicos e mudam dependendo dos Splunk eventos notáveis que você ingere ou do evento selecionado para as amostras de eventos notáveis encaminhadas manualmente. Os critérios inseridos diferenciam maiúsculas de minúsculas e devem corresponder exatamente aos valores do evento notável Splunk Enterprise Security. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console Splunk Enterprise Security e revisar seus eventos notáveis para as palavras-chave.

b. Usando as listas e os campos do construtor de condições, defina filtros para a primeira linha.

c. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
Se **E** for selecionado, todas as condições deverão ser atendidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

d. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser atendidas antes que os incidentes de segurança sejam criados.



(Optional) Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Esse tipo de filtragem de condição de geração de incidente ajuda a restringir os eventos de segurança e limitar o número de incidentes de segurança desnecessários que você cria sem modificar a pesquisa de correlação subjacente ou os filtros em

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk. Se critérios de filtragem adicionais forem definidos, somente eventos notáveis que correspondam a todos os critérios serão mapeados para incidentes.

Nota: Se algum dos nomes de campo de evento tiver caracteres especiais, como aspas (“), hifens ('), sublinhados (-), arroba (@) ou e comercial (&), esses caracteres poderão precisar ser substituídos para fins de tradução de mapeamento e, possivelmente, crie um nome de evento duplicado. O mapeamento pode ser feito corretamente, mas um sufixo numérico é anexado para diferenciar campos com nomes de evento duplicados. Por exemplo, se o primeiro campo de evento for `alerts.alert` e o segundo campo de evento for `alerts@alerts`, esses campos não poderão ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de evento e o campo é renomeado para `alerts@alert(1)`.

(Optional) Critérios de agregação de eventos para lidar com notáveis semelhantes e evitar incidentes duplicados

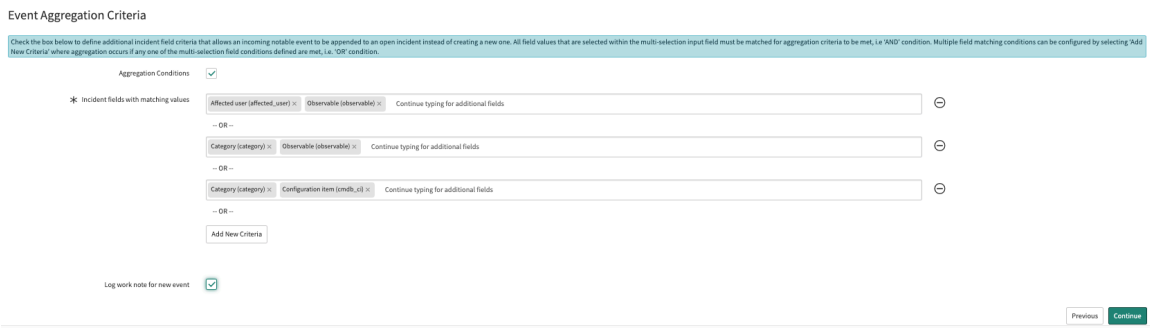
9. Opcional: Para evitar a criação de incidentes de segurança duplicados, defina critérios de agregação de eventos adicionais para que os eventos notáveis de entrada sejam agregados a um incidente de segurança aberto.
Para definir os critérios, siga estas etapas abaixo.

   a. Role até a seção Critérios de agregação de eventos no formulário e marque a caixa de seleção **Condições agregadas** para habilitar essa opção.

      (Optional) Os campos de Incidente com valores correspondentes são exibidos. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

   b. No campo de entrada de seleção múltipla, selecione os valores de campo que você deseja corresponder em incidentes de segurança existentes em seu Now Platform.

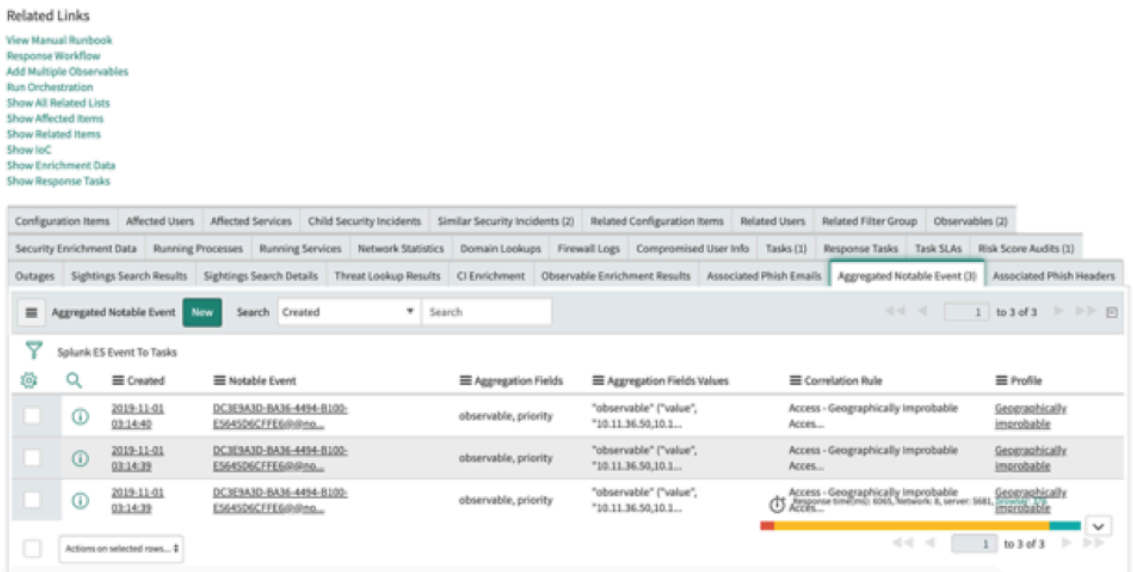
   c. Use **Adicionar novos critérios** para selecionar várias condições de correspondência de campo.
      Todos os valores de campo selecionados no campo de entrada de seleção múltipla são correspondidos para critérios de agregação usando a condição E. Clique em **Adicionar novos critérios** para selecionar várias condições de correspondência de campo em que a agregação ocorre se qualquer uma das condições de campo de seleção múltipla definidas for atendida usando a condição OR.



Se um novo evento notável corresponder a todos os valores selecionados nas condições do campo de agregação na etapa de mapeamento, o novo evento notável será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

eventos notáveis agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os eventos notáveis agregados em um incidente de segurança são exibidos na lista relacionada Splunk de eventos para tarefas. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que esses eventos notáveis estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida, role para o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.



d. Opcional: Para registrar uma anotação de trabalho para um novo evento notável que foi adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra que um novo notável foi adicionado junto com um link para os detalhes do alerta e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho em sua seção de mapeamento.

Você mapeou com sucesso valores de um evento notável Splunk para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidente. Você também anexou eventos notáveis a incidentes de segurança SIR existentes quando os valores do campo de evento correspondem aos critérios de agregação configurados.

10. Escolha um para continuar com a configuração do perfil.

Opção	Descrição
Continuar	O formulário Mapeamento é exibido. A**visualização** está selecionada na barra de andamento. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR.
Atualizar	Seus dados são salvos e a lista Perfis de eventos do Splunk é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Anterior	O formulário Seleção de eventos notáveis é exibido.
Excluir	Exclua este perfil de evento e a lista Perfis de eventos do Splunk será exibida.

O que Fazer Depois
A próxima etapa é visualizar os valores que você mapeou no incidente de segurança.

Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security

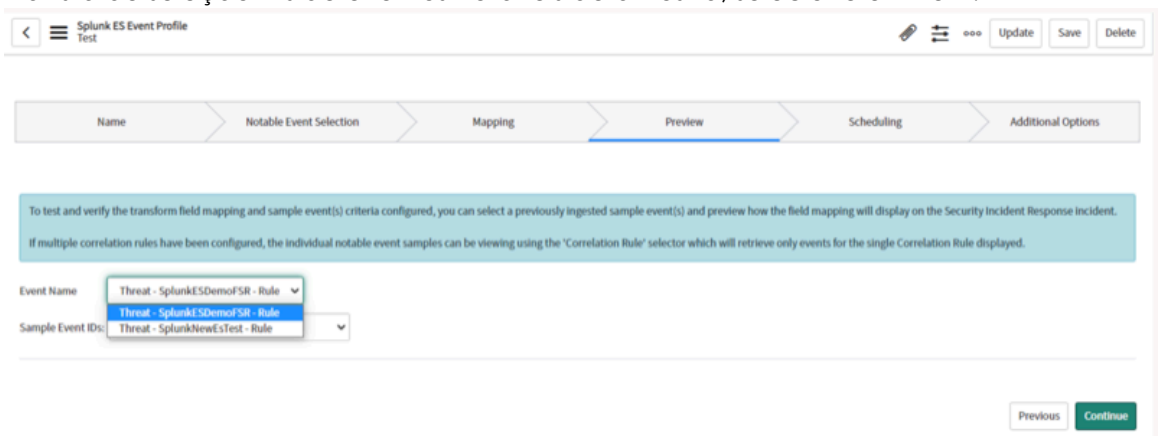
Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um Now Platform® Security Incident Response (SIR) incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos notáveis que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto SIR.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Na lista de seleção Nome do evento, selecione um item se vários eventos foram usados.
3. Selecione IDs de evento na lista de seleção IDs de evento notáveis de amostra.
4. Na lista de seleção IDs de eventos notáveis de amostra, selecione um item.

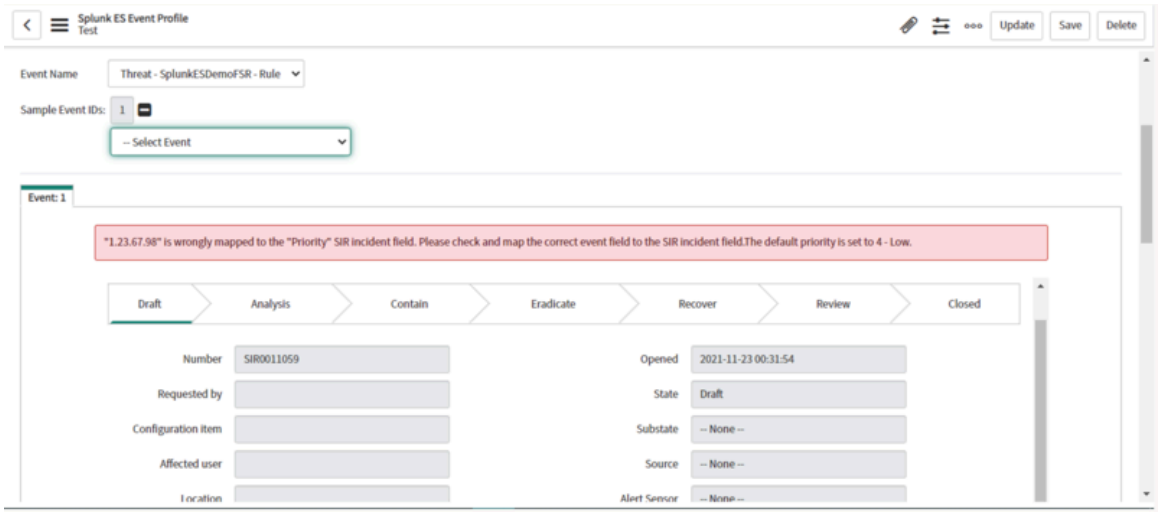


   O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.

5. Revise o mapeamento de campo dos valores de evento notáveis no incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



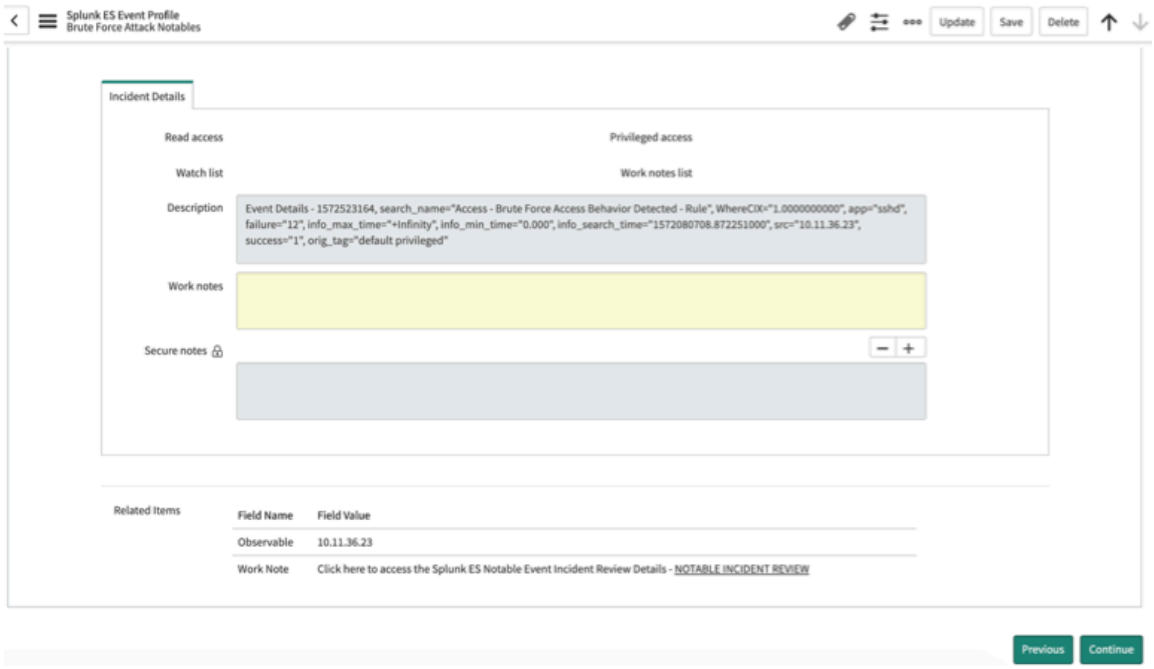
A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um valor de campo do evento notável não tem um valor aceitável para o campo de referência no formulário de incidente SIR. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para o campo `Item de configuração` no ServiceNow® banco de dados de gestão de clientes (CMDB). Como resultado, este valor de campo mapeado não aparecerá no formulário de incidente de segurança SIR sem modificações adicionais.

6. Para resolver este erro, clique em **Mapeamento** na barra de andamento.
7. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
8. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

   A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança SIR depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos das Splunk Enterprise Security amostras de eventos notáveis. O primeiro campo Anotações de trabalho não tem valor. Este campo foi deixado em branco na grade de mapeamento durante a etapa de mapeamento. Os campos de anotação de trabalho adicionais que têm valores foram adicionados à seção de mapeamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Depois de corrigir todos os erros e verificar se os campos estão como você deseja, escolha uma opção para continuar.

Opção	Descrição
Continuar	O formulário Programação é exibido para perfis com eventos notáveis programados. A**programação** é selecionada na barra de andamento.
Concluir	Para perfis configurados para encaminhamento manual de eventos, clique em **Concluir**. Não há etapa de programação para perfis com dados de evento que são exportados sob demanda diretamente do console Splunk Enterprise Security.
Atualizar	Seus dados são salvos e você retorna à lista Splunk de Perfis de eventos.
Anterior	A etapa Mapeamento na barra de andamento é exibida.
Excluir	Exclua este perfil de evento e a lista Splunk de Perfis de Evento será exibida.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campos no incidente de segurança, a próxima etapa é Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion.

Programar e recuperar eventos notáveis novos e atualizados para a integração de ingestão de eventos Splunk Enterprise Security

Para perfis de ingestão de eventos notáveis automatizados, esta etapa é necessária na configuração do perfil de evento. Durante esta etapa, você pode verificar as

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configurações padrão para recuperação de eventos notáveis ou modificar a programação conforme necessário. Esta etapa também permite que você recupere eventos notáveis históricos usando um intervalo de datas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Para perfis de ingestão automatizada de eventos notáveis, você escolhe se deseja ingerir eventos históricos notáveis durante a etapa de Programação. Você também escolhe com que frequência pesquisará novos eventos notáveis futuros e eventos notáveis atualizados que correspondam à configuração do perfil de alerta.

Para perfis de ingestão de eventos notáveis automatizados, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação de alertas. Esta é uma etapa necessária para todos os processos de configuração de perfil de evento para perfis de alertas programados.

Você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de eventos Splunk pode ser afetado pelos diferentes intervalos de pesquisa. Ao programar, você pode preferir equilibrar a redução da sobrecarga de pesquisa no servidor Splunk Enterprise Security com o desejo de ser notificado assim que possível quando um evento notável for criado ou atualizado. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo eventos notáveis novos e atualizados

Quando a programação de pesquisa é definida, o trabalho agendado extrai eventos notáveis novos e atualizados que foram extraídos anteriormente, mas não atenderam aos critérios de filtragem de incidentes. Isso oferece a flexibilidade de criar incidentes com base em critérios que podem não estar presentes quando um evento notável é criado pela primeira vez, mas se torna disponível após uma atualização, por exemplo, durante a fase de investigação. Depois que um incidente é criado para um evento notável específico, suas atualizações subsequentes são ignoradas, pois espera-se que o incidente agora esteja sendo tratado como um incidente de segurança ativo ServiceNow®. No entanto, todos os outros notáveis que foram ingeridos anteriormente, mas não atenderam aos critérios de geração de incidentes, continuarão a ser extraídos e verificados em relação aos critérios de geração de incidentes até que se tornem parte de um incidente ativo.

Procedimento
1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando eventos notáveis são extraídos do console Splunk Enterprise Security.

Opção	Descrição
◦ Campo de ingestão de eventos contínuos selecionado ◦ Campo de recuperação única limpo	Evento contínuo Com base na configuração padrão, a instância Now Platform extrai do servidor Splunk Enterprise Security eventos notáveis novos e atualizados a cada cinco minutos. Os incidentes de segurança serão criados se eventos notáveis forem encontrados e os critérios de filtragem de geração de in-

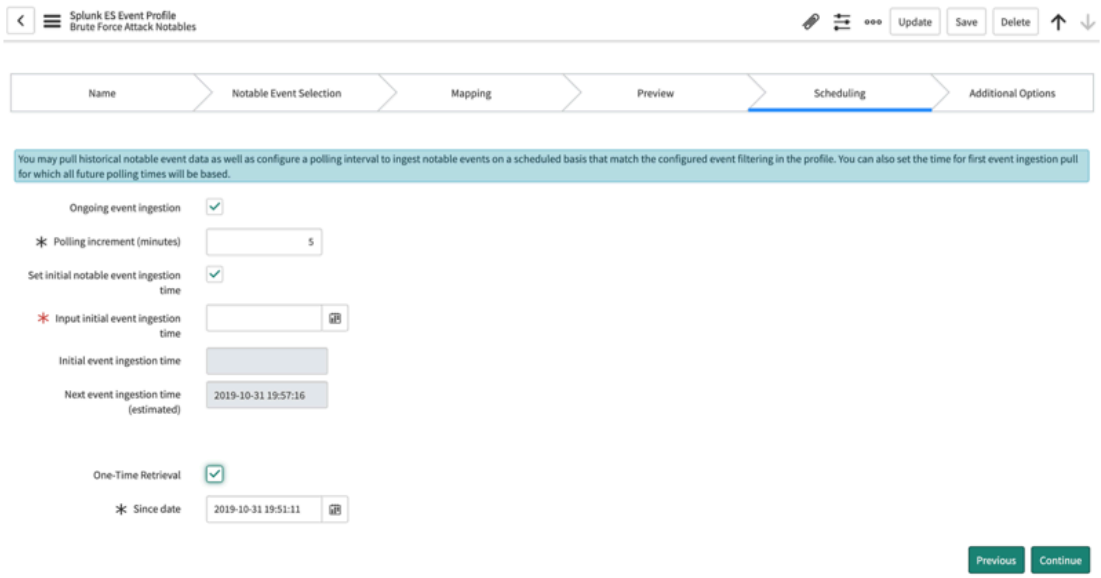
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	cidentes forem correspondidos. Para equilibrar a sobrecarga de pesquisa de ingestão para obter os dados mais atuais, cinco minutos é a configuração padrão. No entanto, este valor pode ser modificado para até um minuto, se necessário.
◦ Campo de Evento Notável em andamento limpo ◦ Campo de recuperação única selecionado	Recuperação Única Use esta configuração se quiser que uma extração única inclua eventos históricos notáveis. Quando esta configuração é definida, um perfil é usado uma vez para recuperar eventos notáveis de eventos históricos que são baseados em um intervalo de datas. À direita do campo Data desde, clique no ícone de calendário. No calendário exibido, selecione a data em que deseja começar a extrair alertas. Começando com o valor de data Desde, eventos notáveis são recuperados até a data atual. Observe que você pode retroceder até sete dias a partir da data atual. Esta funcionalidade não tem como objetivo recuperar quantidades significativas de eventos históricos de Splunk Enterprise Security por motivos de arquivamento, mas sim uma quantidade mínima de eventos em andamento que estão sendo trabalhados ativamente no momento da ativação do perfil. Depois que os eventos notáveis forem extraídos, esta configuração não recuperará mais eventos notáveis para este perfil a partir da data atual. Esta configuração preenche o incidente de segurança com todos os eventos notáveis encontrados para o intervalo inserido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como um exemplo para programar um tempo de ingestão de eventos notáveis inicial, se você tiver uma verificação de segurança diária Splunk que é executada uma vez por dia às 4h, horário local, você pode configurar o perfil de eventos notáveis correspondente em sua instância Now Platform para ser executado em 4 :05 AM, horário local, para capturar o evento de falha de segurança imediatamente e criar um incidente de segurança. Insira `04 05 00` no campo Ingestão de evento inicial. No campo Incrementar (minutos), insira `1440` (24 horas) para programar a próxima ingestão de eventos por 24 horas a partir da ingestão de eventos inicial. O tempo de ingestão do evento inicial e o tempo de ingestão do próximo evento são exibidos nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

a. Com a página Programação exibida, marque a caixa de seleção **Ingestão de eventos contínuos** para habilitar essa opção.

b. No campo Incrementar (minutos), insira `1440` (24 horas).

c. Clique na caixa de seleção **Selecionar ingestão de evento inicial** para habilitar a edição dos campos Ingestão de evento inicial e Próxima ingestão de evento.

d. No campo Ingestão de evento inicial, insira `04 05 00`.
No campo A ingestão do próximo evento (estimada), a hora da ingestão do próximo evento é exibida.

4. Clique em uma das opções a seguir para continuar com a configuração do perfil.

Opção	Descrição
Continuar	O formulário Opções adicionais é exibido. A**opção Opções adicionais** está selecionada na barra de andamento. A próxima etapa é atualizar os eventos notáveis quando o incidente SIR é criado e/ou encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Atualizar	Seus dados são salvos e a lista Splunk Perfis de segurança do evento é exibida.
Anterior	O formulário Programação é exibido.
Excluir	Exclua este perfil de evento e a lista Splunk Enterprise Security de Perfis de Evento será exibida.

Automatizar atualizações e fechamento de eventos notáveis com base no status do incidente SIR

Os incidentes de segurança podem ser criados e atualizados depois de serem criados com uma interface bidirecional com a integração Splunk Enterprise Security.

Antes de Iniciar

A integração Splunk Enterprise Security tem uma interface bidirecional que permite que eventos notáveis criem incidentes de segurança, bem como atualizem os eventos notáveis após o incidente de segurança ser criado e/ou encerrado.

Os detalhes relevantes do incidente incluem SIR número do incidente, grupo de atribuição, SIR URL do incidente. Esta seção é a parte final da configuração do perfil que fornece capacidades opcionais para atualizar os Splunk Enterprise Security eventos notáveis.

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração para atualizar eventos notáveis com base em atualizações de incidentes de segurança.

Opção ou campo	Descrição
Atualizar eventos notáveis após a criação do incidente SIR	Selecione esta opção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente de segurança for criado a partir do evento notável. Isso pode ocorrer para os eventos notáveis de acionamento inicial que criam o incidente de segurança, bem como para eventos agregados.
Atualização de status do evento notável inicial	Você deve selecionar uma opção de status no menu que exibe todos os valores de status disponíveis recuperados do servidor Splunk Enterprise Security. Isso pode incluir um status criado personalizado, como ServiceNow - Atribuído conforme mostrado na captura de tela abaixo. Selecione o valor de status a ser definido para todos os eventos notáveis quando um incidente de segurança for criado para um evento notável ingerido. Isso inclui notáveis que criam novos incidentes e notáveis que são ingeridos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	e agregados a um incidente aberto existente.
Comentários iniciais retornados para o evento notável	Além de atualizar o valor do status de notificação, você também pode publicar comentários no histórico de análise de incidentes de eventos notáveis. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente Security Incident Response.
Fechar eventos notáveis após o fechamento do incidente de SIR	Selecione esta opção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente de segurança for encerrado a partir do evento notável. Isso ocorrerá para os eventos notáveis de acionamento inicial que criam o incidente de segurança, bem como para os eventos agregados.
Atualização de status de evento notável de fechamento	Você deve selecionar uma opção de status no menu de lista que exibe todos os valores de status disponíveis que são recuperados do servidor Splunk Enterprise Security. Isso pode incluir um status criado personalizado, como ServiceNow - Atribuído conforme mostrado na captura de tela abaixo. Selecione o valor de status a ser definido para todos os eventos notáveis quando um incidente de segurança for criado para um evento notável ingerido. Isso inclui notáveis que criam novos incidentes, bem como notáveis que são ingeridos e agregados a um incidente aberto existente.
Comentários de fechamento retornados para o evento notável	Além de atualizar o valor do status de notificação, você também pode publicar comentários de fechamento no histórico de análise de incidentes de eventos notáveis. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo adicionar ou modificar as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente Security Incident Response.

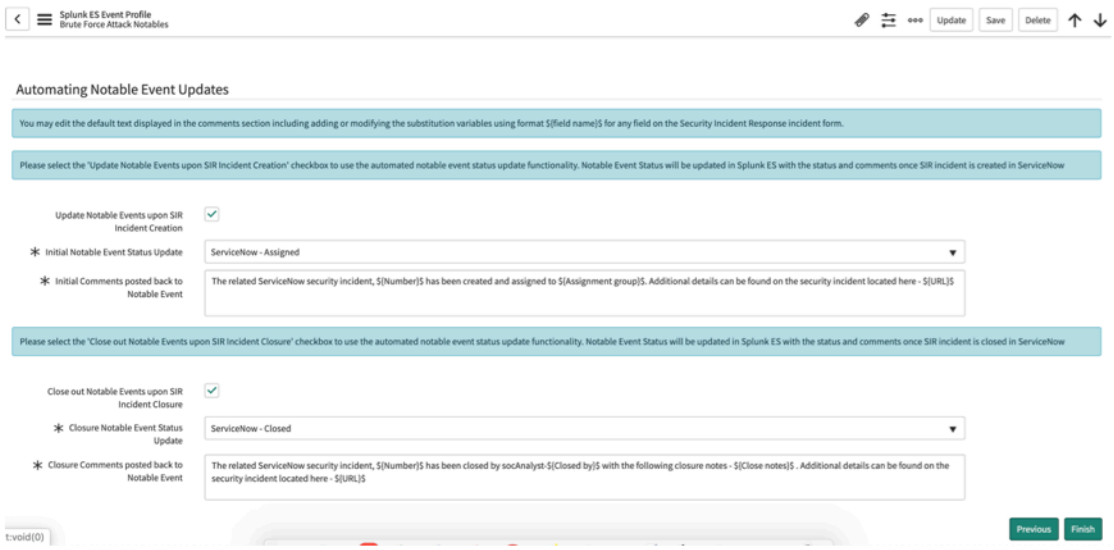
3. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com sucesso a instalação e a configuração da integração. Ative este perfil para extrair eventos notáveis do console Splunk Enterprise Security com base em sua programação. Há um limite de 1.000 incidentes de segurança que podem ser criados em um período de 24 horas. Até

Tradução automática

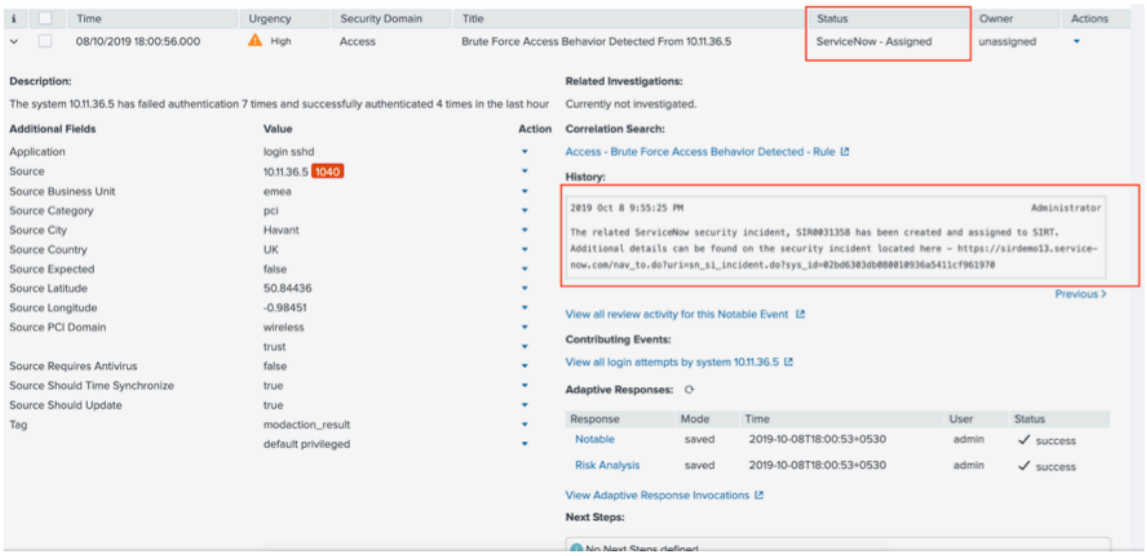
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

100 eventos notáveis são por alerta disparado. Os eventos notáveis subsequentes serão ignorados depois que os limites forem atingidos.

A imagem a seguir mostra a guia Opções adicionais com os valores padrão preenchidos:



Com a configuração de opções adicionais habilitada, a revisão de incidentes de eventos notáveis mostra a mudança de status e uma atualização nos comentários do histórico:



Configurar um perfil para encaminhamento manual de eventos

Dependendo do perfil definido, Splunk ES eventos notáveis são encaminhados manualmente como eventos notáveis discretos para o ambiente Operações de segurança da sua instância Now Platform.

Para configurar um perfil para encaminhamento manual de eventos notáveis:

Tarefa	Seção
Criar um perfil de evento	Veja Criar perfis para eventos encaminhados manualmente

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Seção
Mapear campos de eventos notáveis	Veja Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security
Criar mapeamentos personalizados	Veja Criar mapeamentos para Splunk ES análise de incidentes de eventos notáveis e detalhes do evento de contribuição (encaminhamento manual)
Visualizar o incidente de segurança	Veja Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security
Configurar seu ambiente Splunk para ingestão manual	Veja Configure o ambiente Splunk para ingestão manual de eventos para a integração Splunk Enterprise Security de ingestão de eventos notáveis
Automatizar atualizações e fechamento de eventos notáveis com base no status do incidente SIR	Veja Automatizar atualizações e fechamento de eventos notáveis com base no status do incidente SIR

Criar perfis para eventos encaminhados manualmente

Você pode configurar um perfil para eventos encaminhados manualmente.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

Para criar um perfil que ofereça suporte ao encaminhamento manual de eventos, siga estas etapas.

Para eventos que você encaminha sob demanda do console Splunk Enterprise Security, você pode basear o mapeamento de campo individual em qualquer perfil existente. Como alternativa, você pode criar uma nova grade de mapeamento para dados de anexo exportados. Os eventos encaminhados manualmente não são programados no perfil de eventos.

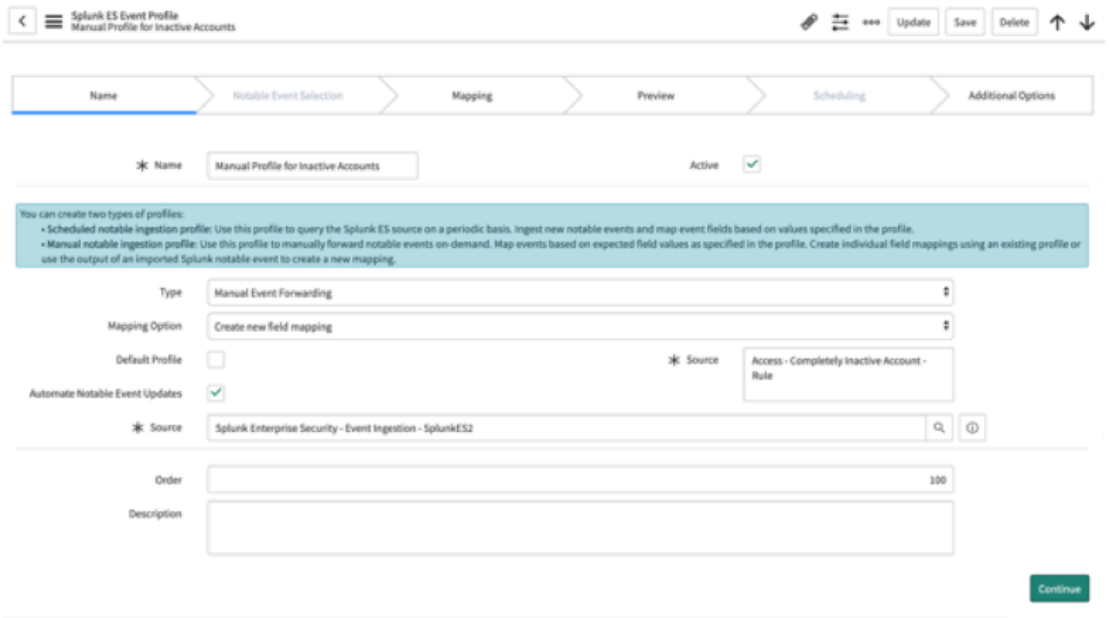
a. Se ainda não estiver selecionado, na lista de seleção do campo Tipo, selecione **Encaminhamento manual de eventos**.

b. No campo Opção de mapeamento exibido, na lista de seleção, escolha uma opção de mapeamento para continuar.

Consulte as imagens e tabelas a seguir para obter mais informações sobre as opções de mapeamento disponíveis na lista de seleção Opções de mapeamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar nova opção de mapeamento de campo

Opção ou campo	Descrição
Criar nova opção de mapeamento de campo	Novo mapeamento de campo para seu evento. Se você não tiver um mapeamento de campo existente semelhante ao perfil que está criando, selecione esta opção para criar um novo mapa.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos os eventos Splunk. O padrão é limpo (desativado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. Este perfil é usado quando não há correspondência na origem do evento encaminhado manualmente. Ele se torna o perfil padrão para todos os eventos com origens desconhecidas. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Origem (campo Evento Notável)	Este é um campo que normalmente define a regra de correlação que acionou o notável, por exemplo, ataques de força bruta. Este campo não estará disponível se a opção de perfil padrão estiver habilitada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

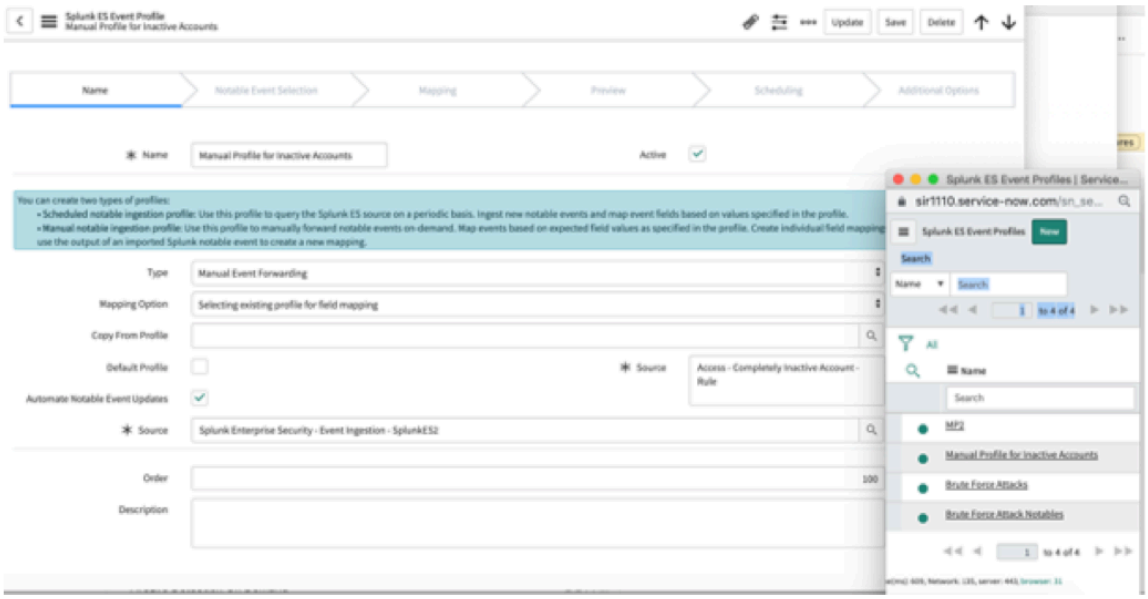
Opção ou campo	Descrição
	Se disponível, este campo permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base na regra de correlação de splunk que normalmente é diferente para diferentes tipos de evento. Se você quiser gerenciar diferentes regras de correlação separadamente, poderá criar diferentes perfis de evento de perfil com base na regra de correlação para atender a esse requisito.
Automatizar atualizações de eventos notáveis	Marque esta caixa de seleção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente SIR for criado a partir do evento notável e/ou quando o incidente SIR for encerrado. Isso ocorrerá para os eventos notáveis de acionamento inicial que criam o incidente SIR, bem como para os eventos agregados.
Origem (Splunk Servidor)	O servidor Splunk que você configurou como a origem de eventos notáveis. Se você tiver vários servidores Splunk configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão atualizados para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração no padrão. Se você criou um grande número de perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Para um perfil com um novo mapeamento de campo, verifique se você inseriu um valor no campo Tipo de origem e clique em **Continuar** para prosseguir para a etapa de mapeamento da configuração.

Para um perfil com um mapeamento de campo existente, consulte a figura e a tabela a seguir para obter mais informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Selecione o perfil existente para a opção de mapeamento de campo

Opção ou campo	Descrição
Selecionar perfil existente para mapeamento de campo	Reutilize um mapeamento de campo existente para o novo perfil de eventos notáveis. O campo Copiar do perfil é exibido. Siga estas etapas para copiar um mapeamento de campo existente para este perfil. **i.** À esquerda do campo Copiar do perfil exibido, clique no ícone de pesquisa. **ii.** Na lista Splunk Perfis de eventos ES exibida, clique no nome do perfil que tem o mapa que você deseja copiar. O nome do perfil é exibido no campo Copiar do perfil.
Perfil padrão	Perfil de encaminhamento de eventos padrão para todos os Splunk eventos notáveis com origem incompatível. O padrão é limpo (desabilitado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento manual de eventos. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Origem (campo Evento Notável)	Este é um campo que normalmente define a regra de correlação que acionou o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	notável, por exemplo, ataques de força bruta. Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, este campo permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base na regra de correlação de splunk que normalmente é diferente para diferentes tipos de evento. Se você quiser gerenciar diferentes regras de correlação separadamente, poderá criar diferentes perfis de evento de perfil com base na regra de correlação para atender a esse requisito.
Automatizar eventos notáveis	Marque esta caixa de seleção se quiser atualizar o status do evento notável e adicionar comentários adicionais quando um incidente de segurança for criado a partir do evento notável ou quando o incidente de segurança for encerrado. Isso ocorre para os eventos notáveis de acionamento inicial que criam o incidente de segurança, bem como para os eventos agregados.
Origem (Splunk Servidor)	Splunk servidor ou extremidade da pesquisa que você configurou como a origem de eventos notáveis. Se você tiver vários servidores Splunk configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão atualizados para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração no padrão. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução de tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Na parte inferior do formulário para selecionar um mapeamento existente para o seu perfil, clique em **Concluir** para concluir a configuração do perfil.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar mapeamentos para Splunk ES análise de incidentes de eventos notáveis e detalhes do evento de contribuição (encaminhamento manual)

Durante a etapa de mapeamento do campo de eventos notáveis, você mapeia campos de eventos individuais de eventos notáveis para campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Mapeie até cinco eventos notáveis da coluna Ingestão de amostra de eventos notáveis à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos padrão que são normalmente campos importantes a serem preenchidos no formulário de incidente SIR são exibidos. No entanto, esses campos podem ser removidos e quaisquer campos adicionais podem ser exibidos usando os botões + e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. A personalização dos campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no incidente de segurança SIR.

Procedimento
1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Siga estas etapas para carregar dados de anexo em sua instância Now Platform®.

   a. Se ainda não estiver conectado, faça login no console do Splunk Enterprise.

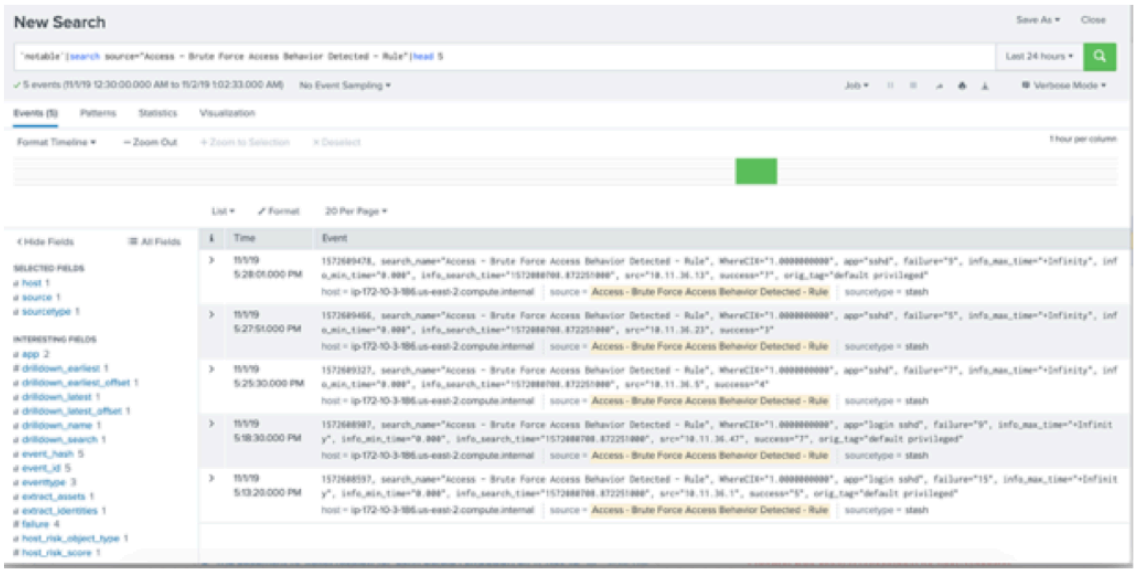
   b. Navegue até a guia Pesquisar e insira um nome para uma pesquisa que tenha os dados de eventos notáveis que você deseja exportar.
   Um exemplo de formato de pesquisa para recuperar eventos notáveis para a regra de correlação de comportamento de acesso de força bruta seria o seguinte: `notable` | search source="Access - Brute Force Access Behaviour Detected - Rule".

   c. Expanda o evento notável e, na coluna Campo, selecione os campos que você deseja importar.

   Esses campos são os pares de campo-valor que são exportados e exibidos na página Mapeamento em sua instância Now Platform®.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

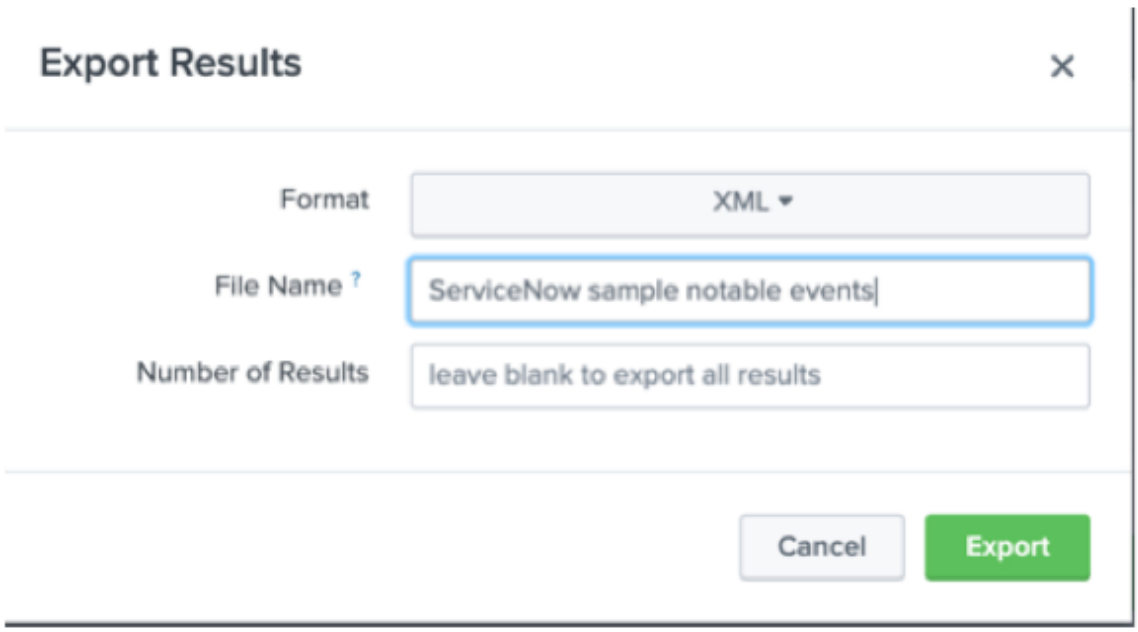


d. No console Splunk Enterprise, no canto superior direito da página Pesquisar, clique no ícone **Exportar**.

e. Na lista de seleção do campo Formato na caixa de diálogo exibida, clique em **Formato XML**.

f. Opcional: Insira um novo nome de arquivo.

g. Clique em **Exportar**.



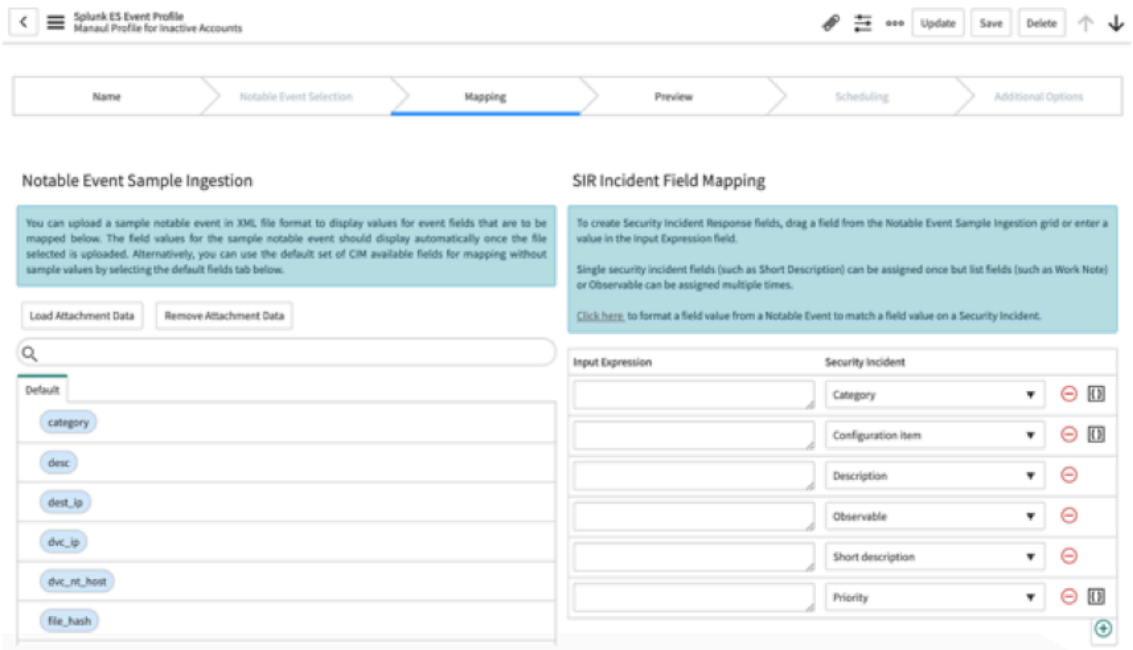
O arquivo XML de eventos notáveis Splunk exportado agora deve ser carregado para sua instância Now Platform®.

h. Se a página Mapeamento ainda não estiver exibida na sua instância Now Platform®, clique em **Mapeamento** na barra de andamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Na coluna Ingestão de amostra de evento notável, clique em **Carregar dados de anexo**.



j. Na caixa de diálogo exibida, clique em **Escolher arquivos**, navegue até o arquivo `.xml` que você exportou e clique em **Abrir**.
Depois de clicar para carregar dados de anexo para eventos encaminhados manualmente, os Splunk ES campos de evento notáveis são preenchidos no lado esquerdo do formulário. Esses valores são os valores de campo que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente de Sir do formulário.
Os pares de valores dos campos que você exportou para o evento são exibidos no lado esquerdo do formulário de mapeamento.

3. Siga as etapas 5 a 10 na seção Criar mapeamentos para Splunk ES revisão de incidentes de eventos notáveis e detalhes do evento de contribuição (ingestão programada).

Configure o ambiente Splunk para ingestão manual de eventos para a integração Splunk Enterprise Security de ingestão de eventos notáveis

Instale e configure a aplicação ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security no console empresarial Splunk ou na instância do Splunk Cloud se quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise Security para esta integração.

Antes de Iniciar

A instalação e configuração da aplicação ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security no console empresarial Splunk ou na instância do Splunk Cloud é opcional.

Verifique se você instalou a aplicação para esta integração do ServiceNow Store antes de instalar o plug-in de complemento do splunkbase que é necessário para a ingestão manual de eventos. Se você não instalou a aplicação para a integração de ServiceNow Store, consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security e siga as instruções para instalá-la.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: Splunk Enterprise Security administrador

Por Que e Quando Desempenhar Esta Tarefa

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para a integração, baixe, instale e configure o ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security do splunkbase no console Splunk Enterprise Security. Este ServiceNow complemento de extensão é necessário para que incidentes de segurança possam ser criados a partir de eventos exportados manualmente em sua instância Now Platform. Este ServiceNow Complemento de ingestão de eventos das Operações de segurança para a aplicação Splunk Enterprise Security está disponível em splunkbase .

Para o encaminhamento manual de eventos, você pode identificar até dois Now Platform endpoints (instâncias) diferentes no console Splunk Enterprise Security. Você encaminha os eventos para o endpoint ou endpoints manualmente para criar incidentes de segurança. Por exemplo, você pode especificar uma instância de preparação (desenvolvimento) e uma instância de produção. Ao especificar instâncias separadas e nomear fluxos de trabalho primários e secundários para cada instância, você pode escolher para onde deseja encaminhar eventos diferentes.

Procedimento

1. Se você ainda não instalou o ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise Security, siga estas etapas para instalá-lo e configurá-lo.

   a. Navegue até splunkbase .

   b. Pesquise o ServiceNow Operações de segurança Complemento de ingestão de eventos das Operações de segurança para Splunk Enterprise Security.

      Nota: Verifique se você selecionou ServiceNow Operações de segurança Complemento de ingestão de eventos para Splunk Enterprise Security. Há complementos ServiceNow adicionais que são exibidos nesta lista. Esses complementos são para diferentes ServiceNow Splunk integrações e não são necessários para esta integração.

   c. Baixe a aplicação.

   d. Abra sua conta Splunk Enterprise Security.

   e. Na página Aplicações, clique no ícone de engrenagem ou no atalho **Gerenciar aplicações** na lista suspensa do menu.

   f. No canto superior esquerdo da página Aplicações exibida, clique em **Instalar app a partir do arquivo**.

   g. Clique em **Escolher arquivo**, selecione ServiceNow Complemento de ingestão de eventos das Operações de segurança para Splunk Enterprise Securitye clique em **Carregar**.

   h. Se solicitado, reinicie Splunk Enterprise.
   O ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise Security está instalado no console Splunk Enterprise Security. A próxima etapa para configurar o complemento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Para configurar o complemento, siga estas etapas.

a. Em Splunk Enterprise Security, clique no ícone de engrenagem de **aplicações** ou em **Gerenciar aplicações** na lista suspensa do menu.

b. Na lista de aplicações exibida, na coluna **Ações**, clique em **Configurar** para ServiceNow Operações de segurança Complemento de ingestão de eventos para Splunk Enterprise Security.

c. Preencha o formulário.

A figura a seguir é um exemplo de um formulário preenchido no console do Splunk Enterprise Security.

Campo na seção Especificar instância primária da ServiceNow	Descrição
Rótulo de ação de fluxo de trabalho	Nome do fluxo de trabalho Now Platform para sua instância de produção (primária). Este nome é o nome de uma instância Now Platform que os usuários que estão monitorando eventos Splunk identificam como uma instância primária, por exemplo, ingestão de eventos da ServiceNow (produção).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
	O padrão para este campo é Ingestão de eventos da ServiceNow (produção). No console Splunk Enterprise Security, este nome de fluxo de trabalho é exibido para a instância de produção (primária) na lista suspensa `Ações de evento` expandidas de uma pesquisa. Este nome é o nome da sua instância de produção. Você pode editar o nome.
URL	O URL da instância Now Platform que você inseriu no campo de rótulo de ação de fluxo de trabalho anterior. Copie o URL no navegador e cole-o neste campo do formulário.
Endpoint	Caminho da API base. Para obter mais informações, consulte a figura que segue a tabela. Se você não tiver um valor para o endpoint da sua instância de produção Now Platform, siga estas etapas. **a.** Faça login na sua instância de produção Now Platform como um usuário com a função de administrador do sistema (admin). **b.** Insira `Scripted REST APIs` no painel de navegação. **c.** Depois que o painel de navegação for atualizado, selecione o módulo **Scripted REST APIs** que será exibido. **d.** Se a Ingestão de eventos não estiver listada na coluna Nome da lista de `Scripted REST APIs` exibida, no campo de pesquisa na parte superior, insira `Ingestão de eventos`. **e.** Na coluna Caminho da API base na página atualizada, copie este valor e cole-o no campo Endpoint do formulário. Um exemplo de caminho de API base é `/api/sn_sec_splunk_v2/event_ingestion`.
Nome de usuário	Nome de usuário para sua instância Now Platform. Este nome é o nome de usuário da instância Now Platform na qual você atribuiu um usuário com a função (sn_sec_splunk_v2.api_account_access) para encaminhamento manual de eventos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

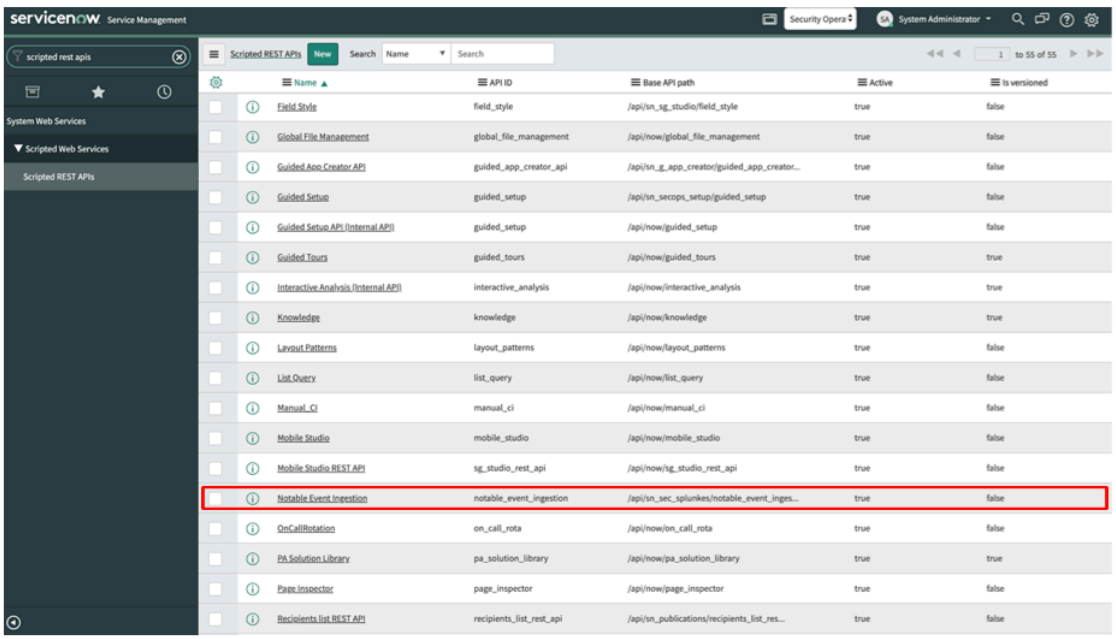
Campo na seção Especificar instância primária da ServiceNow	Descrição
	Para obter mais informações sobre como atribuir essa função, consulte Configure sua instância Now Platform para a integração Splunk Enterprise Event Ingestion.
Senha	Senha para sua instância Now Platform. Esta senha é a senha para a instância Now Platform na qual você atribuiu um usuário com a função (sn_sec_splunk_v2.api_account_access) para encaminhamento manual de eventos.
(Opcional) Campos na seção Especificar instância secundária da ServiceNow	Descrição Esses campos são opcionais. Você não é obrigado a especificar uma instância secundária.
Rótulo de ação de fluxo de trabalho	Nome do fluxo de trabalho Now Platform para sua instância secundária (preparação). Este nome é o nome de uma instância Now Platform que os usuários que estão monitorando eventos Splunk identificam como uma instância secundária, por exemplo, ServiceNow ingestão de eventos (preparação). No console Splunk Enterprise Security, este nome de fluxo de trabalho é exibido para a instância de preparação (secundária) na lista suspensa Ações de evento expandidas de uma pesquisa. Esta instância Now Platform é sua instância de preparação. Você pode editar o nome.
URL	O URL da instância Now Platform que você inseriu no campo de rótulo de ação de fluxo de trabalho anterior para a instância Now Platform secundária. Copie o URL no navegador e cole-o neste campo do formulário.
Endpoint	Caminho da API base. Este valor para o caminho da API de base para sua instância secundária é o mesmo valor que o caminho da API de base para sua instância primária. Consulte a figura anterior do formulário para obter mais informações.
Nome de usuário	Nome de usuário da sua instância de preparação Now Platform. O usuário deve ter a função (sn_sec_splunk_v2.api_account_access).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo na seção Especificar instância primária da ServiceNow	Descrição
Senha	Senha para sua instância de preparação Now Platform. O usuário deve ter a função (sn_sec_splunkes.api_account_access).

A figura a seguir é um exemplo da lista de Scripted REST APIs em seu Now Platform. A lista exibe o local do valor do endpoint de uma instância Now Platform que você insere no formulário como parte da configuração da extensão ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security no console Splunk Enterprise Security.



3. No formulário de configuração do console Splunk Enterprise Security, clique em **Salvar** para salvar suas edições.

   Depois de alguns momentos, na parte superior esquerda do formulário no console Splunk Enterprise Security, será exibida uma mensagem informando que o registro foi atualizado com sucesso.

   Depois de salvar o formulário, os nomes (rótulos de ação de fluxo de trabalho) das instâncias Now Platform que você criou no formulário ficam disponíveis na lista de seleção Ações de evento em um evento selecionado de uma pesquisa no console Splunk Enterprise Security.

O que Fazer Depois

Se você ainda não salvou as pesquisas no console Splunk Enterprise Security, a próxima etapa é salvar pesquisas como alertas no console Splunk Enterprise Security.

Copiar um perfil de evento para a integração de ingestão de eventos Splunk Enterprise Security

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, talvez prefira copiar os perfis de alarme para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

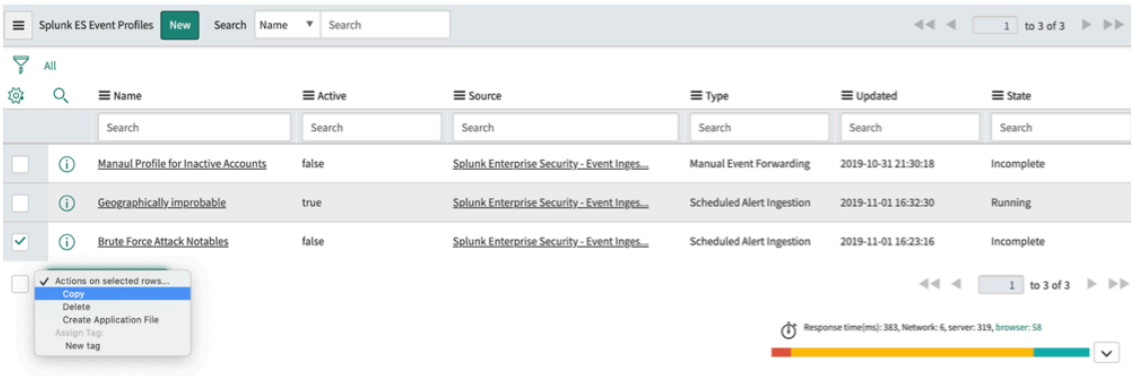
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

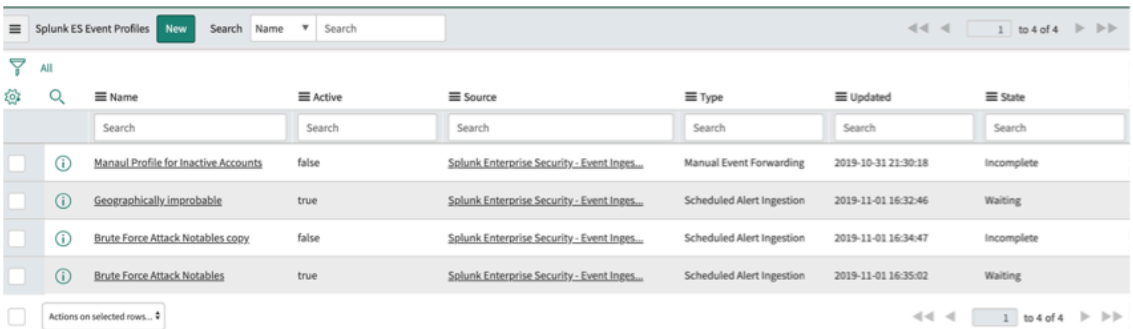
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desativado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Todos** > **Splunk Integration** > **Perfil de eventos do Splunk**.
2. Na lista Splunk Perfis de eventos exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo a configuração de mapeamento e programação. O nome do perfil contém cópia. Embora o perfil original esteja ativado (`verdadeiro`), a cópia está desabilitada neste ponto (`falso`). Você pode preferir editar valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir a etapa de configuração.

Use o editor de script para formatar valores de alerta para a integração de ingestão de eventos Splunk Enterprise Security

Além dos campos mapeados diretamente dos valores de evento notáveis ingeridos e dos valores inseridos manualmente, use o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

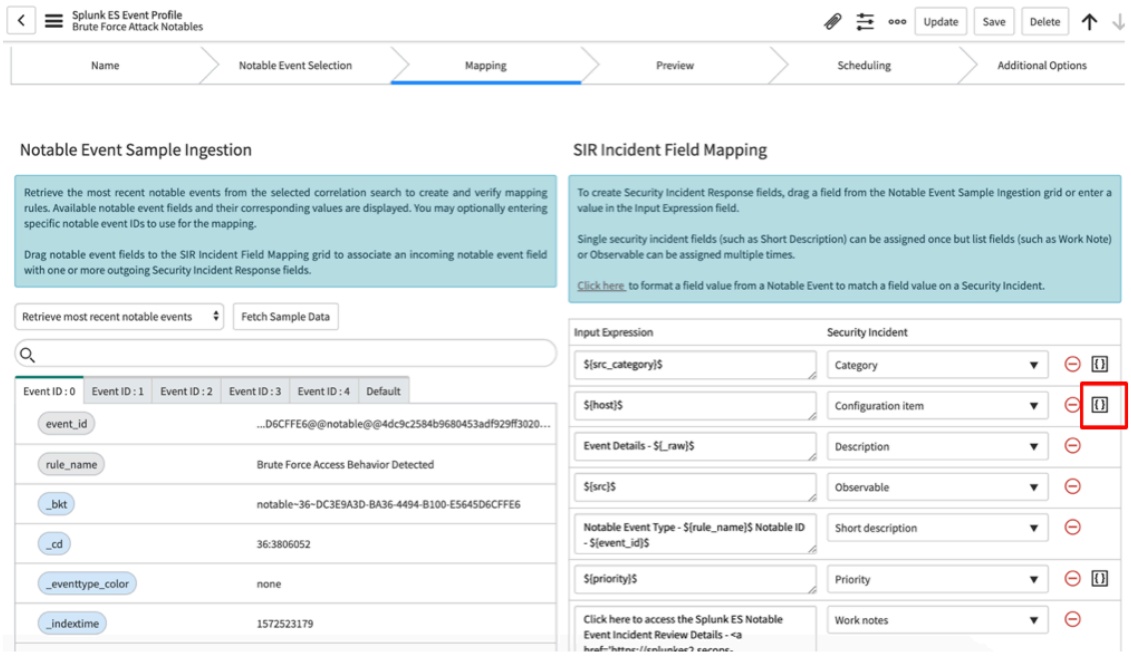
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Em determinados casos, Splunk Enterprise Security valores de eventos notáveis são mapeados para os campos Categoria, Item de configuração (IC) e Observável no incidente SIR. Você pode preferir editar os valores mapeados. Se você quiser converter o valor de um evento notável Splunk Enterprise Security para um valor que seja compatível com esses campos no incidente de segurança SIR, use o editor de script.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de script.



2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente SIR, clique no ícone de colchete `[{}]` ao lado de um campo para abrir o editor de script desse campo.

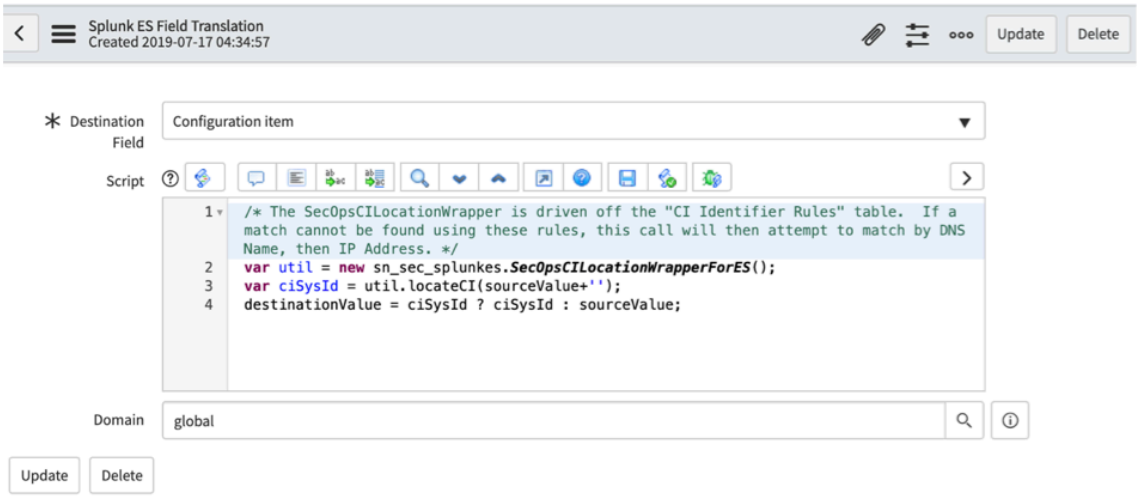
   Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um evento notável, por exemplo, um valor para o item de configuração pode não ser correspondido.

   Conforme mostrado na figura a seguir, se uma correspondência para um nome de host não puder ser encontrada no Now Platform® CMDB para o campo Item de configuração, você poderá editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

   O editor é aberto com o campo exibido em Campo de destino. A imagem a seguir mostra o editor com o campo `Item de configuração` como o Campo de destino.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira todas as mudanças no script e clique em **Atualizar** para salvar suas mudanças. A tabela Splunk Traduções de Campo é exibida.
5. Feche a tabela para retornar ao formulário Mapeamento.

Copiar Splunk Enterprise Security perfis de uma instância para outra usando a funcionalidade de exportação/importação

Você pode exportar e importar Splunk Enterprise Security configurações de perfis de uma instância Now Platform para uma instância Now Platform diferente.

Antes de Iniciar

As configurações que você pode exportar e importar incluem nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Essa funcionalidade permite que o administrador de segurança copie perfis que foram testados e verificados em uma instância Now Platform, por exemplo, em não produção, para outra instância Now Platform, por exemplo, produção, sem a necessidade de refazer todas as definições de configuração. As configurações que são exportadas e importadas incluem nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Nota: Quando você exporta um tipo de perfil de encaminhamento de eventos manual, os dados de anexo usados para o mapeamento do campo de amostra são copiados, no entanto, o arquivo de anexo em si não é exportado.

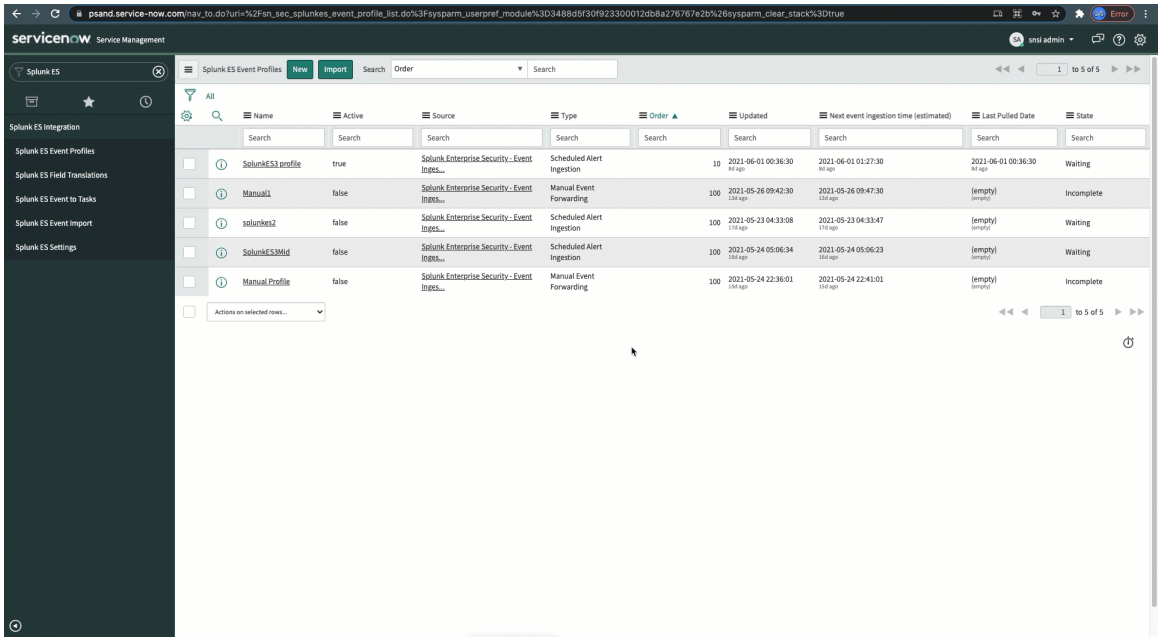
Procedimento

1. Navegar até **Todos** > **Splunk ES Integration** > **Perfis de eventos do Splunk ES**.
2. Selecione um perfil que você deseja exportar para outra instância Now Platform. Você pode selecionar vários perfis para exportação.
3. No menu Ações, clique em **Exportar**.
4. Quando a mensagem de exportação concluída for exibida, clique em **Download**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra a exportação de um perfil (SplunkES3profile) da instância Now Platform (psand.service-now.com).



O arquivo payload.xml exportado é baixado no seu computador. O arquivo contém o nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração. Quando você seleciona e baixa vários perfis, eles aparecem no mesmo arquivo payload.xml.

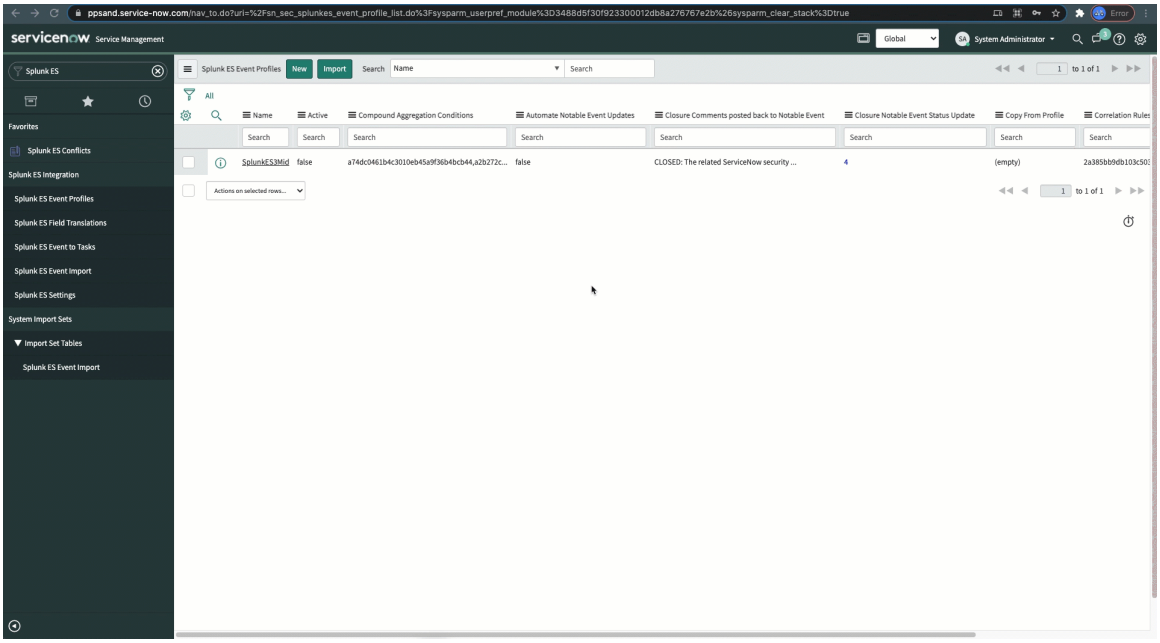
Agora você pode prosseguir para importar o perfil em outra instância Now Platform.

5. Navegar até **Splunk ES Integration** > **Perfis de eventos do Splunk ES**.
6. Clique em **Importar**.
7. Clique **em Escolher arquivo** e selecione o arquivo xml no seu computador.
8. Clique em **Carregar**.
9. Clique **em Fechar e recarregar perfis**.

A ilustração a seguir mostra a importação de um perfil (SplunkES3profile) da instância Now Platform (psand.service-now.com) para a instância Now Platform (ppsand.service-now.com).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você importou com sucesso o perfil de outra instância Now Platform.

Verifique se a origem exportada (Splunk conta de API e Splunk URL do servidor) e as definições de configuração do MID Server são válidas e estão disponíveis na instância Now Platform importada. Atualize sua configuração Splunk Enterprise Security, se necessário.

10. Opcional: Verifique as configurações do MID Server após importar um perfil.
11. Opcional: Navegar até **Operações de segurança** > **Configurações de Integração**.
12. Opcional: Selecione o bloco de configuração Splunk Enterprise Security e clique em **Atualizar**.
13. Opcional: Revise e atualize os detalhes de origem e do MID Server conforme necessário.

Check-list para a integração de ingestão de eventos notáveis Splunk Enterprise Security

Use esta check-list para se orientar em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem os resultados esperados para a integração.

Antes de Iniciar

Funções necessárias: administrador, sn_si.admin, sn_si.analyst, Splunk Enterprise Security administrador

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe o andamento da configuração, instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada linha da tabela lista as tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

As funções necessárias para cada tarefa são listadas com cada etapa na tabela a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Acompanhe seu andamento com a configuração, a instalação e a configuração da integração.
   Conclua todas as tarefas de uma etapa antes de passar para a próxima.
2. Siga as etapas na tabela na ordem em que são apresentadas.

Check-list

☐	Como um usuário com a função de administrador Now Platform, configure sua instância Now Platform. ◦ Atribua usuários com as funções sn_si.admin e sn_si.analyst conforme necessário. ◦ Instale e configure um MID Server se o servidor Splunk estiver implantado em sua rede corporativa. ◦ Verifique se os plug-ins ServiceNow Security Incident Response estão ativados para a versão do Now Platform. ◦ (Opcional) Se você quiser encaminhar eventos manualmente do console [Splunk Enterprise Security para a instância Now Platform, verifique se atribuiu a função (sn_sec_splunkes.api_account_access) a um usuário com a permissão de administrador Splunk Enterprise Security. Para obter mais informações, consulte Configure sua instância Now Platform para a integração Splunk Enterprise Security.
☐	Como um usuário com a função de administrador Now Platform, instale e configure a aplicação Splunk Enterprise Security a partir do ServiceNow Store. **a.** Baixe e instale a aplicação em sua instância Now Platform. **b.** Configure a aplicação e conecte-se ao console Splunk Enterprise Security. Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security.
☐	(Opcional) Se você pretende exportar eventos manualmente do console [Splunk Enterprise Security para a instância Now Platform, execute as seguintes tarefas: ◦ Como um administrador Splunk Enterprise Security, instale, configure e habilite o ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise Security do splunkbase no console Splunk Enterprise Security. ◦ Como um administrador Splunk Enterprise Security, se ainda não estiver configurado, salve pesquisas como eventos notáveis no console Splunk Enterprise Security.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Para obter mais informações, consulte Configure o ambiente Splunk para ingestão manual de eventos para a integração Splunk Enterprise Security de ingestão de eventos notáveis.
☐	Como um usuário com a função Now Platform sn_si.admin, crie e nomeie um perfil de evento. Selecione o tipo de perfil na lista de seleção. As opções são um perfil de alerta programado que você usa para ingerir dados de amostra ou um perfil de evento que você usa para exportar dados de anexo manualmente do console Splunk Enterprise Security. ◦ Para um alerta programado, selecione um alerta disponível. ◦ Para o perfil de dados exportados manualmente, crie um novo mapa ou copie um mapa existente. Para obter mais informações, consulte Criar e nomear um perfil de evento para a integração de ingestão de eventos Splunk Enterprise Security.
☐	Como um usuário com a função Now Platform sn_si.admin, mapeie valores ingeridos ou dados de anexo que são exportados de Splunk Enterprise Security para Now Platform incidentes de segurança. **a.** Buscar dados de amostra para um alerta programado. **b.** (Opcional) Exporte dados de anexo manualmente de Splunk Enterprise Security para um evento. **c.** Edite a configuração de mapeamento padrão. **d.** Opcionalmente, adicione critérios de filtragem, anexe um alerta a um incidente de segurança existente e use o editor de script. Para obter mais informações, consulte Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security e Criar mapeamentos para Splunk ES revisão de incidentes de eventos notáveis e detalhes do evento de contribuição (ingestão programada).
☐	◦ Como um usuário com a função Now Platform sn_si.admin, visualize os dados de Splunk Enterprise que são exibidos em um incidente de segurança Now Platform. ◦ Corrija quaisquer erros ou adicione dados ausentes para que nenhuma mensagem de erro seja exibida. Para obter mais informações, consulte Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security.
☐	Como um usuário com a função Now Platform sn_si.admin, programe a recuperação de alertas para um perfil com um alerta programado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Para obter mais informações, consulte Programar e recuperar eventos notáveis novos e atualizados para a integração de ingestão de eventos Splunk Enterprise Security.

Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.

Splunk - Integração de aprimoramento de incidentes

A integração Splunk - Incident Enrichment pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	Configuração Comece com Splunk Integração de pesquisa para Operações de segurança
Usar • Executar uma pesquisa de detecções • Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções • Integração de Operações de segurança - Fluxo de trabalho de Pesquisa de detecções de Splunk • Exibir detalhes da pesquisa de detecções • Exibir resultados da pesquisa de detecções	Desenvolver • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solução de problemas e informações adicionais • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Comece com Splunk Integração de pesquisa para Operações de segurança

O softwareSplunk pesquisa, monitora e analisa big data gerado por máquina e se integra facilmente com Operações de segurança. Antes de poder usar a integração Splunk - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL base da API e as credenciais de login apropriadas.

Antes de Iniciar

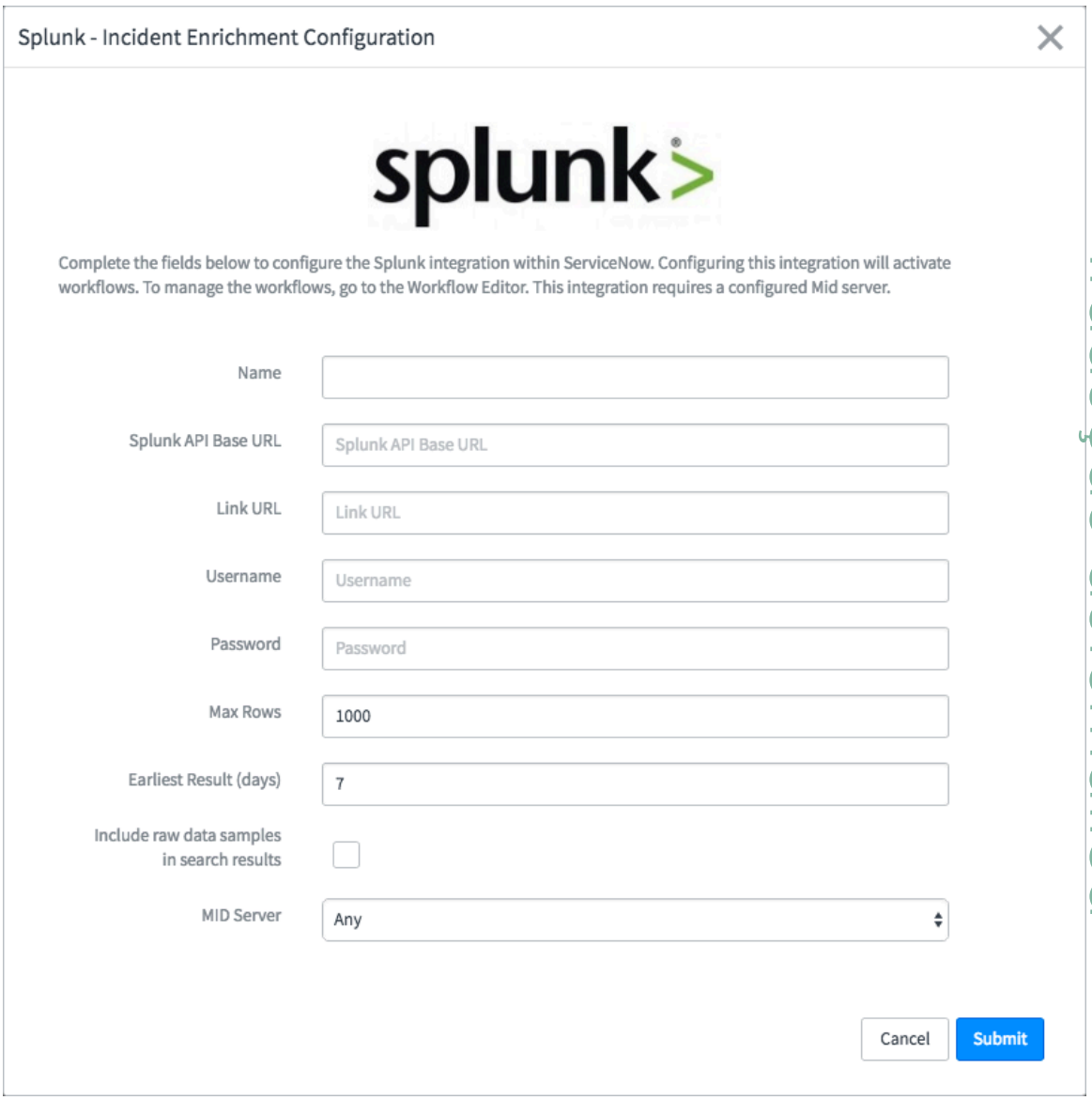
Função necessária: sn_si_admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Splunk e obtenha a chave de API e o ID de API no seu perfil.
3. Em sua instância, navegue até **Operações de segurança** > **Configuração de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Splunk - Incident Enrichment, clique em **Novo**.



5. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL base da API Splunk	A URL base que você adquiriu do site Splunk.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL do Link	[Opcional] A URL do link que vincula à interface da Web Splunk, quando disponível.
Nome de usuário	Seu nome de usuário do Splunk.
Senha	Sua senha do Splunk.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho .

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Experiência Mobile para Security Incident Response

Use seu dispositivo móvel Android ou iOS para gerenciar suas tarefas do centro de operações de segurança (SOC).

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Security Incident Response

Se você não estiver familiarizado com os conceitos básicos do produto Security Incident Response (SIR) em sua instância Now Platform®, consulte Security Incident Response Visão geral para obter mais informações sobre inteligência contra ameaças e como esse produto pode ajudá-lo a priorizar e resolver ameaças cibernéticas à sua organização.

Visão geral

Como gerente do centro de operações de segurança (SOC) ou usuário com a função Now Platform de analista de segurança (sn_si.analyst), você pode fazer login em uma instância Now Platform diretamente do seu dispositivo móvel. Com o Aplicativo Security Incident

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Response Mobile, você pode exibir, editar e atribuir seus incidentes de segurança e tarefas de resposta mais atuais e críticos SIR. As notificações informam quando chegam incidentes de segurança críticos atribuídos a você.

Com o Aplicativo Security Incident Response Mobile, você pode executar as seguintes tarefas relacionadas a SIR no seu dispositivo móvel:

- Exiba uma lista de incidentes de segurança críticos e tarefas de resposta.
- Receba notificações detalhadas sobre incidentes e tarefas de segurança que atendam a critérios de notificação predefinidos.
- Exiba agrupamentos de incidentes de segurança ou tarefas que são baseados em um conjunto predefinido de consultas ou filtros.
- Exiba as anotações de trabalho e as listas relacionadas de incidentes de segurança.
- Atualize incidentes de segurança e adicione anotações de trabalho ou anexos.
- Edite os campos em incidentes de segurança.
- Atribua incidentes de segurança a você ou a outros membros da sua equipe de segurança.

Quando eles são preenchidos, você pode exibir as seguintes listas relacionadas em SIR incidentes de segurança com o Aplicativo Security Incident Response Mobile:

- Item de Configuração
- Usuário afetado
- Serviços afetados
- Incidentes de segurança secundário
- Incidentes de segurança semelhantes (sem suporte da Now Platform)
- Observáveis
- Tarefas de Resposta
- Tarefas
- ANS de tarefa
- Anexos (sem suporte da Now Platform)

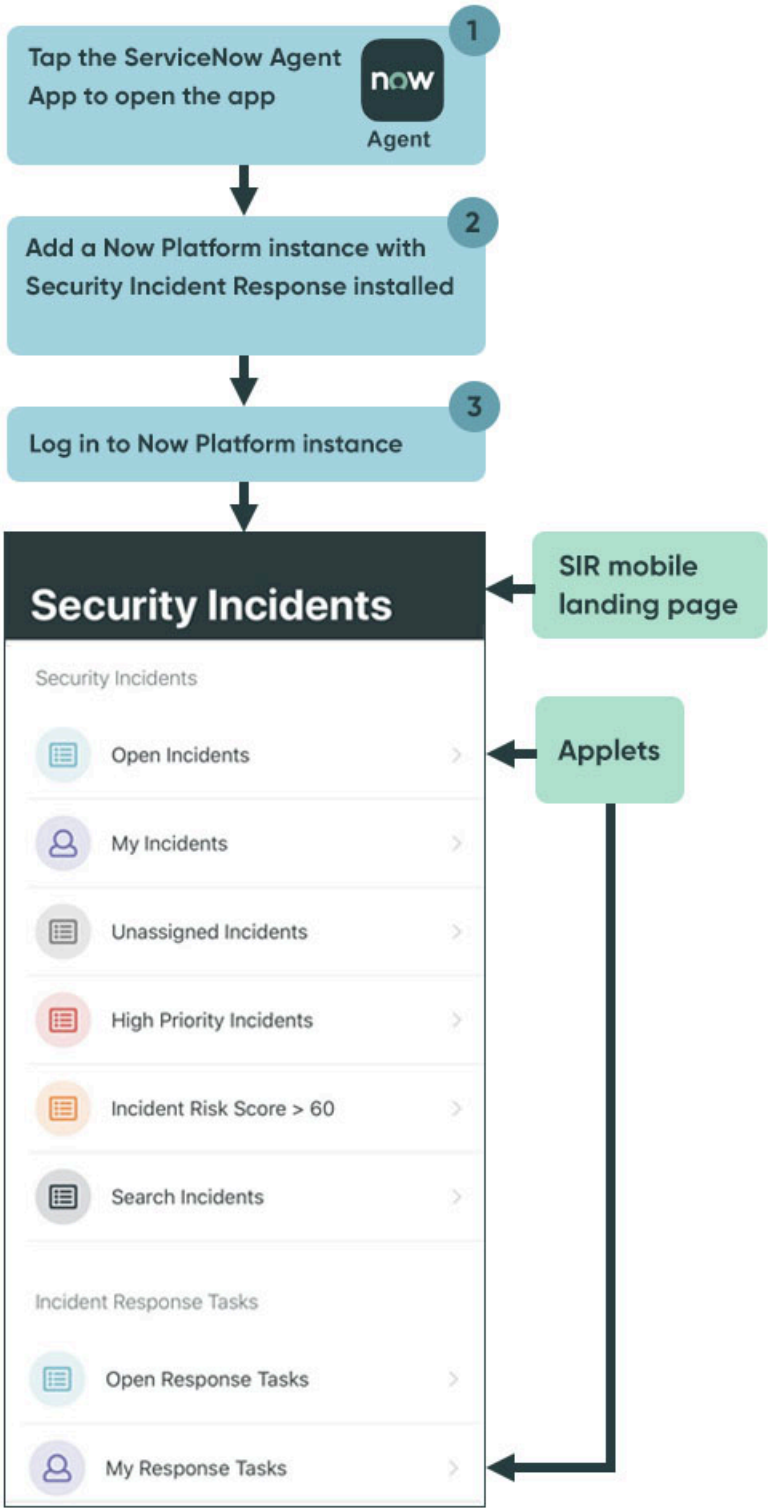
A figura a seguir ilustra como você faz login na sua instância Now Platform do seu dispositivo móvel e a estrutura da tela inicial do Aplicativo Security Incident Response Mobile que é reproduzida após o login.

Para obter instruções passo a passo sobre como configurar sua instância Now Platform e instalar o Aplicativo Security Incident Response Mobile, consulte Configurar check-list para o Aplicativo Security Incident Response Mobile. Para obter instruções sobre como fazer login, consulte Faça login no Aplicativo Security Incident Response Mobile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicativo Security Incident Response Mobile



Aplicações

Aplicações são os ServiceNow® componentes de software, como Security Incident Response (SIR), Resposta a vulnerabilidades (VR), Governança, risco e conformidade (GRC) que fornecem recursos e funcionalidades específicos em sua instância Now Platform. Depois de instalar a aplicação principal Security Incident Response e o Aplicativo Security Incident Response Mobile em sua instância Now Platform, o ícone da aplicação principal será exibido na parte inferior do seu dispositivo móvel Android ou iOS após o login.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicativo Security Incident Response Mobile Ícone (Incidentes de segurança)

Pastas

Cada aplicação ServiceNow® mobile contém pastas que separam os applets por categoria. Na imagem anterior da página principal, **Incidentes de segurança** e **Tarefas de resposta** a incidentes são pastas.

Applets

Applets são as diferentes opções na aplicação. Os ícones nas seções **Incidentes de segurança** e **Tarefas de resposta** a incidentes são os applets disponíveis do Aplicativo Security Incident Response Mobile.

Configurar check-list para o Aplicativo Security Incident Response Mobile

A check-list a seguir inclui as tarefas de configuração que você deve concluir na instância Now Platform® e no dispositivo móvel antes de usar o Aplicativo Security Incident Response Mobile.

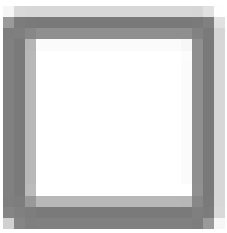
Antes de Iniciar

Como opção, imprima esta check-list e use-a para orientá-lo nas tarefas de configuração necessárias para o Aplicativo Security Incident Response Mobile. Verifique se cada item da lista está concluído para que você possa exibir e editar SIR incidentes de segurança no seu dispositivo móvel.

Os itens da check-list são exibidos em texto realçado. Mais informações seguem cada item na coluna à direita. Tempo estimado para concluir esta tarefa: 15 a 20 minutos.

Funções necessárias: admin, sn_si.analyst

Check-list para dispositivos móveis

Item	Descrição
	Como um usuário com a função de administrador, verifique se você tem a aplicação principal Security Incident Response instalada em uma instância Now Platform. Esta é a instância Now Platform que você exibe no seu dispositivo móvel. **Nota:** A aplicação principal Security Incident Response e a instância Now Platform devem ser da mesma versão da família. 1. Para verificar se a aplicação principal está instalada em sua instância, navegue até Plug- **ins** e pesquise por Security Incident Response. 2. Se a aplicação principal Security Incident Response ainda não estiver instalada, clique em **Instalar** para instalá-la. Para obter mais informações sobre como instalar a aplicação principal Security Incident Response, consulte Instalar e configurar Security Incident Response. Se a aplicação principal Security Incident Response não estiver visível em Plug-ins, para obter mais informações sobre como instalar aplicações principais e direitos para aplicações, consulte .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para dispositivos móveis

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você tem o Aplicativo Security Incident Response Mobile instalado na instância Now Platform que deseja exibir no seu dispositivo móvel. **Nota:** as instâncias Aplicativo Security Incident Response Mobile e Now Platform devem ser da mesma versão da família. Baixe e instale o Aplicativo Security Incident Response Mobile do ServiceNow Store na sua instância Now Platform. Quando você instala o Aplicativo Security Incident Response Mobile, suas dependências, com.glide.sg e com.glide.sg.agent_native_client, também são instaladas. Para verificar se essas dependências estão instaladas: **1.** Navegue até Plug- **ins**. **2.** Pesquise os IDs de plug-in (com.glide.sg e com.glide.sg.agent_native_client). **3.** Se eles não estiverem ativados, ative esses plug-ins. Esses plug-ins são necessários para o Aplicativo Security Incident Response Mobile. Para obter mais informações sobre como instalar aplicações e direitos para aplicações, consulte .
☐	Como um usuário com a função de administrador Now Platform, verifique se você atribuiu usuários móveis com as funções necessárias em sua instância Now Platform. **1.** Para exibir as funções atribuídas a um usuário, navegue até **Usuários e Grupos** > **Usuários**. **2.** Selecione o nome de usuário seguido pela lista relacionada de funções. Todas as funções atribuídas a este usuário são exibidas. **3.** Verifique se um usuário está atribuído ou atribua um usuário com a função de biblioteca de infraestrutura de TI (itil). Usuários com a função itil podem criar, abrir, atualizar e fechar incidentes de segurança. Somente usuários com a função itil podem ter tarefas atribuídas a eles. **4.** Verifique se um usuário está atribuído ou atribua a um usuário a função de analista de segurança (sn_si.analyst). Usuários com a função sn_si.analyst podem ler e editar registros de incidentes de segurança. Esta função é adicionada automaticamente quando você atribui a função itil. **5.** Verifique se você criou todos os grupos de atribuição necessários e atribuiu usuários móveis a esses grupos. **Nota:** Se você tiver um grande número de usuários para o aplicativo para celular, como alternativa, poderá atribuir a função sn_si.analyst a um grupo. Cada usuário adicionado ao grupo herda esta função.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para dispositivos móveis

Item	Descrição
	Para obter mais informações sobre analistas de segurança, consulte Atribuição de analistas de segurança. Para obter mais informações sobre usuários e atribuição de funções a usuários e grupos, consulte Administração de usuários .
☐	Como um usuário com a função sn_si.analyst, baixe o aplicativo ServiceNow® Agent mais atual no seu dispositivo móvel. A versão mais atual do app Agent está disponível na Apple iOS App Store e na Google Play Store.
☐	Como um usuário com a função sn_si.analyst, verifique se as notificações estão habilitadas no seu dispositivo móvel e na sua instância Now Platform. As notificações informam quando incidentes de segurança críticos são atribuídos a você ou ao seu grupo de atribuição. Para ajudá-lo com a correção oportuna, depois de habilitar as notificações, clique em uma notificação no Aplicativo Security Incident Response Mobile para navegar diretamente para o incidente de segurança. Para habilitar notificações em sua instância Now Platform para que sejam exibidas em seu dispositivo móvel, siga estas etapas. **1.** Verifique se você baixou e instalou o Aplicativo Security Incident Response Mobile em sua instância Now Platform. **2.** Em Configurações do sistema na sua instância Now Platform, em Notificações, verifique se você habilitou o **Aplicativo para celular da ServiceNow**. Para obter mais informações sobre como definir notificações, consulte Como definir preferências de notificação do usuário na IU principal .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para dispositivos móveis

Item	Descrição
	Now Platform notificações também são exibidas na tela de mensagens do seu dispositivo móvel. Verifique se as notificações também estão habilitadas nas configurações do seu dispositivo móvel.

Você configurou com sucesso seu dispositivo móvel e o Now Platform para o Aplicativo Security Incident Response Mobile. A próxima etapa é fazer login na sua instância Now Platform com seu dispositivo móvel.

Faça login no Aplicativo Security Incident Response Mobile

Abra o aplicativo Security Incident Response Mobile e adicione uma instância Now Platform® com o Security Incident Response ao seu dispositivo móvel.

Antes de Iniciar

Função necessária: sn_si.analyst

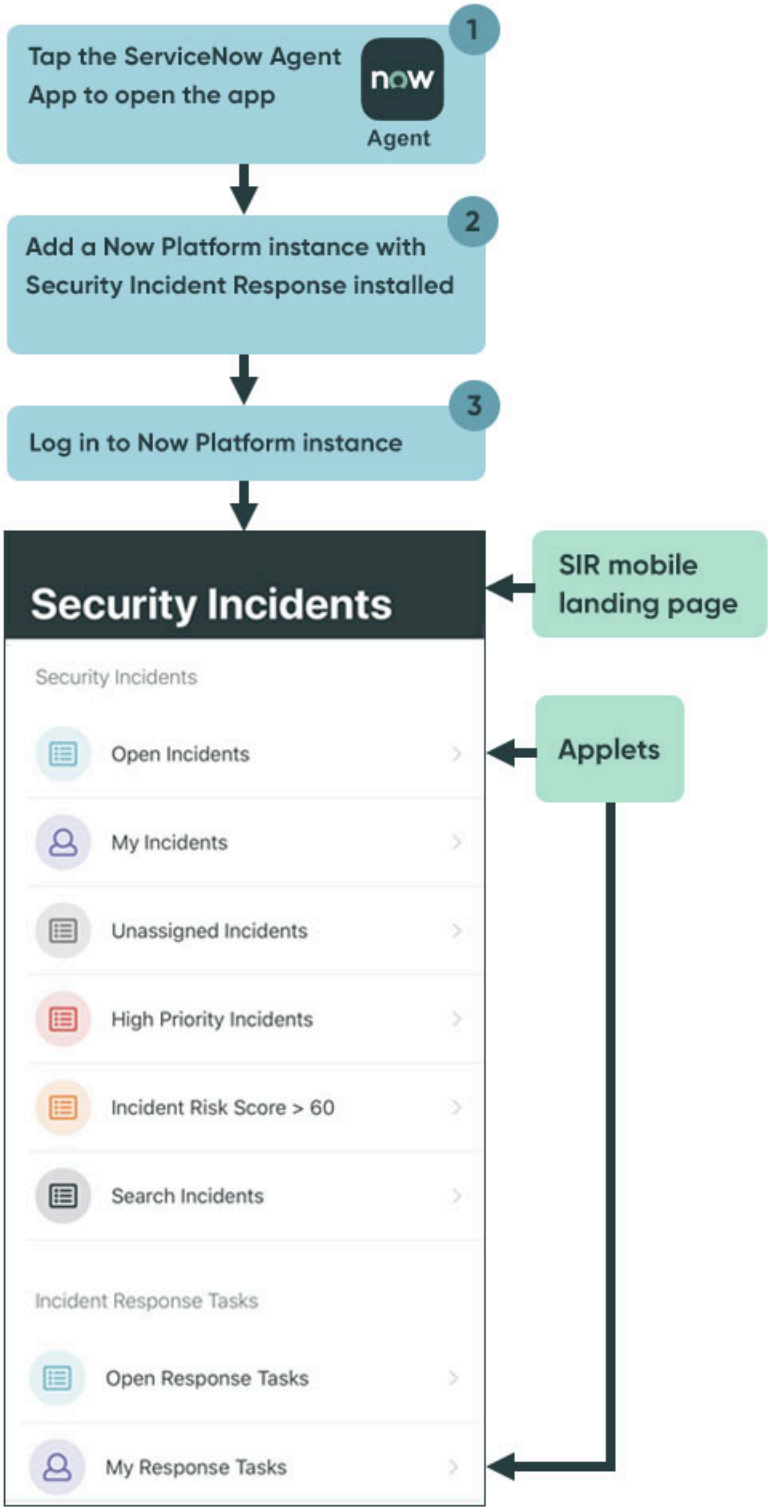
Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 a 10 minutos.
Verifique se você concluiu as etapas de configuração descritas em Configurar check-list para o Aplicativo Security Incident Response Mobile.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

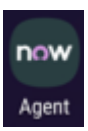
Aplicativo Security Incident Response Mobile



Tradução automática

Procedimento

1. No seu dispositivo móvel, toque no aplicativo **ServiceNow Agent** para abri-lo.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você ainda não estiver conectado a uma instância Now Platform, a tela Instâncias será exibida.

2. Se a instância Now Platform com a aplicação principal Security Incident Response ainda não tiver sido adicionada ao seu dispositivo móvel, siga estas etapas para adicioná-la.

   a. Na tela Instâncias exibida, toque no .
   Uma tela é exibida solicitando que você insira e salve um endereço de uma instância Now Platform.

   b. Preencha os campos.

Campo	Descrição
Insira o endereço da instância ou leia um código QR.	Escolha uma para continuar: ▪ Antes de `.service-now.com`, insira o nome da sua instância Now Platform, por exemplo, `sirmobileny`. ▪ Insira um endereço. Este endereço é o URL da sua instância Now Platform que você deseja exibir no seu dispositivo móvel, por exemplo, https://sirmobileny.service-now.com. ▪ Verificar um código QR.
(Opcional) Insira o apelido	Insira um apelido para esta instância. Se você tiver várias instâncias adicionadas ao dispositivo, os apelidos poderão ajudá-lo a localizar rapidamente uma instância do Now Platform.

   c. Toque em **Salvar e fazer login**.

3. Na tela de login ServiceNow exibida, insira o Nome de usuário e a Senha da instância Now Platform que você deseja adicionar e toque em **Login**.
   A tela inicial de Incidentes de segurança é exibida. Você fez login com sucesso no Aplicativo Security Incident Response Mobile.
4. Depois de fazer login, verifique se as notificações estão habilitadas no Aplicativo Security Incident Response Mobile.

   a. Na tela inicial na parte inferior, toque em **Notificação**.

   b. Na tela Notificações, toque em **Habilitar notificações** se não estiver habilitado.
   As notificações do Now Platform são exibidas na tela Notificações no Aplicativo Security Incident Response Mobile.

5. Depois de fazer login em uma instância no seu dispositivo móvel, é a instância Now Platform padrão no dispositivo.
   Se você quiser exibir outro Now Platform no dispositivo, será necessário fazer logout da instância padrão. Para sair:

   a. Toque no ícone de configurações.

   b. Toque **em Logout**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tela Instâncias é exibida com todas as instâncias Now Platform que você adicionou ao dispositivo móvel.

c. Opcional: Toque em outra instância para fazer login nela ou, como alternativa, siga as etapas anteriores para adicionar outra instância.

Se a tela de instâncias do Aplicativo Security Incident Response Mobile não for exibida depois que você tocar no app **ServiceNow Agent** no seu dispositivo, verifique se o **ServiceNow Agent** é permitido como um app confiável no seu dispositivo. Para permitir o acesso como um app confiável, navegue até as configurações e gestão geral de dispositivos no seu dispositivo e toque na opção (app Truste etc.) para permitir o acesso.

Se uma mensagem de erro for exibida depois que você inserir suas credenciais na tela de login, verifique se o nome de usuário e a senha da instância Now Platform estão corretos.

Se você tiver problemas para visualizar a tela inicial, verifique sua conexão de rede.

Se você não conseguir exibir a tela Instâncias depois de tocar no aplicativo **ServiceNow Agent**, tente desinstalá-lo do seu dispositivo. Verifique se você tem a versão mais atual do app na Apple iOS App Store ou na Google Play Store e tente reinstalá-la.

Exibir, editar e atribuir incidentes de segurança em aberto com o Aplicativo Security Incident Response Mobile

Como analista de incidentes de segurança, exiba, edite e atribua Security Incident Response (SIR) incidentes de segurança abertos a partir do seu dispositivo móvel. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Na lista de registros, atribua um incidente de segurança em aberto a você mesmo ou reatribua-o. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

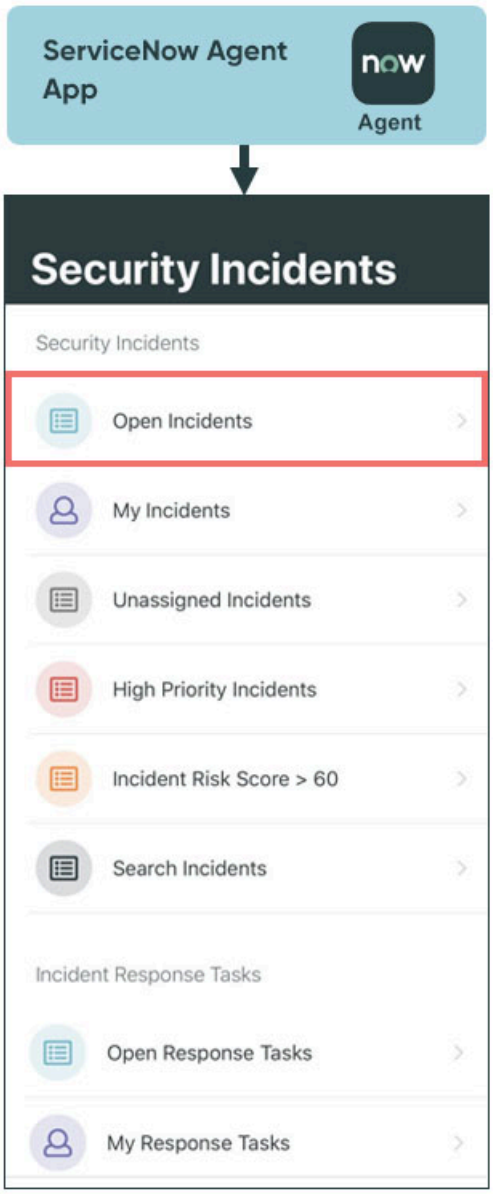
Procedimento

1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a página principal de Incidentes de segurança exibida, toque **em Incidentes abertos**.

   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

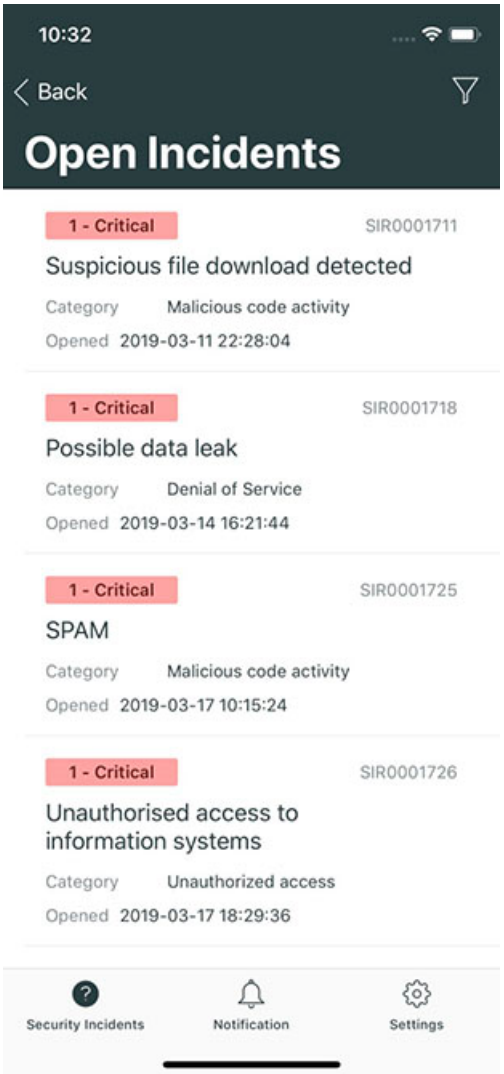
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Incidentes em aberto é exibida com uma lista de registros de incidentes de segurança em aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (Ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

4. Para atribuir um incidente a você mesmo ou reatribuí-lo diretamente da lista de incidentes de segurança em aberto, deslize para a esquerda em um registro para abrir o menu.

5. Escolha um no menu exibido para continuar.

Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a si mesmo. Se o incidente de segurança já estiver atribuído a você, esta opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição:

Tradução automática

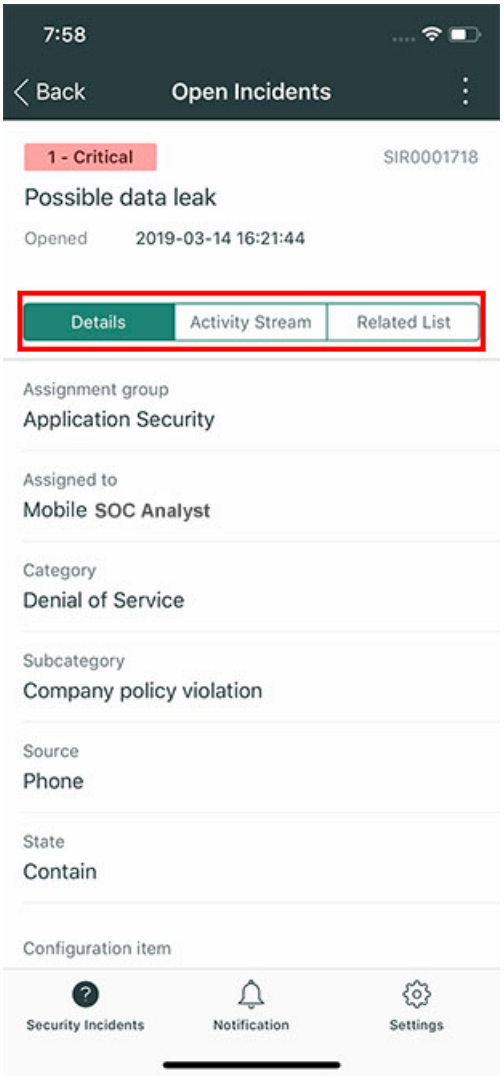
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Toque em **Grupo de atribuição**. **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque **em Atribuído a**. **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio (ícone) ou em **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes de um registro de incidente de segurança aberto e ver mais registros associados e listas relacionadas, com a tela Incidentes abertos exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Toque no ícone de menu (ícone de ⋮) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para reatribuir o incidente, toque em **Reatribuir** ou **Atribuir a mim**. Siga as instruções descritas na tabela anterior. Depois de concluir as edições, toque no ícone de envio (ícone ➤) ou em **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, revise a trilha de auditoria de anota-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ções de trabalho, atividades e comentários adicionais do registro. Toque no ícone de) para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens de todas as Listas relacionadas do incidente de segurança que estão preenchidos. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidas, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas associadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone Incidentes de segurança para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do Aplicativo Security Incident Response Mobile. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual.

Tradução automática

Exibir, editar e reatribuir incidentes de segurança atribuídos a você com o Aplicativo Security Incident Response Mobile

Como analista de incidentes de segurança, exiba, edite e reatribua Security Incident Response (SIR) incidentes atribuídos a você. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

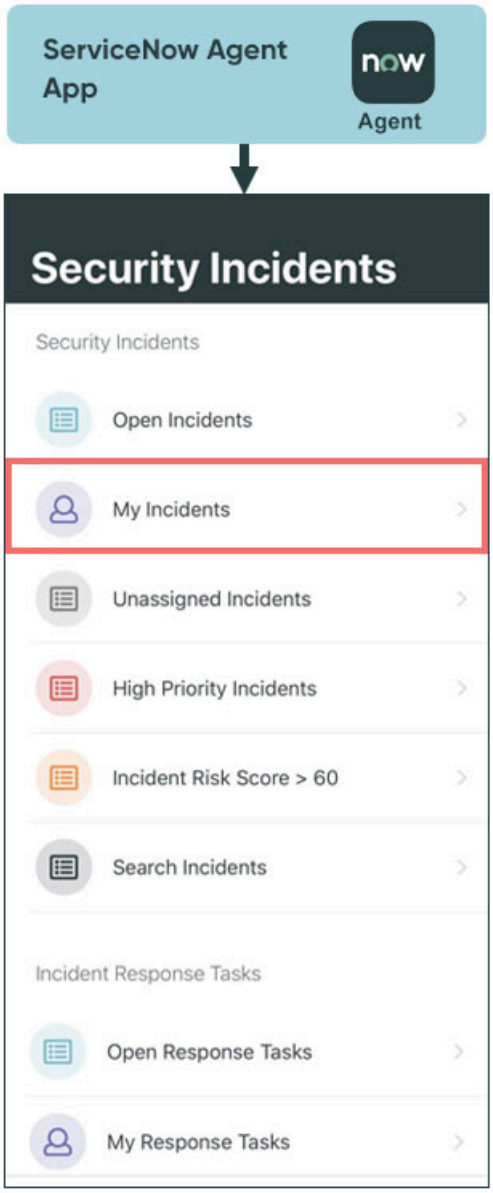
Reatribua um incidente de segurança em aberto a outro analista do seu grupo na lista de registros. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Meus incidentes**.

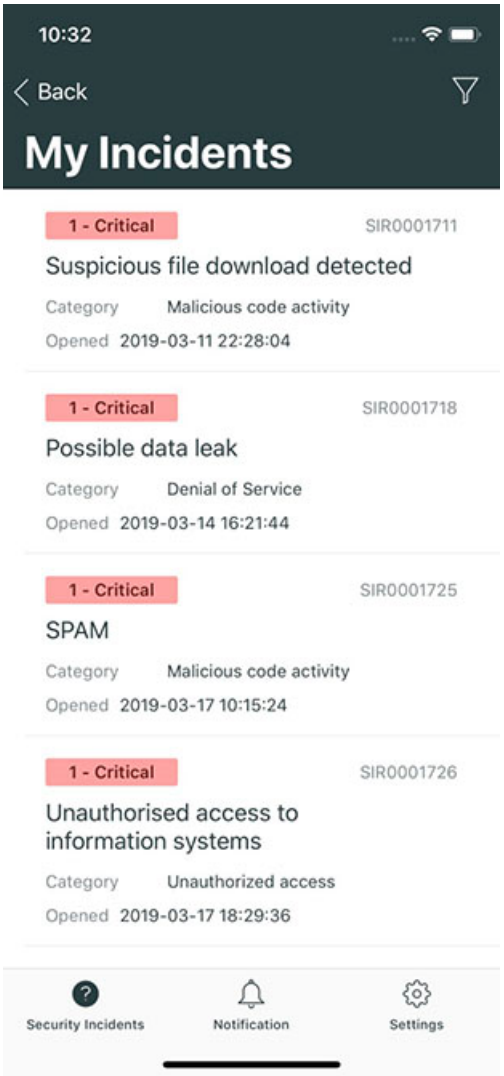
   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



   A tela Meus incidentes é exibida com uma lista de registros de incidentes de segurança abertos atribuídos a você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



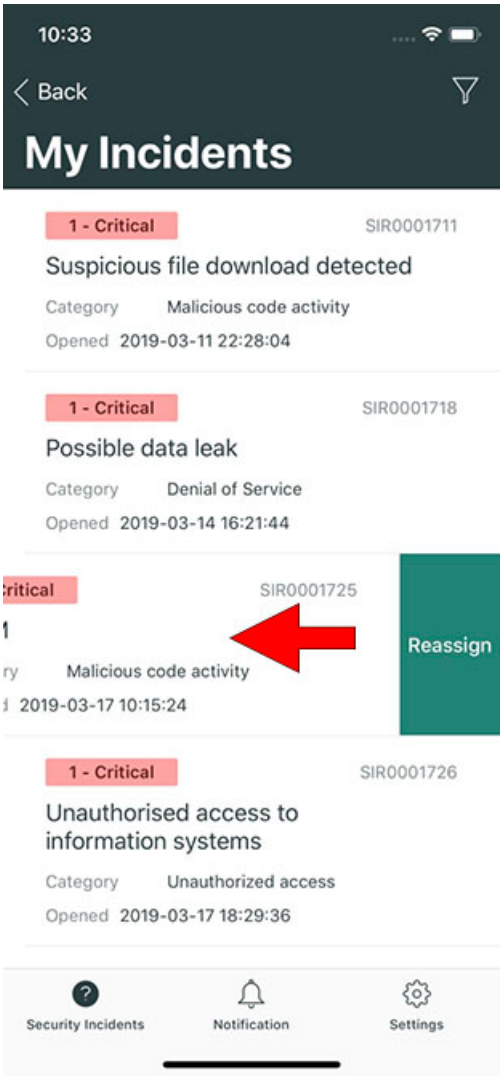
3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( ) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

4. Para reatribuir um incidente diretamente da lista, com a lista de registros de incidentes de segurança abertos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

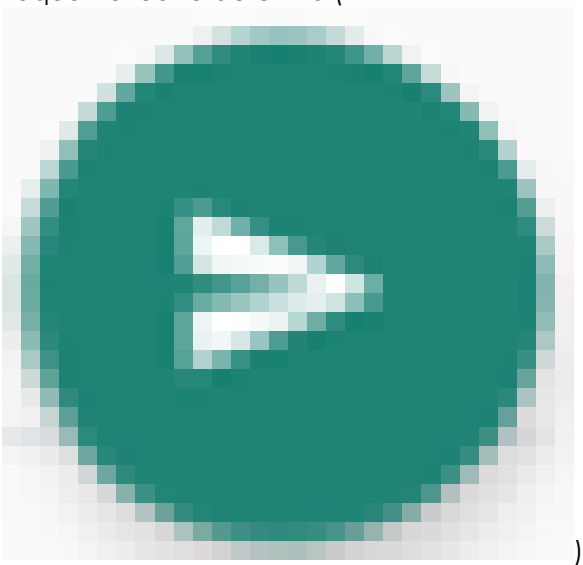


5. Edite os campos Grupo de atribuição ou Atribuído a no menu exibido.

Opção	Descrição
Reatribuir	Para reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição: **a.** Toque **em Atribuído a**. **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa.

Tradução automática

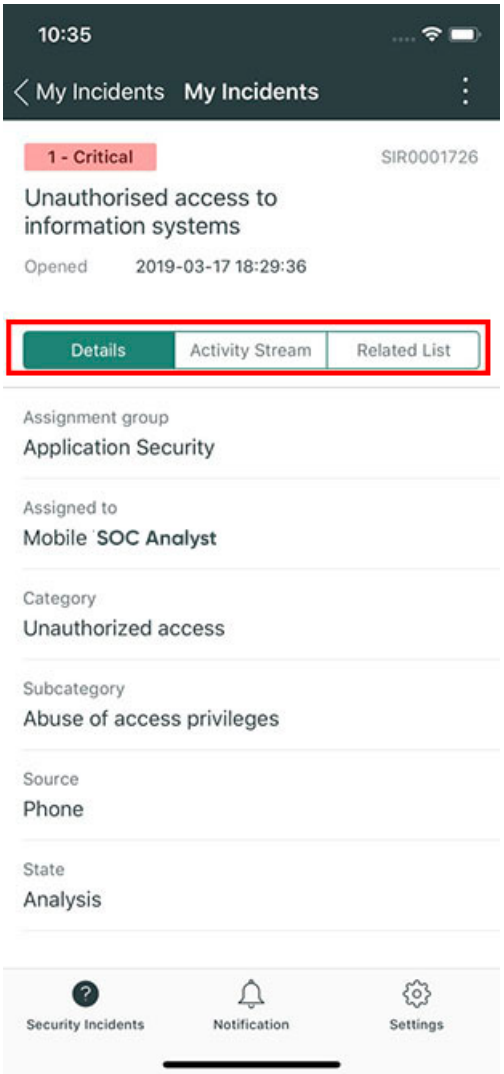
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Toque no ícone de envio () ou em **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes do registro de incidente de segurança aberto, com a tela Meus incidentes exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

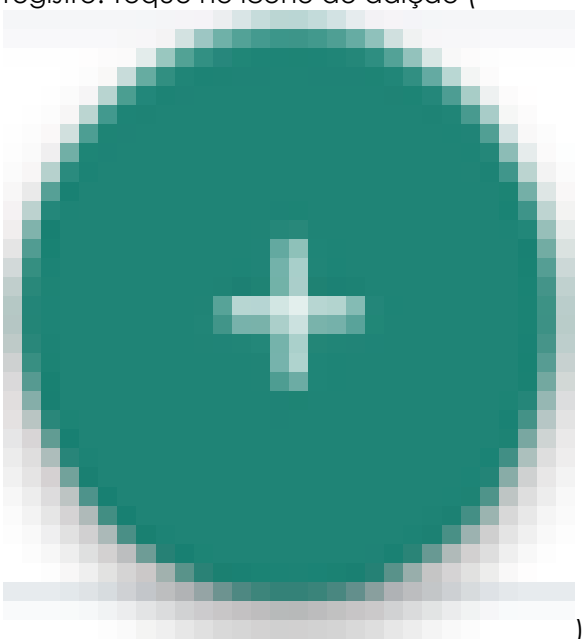
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Toque no ícone de menu ( ) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para reatribuir o incidente, toque **em Reatribuir**. Siga as instruções descritas na tabela anterior. Depois de concluir as edições, toque no ícone de envio (

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	) ou em **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição () para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em todas as listas relacionadas que estão preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nas listas de itens exibidas, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas associadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone Incidentes de segurança para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do Aplicativo Security Incident Response Mobile. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual.

Exibir, editar e atribuir incidentes de segurança não atribuídos com o Aplicativo Security Incident Response Mobile

No seu dispositivo móvel, exiba, edite e atribua Security Incident Response (SIR) incidentes não atribuídos. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança aberto e não atribuído a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

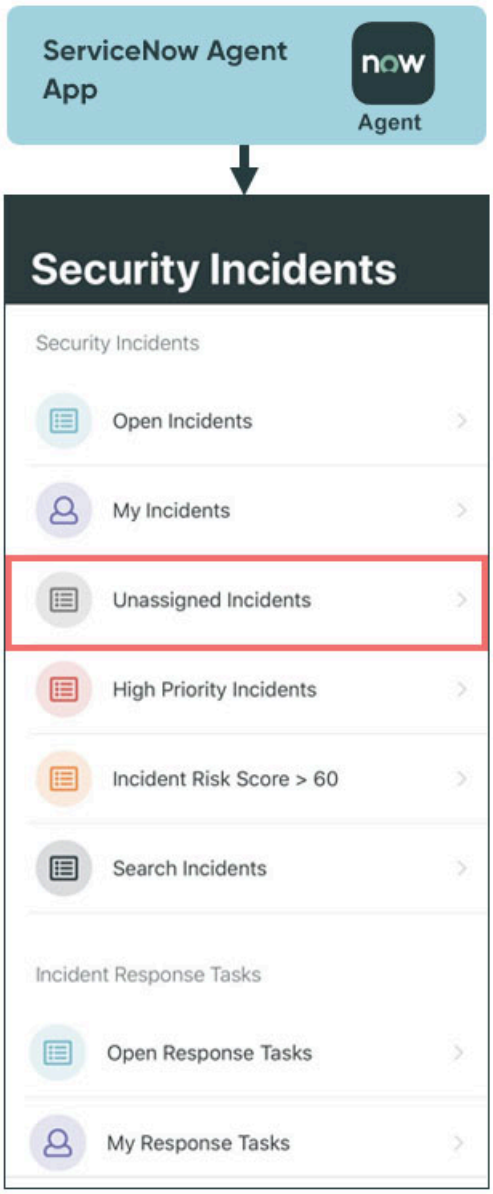
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Incidentes não atribuídos**.

   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

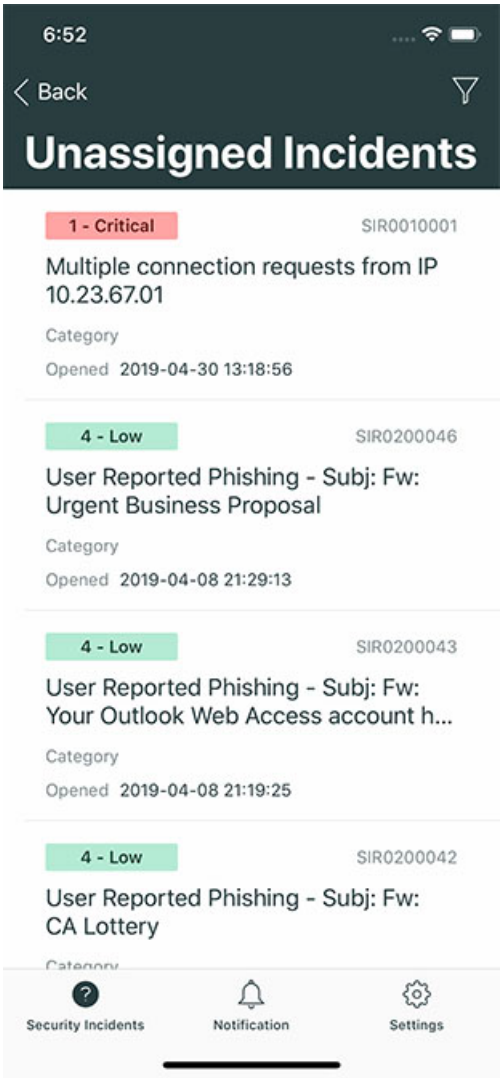
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Incidentes não atribuídos é exibida com uma lista de registros de incidentes de segurança não atribuídos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



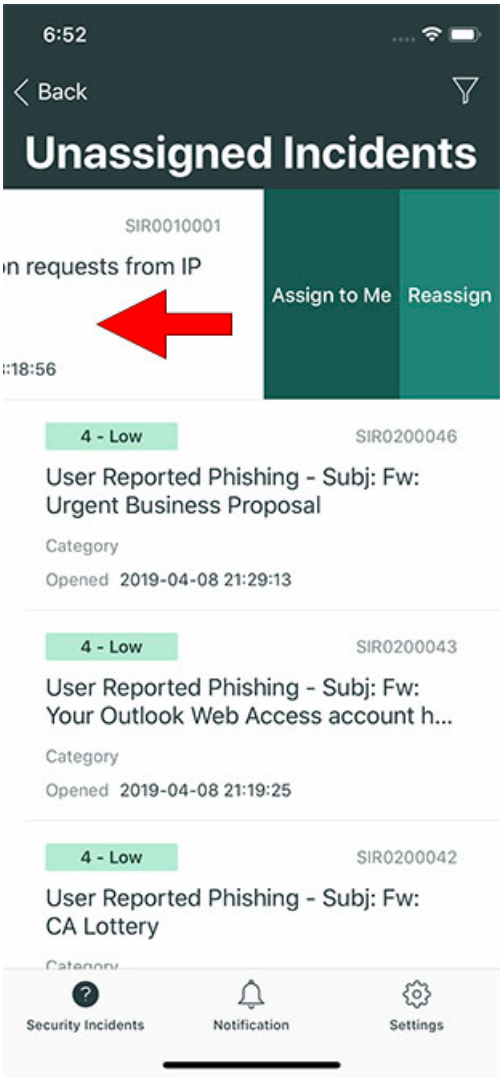
3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (Ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

4. Para atribuir ou reatribuir um registro de incidente de segurança em aberto diretamente da lista, com a lista de registros de incidentes de segurança em aberto não atribuídos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Escolha um no menu para continuar.

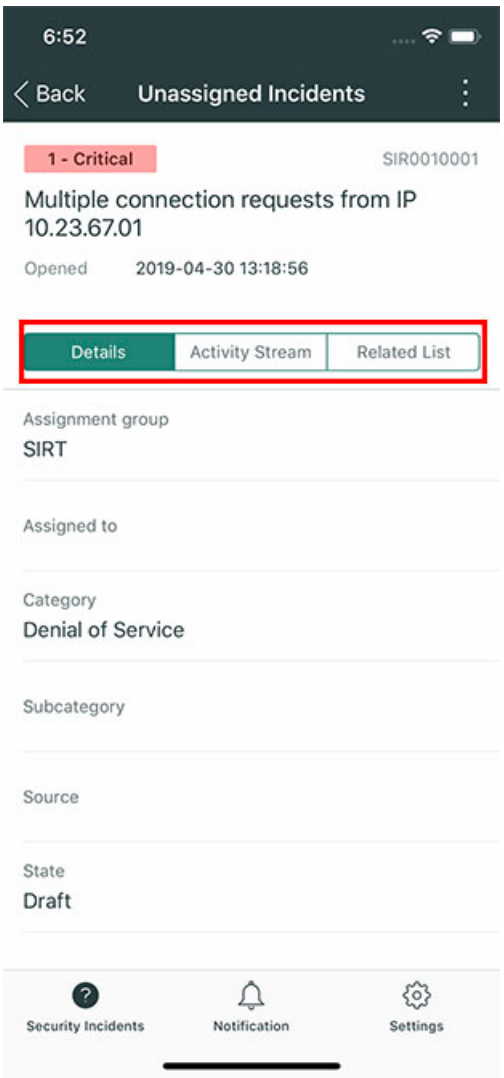
Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a si mesmo. Se o incidente de segurança já estiver atribuído a você, esta opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Toque **em Atribuído a**. **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio (ícone) ou em **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, com a tela Incidentes não atribuídos exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.



Opção	Descrição
Toque no ícone de menu (ícone de) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para atribuir ou reatribuir o incidente, toque em **Reatribuir** ou **Atribuir a mim**. Siga as instruções descritas na tabela anterior. Depois de concluir as edições, toque no ícone de envio (ícone) ou em **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de) para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em qualquer uma das Listas relacionadas que estão preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidas, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas associadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone Incidentes de segurança para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do Aplicativo Security Incident Response Mobile. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir, editar e atribuir incidentes de alta prioridade com o Aplicativo Security Incident Response Mobile

No seu dispositivo móvel, exiba, edite e atribua Security Incident Response (SIR) incidentes de alta prioridade. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança crítico em aberto a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

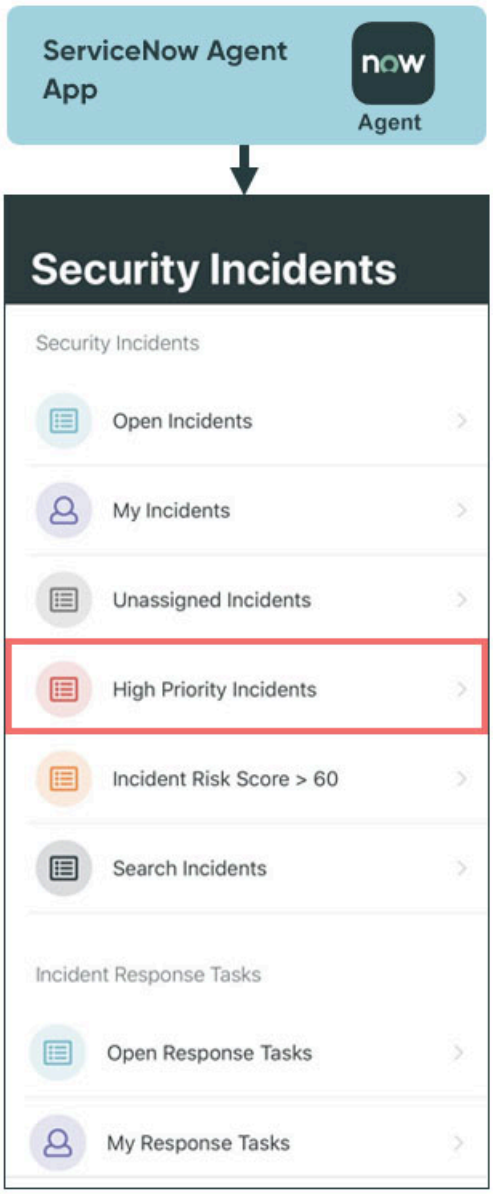
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Incidentes de alta prioridade**.

   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

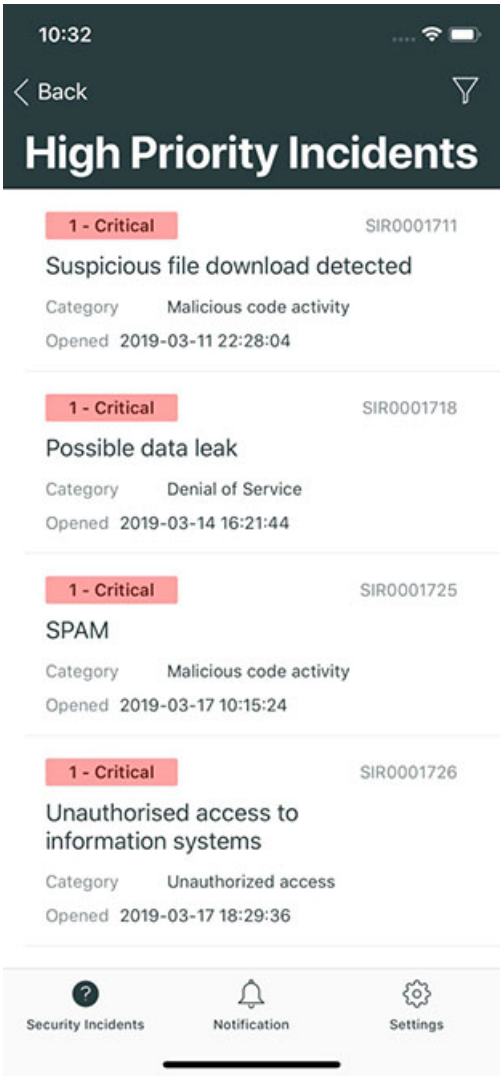
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Incidentes de alta prioridade é exibida com uma lista de incidentes de segurança críticos (alta prioridade).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



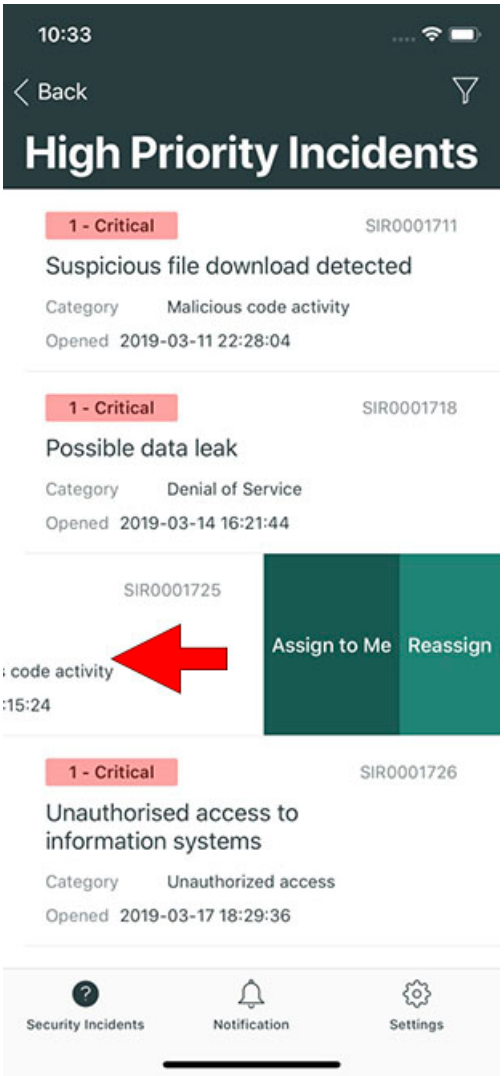
3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( ) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

4. Com a lista de registros de incidentes de segurança de alta prioridade em aberto exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

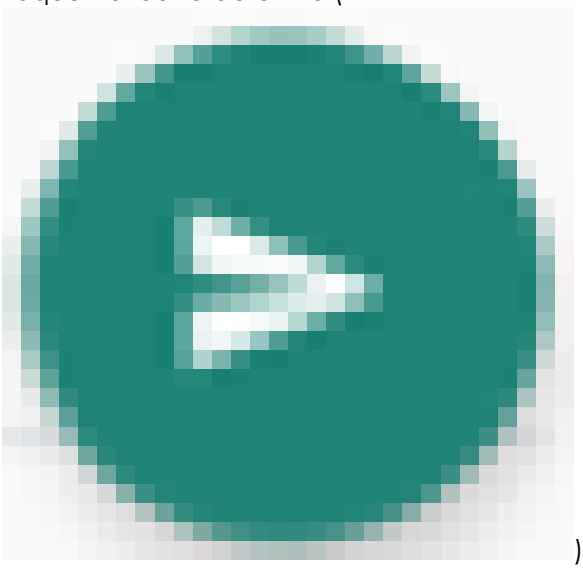


5. Escolha um para continuar.

Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a si mesmo. Se o incidente de segurança já estiver atribuído a você, esta opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição: **a.** Tocar **em Grupo de atribuição** **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

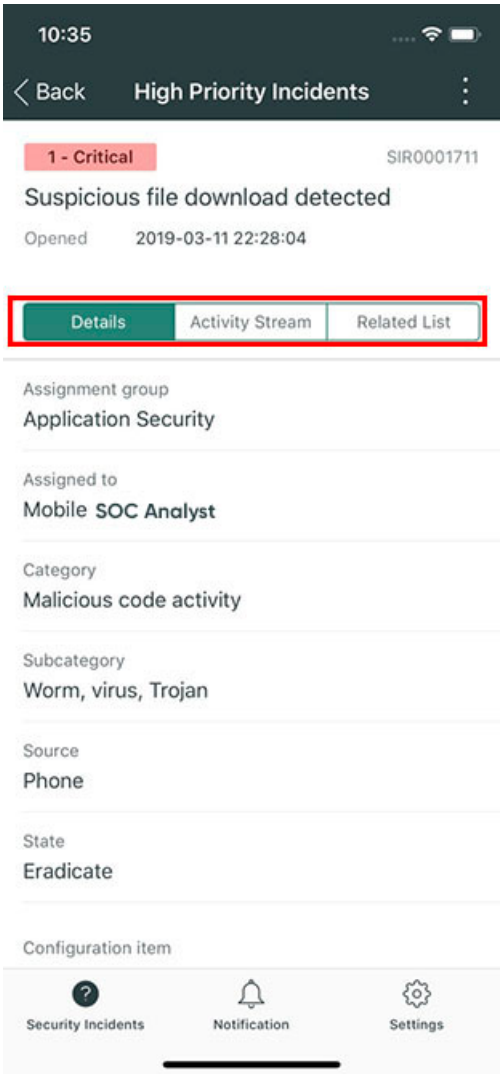
Opção	Descrição
	a. Toque **em Atribuído a**. **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio () ou em **Enviar** para salvar e enviar suas mudanças.

6. Para exibir os detalhes de um registro de incidente de segurança aberto e ver mais registros associados e listas relacionadas, com a tela Incidentes de alta prioridade exibida, toque em um registro na lista.

7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

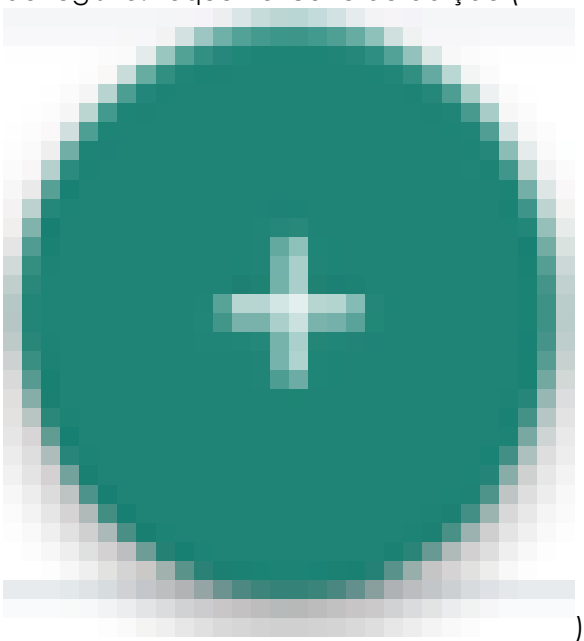
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Toque no ícone de menu ( ) no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para reatribuir o incidente, toque em **Reatribuir** ou **Atribuir a mim**. Siga as instruções descritas na tabela anterior. Depois de concluir as edições, toque no ícone de envio (

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	) ou em **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Atividade selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de adição () para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em qualquer uma das Listas relacionadas que estão preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidas, toque em um item para continuar a exibir os fluxos de atividades e as listas re-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	lacionadas associadas ao incidente de segurança primário.
Toque em um ícone de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone Incidentes de segurança para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do Aplicativo Security Incident Response Mobile. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual.

Exibir, editar e atribuir incidentes de segurança com uma pontuação de risco maior que 60 com o Aplicativo Security Incident Response Mobile

No seu dispositivo móvel, exiba e edite Security Incident Response (SIR) incidentes com um valor no campo de pontuação de risco maior que 60. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre incidentes.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Na lista de registros, atribua um incidente de segurança em aberto que tenha uma pontuação de risco maior que 60 a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

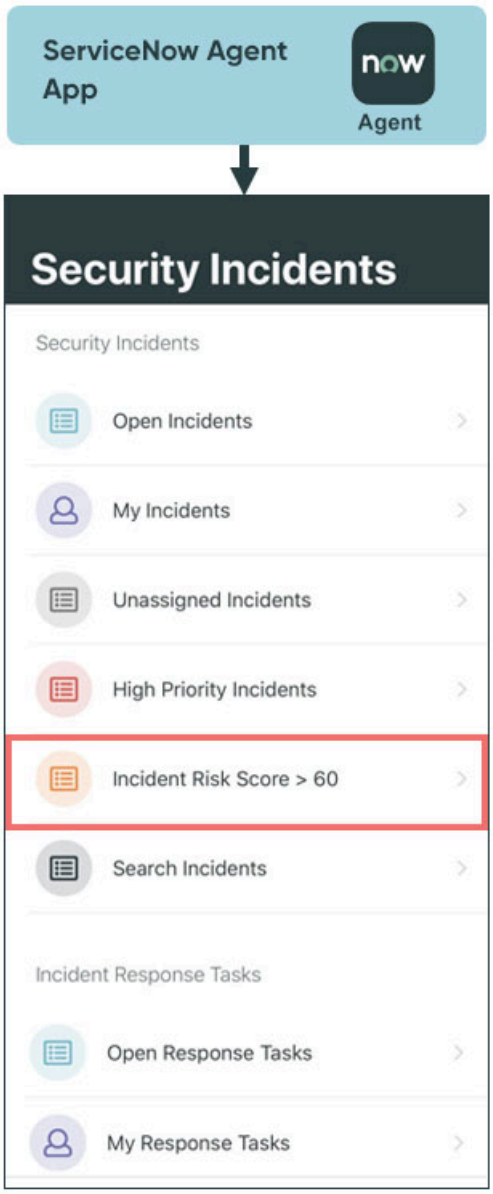
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Pontuação de risco > 60**.

   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

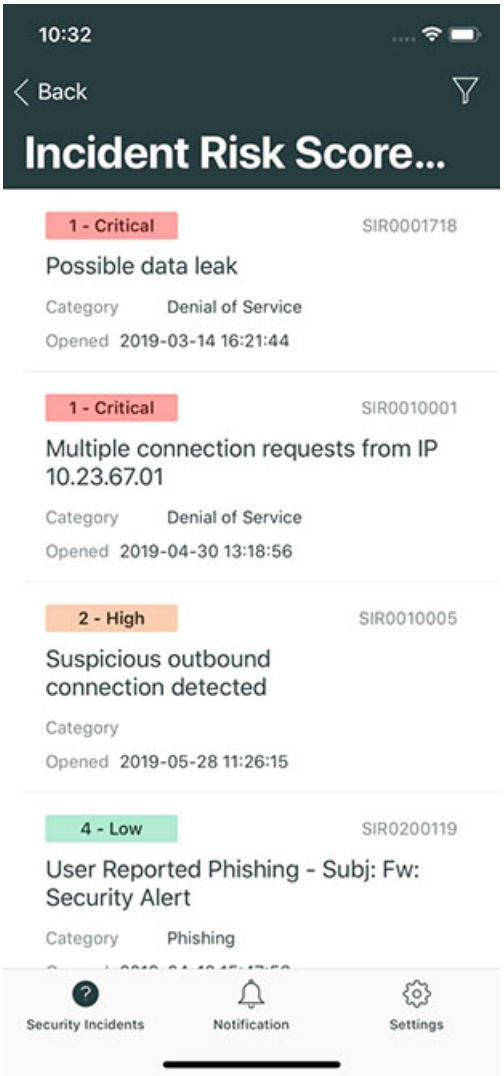
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Pontuação de risco do incidente é exibida com uma lista de incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



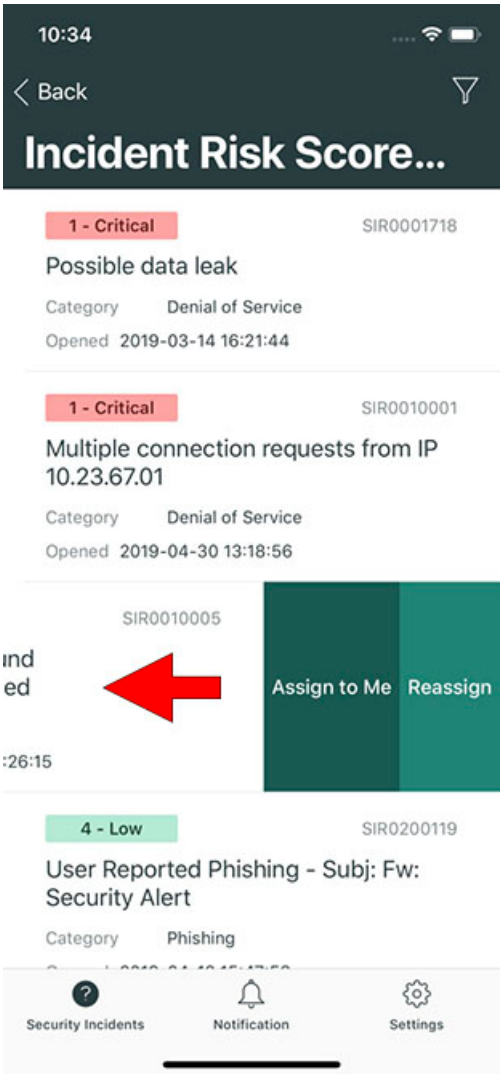
3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (Ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

4. Para atribuir um incidente de segurança a você mesmo ou reatribuí-lo diretamente na lista de registros de incidentes de segurança abertos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Escolha um para continuar.

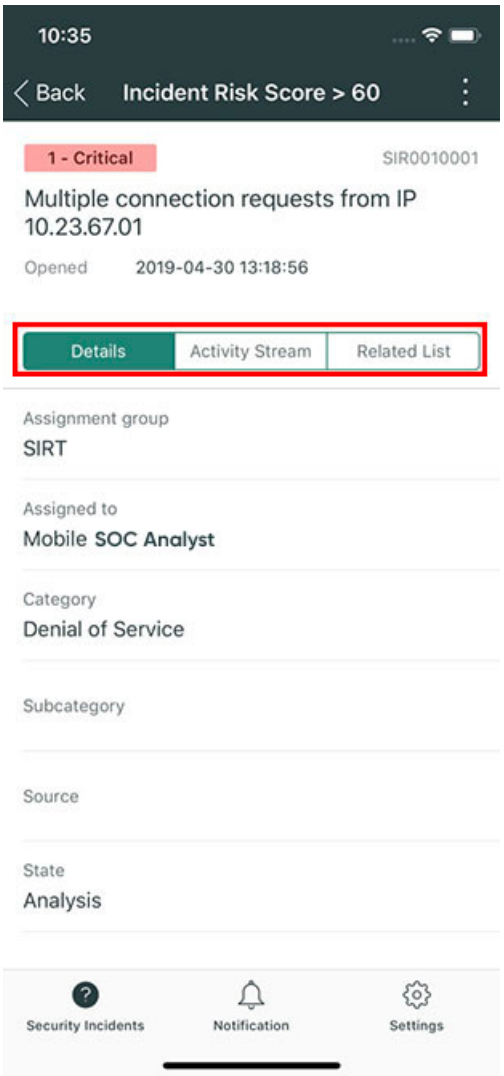
Opção	Descrição
Atribuir a Mim	Atribua o incidente de segurança a si mesmo. Se o incidente de segurança já estiver atribuído a você, esta opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição: **a.** Toque em **Grupo de atribuição**. **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir o incidente de segurança a um membro do grupo de atribuição:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Toque **em Atribuído a** e **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Toque no ícone de envio (ícone) ou em **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes de um registro de incidente de segurança aberto e ver mais registros associados e listas relacionadas, com a tela Pontuação de risco do incidente exibida, toque em um registro na lista.
7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.



Opção	Descrição
Toque no ícone de menu Ícone de no canto superior direito da tela.	No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar incidente de segurança exibida, toque em um campo para expandi-lo e escolha

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para reatribuir o incidente, toque em **Reatribuir** ou **Atribuir a mim**. Siga as instruções descritas na tabela anterior. Depois de concluir as edições, toque no ícone de envio (ícone) ou em **Enviar** para salvar suas mudanças e atualizar o incidente de segurança.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, revise a trilha de auditoria de anotações de trabalho, atividades e comentários adicionais do registro. Toque no ícone de) para adicionar uma anotação de trabalho ou anexar um arquivo.
Guia Lista relacionada	Com a guia Lista relacionada selecionada, exiba os itens em qualquer uma das Listas relacionadas que estão preenchidas no incidente de segurança. Toque em um item na lista exibida para exibir os detalhes de uma lista relacionada. Nas listas de itens exibidas, toque em um item para continuar a exibir os fluxos de atividades e as listas relacionadas associadas ao incidente de segurança primário.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Toque no ícone Incidentes de segurança para retornar à tela inicial. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações do Now Platform e do Aplicativo Security Incident Response Mobile. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exiba informações sobre a instância Now Platform no seu dispositivo. ▪ Faça logout da instância Now Platform atual.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile

Pesquise Security Incident Response (SIR) incidentes de segurança em uma instância Now Platform®. Somente os incidentes que correspondem aos critérios de pesquisa específicos inseridos são exibidos.

Antes de Iniciar
Função necessária: sn_si.analyst

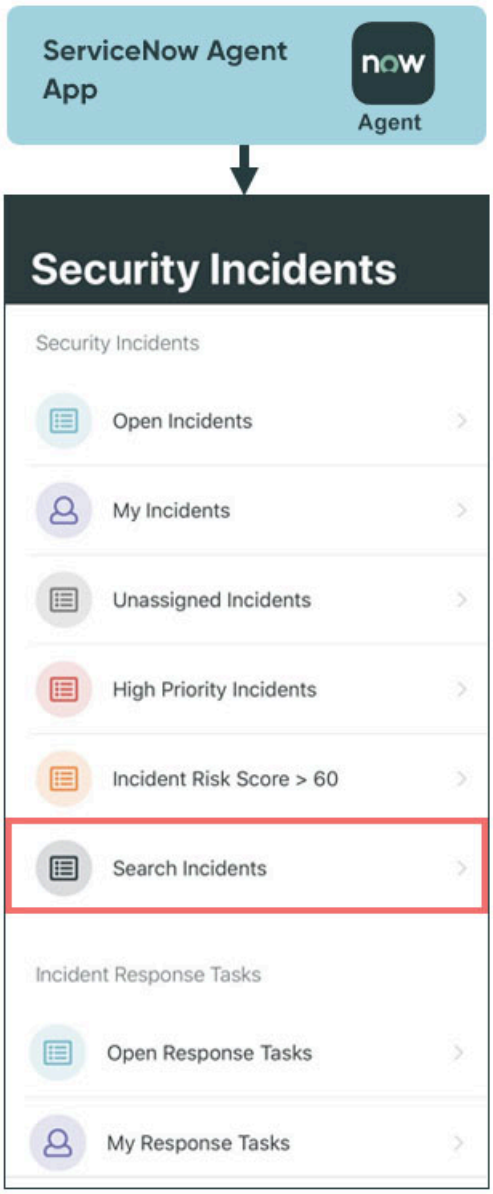
Por Que e Quando Desempenhar Esta Tarefa
Tempo para concluir esta tarefa: 5 a 10 minutos.

Procedimento
1. Se você não estiver conectado à sua instância da Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Pesquisar incidentes**.

   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para limitar o número de resultados de pesquisa retornados, talvez você prefira preencher o maior número possível de campos no formulário.
Para adicionar critérios de pesquisa, consulte a tabela a seguir. Siga as instruções após a tabela para editar os critérios de pesquisa existentes, limpar os critérios de pesquisa ou enviar uma pesquisa.

Tocar neste campo	**Para adicionar uma entrada em** Android **dispositivos**	**Para adicionar uma entrada em** iOS **dispositivos**
Número	Insira um valor alfanumérico para um incidente de segurança, por exemplo, `SIR0010004`. Este número é exibido no canto superior direito do incidente de segurança.	Insira um valor alfanumérico para um incidente de segurança, por exemplo, `SIR0010004`. Este número é exibido no canto superior direito do incidente de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android **dispositivos**	Para adicionar uma entrada em iOS **dispositivos**
	O recurso pesquisa cadeias de caracteres numéricas e cadeias numéricas parciais. Para pesquisas mais refinadas, insira mais dígitos. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou para enviar uma pesquisa.	O recurso pesquisa cadeias de caracteres numéricas e cadeias numéricas parciais. Para pesquisas mais refinadas, insira mais dígitos. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou em **Pesquisar** para enviar uma pesquisa.
Descrição resumida	Insira texto no campo, por exemplo, `malware`. O recurso pesquisa cadeias de caracteres de texto e cadeias de caracteres de texto parciais do campo Descrição resumida. Para pesquisas mais refinadas, insira mais texto. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou para enviar uma pesquisa.	Insira texto no campo, por exemplo, `malware`. O recurso pesquisa cadeias de caracteres de texto e cadeias de caracteres de texto parciais do campo Descrição resumida. Para pesquisas mais refinadas, insira mais texto. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou em **Pesquisar** para enviar uma pesquisa.
Prioridade	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar incidentes.
Categoria	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar incidentes.
Estado	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android **dispositivos**	Para adicionar uma entrada em iOS **dispositivos**
	uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar incidentes.
Atribuído a	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.
Grupo de atribuição	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.

Para dispositivos Android, com a tela Pesquisar incidentes exibida e todos os seus critérios inseridos, escolha um para continuar.

Opção	Descrição
Limpar ou modificar os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios inseridos, com a tela Pesquisar incidentes exibida, toque na seta para voltar para limpar todos os campos e retornar à tela inicial de Incidentes de segurança. A pesquisa não foi enviada e os critérios de pesquisa foram limpos. Como alternativa, para editar um campo: ◦ Com a tela Pesquisar incidentes exibida, toque em um campo com critérios de pesquisa para expandi-lo. ◦ Toque em um item para desmarcá-lo. Toque em **Todos** para selecionar todos os itens. Toque em **Todos** novamente para limpar todos os itens. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**. ◦ Toque no ícone de marca de seleção para salvar as mudanças e retornar à tela Pesquisar incidentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Enviar uma pesquisa	Com a tela Pesquisar incidentes exibida com os critérios de pesquisa inseridos, toque no ícone enviar (ícone). Os incidentes de segurança que correspondem aos seus critérios de pesquisa são exibidos. Depois que a pesquisa é concluída, os critérios de pesquisa não são salvos.

4. Para dispositivos iOS, com a tela Pesquisar incidentes exibida, escolha um para continuar.

Opção	Descrição
Limpar ou modificar os critérios de pesquisa antes de executar uma pesquisa	Para limpar todos os critérios e retornar à tela inicial, toque no ícone de fechar (X). Os critérios de pesquisa inseridos não são salvos. Como alternativa, para editar um campo: ◦ Com a tela Pesquisar incidentes exibida, toque em um campo com critérios de pesquisa para expandi-lo. ◦ Toque em um item da lista para desmarcá-lo ou toque em **Limpar tudo**. Para limpar um valor dos campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**. ◦ Toque em **Concluído** para salvar as mudanças e retornar à tela Pesquisar incidentes.
Enviar uma pesquisa	Com a tela Pesquisar incidentes exibida com os critérios de pesquisa inseridos, toque em **Pesquisar**. Os incidentes de segurança que correspondem aos seus critérios de pesquisa são exibidos. Depois que a pesquisa é concluída, os critérios de pesquisa não são salvos.

5. Opcional: Se a pesquisa retornar vários registros, você pode Filtrar registros com o Aplicativo Security Incident Response Mobile para refinar os resultados da pesquisa.

Exibir, editar e atribuir tarefas de resposta em aberto com o Aplicativo Security Incident Response Mobile

Exibir, editar e atribuir tarefas de resposta em aberto. Suas mudanças são salvas na tarefa de resposta a incidentes de segurança do incidente de segurança primário.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

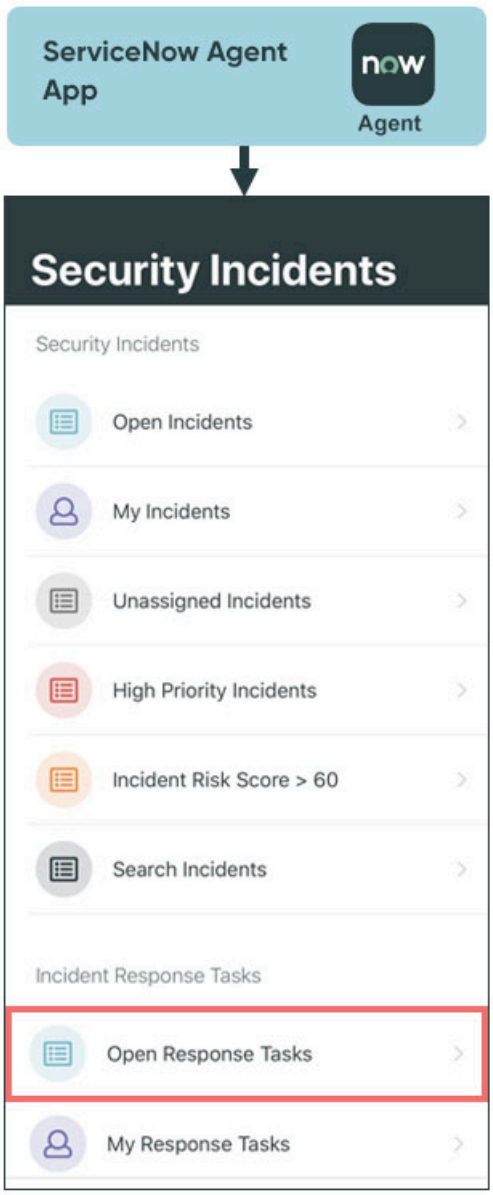
Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua uma tarefa de resposta aberta e não atribuída a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

Procedimento

1. Se você não estiver conectado à sua instância da Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Tarefas de resposta aberta**.

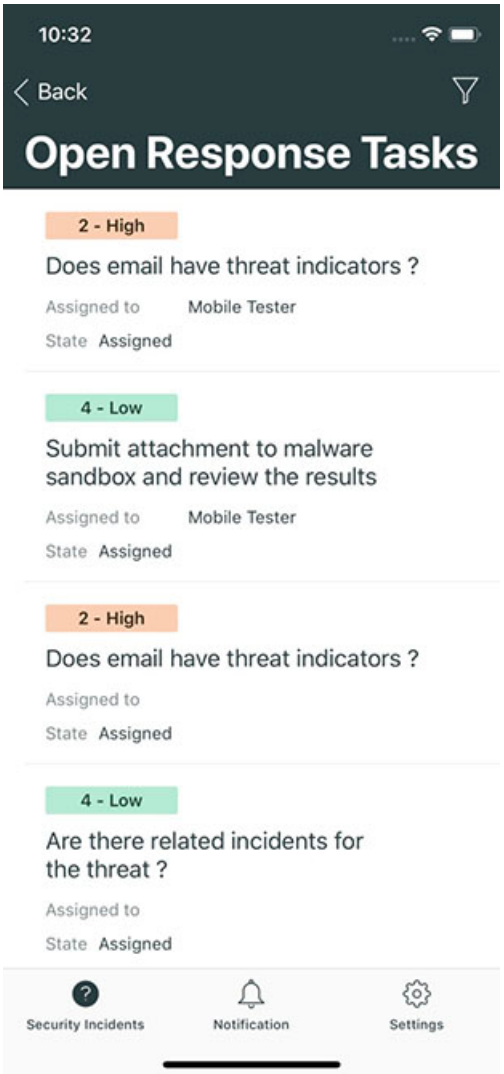
   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A tela Tarefas de resposta em aberto é exibida com uma lista de tarefas em aberto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar tarefas que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (Ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.
4. Com a lista de tarefas de resposta em aberto exibida, para atribuir ou reatribuir diretamente da lista, deslize para a esquerda em um registro para abrir o menu.
5. Escolha um para continuar.

Opção	Descrição
Atribuir a Mim	Atribua a tarefa de resposta a si mesmo. Se a tarefa já estiver atribuída a você, esta opção não será exibida.
Reatribuir	Para atribuir ou reatribuir o grupo de atribuição:

Tradução automática

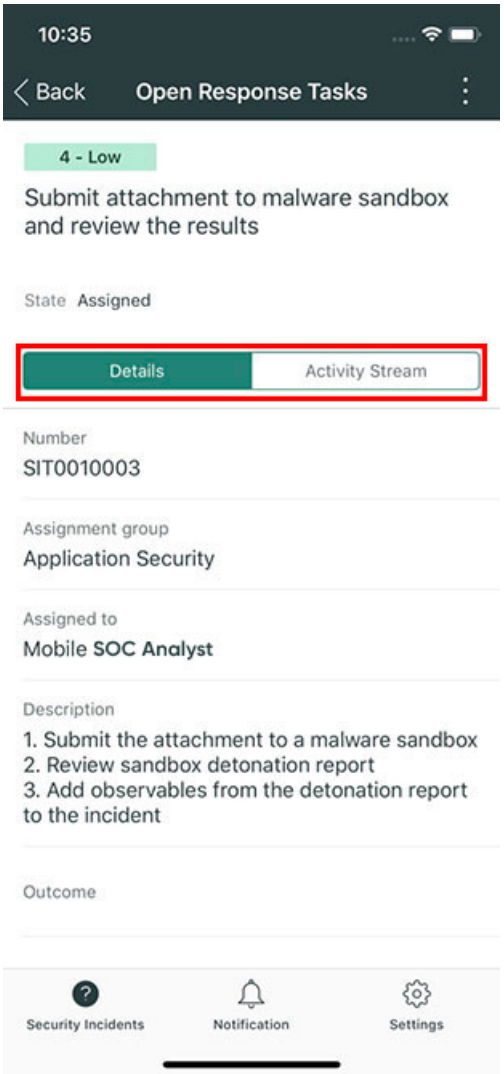
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. Tocar **em Grupo de atribuição** **b.** Toque em um grupo na lista exibida ou insira o texto no campo de pesquisa. O grupo deve ser um grupo de atribuição relacionado à segurança. Para atribuir ou reatribuir a tarefa a um membro do grupo de atribuição: **a.** Toque **em Atribuído a** e **b.** Toque em um nome na lista exibida ou insira o texto no campo de pesquisa. Uma mensagem é exibida confirmando que o registro foi atualizado. A tarefa no incidente de segurança primário é atribuída a um novo usuário e atualizada em sua instância Now Platform. Toque no ícone de envio (ícone) ou em **Enviar** para salvar e enviar suas mudanças.

6. Como alternativa, para exibir os detalhes de um registro de tarefa de resposta em aberto, com a tela Tarefas de resposta em aberto exibida, toque em um registro na lista.
7. Com as guias no registro da tarefa de resposta exibidas, escolha uma na tabela a seguir para continuar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos na tarefa de resposta. Para editar campos ou atribuir a tarefa, toque no ícone de menu (ícone de ⋮). No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar tarefa de resposta exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para reatribuir a tarefa, toque em **Reatribuir** ou **Atribuir a mim**. Depois de concluir as edições, toque no ícone de envio (ícone ➤) ou em **Enviar** para salvar suas mudanças e atualizar o registro. A tarefa de resposta a incidentes de segurança no incidente de segurança primá-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	rio em sua instância Now Platform foi atualizada.
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ◦ Exiba a trilha de auditoria criada pelas Anotações de trabalho no registro. Para adicionar uma anotação de trabalho ou anexar um arquivo, toque no ícone de). ◦ Toque no ícone de menu (ícone de) para editar ou reatribuir a tarefa.
Ícones de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Se exibido, toque em um ícone para abrir outro ServiceNow® aplicativo para celular. ◦ Toque em **Notificação** para exibir notificações de incidentes de segurança críticos atribuídos a você ou ao seu grupo de atribuição. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exibir informações sobre a instância Now Platform. ▪ Faça logout da instância atual. Para fazer logout de uma instância Now Platform no seu dispositivo, com a página de detalhes exibida, toque em **Logout**.

Tradução automática

Exibir, editar e reatribuir suas tarefas de resposta com o Aplicativo Security Incident Response Mobile

Exibir, editar e reatribuir tarefas de resposta atribuídas a você. Suas mudanças são salvas na tarefa de resposta a incidentes de segurança do incidente de segurança primário.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

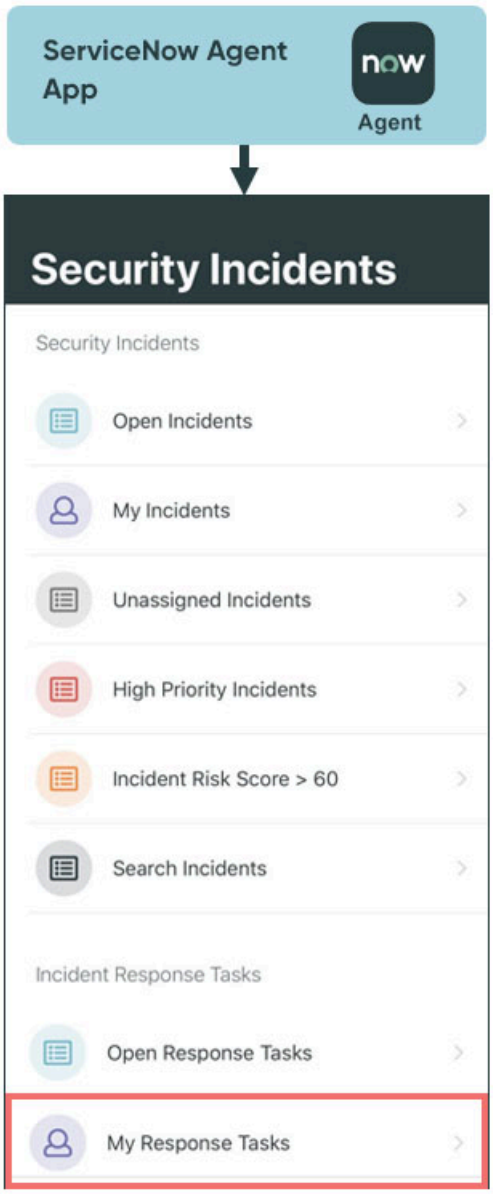
Na lista de registros, reatribua uma tarefa de resposta em aberto atribuída a você para outro analista do seu grupo. Como alternativa, exiba os detalhes do registro ou adicione uma anotação de trabalho antes da reatribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não estiver conectado à sua instância da Now Platform no seu dispositivo móvel, para obter mais informações, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Minhas tarefas de resposta**.

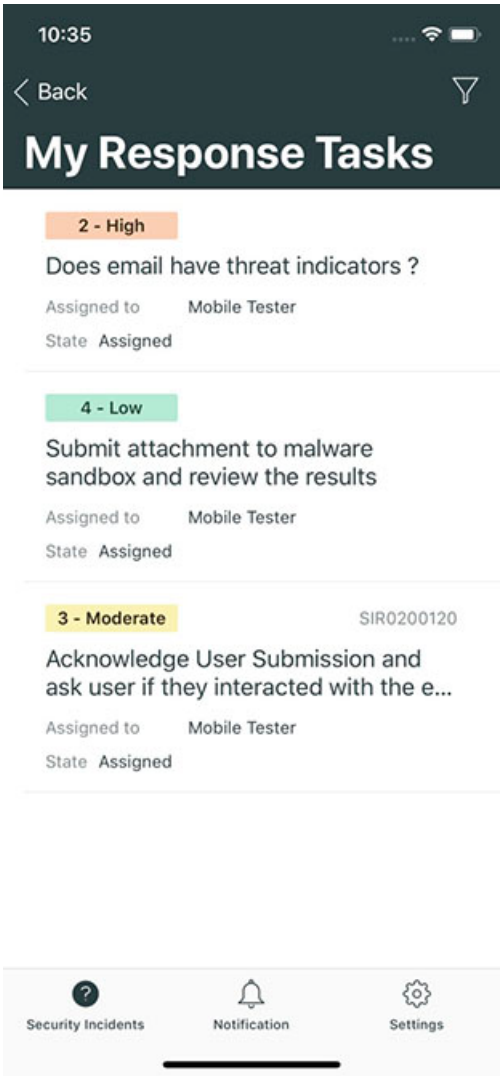
   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent (Executante) a qualquer momento para retornar à última tela exibida.



   A tela Minhas tarefas de resposta é exibida com uma lista das tarefas de resposta atribuídas a você.

Tradução automática

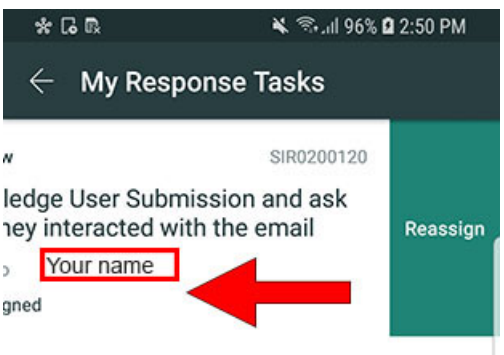
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Opcional: Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar tarefas que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( ) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

4. Para reatribuir uma tarefa diretamente da lista de registros de tarefa atribuídos a você, deslize para a esquerda em um registro para abrir o menu.

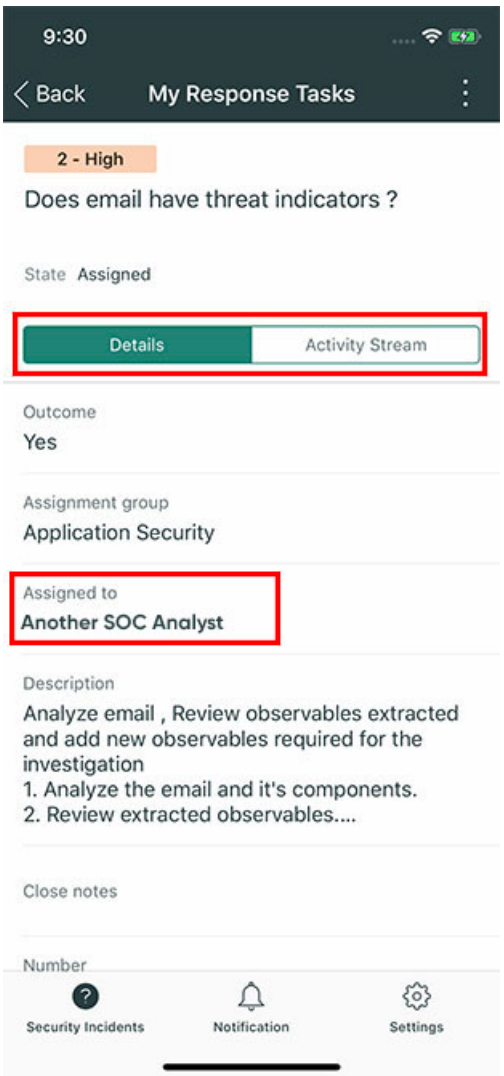


5. Toque **em Reatribuir**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

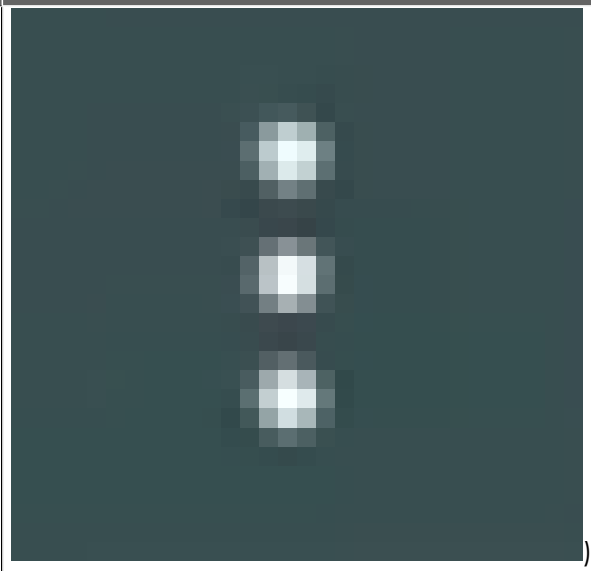
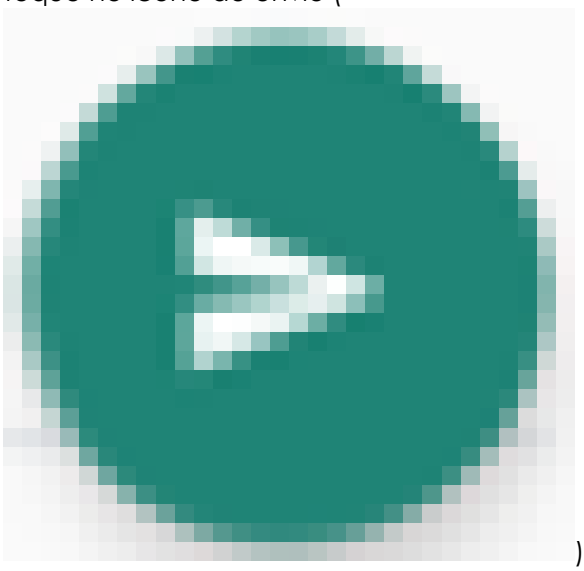
6. Na tela Atribuir tarefa de resposta a outro que é exibida, toque em um campo para expandi-lo e selecione outro grupo ou usuário para a tarefa.
7. Toque no ícone de envio ( ) ou em **Enviar** para salvar suas mudanças e atualizar a tarefa de resposta.
   Uma mensagem é exibida confirmando que o registro foi atualizado. A tarefa foi atribuída a um novo usuário no incidente de segurança primário e sua instância Now Platform foi atualizada.
8. Para exibir os detalhes de uma tarefa de resposta em aberto e as anotações de trabalho, com a tela Minhas tarefas de resposta exibida, toque em um registro na lista.
9. Com os campos na tarefa de resposta exibidos, escolha um na tabela a seguir para continuar.



Opção	Descrição
Guia de detalhes	Com a guia Detalhes selecionada, revise os campos na tarefa de resposta. Para editar campos ou reatribuir a tarefa, toque no ícone de menu (

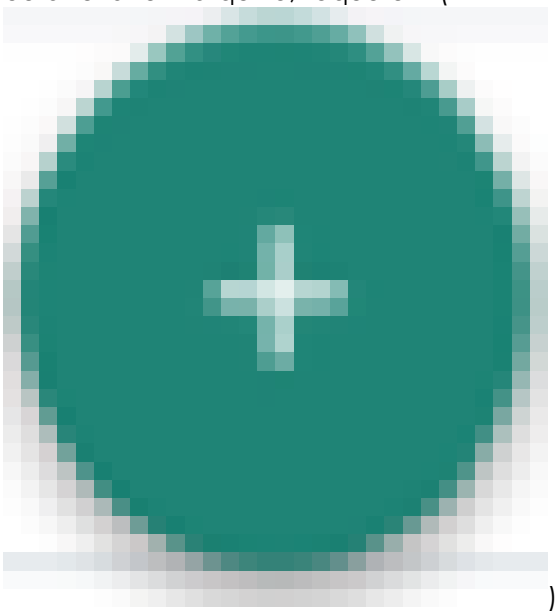
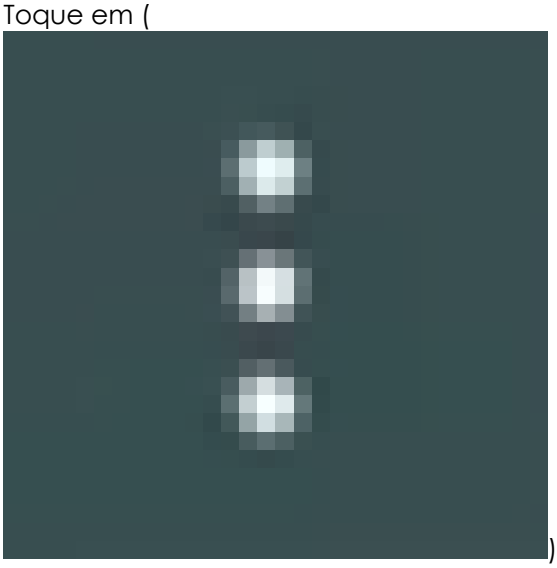
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	). No menu exibido, escolha uma das seguintes opções. ◦ Toque em **Editar**. Com a tela Editar tarefa de resposta exibida, toque em um campo para expandi-lo e escolha uma ou mais das opções exibidas. Como alternativa, toque no ícone de pesquisa e insira o texto. ◦ Para reatribuir a tarefa, toque **em Atribuir a outro**. Depois de concluir as edições, toque no ícone de envio () ou em **Enviar** para salvar suas mudanças e atualizar o registro. A tarefa de resposta a incidentes de segurança no incidente de segurança primário em sua instância Now Platform foi atualizada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Guia Fluxo de atividades	Com a guia Fluxo de atividades selecionada, escolha uma para continuar. ◦ Exiba a trilha de auditoria criada pelas Anotações de trabalho no registro da tarefa. Para adicionar uma anotação de trabalho ou anexar um arquivo, toque em (). ◦ Toque em () para editar ou reatribuir a tarefa.
Toque em um ícone de tela na parte inferior da tela.	Na parte inferior da tela, escolha um para continuar. ◦ Se exibido, toque em outro ícone para abrir outra aplicação principal ServiceNow® para abri-la. ◦ Toque em **Notificação** para exibir notificações de incidentes de segurança críti-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	cos atribuídos a você ou ao seu grupo de atribuição. ◦ Toque em **Configurações** e escolha uma para continuar. ▪ Exibir informações sobre a instância Now Platform. ▪ Faça logout da instância atual. Para fazer logout de uma instância Now Platform no seu dispositivo, com a página de detalhes exibida, toque em **Logout**.

Filtrar registros com o Aplicativo Security Incident Response Mobile

Defina filtros adicionais para limitar o número de registros exibidos em uma tela. A filtragem de registros no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 minutos.

Procedimento

1. Para refinar ainda mais os resultados da pesquisa ou para inserir critérios de filtro adicionais em qualquer lista de registros exibida, toque no ícone de filtro (ícone de).
2. Com a tela Filtros exibida, toque em um campo para expandi-lo.
3. Nas opções exibidas, toque na caixa de seleção ou toque em um item para o filtro.
   Para muitos dos filtros, você pode selecionar mais de uma opção.
4. Toque na seta) ou em **CONCLUÍDO** para salvar suas mudanças em um campo.
   Os critérios escolhidos são exibidos na tela Filtros. O número de registros que correspondem aos seus critérios também é exibido na parte superior da tela. Toque em **REDEFINIR** para remover todos os filtros e restaurar a configuração padrão.
5. Opcional: Repita as etapas 1 a 4 com a tela Filtros exibida para continuar definindo seus critérios de filtro.
6. Toque no ícone de interseção ícone para criar condições E.
   Como alternativa, toque no ícone de interseção Ícone para criar condições OR.
7. Depois de adicionar todos os critérios desejados, com a tela Filtros exibida, toque em **CONCLUÍDO**.
   Na tela, somente os registros que correspondem aos critérios de filtro são exibidos.

Orquestração do Security Incident Response

Orquestração do Security Incident Response As atividades permitem que os usuários interajam e recuperem dados de sistemas e ambientes baseados no Windows ou UNIX usando a orquestração de fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar Orquestração do Security Incident Response.

Antes de usar Orquestração do Security Incident Response, execute as etapas para configurar várias partes do sistema, incluindo o preenchimento do CMDB, a configuração do mid-server e a configuração de credenciais.

Antes de Iniciar

Função necessária: administrador
Para usar Security Incident Response, você precisa de um CMDB totalmente preenchido com nomes de domínio. Para obter mais informações, consulte Descoberta .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Ative o plug-in Security Incident Response.
2. Configurando MID Servers .
3. Configure as credenciais de serviço do Windows MID Server .

Entenda os fluxos de trabalho e os modelos de fluxo de trabalho da Orquestração de resposta a incidentes de segurança

O sistema base Security Incident Response inclui uma série de fluxos de trabalho e modelos de fluxo de trabalho projetados para funcionar com registros de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa

Você pode personalizar todos os fluxos de trabalho e modelos de fluxo de trabalho para melhor atender às suas necessidades, desde que tenha a função apropriada: sn_sec_cmn.admin. Fluxos de trabalho são usados em todo o sistema Operações de segurança para executar uma variedade de tarefas.
Os modelos de fluxo de trabalho, no entanto, são acionados ao selecionar um valor no campo **Categoria** em um incidente de segurança. Quando isso ocorre, o modelo de fluxo de trabalho associado à seleção inicia um modelo de fluxo de trabalho que instrui os analistas de segurança a lidar com um tipo específico de ameaça.

Por exemplo, se você selecionar **Negação de serviço** no campo **Categoria** em um incidente de segurança, o **Incidente de segurança - Negação de serviço - Modelo** será executado e o analista será direcionado para determinar se o destino do DOS é crítico para os negócios. Em caso afirmativo, a próxima tarefa faz com que a prioridade do incidente de segurança seja definida como **1 - Crítico**e, em seguida, executa a próxima tarefa. E assim por diante.

Portanto, Security Incident Response fluxos de trabalho e modelos de fluxo de trabalho são essencialmente os mesmos, exceto que os modelos são usados para um conjunto específico de funções em um incidente de segurança.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Fluxos de trabalho** > **Exibir Fluxos de Trabalho de Segurança**.
2. Uma lista dos fluxos de trabalho e modelos de fluxo de trabalho enviados no sistema de base é exibida.
   Todos os novos fluxos de trabalho que você criou no pacote de aplicações Operações de segurança também são incluídos na lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique no nome do fluxo de trabalho ou do modelo de fluxo de trabalho que você deseja exibir.

> **Nota:** Os fluxos de trabalho podem ser acionados de várias maneiras diferentes. Esteja ciente de que a associação de um fluxo de trabalho a um gatilho de fluxo de trabalho não significa necessariamente que o fluxo de trabalho está ativo.

Orquestração do Security Incident Response fluxos de trabalho e atividades

Vários fluxos de trabalho e atividades estão incluídos no Orquestração do Security Incident Response.

Somente usuários com a função sn_sec_cmn.admin podem Editor de fluxo de trabalho .

Criar solicitação de pesquisa para fluxo de trabalho de mudanças de IoC

O fluxo **Security Incident Response - Criar solicitação de pesquisa para mudanças de IoC** é acionado por uma regra de negócio para ser executado automaticamente quando um IoC é adicionado ou alterado. As verificações de malware são acionadas somente quando novos dados são inseridos e somente os novos dados são verificados.

Antes de Iniciar

Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa

Se o IoC estiver vazio, o fluxo de trabalho não será executado. As verificações históricas são retidas e podem ser vistas na guia **Solicitações de verificação de segurança** e nas anotações de trabalho do incidente de segurança. Os incidentes de segurança existentes são atualizados automaticamente.

> **Importante:**
>
> O fluxo de trabalho **Security Incident Response - Criar solicitação de pesquisa para mudanças de IoC** é migrado para o Flow Designer. O fluxo é acionado somente quando o sn_ti_scanner tem pelo menos um registro.

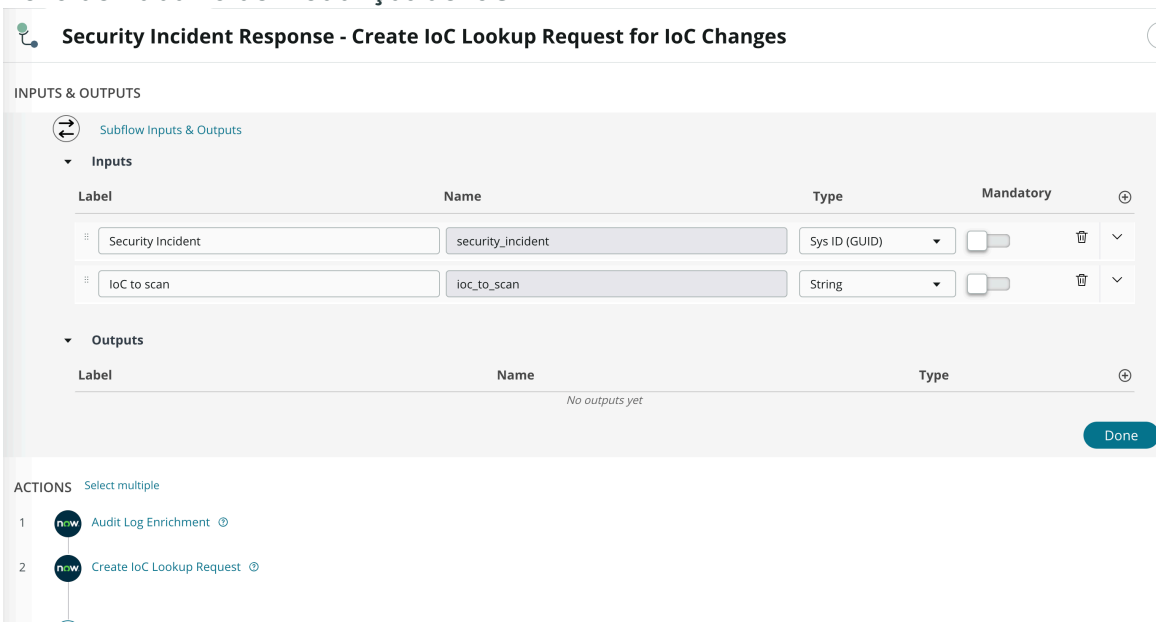
As ações do Flow Designer incluem:

- Aprimoramento do log de auditoria
- Atividade Criar solicitação de pesquisa de IoC

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de mudanças de IoC



Atividade Criar solicitação de pesquisa de IoC

A atividade **Criar solicitação de pesquisa de IoC** pode ser usada com qualquer fluxo de trabalho para criar uma solicitação de pesquisa de malware para campos de IoC adicionados ou modificados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Solicitação de pesquisa criada.
Falha	Solicitação de pesquisa não criada.

Variáveis de entrada

Variável	Descrição
IocString	Informações de IoC no formato JSON. IP, hash, URL.
sild	Identificador do sistema de incidentes de segurança

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
scnReqID	Identificador de solicitação de pesquisa

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho do Security Incident Response - Obter estatísticas de rede

O **Resposta a incidentes de segurança** > **Obter estatísticas de rede** O fluxo de trabalho recupera as estatísticas de rede de um recurso baseado no Windows afetado quando adicionado a um incidente de segurança no estado **Análise**.

Antes de Iniciar

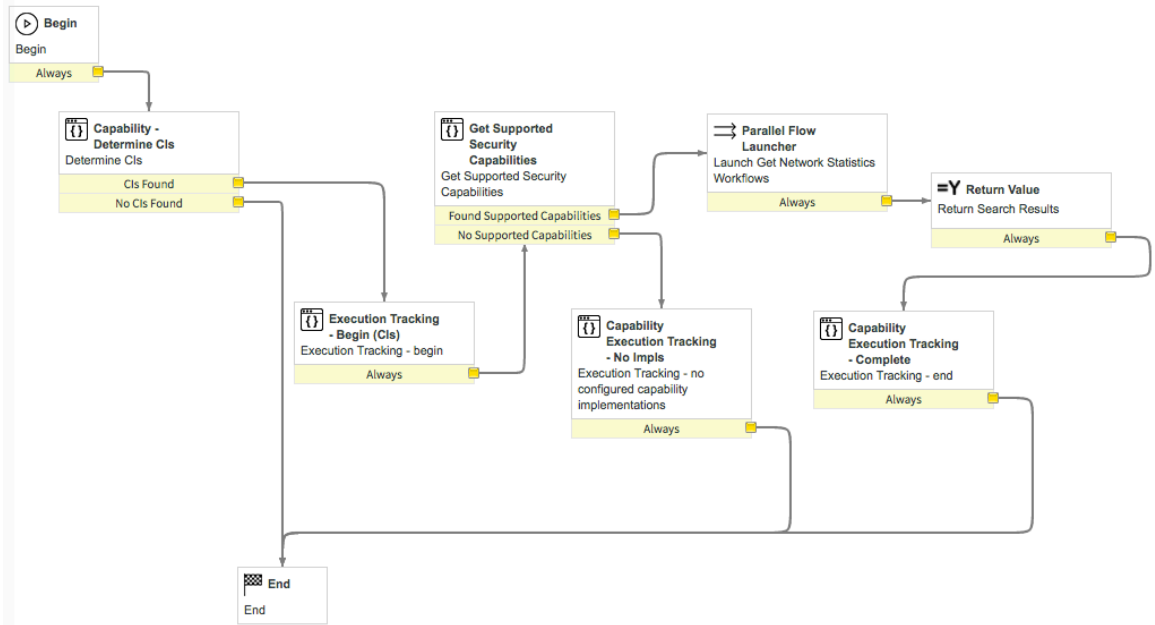
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Para novos incidentes de segurança que contêm itens de configuração, o fluxo de trabalho é executado automaticamente quando o estado muda para **Análise**.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

Obter estatísticas de rede



As atividades do processo de fluxo de trabalho incluem:

- Atividade Obter FQDN do item de configuração
- Determinar script de shell por sistema operacional
- Se a instrução for executada pelo PowerShell
- Acompanhamento de execução - Iniciar atividade
- Obter estatísticas de rede por meio da atividade netstat
- Acompanhamento da execução da capacidade - Atividade com falha
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento da execução da capacidade - Atividade com falha - Retorna o ID de aprimoramento.
- Acompanhamento da execução da capacidade - Concluir atividade

Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adicione um item de configuração (computador, servidor ou semelhante).
4. Clique em **Atualizar**.
   Orquestração do Security Incident Response fornece informações de estatísticas de rede no **Links relacionados** > **Aprimoramentos de incidentes de segurança** guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

   As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Fluxo de trabalho do Security Incident Response - Obter serviços em execução

O **fluxo de trabalho Resposta a incidentes de segurança - Obter serviços em execução** recupera uma lista de serviços em execução de itens de configuração (ICs) baseados no Windows, ServiceNow. Este fluxo de trabalho é usado para enriquecimento de incidentes durante as investigações.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
O **fluxo de trabalho do Security Incident Response - Obter serviços em execução** é executado automaticamente quando você adiciona um novo item de configuração a um incidente de segurança do Windows depois que o estado muda para **Análise**. As informações que este fluxo de trabalho obtém são exibidas nas guias **Mostrar dados** de aprimoramento do incidente de segurança.

Nota: Se o incidente de segurança permanecer no estado **Rascunho**, o **fluxo de trabalho Resposta a incidentes de segurança - Obter serviços em execução** não será executado.

As atividades de fluxo de trabalho incluem:

Atividade Script de aprimoramento de logs de auditoria

Atividade Obter FQDN do item de configuração

Determinar script de shell por atividade do SO

É uma atividade de execução via PowerShell

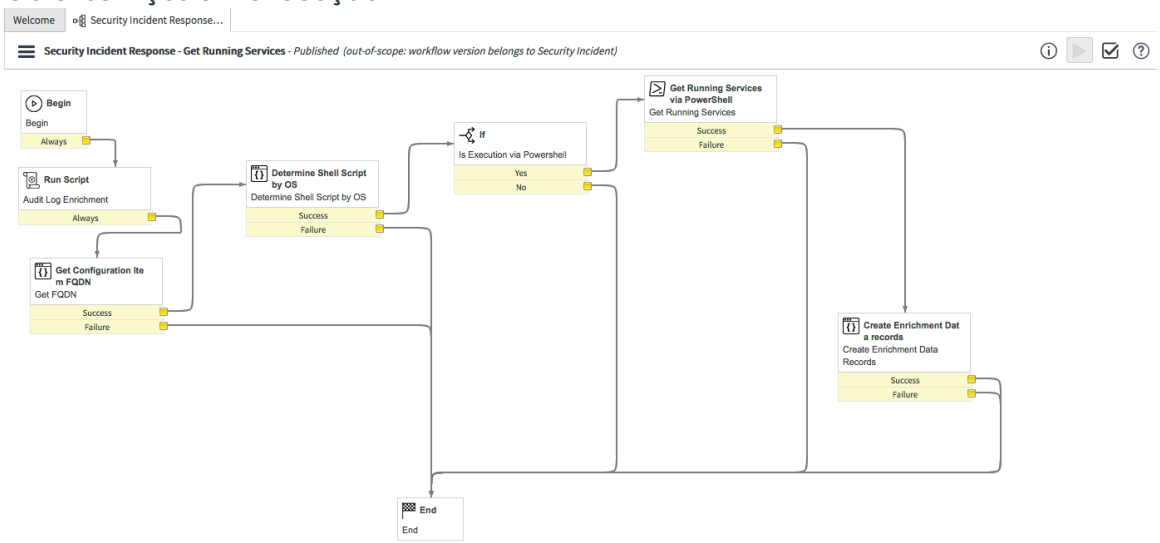
Obter serviços em execução - Atividade de aprimoramento de WMI

Atividade Criar registros de dados de aprimoramento

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter serviços em execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração baseado no Windows (servidor, laptop ou semelhante).
4. Clique em **Atualizar**.
   Security Incident Response fornece informações de serviços em execução no **Links relacionados** > **Aprimoramentos de incidentes de segurança**guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

Determinar script de shell por atividade do SO

A atividade de fluxo de trabalho Determinar Shell Script por SO determina qual sistema operacional será usado no fluxo de trabalho

A atividade Determinar Script de Shell por SO pode ser usada com qualquer fluxo de trabalho para determinar qual script de shell executar com base no sistema operacional em execução no sistema que contém o item de configuração.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sistema operacional encontrado.
Falha	Nenhum sistema operacional encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
ciSysId	Identificador do sistema do item de configuração.
processType	Identificador interno que define qual script extrair da tabela.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
processScript	Agente de ECC que reúne o processo em execução.
execuçãoTemplate	Determina se o script é executado por meio de uma probe ou usando o PowerShell.
richmentMappingId	Identificador do sistema do mapeamento de aprimoramento usado para transformar os dados de resposta.

Obter serviços em execução - Aprimoramento de WMI

O fluxo de trabalho **Resposta a incidentes de segurança - Obter** serviços em execução reúne serviços em execução em um item de configuração adicionado a um incidente de segurança.

A atividade **Obter serviços em execução - Aprimoramento de WMI** é iniciada automaticamente para recuperar informações de serviços em execução para um host do Windows.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome do domínio totalmente qualificado (FQDN) do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os serviços em execução no sistema de destino. Os dados JSON incluem: nome

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
	O nome do serviço PID O identificador de processo do serviço em execução service_type (Opcional) O tipo de serviço em execução. nome_início O nome do sistema para o serviço caminho O caminho do arquivo do executável do serviço em execução modo_início O modo de início do serviço em execução. display_name O nome do serviço em execução como ele aparece para o usuário

Restrições

O MID Server deve oferecer suporte ao **PowerShell**.

O hash SHA-256 requer o PowerShell V4.

Executar fluxo de trabalho de procdump

O fluxo de trabalho **Executar procdump** executa um despejo de processo em um processo especificado e o salva em um arquivo que pode ser direcionado por analistas de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

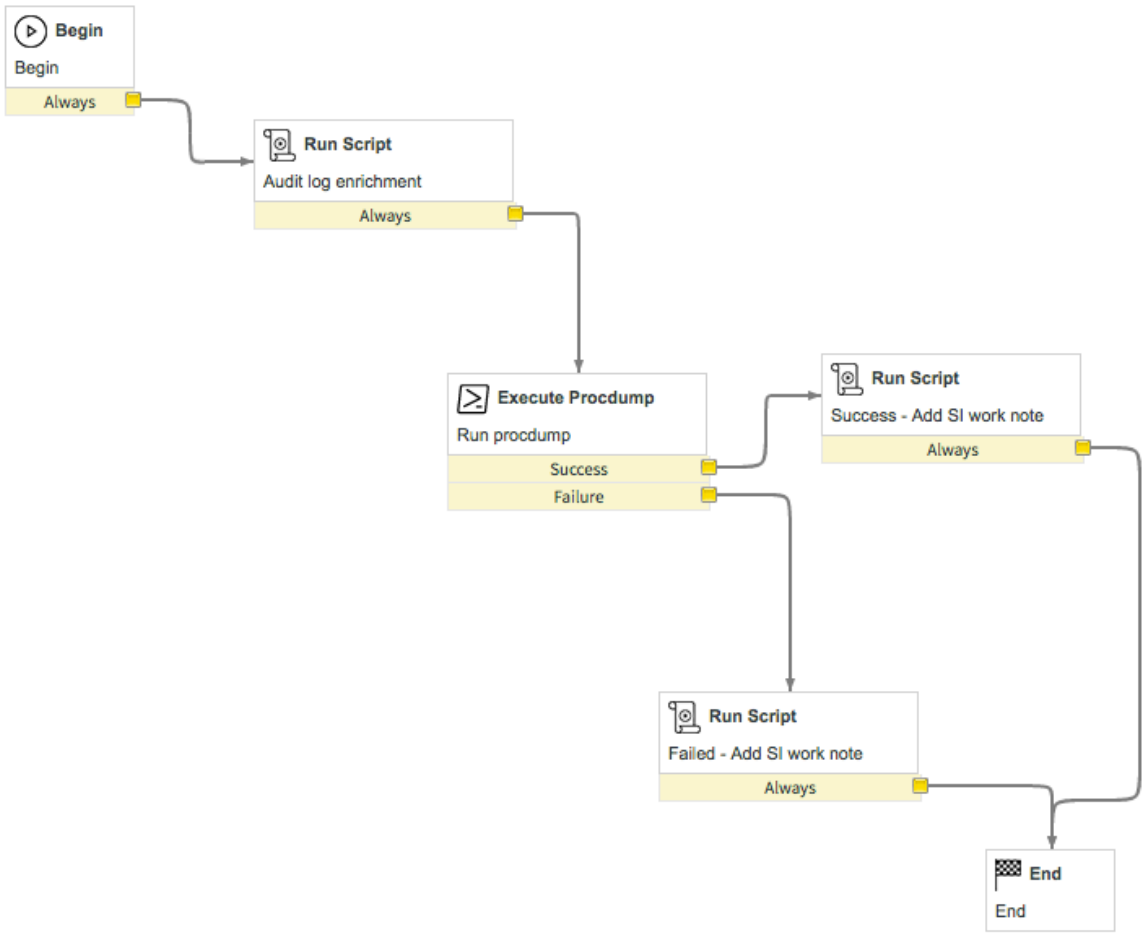
Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado quando processos aprimorados são selecionados e uma ação de IU **Executar procdump** é executada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar procdump



Tradução automática

As atividades do processo de fluxo de trabalho incluem:

- Executar script (enriquecimento de log de auditoria): executa um script para adicionar um log de auditoria ao incidente de segurança.
- Executar atividade de procdump
- Executar script (Êxito – Adicionar anotação de trabalho de SI): executa um script para adicionar uma anotação de trabalho quando o procdump é bem-sucedido.
- Executar script (falha - Adicionar anotação de trabalho de SI): executa um script para adicionar uma anotação de trabalho quando o procdump falha. Os motivos pelos quais o procdump pode falhar incluem:
  - Caminho de despejo inválido
  - Caminho de compartilhamento de arquivo inválido
  - Não é possível obter o nome de domínio totalmente qualificado da máquina Windows em que o procdump está sendo executado
  - O nome do processo não está especificado
  - A variável de ambiente PROCDUMP não foi encontrada
  - Uma cópia do arquivo de despejo falha ao copiar do caminho de despejo para o caminho de compartilhamento de arquivo

Executar atividade de procdump

Executar procdump é uma atividade do PowerShell que executa o procdump nos processos selecionados, descarrega os dados em um arquivo e os publica em um site compartilhado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em uma rede interna. Um analista pode exibir um processo da lista de proibições, realçado em vermelho em um incidente de segurança, e executar análises adicionais no arquivo.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O procdump foi executado com sucesso no process_name e os detalhes estão disponíveis em activityOutput.response.
Falha	Falha ao executar o procdump em process_name e os detalhes estão disponíveis em activityOutput.response.

Variáveis de entrada

Variáveis de entrada são usadas para criar as saídas solicitadas.

Variáveis de entrada

Variável	Descrição
targetId	[Obrigatório] O ID de destino no qual executar o procdump.
process_name	[Obrigatório] O nome do processo para o procdump.
despejo_caminho	[Obrigatório] O caminho do arquivo local no qual o arquivo de despejo gerado será salvo.
despejo_nome_do_arquivo	[Obrigatório] O nome do arquivo gerado pelo procdump. Todos os caracteres especiais serão substituídos por hífens (-) do nome do arquivo de despejo quando o arquivo for gerado.
caminho_compartilhado_arquivo	[Obrigatório] O caminho de compartilhamento do arquivo para o qual o arquivo de despejo será copiado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
share_path	O caminho de compartilhamento de arquivo para o qual o arquivo de despejo foi copiado.
resposta	Uma representação JSON do resultado do procdump.
resultado	O resultado do procdump.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança - Avaliar fluxo de trabalho do resultado da tarefa de resposta

O fluxo de trabalho de resultado da tarefa Incidente de segurança - Avaliar resposta determina a tarefa a ser usada, invoca um fluxo de trabalho escolhido e um script de avaliação com base no registro do avaliador de resultados fornecido como entrada para o fluxo de trabalho escolhido.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho deve ser executado ao mesmo tempo que a atividade de criação de tarefa a ser avaliada. O script de avaliação consulta os artefatos (como registros de pesquisa de detecções ou processos em execução) da capacidade configurada usando informações de contexto da tarefa de resposta (como o incidente de segurança primário) para determinar o resultado apropriado para a tarefa de resposta. O resultado pode ser dependente da atividade de fluxo de trabalho, mas geralmente é **sim** ou **não**. Ao criar um avaliador de resultados, somente as capacidades que têm um fluxo de trabalho configurado, com a caixa **Capacidade baseada em tarefa** marcada e um conjunto de variáveis de entrada de tarefa estão disponíveis para seleção.

As atividades do processo de fluxo de trabalho incluem:

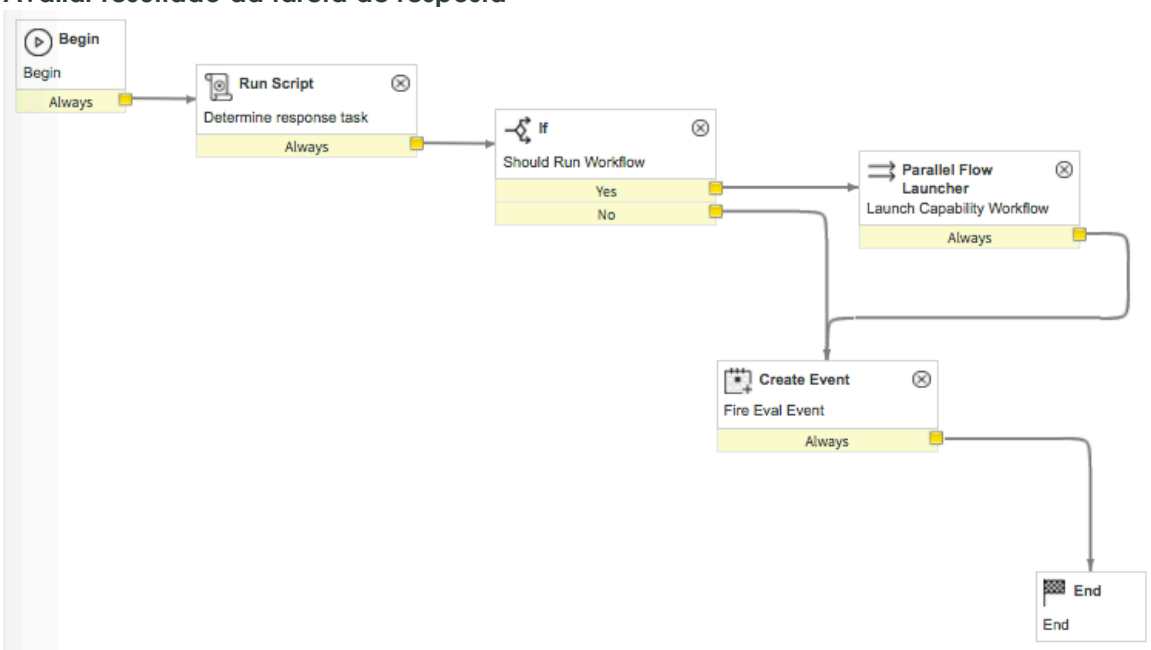
Executar script para determinar a tarefa de resposta

Deve executar fluxo de trabalho

Fluxo de trabalho da capacidade de inicialização do inicializador de fluxo paralelo

Criar evento de avaliação

Avaliar resultado da tarefa de resposta



Modelos de fluxo de trabalho do Security Incident Response

Os modelos de fluxo de trabalho são fornecidos com Orquestração do Security Incident Response para permitir que você execute procedimentos básicos de análise relacionados a operações de segurança. Os modelos podem ser usados como estão ou você pode personalizá-los para criar fluxos de trabalho que atendam melhor às suas necessidades específicas. Os modelos de fluxo de trabalho são desativados por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Somente usuários com a função sn_sec_cmn.admin podem usar o Editor de fluxo de trabalho.

Modelo de fluxo de trabalho de Exposição de dados confidenciais de incidente de segurança

O modelo Incidente de segurança - Exposição de dados confidenciais - permite que você execute uma série de tarefas projetadas para lidar com a exposição de dados confidenciais.

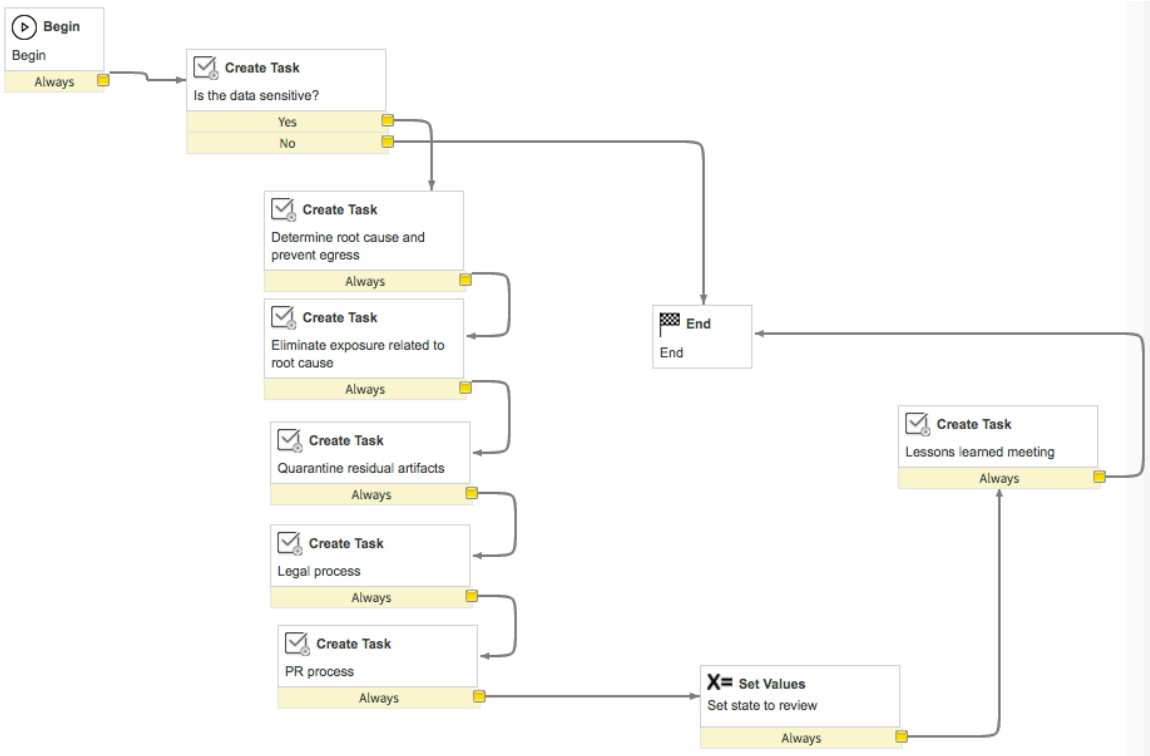
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida ou alterada para **Exposição de dados de identidade pessoal confidencial**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Exposição de dados de identidade pessoal confidencial



Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com a exposição a dados confidenciais ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Exposição de dados de identidade pessoal confidencial**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de exposição de dados confidenciais

Tarefa de resposta	Descrição	Resultados
Os dados são confidenciais?	Determine se os dados associados a este incidente de segurança são confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionou **Sim**, a próxima tarefa de resposta será executada. Se você selecionou **Não**, o fluxo será encerrado.
Determinar a causa raiz e impedir a saída	Determine a causa raiz do ataque e adicione a filtragem de saída para interromper a exfiltração, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Eliminar exposição relacionada à causa raiz	Com base na causa raiz, execute as etapas para eliminar a exposição, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Colocar artefatos residuais em quarentena	Execute as etapas para colocar em quarentena quaisquer artefatos residuais, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Processo jurídico	Execute as etapas para atender aos requisitos jurídicos desta análise, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Processo de RC	Execute as etapas para atender aos requisitos de RC desta análise, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado nesses dados confidenciais, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o incidente de segurança permanecerá no estado **Revisão** até que você o feche.

Tradução automática

Modelo de fluxo de trabalho de negação de serviço de incidente de segurança

O modelo Incidente de segurança - Negação de serviço - permite que você execute uma série de tarefas projetadas para lidar com ataques de negação de serviço (DOS).

Antes de Iniciar

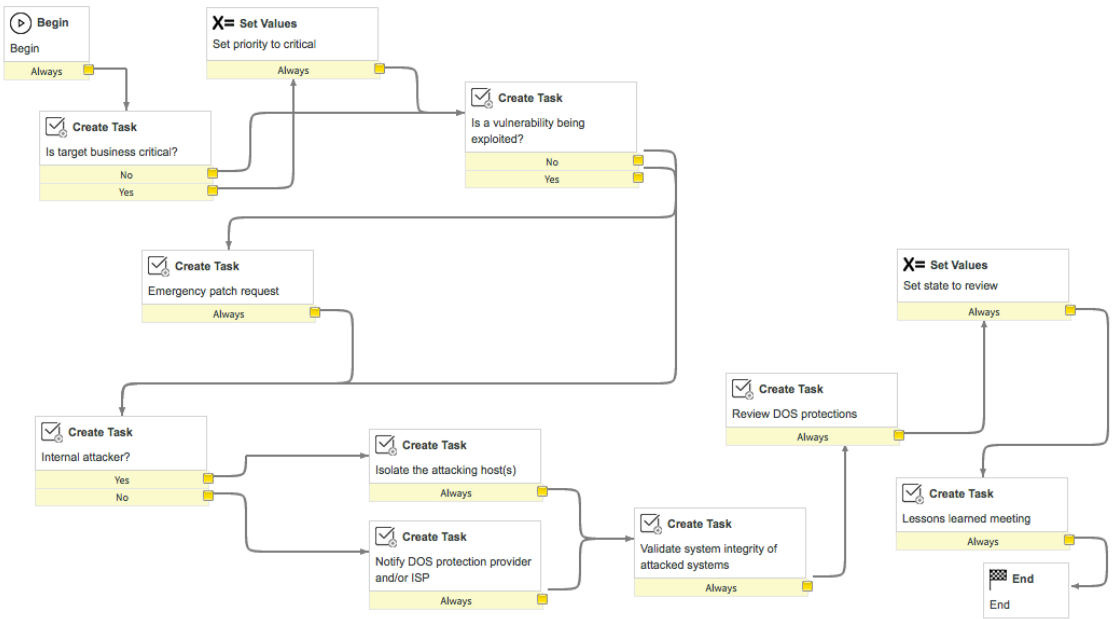
Função necessária: sn_si.write

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Negação de serviço**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Negação de serviço (DOS)



Procedimento

1. Abra o incidente de segurança para esta ocorrência de negação de serviço ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Negação de serviço**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de negação de serviço

Tarefa de resposta	Ação	Resultados
A meta é crítica para os negócios?	Determine se o alvo deste ataque do DOS é crítico para os negócios. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Definir prioridade para crítica** será executada. Se você selecionar **Não**, **uma vulnerabilidade está sendo explorada?** tarefa foi executada.
Definir prioridade como crítica	Nenhuma ação necessária.	A **Prioridade** do incidente de segurança é alterada automaticamente para **Crítica**e a **resposta Uma**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
		vulnerabilidade está sendo explorada? tarefa foi executada.
Há uma vulnerabilidade sendo explorada?	Determine se este ataque do DOS explora uma vulnerabilidade de software. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **de solicitação de patch emergencial** será executada. Se você selecionar **Não**, o **invasor interno?** tarefa foi executada.
Solicitação de patch emergencial	Emita uma solicitação de patch de emergência para os sistemas que estão sendo atacados. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Invasor interno?	Determine se a origem deste ataque do DOS é interna à sua organização. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Isolar host(es) de ataque** será executada. Se você selecionar **Não**, a tarefa do **provedor de proteção e/ou ISP do Notify** será executada.
Isolar o(s) host(s) de ataque	Execute as etapas necessárias para isolar os hosts internos responsáveis pelo ataque. Atualize o campo **Estado** na tarefa conforme apropriado.	Depois de concluir esta etapa, a tarefa **Validar integridade do sistema dos sistemas atacados** será executada.
Notificar o provedor de proteção do DOS e/ou ISP	Execute as etapas necessárias para entrar em contato com o provedor de proteção contra negação de serviço e/ou com o provedor de serviços de internet para notificá-los sobre o ataque. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Validar a integridade do sistema dos sistemas atacados	Execute as etapas necessárias para avaliar e validar a integridade dos computadores atacados. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Revisar proteções do DOS	Realize uma revisão das proteções e procedimentos existentes do DOS. Faça as alterações necessárias.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	Atualize o campo **Estado** na tarefa conforme apropriado.	próxima tarefa de resposta será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**. A tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de negação de serviço. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o fluxo será encerrado.

Modelo de fluxo de trabalho de equipamento perdido de incidente de segurança

O modelo Incidente de segurança - Equipamento perdido - permite que você execute uma série de tarefas projetadas para lidar com equipamentos perdidos.

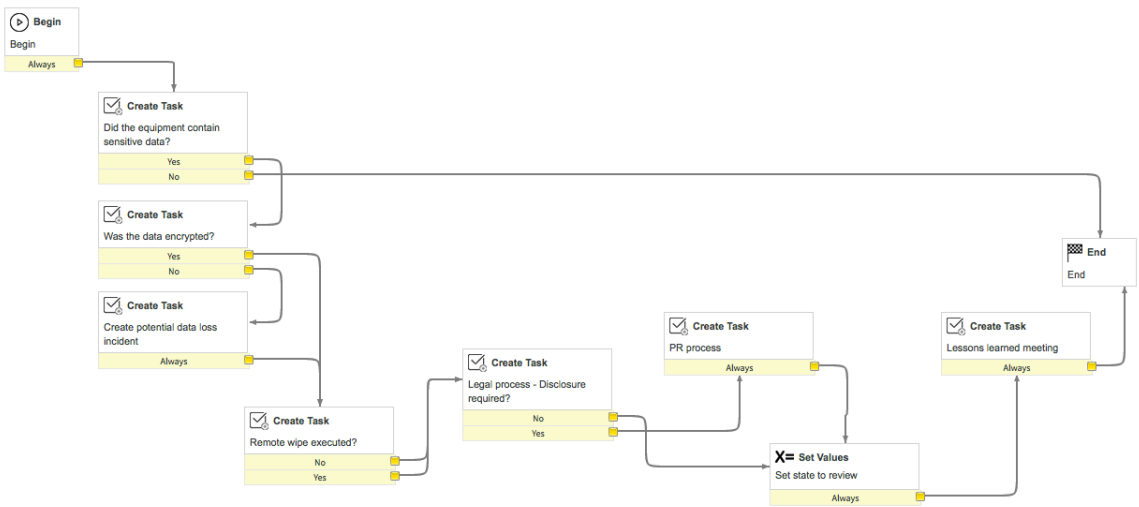
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Perda de equipamento**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Perda de equipamento



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança referente à perda de equipamento ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Perda de equipamento**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de equipamento perdido

Tarefa de resposta	Ação	Resultados
O equipamento continha dados confidenciais?	Determine se o equipamento associado a este incidente de segurança continha informações confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	Se você selecionar **Sim**, a **mensagem Os dados foram criptografados?** tarefa foi executada. Se você selecionar **Não**, o fluxo será encerrado.
Os dados foram criptografados?	Determine se os dados confidenciais no dispositivo perdido foram criptografados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	Se você selecionar **Sim**, o **apagamento remoto criado?** tarefa de resposta foi executada. Se você selecionar **Não**, a tarefa **Criar possível resposta a incidentes com perda de dados**será executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um possível incidente de perda de dados. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A **limpeza remota foi criada?** tarefa de resposta foi executada.
Apagamento remoto criado?	Execute as etapas necessárias para executar um apagamento remoto do equipamento perdido. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	A tarefa **Processo jurídico - divulgação necessária** é executada.
Processo jurídico - divulgação necessária?	Execute as etapas para atender aos requisitos jurídicos desta análise. Selecione **Sim** se uma divulgação jurídica for necessária ou **Não**se não for.	A tarefa de **reunião de Lições aprendidas** é executada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Processo de RC	Execute as etapas necessárias para atender aos requisitos de RC desta análise. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa **Definir estado para revisão** é executada.
Definir estado como revisão	Nenhuma ação é necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de perda de equipamento. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	O fluxo termina.

Modelo de fluxo de trabalho de software malicioso de incidente de segurança

O modelo Incidente de segurança - Software malicioso - permite que você execute uma série de tarefas projetadas para lidar com software malicioso em sua rede.

Antes de Iniciar

Função necessária: sn_si.write

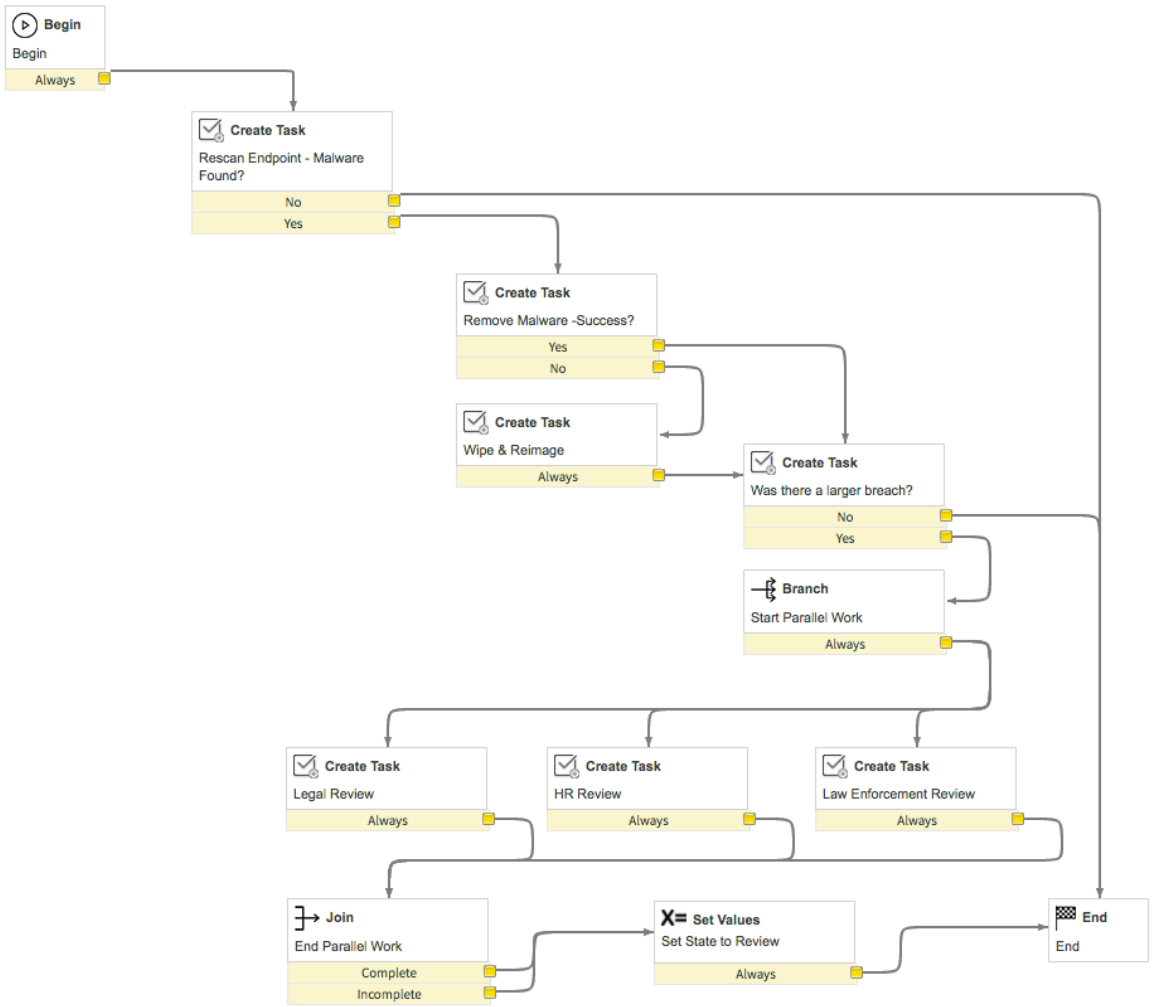
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Software mal**-intencionado. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Software malicioso



Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Atividade de código malicioso**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de software malicioso

Tarefa de resposta	Ação	Resultados
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se foi encontrado malware. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Remover malware - Sucesso?** tarefa foi executada. Se você selecionar **Não**, o fluxo será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Remover malware - sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, **Ocorreu uma violação maior?** tarefa foi executada. Se você selecionar **Não**, a tarefa **Limpar e recriar imagem** será executada.
Limpar e recriar imagem	Se você não removeu com sucesso o malware encontrado, esta tarefa instrui você a executar uma limpeza e recriação de imagem nos computadores infectados com o malware.	Depois que a tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Houve uma violação maior?	Determine se a violação causada pelo software mal-intencionado é maior do que se acredita. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas serão executadas em paralelo: ◦ Revisão jurídica ◦ Revisão de RH ◦ Revisão da aplicação da lei Se você selecionar **Não**, o fluxo será encerrado.
Revisão jurídica Revisão de RH Revisão da aplicação da lei	Execute as etapas necessárias para que cada um desses departamentos revise o processo que você seguiu para erradicar o software mal-intencionado.	Quando as tarefas são concluídas, a tarefa **Definir estado para revisão** é executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e o fluxo termina.

Tradução automática

Modelo de fluxo de trabalho de phishing de incidente de segurança

O modelo Incidente de segurança - Phishing - permite que você execute uma série de tarefas projetadas para lidar com e-mails de Spear Phishing em sua rede.

Antes de Iniciar

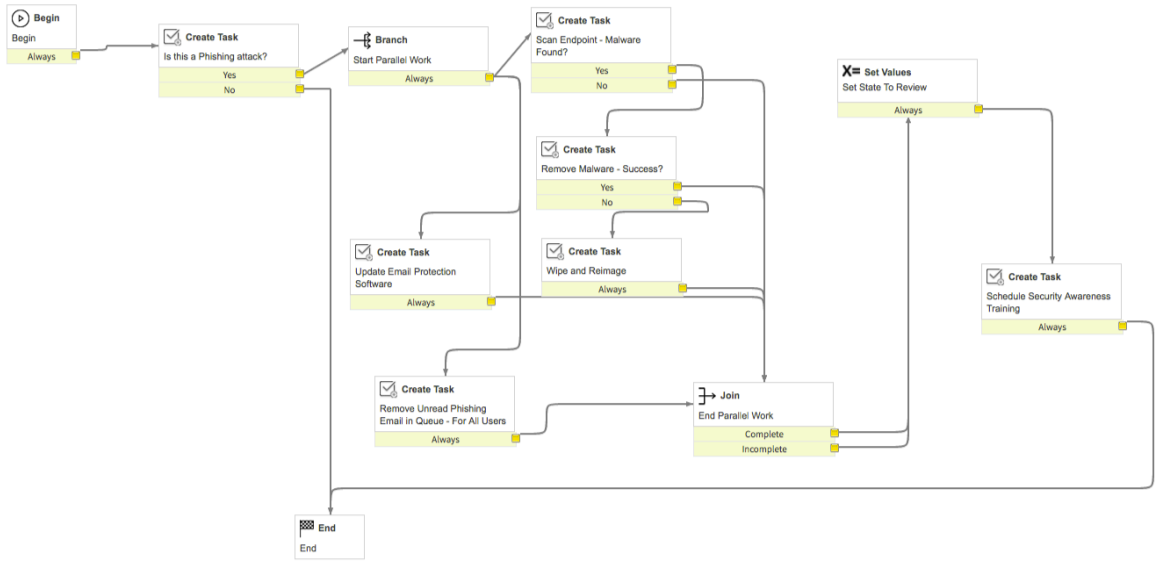
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Spear Phishing**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Spear Phishing



Procedimento

1. Abra o incidente de segurança para este possível ataque de Spear Phishing ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Spear Phishing**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de Spear Phishing

Tarefa de resposta	Ação	Resultados
É um ataque de phishing?	Determine se este é um ataque de phishing. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas serão executadas em paralelo: ◦ Endpoint de verificação - Malware encontrado? ◦ Atualizar software de proteção de e-mail ◦ Remover e-mail de phishing não lido da fila - para todos os usuários Se você selecionar **Não**, o fluxo será encerrado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se foi encontrado malware. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Remover malware - Sucesso?** tarefa foi executada. Se você selecionar **Não**, a tarefa **Definir estado para revisão** será executada.
Remover malware - sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Definir estado para revisão** será executada. Se você selecionar **Não**, a tarefa **Limpar e recriar imagem** será executada.
Limpar e recriar imagem	Se você não removeu com sucesso o malware encontrado, esta tarefa instrui você a executar uma limpeza e recriação de imagem nos computadores infectados com o malware.	Depois que a tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Atualizar software de proteção de e-mail	Se for determinado que este é um ataque de phishing, você será solicitado a atualizar o software de proteção de e-mail de acordo.	Quando a tarefa é concluída, a tarefa **Definir estado para revisão** é executada.
Remover e-mail de phishing não lido da fila - para todos os usuários	Execute as etapas necessárias para remover o e-mail de phishing que ainda está na fila para todos os usuários.	Quando a tarefa é concluída, a tarefa **Definir estado para revisão** é executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**. A tarefa **Programar treinamento de conscientização de segurança** é executada.
Programar treinamento de conscientização de segurança	Programe treinamento para aumentar a conscientização de segurança por parte de seus funcionários. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando a tarefa é concluída, o fluxo termina.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de fluxo de trabalho de violação da política de incidente de segurança

O modelo Incidente de segurança - Violação de política - permite que você execute uma série de tarefas projetadas para lidar com violações de política de segurança.

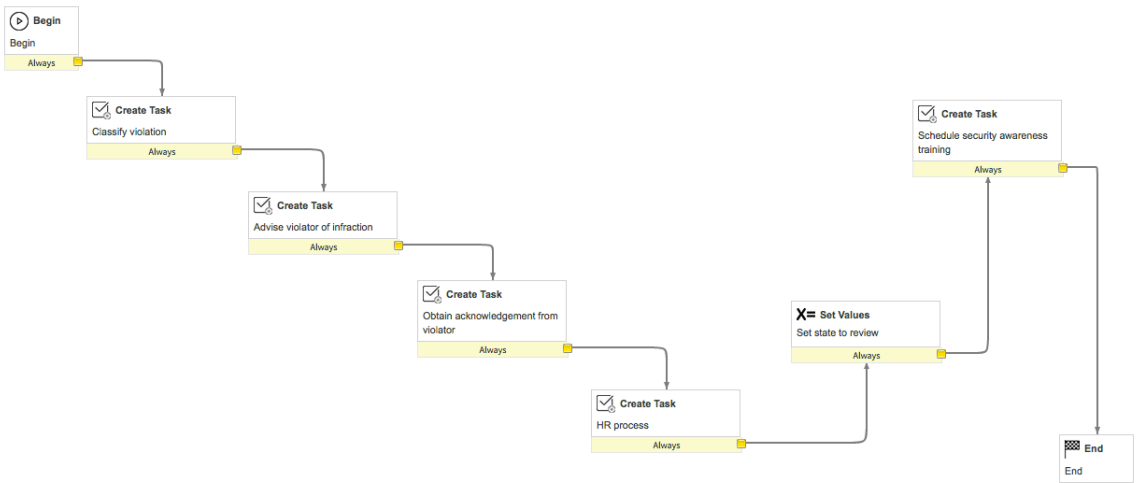
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Violação de política**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Violação de política



Procedimento

1. Abra o incidente de segurança referente à violação de política ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Violação de política**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de violação de política

Tarefa de resposta	Ação	Resultados
Classificar violação	Classifique como esta infração viola as políticas de segurança da sua organização. Atualize o campo **Estado** na tarefa depois de concluí-la.	A tarefa **Aconselhar infrator sobre resposta de infração** é executada.
Avisar infrator sobre infração	Comunique a natureza da infração ao violador.	A tarefa **Obter confirmação da resposta do violador** foi executada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	Atualize o campo **Estado** na tarefa depois de comunicá-la.	
Obter confirmação do violador	Obtenha uma confirmação do infrator da infração. Atualize o campo **Estado** na tarefa conforme apropriado.	A tarefa de resposta do **processo de RH** é executada.
Processo de RH	Comunique todas as informações necessárias sobre esta violação ao RH. Atualize o campo **Estado** na tarefa conforme apropriado.	A tarefa **Definir estado para revisar a** resposta é executada.
Definir estado como revisão	Nenhuma ação é necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**.
Programar treinamento de conscientização de segurança	Realize um treinamento de conscientização de segurança para instruir a equipe sobre como evitar violações de segurança semelhantes no futuro. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o fluxo será encerrado.

Modelo de fluxo de trabalho de reconhecimento de incidente de segurança

O reconhecimento geralmente é uma etapa preliminar em direção a um novo ataque que busca explorar um dispositivo ou sistema. O modelo Incidente de segurança - Reconhecimento - permite que você execute uma série de tarefas projetadas para lidar com o reconhecimento em sua rede.

Antes de Iniciar

Função necessária: sn_si.write

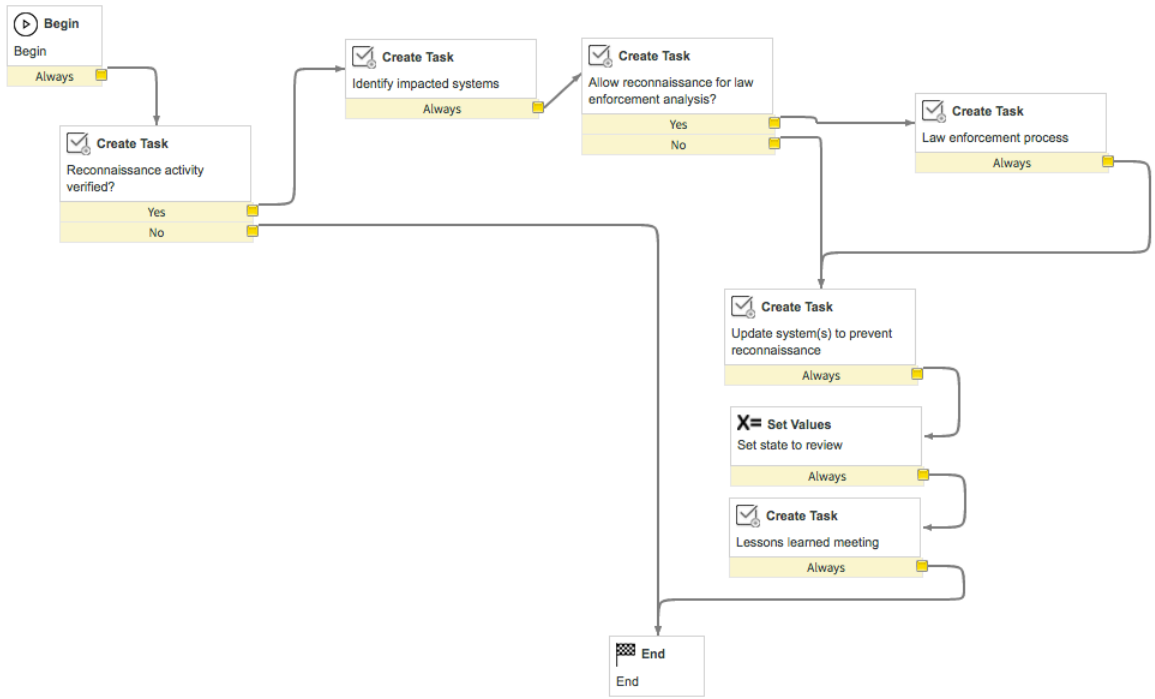
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como a **atividade de reconhecimento**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de reconhecimento



Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Atividade de reconhecimento**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de reconhecimento

Tarefa de resposta	Ação	Resultados
Atividade de reconhecimento verificada?	Determine se algum reconhecimento observado foi verificado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Identificar sistemas afetados** será executada. Se você selecionar **Não**, o fluxo será encerrado.
Identificar sistemas afetados	Determine os sistemas afetados pelo reconhecimento.	Quando esta tarefa estiver concluída, a **mensagem Permitir reconhecimento para análise de aplicação da lei?** tarefa foi executada.
Permitir reconhecimento para análise de aplicação da lei?	Determine se você deseja que o reconhecimento seja analisado por agências de segurança.	Se você selecionar **Sim**, a tarefa do **processo de aplicação da lei** será executada. Se você selecionar **Não**, a tarefa **de reconhecimento Atualizar**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	**sistema(s) para impedir** será executada.
Processo de aplicação da lei	Execute o processo de imposição da lei conforme definido pela sua empresa.	Quando esta tarefa for concluída, a tarefa **de reconhecimento Atualizar sistema(s) para impedir** será executada.
Atualizar sistema(s) para impedir reconhecimento	Execute as etapas necessárias para atualizar os sistemas afetados pelo reconhecimento.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**e a tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de reconhecimento. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando esta tarefa for concluída, o fluxo será encerrado.

Modelo de fluxo de trabalho de serviço ou servidor não autorizado de incidente de segurança

O Incidente de segurança - servidor ou serviço não autorizado - Modelo permite que você execute uma série de tarefas projetadas para lidar com atividades de servidores ou serviços não autorizados que afetam sua rede.

Antes de Iniciar

Função necessária: sn_si.write

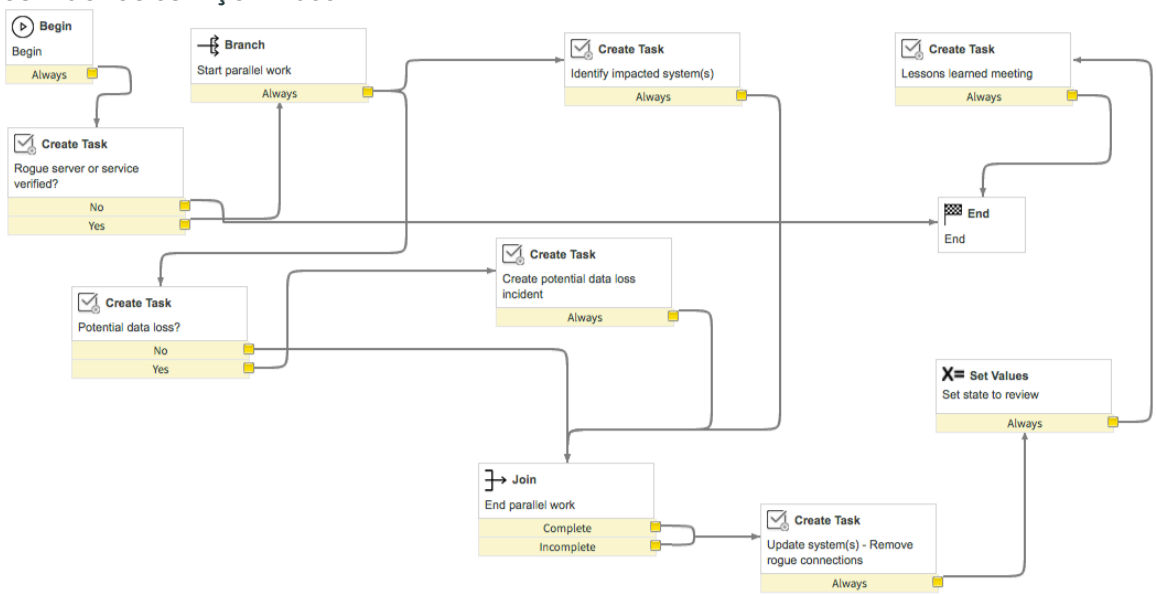
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Servidor ou serviço**não autorizado. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Servidor ou serviço invasor



Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Servidor não autorizado ou atividade de serviço**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no servidor não autorizado ou no modelo de serviço

Tarefa de resposta	Ação	Resultados
Servidor ou serviço não autorizado verificado?	Determine se uma conexão com um servidor ou serviço não autorizado foi verificada em sua rede. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as duas tarefas a seguir serão executadas em paralelo: ◦ **Identificar sistemas afetados** ◦ **Possível perda de dados?** Se você selecionar **Não**, o fluxo será encerrado.
Identificar sistemas afetados	Determine os sistemas afetados pelo contato com o servidor ou serviço não autorizado.	Quando esta tarefa for concluída, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Possível perda de dados?	Determine se a conexão com o servidor ou serviço não autorizado causou possível perda de dados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Criar possível incidente de perda de dados** será executada. Se você selecionar **Não**, a tarefa **Atualizar sistema(s) - Remover**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
		conexões não autorizadas será executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um incidente de segurança para a possível perda de dados.	Quando esta tarefa for concluída, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Atualizar sistema(s) - Remover conexões não autorizadas	Execute as etapas necessárias para remover as conexões não autorizadas.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**e a tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Conduza uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de serviço ou servidor não autorizado. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando esta tarefa for concluída, o fluxo será encerrado.

Modelo de fluxo de trabalho de spam de incidente de segurança

O Incidente de segurança - Spam - Modelo permite que você execute uma série de tarefas projetadas para lidar com spam de e-mail em sua rede.

Antes de Iniciar

Função necessária: sn_si.write

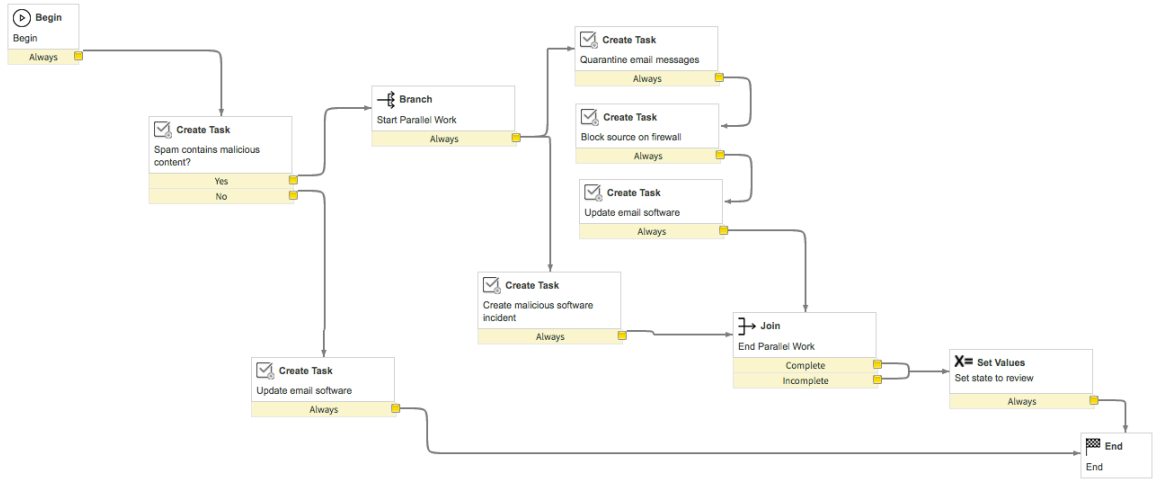
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida ou alterada para **Origem de spam**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem do spam



Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com spam de e-mail ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Origem do spam**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de spam

Tarefa de resposta	Ação	Resultados
O spam contém conteúdo malicioso?	Determine se o spam contém software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionou **Sim**, as seguintes tarefas de resposta serão executadas: ◦ **Mensagem de e-mail em quarentena** ◦ **Criar incidente de software mal-intencionado** Se você selecionou **Não**, a **atualização do software de e-mail** será executada.
Criar incidente de software mal-intencionado	Execute as etapas para criar um incidente de segurança, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, essa tarefa de resposta aguardará até que as próximas três tarefas de resposta sejam concluídas. O estado do incidente de segurança muda para **Revisão**.
Mensagem de e-mail em quarentena	Execute as etapas para colocar o spam em quarentena, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Bloquear origem no firewall	Execute as etapas para bloquear o endereço de e-mail no firewall, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Atualizar software de e-mail	Adicione o endereço de e-mail à sua lista de bloqueios, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada. **Nota:** Esta tarefa de resposta também será executada se você tiver respondido **Não** para a pergunta O **spam contém conteúdo mal-intencionado?** tarefa de resposta.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**.

Modelo de fluxo de trabalho de acesso não autorizado de incidente de segurança

O modelo Incidente de segurança - Acesso não autorizado - permite que você execute uma série de tarefas projetadas para lidar com o acesso não autorizado à sua rede.

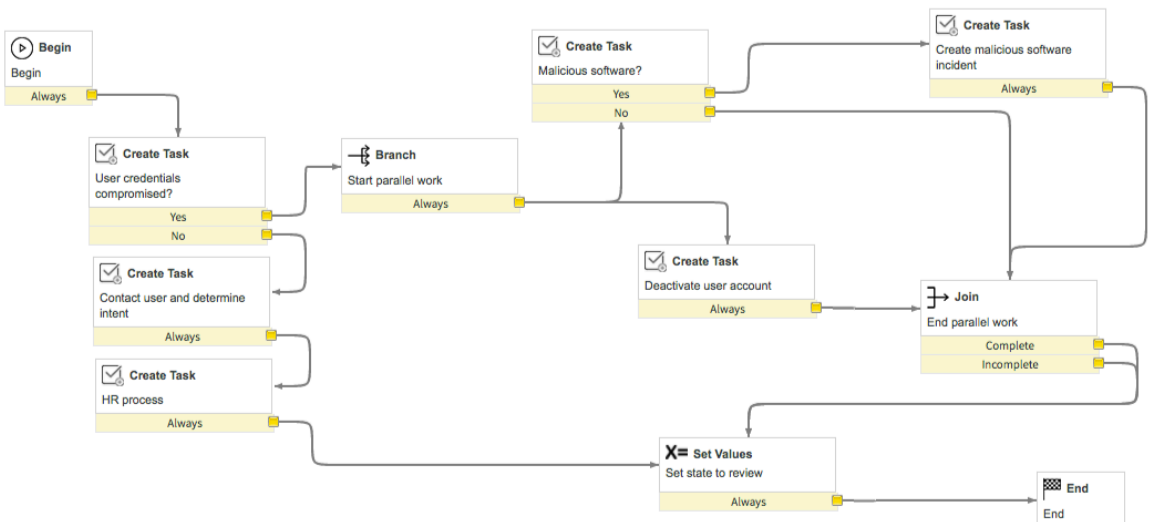
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Acesso não autorizado**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Acesso não autorizado



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Acesso não autorizado**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de acesso não autorizado

Tarefa de resposta	Ação	Resultados
Credenciais de usuário comprometidas?	Determine se as credenciais de usuários foram comprometidas. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as duas tarefas a seguir serão executadas em paralelo: ◦ **Software malicioso?** ◦ **Desativar conta do usuário** Se você selecionar **Não**, a tarefa **Entrar em contato com o usuário e determinar a intenção** será executada.
Software malicioso?	Determine se o acesso não autorizado resultou na introdução de software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Criar incidente de software mal-intencionado** será executada. Se você selecionar **Não**, a tarefa **Definir estado para revisão** será executada.
Criar incidente de software mal-intencionado	Execute as etapas necessárias para criar um incidente de segurança para o acesso não autorizado.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Desativar conta do usuário	Execute as etapas necessárias para desativar a conta de usuário comprometida.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Entrar em contato com o usuário e determinar a intenção	Execute as etapas necessárias para entrar em contato com o usuário responsável pelo acesso não autorizado e determine o motivo da tentativa de acesso.	Quando esta tarefa for concluída, a tarefa de **processo de RH** será executada.
Processo de RH	Execute as etapas necessárias para entrar em contato com os recursos humanos para implementar a ação disciplinar, se necessário.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e o fluxo termina.

Modelo de fluxo de trabalho de desfiguração de BBS/Web de incidente de segurança

O Incidente de segurança - Deformidade de Web/BBS - O modelo permite que você execute uma série de tarefas projetadas para lidar com o vandalismo direcionado contra um dos BBS ou sites da web da sua organização.

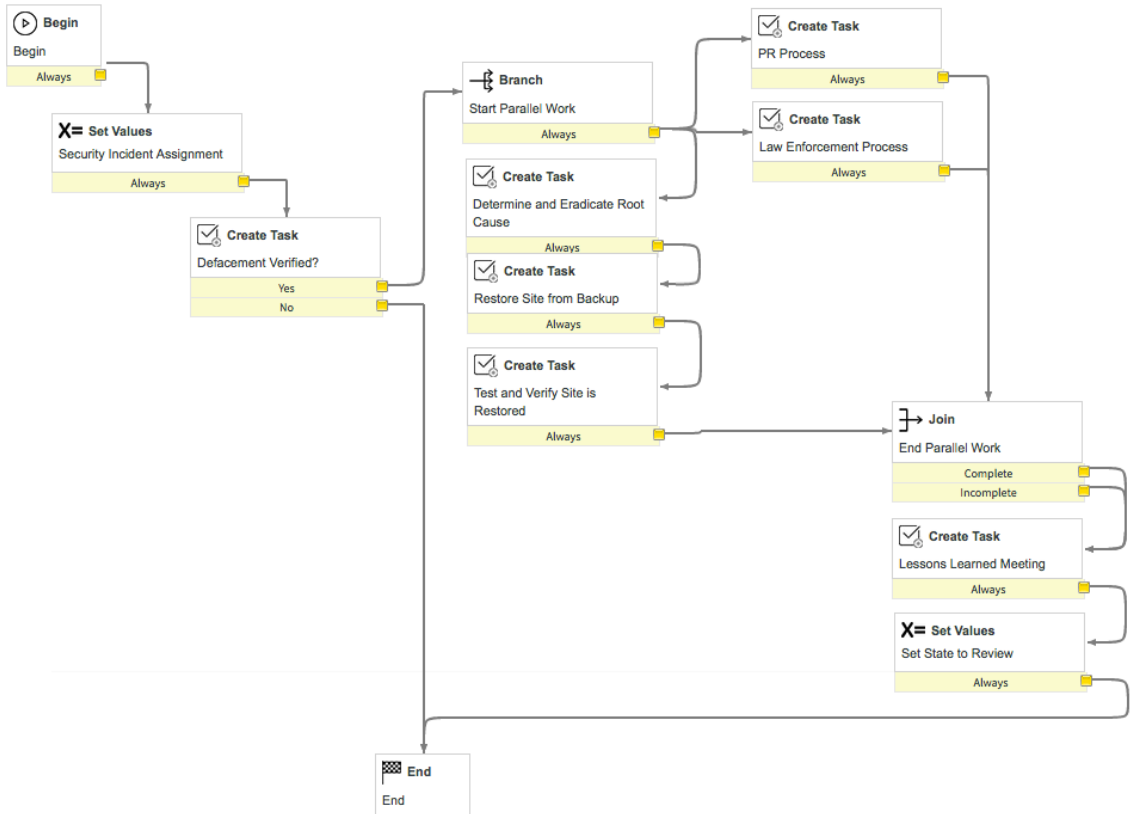
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como Deformidade de **Web/BBS**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Destruição da web/BBS



Procedimento

1. Abra o incidente de segurança para esta ocorrência de violação da Web ou BBS ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione Desfiguração de **Web/BBS**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de destruição da Web/BBS

Tarefa de resposta	Ação	Resultados
Atribuição de incidente de segurança	Crie um incidente de segurança para cada incidente relatado de violação de site ou BBS.	A próxima tarefa de resposta é executada.
Desfiguração verificada?	Determine se o site ou o BBS foi de fato adulterado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas de resposta serão executadas: ◦ **Processo de RC** ◦ **Processo de aplicação da lei** ◦ **Determinar e erradicar a causa raiz** Se você selecionar **Não**, o fluxo será encerrado.
Processo de RC	Execute as etapas necessárias para notificar o público de que o site ou o BBS foi desfigurado. Quando terminar o processo de RC, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Processo de aplicação da lei	Execute as etapas necessárias para envolver as agências de segurança apropriadas em relação ao ataque. Quando terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Determinar e erradicar a causa raiz	Execute as etapas necessárias para descobrir e eliminar a causa raiz da violação. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Restaurar site a partir do backup	Execute as etapas necessárias para fazer backup e restaurar o site ou o BBS. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Testar e verificar se	Verifique se o site foi restaurado.	A tarefa de **reunião de Lições aprendidas** é executada.

Tradução automática

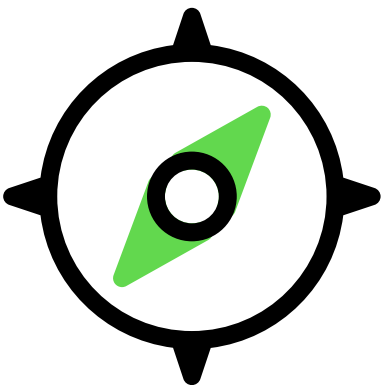
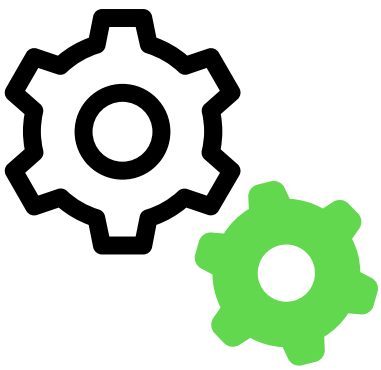
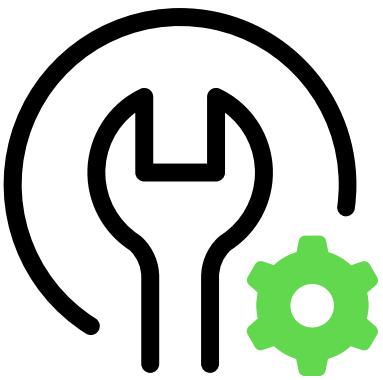
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
o site foi restaurado	Quando terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de violação de site/BBS. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisão**. O fluxo termina.

Inteligência contra ameaças

A aplicação ServiceNow® Inteligência contra ameaças permite que você encontre indicadores de comprometimento (IoC) e aprimore os incidentes de segurança com dados de inteligência contra ameaças.

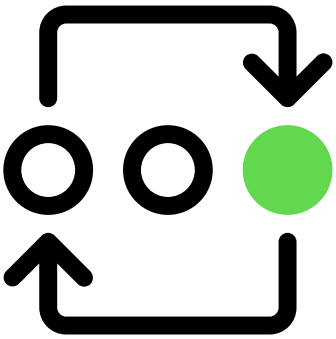
Iniciar

Explorar	Configurar	Administrar
		
Aprenda os conceitos de Inteligência contra ameaças e seus principais recursos.	Configure e aprenda os componentes instalados e as funções do usuário necessárias para atender às necessidades de negócio.	Defina as propriedades de Inteligência contra ameaças.

Tradução automática

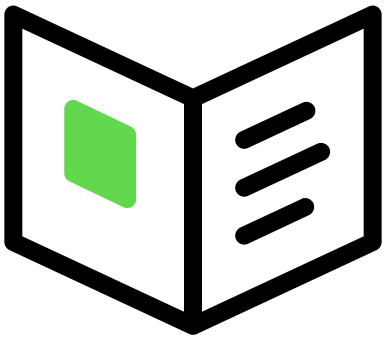
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrar



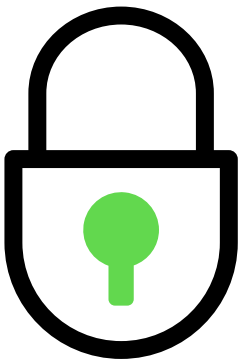
Amplie as capacidades de Inteligência contra ameaças integrando com a ServiceNow e aplicações de terceiros.

Uso



Gerencie Indicadores de Comprometimento (IoC) e vários artefatos.

Estrutura do MITRE ATT&CK



Gerenciar a estrutura do MITRE-ATT&CK identifica rapidamente ameaças e coordena as respostas a ataques cibernéticos.

Security Case Management

Gerencie a Gestão de casos de segurança coletando informações sobre atividades suspeitas.

Tradução automática

Recursos de aprendizado

- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solucionar problemas e obter ajuda

- Faça perguntas e explore outros recursos para Inteligência contra ameaças no ServiceNow Community
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Noções básicas do Inteligência contra ameaças

A aplicação Inteligência contra ameaças permite que você acesse e forneça um ponto de referência para os dados doSTIX™ (Structured Threat Information Expression) da sua empresa. Incluído em Inteligência contra ameaças está a aplicação Gestão de casos de segurança, que fornece um meio de analisar ameaças à sua organização representadas por campanhas direcionadas ou agentes de estado.

STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. Usando dados STIX e perfisTAXII™ (Trusted Automated Exchange of Indicator Information), os profissionais de ameaças podem usar informações compartilhadas de ameaças cibernéticas para isolar ameaças que foram identificadas anteriormente por sua empresa e de outras fontes. O TAXII possibilita a troca automatizada generalizada de informações sobre ameaças cibernéticas.

Inteligência contra ameaças O é compatível com STIX versões 1.1, 2.0 e 2.1.

STIX™ e TAXII™ são marcas comerciais da The MITRE Corp.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Domain Separation e Inteligência contra ameaças

O Domain Separation é compatível com o módulo Inteligência contra ameaças, que está disponível como parte do Security Incident Response. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

No módulo Inteligência contra ameaças (como parte da aplicação Security Incident Response), o Domain Separation permite que os provedores de serviço (SPs) criem e gerenciem o repositório de inteligência contra ameaças das seguintes maneiras:

- Origens de ameaças e perfis TAXII (Trusted Automated Exchange of Indicator Information, troca automatizada confiável de informações de indicadores)
- Observáveis
- Indicadores de comprometimento
- Modos/métodos de ataque de ameaças e gestão de casos em toda a base de clientes que atendem com custos operacionais reduzidos e uma qualidade de serviço superior

Ter espaços de trabalho do cliente separados para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínio em Inteligência contra ameaças por versão

O Domain Separation para o módulo Threat Intelligence (como parte da aplicação Security Incident Response) abrange a seguinte funcionalidade do produto:

- Os observáveis de incidente de segurança são direcionados para o domínio apropriado do usuário cujo ID/credencial/escopo gera o incidente. Os observáveis extraídos do incidente são armazenados no domínio do incidente de segurança.
- Configuração de perfis de serviço TAXII para baixar uma ou mais coleções TAXII que oferecem feeds de informações de ameaças cibernéticas. A configuração é armazenada no domínio sob o qual o perfil está sendo configurado.
- Configurar o download de feeds de ameaças para o repositório IOC no domínio em que a configuração está sendo realizada.
- Criação de modo/métodos de ataque no domínio da origem de inteligência contra ameaças que fornece as informações automaticamente ou o domínio sob o qual um novo modo/método de ataque está sendo adicionado manualmente pelo usuário
- Criação de casos para investigação de longo prazo de incidentes, observáveis, ICs, usuários e indicadores de comprometimento (IOC) associados ao caso. O caso é armazenado no domínio criado pelo usuário.

Nota: Em todos os casos acima, aplicam-se os princípios abrangentes de visibilidade em domínios separados na NOW Platform. Como sempre, um incidente no domínio primário pode fazer referência a artefatos no domínio secundário, mas não o contrário.

Como o Domain Separation funciona em Inteligência contra ameaças (como parte de Security Incident Response)

A Inteligência contra ameaças faz parte do Security Incident Response nos níveis Professional e Enterprise, mas não com o nível Standard. Portanto, um plug-in separado é necessário. O módulo Inteligência contra ameaças (como parte da aplicação Security Incident Response) cria e gerencia as informações de inteligência contra ameaças associadas a incidentes de segurança em uma organização. Os seguintes casos de uso reconhecem a separação de domínios:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Criação de observáveis de incidentes de segurança no momento da criação do incidente
  - De analisadores de e-mail (baseado em plataforma, phishing relatado pelo usuário, personalizado)
  - De aplicações em armazenamentos de gestão de eventos e informações de segurança (SIEM) de terceiros
  - Digitado manualmente pelo analista do SOC
- Coleta de observáveis de origens de feed de ameaças - Origens de inteligência contra ameaças de coleções TAXII
- Gerenciar observáveis de incidentes de segurança
  - Associar observáveis a indicadores relacionados
  - Associar observáveis a incidentes de segurança
  - Associar observáveis a observáveis secundários
  - Associar observável à origem do feed de ameaças
  - Adicionar anotações de segurança a observáveis
- Gerenciar indicadores de comprometimento
  - Associar indicadores a observáveis relacionados
  - Associar indicadores ao modo/método de ataque
  - Associar indicadores a tipos de indicador
  - Associar indicadores à origem do feed de ameaças
  - Adicionar anotações de segurança aos indicadores
- Gerenciar casos
  - Criar caso (manualmente ou a partir de um incidente)
  - Edite um novo caso para adicionar detalhes (escolha o tipo de caso e a gravidade, adicione incidentes, observáveis, itens de configuração, usuários, indicadores)
  - Excluir um caso

Configuração do Domain Separation

A configuração do Domain Separation para Inteligência contra ameaças não requer etapas adicionais. Todas as tabelas de Inteligência contra ameaças adquirem a coluna Domínio depois que a instância é separada por domínio.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os observáveis de incidente de segurança em um domínio não podem ser exibidos no escopo de outros domínios.
- Indicadores de comprometimento em um domínio não podem ser exibidos no escopo de outros domínios.
- Os modos/métodos de ataque associados a um domínio não podem ser exibidos no escopo de outros domínios.
- Os perfis de serviço TAXII associados a um domínio não podem ser exibidos no escopo de outros domínios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As origens de inteligência contra ameaças associadas a um domínio não podem ser exibidas no escopo de outros domínios.
- Casos associados a um domínio não podem ser exibidos no escopo de outros domínios.

As propriedades de Inteligência contra ameaças são definidas no nível global e, portanto, não são separadas por domínio. As configurações incluem:

- O nome do domínio para recuperar informações adicionais para endereços IP/URLs
- A chave de API a ser usada para recuperação
- Pesquisa de tabelas IoC locais antes de enviar para o scanner remoto
- Número de dias em que os observáveis locais são considerados
- Marcar um modo/método de ataque como inativo quando não for recebido de fontes de informações sobre ameaças
- Marcar um indicador como inativo quando não for recebido de nenhuma origem por um número especificado de dias

Configuração

Todos os aspectos da configuração da funcionalidade de inteligência contra ameaças são autocontidos em um ambiente separado por domínio.

As seguintes tarefas podem ser configuradas por domínio:

1. Criação de perfis de serviço TAXII
   - Escolha uma configuração de serviço de descoberta
   - Escolha uma configuração de serviço de coleta - Atribua funções a usuários e grupos de usuários
2. Criação de origens de inteligência contra ameaças
   - Configurar o serviço REST que fornece as informações de inteligência sobre ameaças
   - Programar o download de informações de inteligência contra ameaças
   - Escolha as informações de detalhes da ameaça para atribuir à origem
3. Criação de modo/métodos de ataque (manual)
   - Origem, tipo de malware, mecanismo de ataque, tipo de agente da ameaça, descrição, manipulação, efeito pretendido, visto pela primeira vez, visto pela última vez
   - Indicadores relacionados, modo/método de ataque secundário, incidentes de segurança associados

   Nota: Os modos/métodos de ataque também são criados automaticamente a partir das origens do feed de ameaças.

4. Definição de listas padrão para as seguintes categorias de informações de ameaças:
   - Mecanismos de ataque
   - Métodos de descoberta
   - Feeds
   - Tipos de indicador
   - Efeitos pretendidos
   - Notificações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tipos de observável
- Definições de limite de taxa
- Tipos de agente da ameaça
- Motivações de ataque
- Tipos de infraestrutura
- Capacidades de malware
- Tipos de malware
- Tipos de relatório
- Funções de agente da ameaça
- Tipos de ferramenta

Como os domínios de locatário gerenciam seus dados de aplicação próprios

- Os proprietários de domínio de locatário podem criar seus próprios perfis de serviço TAXII.
- Os proprietários de domínio de locatário podem criar suas próprias origens de inteligência contra ameaças.
- Os proprietários de domínio de locatário podem criar seus próprios modos/métodos de ataque.
- Os proprietários de domínio de locatário podem criar suas próprias listas padrão para categorias de informações de ameaça.

Nota: A lógica e os processos de negócios permitem que os cronogramas de download da origem da inteligência contra ameaças sejam separados por domínio pelo proprietário da instância.

Informações relacionadas

Domain Separation para provedores de serviço

Configurar Inteligência contra ameaças.

Antes de executar Inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow Store. Você também pode configurar propriedades e definir uma origem de ameaça.

Como instalar Inteligência contra ameaças

Antes de executar Inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar
Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração tranquilas.

Tarefas de configuração	Descrição
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	• Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá a função de administrador de ameaças [sn_ti.admin]. • O administrador de ameaças [sn_ti.admin] supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

Siga as instruções para download de uma aplicação do ServiceNow Store.

O que Fazer Depois

Definir Inteligência contra ameaças propriedades.

Componentes instalados com Inteligência contra ameaças

Vários tipos de componentes são instalados com a ativação do plug-in Inteligência contra ameaças, incluindo tabelas e funções do usuário.

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de ameaças [sn_ti.admin]	Tem controle total sobre todas as propriedades de ameaça, ANS e notificações.	sn_ti.write
Leitor de ameaças [sn_ti.read]	Tem acesso de leitura às informações da ameaça.	sn.sec_cmn.int_read
Gravador de ameaças [sn_ti.write]	Tem acesso de gravação às informações da ameaça. Não é possível excluir modos de ataque, indicadores ou observáveis. Somente um administrador de ameaças pode excluí-los.	• sn_sec_cmn.int_write • sn_ti.read
Analista de MITRE [sn_ti.mitre_analyst]	Esta função permite o acesso de leitura aos módulos [MITRE-ATT&CK em Inteligência contra ameaças e ao módulo SIR.	• sn_ti.read • sn_si.read

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instaladas

Tabela	Descrição
Mecanismo de ataque [sn_ti_attack_mecanismo]	Organiza padrões de ataque hierarquicamente com base em mecanismos que são empregados com frequência ao explorar uma vulnerabilidade. As categorias que são membros desta exibição representam as diferentes técnicas usadas para atacar um sistema.
Modo/método de ataque [sn_ti_attack_mode]	Modos e métodos de ataque são representações do comportamento de adversários cibernéticos. Eles caracterizam o que um adversário faz e como ele faz isso em níveis crescentes de detalhe.
Método de descoberta [sn_ti_discovery_method]	Uma expressão de como um incidente foi descoberto.
Feed [sn_ti_feed]	Usado para configurar o feed de ameaças (RSS) na visão geral da ameaça.
Modo/método de ataque do indicador [sn_ti_m2m_indicator_attack_mode]	Usado para mapear modos/métodos de ataque para indicadores.
Indicador de compromisso [sn_ti_indicator]	Usado para transmitir padrões observáveis específicos combinados com informações contextuais destinadas a representar artefatos e/ou comportamentos de interesse em um contexto de segurança cibernética.
Indicador de metadados de comprometimento [sn_ti_indicator_metadata]	Usado para preencher registros TAXII.
Origem do indicador [sn_ti_m2m_indicator_source]	Usado para coletar todas as origens que relatam o indicador específico.
Tipo de Indicador [sn_ti_indicator_type]	Caracteriza um indicador de ameaça cibernética composto por um padrão que identifica determinadas condições observáveis, bem como informações contextuais sobre o significado dos padrões, como e quando eles atuam e assim por diante.
Tipo de indicador associado [sn_ti_m2m_indicator_indicator_type]	Vincula os indicadores aos tipos aplicáveis

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Contagem de incidentes [sn_ti_observable]	Número de incidentes de segurança associados a um observável.
Efeito pretendido [sn_ti_intended_efeito]	Usado para expressar o efeito pretendido de um agente de ameaça.
Resultado da verificação de IP [sn_ti_ip_result]	Usado para mostrar os resultados de uma pesquisa de IP.
Limite de taxa de malware [sn_ti_rate_limit]	Define um limite de taxa a ser usado em uma origem de pesquisa.
Verificação de malware [sn_ti_scan]	Uma pesquisa. Contém o que pesquisar, com qual origem de pesquisa e um resumo dos resultados da pesquisa.
Entrada da fila de verificação de malware [sn_ti_scan_q_entry]	Um registro de pesquisa enfileirado para pesquisa ou processamento. Facilita as solicitações dentro dos limites de taxa declarados.
Resultado da verificação de malware [sn_ti_scan_result]	Exibe o resultado de uma pesquisa.
Verificador de malware [sn_ti_scanner]	Define origens de pesquisa de terceiros a serem usadas na execução de pesquisas.
Limite de taxa do scanner de malware [sn_ti_scanner_rate_limit]	Associa uma origem de pesquisa a um limite de taxa.
Tipo de malware [sn_ti_malware_type]	Usado para expressar os tipos de instâncias de malware.
Observável [sn_ti_observable]	Os observáveis no STIX representam propriedades com monitoramento de estado ou eventos mensuráveis pertinentes à operação de computadores e redes.
Tipo de contexto de observável [sn_ti_observable_context_type]	Armazena o contexto (origem, destino de um endereço IP e assim por diante) para um observável.
Indicador de observável [sn_ti_m2m_observable_indicator]	Usado para relacionar observáveis a indicadores.
Origem de Observável [sn_ti_observable_source]	Usado para relacionar observáveis a origens de ameaça.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Tipo de Observável [sn_ti_observable_type]	Lista os vários tipos de observáveis, como endereços IP.
Categoria de Tipo de Observável [sn_ti_observable_type_category]	Armazena a primeira categorização de observáveis (por exemplo, endereços IP e URLs). É usado para determinar com mais precisão os tipos de observável.
Modo/método de ataque relacionado [sn_ti_m2m_attack_mode_attack_mode]	Usado para relacionar os modos de ataque entre si.
Observáveis Relacionados [sn_ti_m2m_observables]	Usado para relacionar observáveis entre si.
Tipo de verificação [sn_ti_scan_type]	A definição de um tipo de pesquisa, com registros iniciais para arquivo, URL e IP.
Caso de segurança [sn_ti_case]	Armazena registros de caso de segurança criados usando a Gestão de casos.
IoC do caso de segurança [sn_ti_case_ioc]	Usado para gerenciar o relacionamento entre observáveis e casos.
Tarefa relacionada ao caso de segurança [sn_ti_m2m_case_task]	Usado para gerenciar o relacionamento entre tarefas (incidentes de segurança, solicitações de mudança e assim por diante) com casos de segurança.
Exclusão de relacionamento de caso de segurança [sn_ti_case_relationship_exclusion]	Fornece a definição de inclusão e exclusão de registros relacionados em casos de segurança.
Detecção [sn_ti_sighting]	O link m2m entre o observável e o resultado detalhado da Pesquisa de detecções usado na execução de uma solicitação de pesquisa de detecções.
Itens de Configuração de detecções [sn_ti_m2m_sighting_ci]	Mapeia itens de configuração para uma Pesquisa de detecções.
Detalhe da pesquisa de detecções [sn_ti_sighting_search_detail]	Detalhes de uma Pesquisa de detecções, por exemplo, o número de itens internos externos encontrados.
Resultado da pesquisa de detecções [sn_ti_sighting_search]	O cabeçalho de uma execução da Pesquisa de detecções.
Tipos de observável compatíveis	Relaciona os tipos de indicador a tipos de observável válidos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_m2m_ind_type_obs_type]	
Tipo de verificação compatível [sn_ti_supported_scan_type]	Mapeia o tipo de pesquisa para uma implementação específica de origem/ fornecedor de pesquisa. Indica que uma origem de pesquisa específica é compatível com o tipo.
Modo/método de ataque de tarefa [sn_ti_m2m_task_attack_mode]	Relaciona modos de ataque a tarefas.
Indicador de tarefa [sn_ti_m2m_task_indicator]	Relaciona indicadores a tarefas.
Observável de tarefa [sn_ti_m2m_task_observable]	Relaciona observáveis a tarefas.
Detecção de tarefa [sn_ti_m2m_task_sighting]	Armazena registros de tarefas (incidentes e casos de segurança) relacionados a um registro de detecção.
Coleta TAXII [sn_ti_taxii_collection]	Define um feed de inteligência de risco cibernético que pode ser importado por um servidor TAXII.
Perfil TAXII [sn_ti_taxii_profile]	Define um repositório para compartilhar inteligência de risco cibernético. Contém coleções TAXII.
Tipo de agente da ameaça [sn_ti_threat_actor_type]	Fornece caracterizações de agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo a intenção presumida e o comportamento observado ao longo do tempo.
Origem da inteligência contra ameaças [sn_ti_source]	Define uma origem para importar dados de ameaças.
Motivação de ataque associada [sn_ti_stix2_m2m_object_attack_moration]	Coleta todas as motivações de ataque associadas a um objeto STIX.
Tipo de infraestrutura associada [sn_ti_stix2_m2m_infra_type]	Vincula a infraestrutura com seus tipos.
Fase da cadeia de eliminação associada [sn_ti_stix2_m2m_indicator_kill_chain_phase]	Vincula as fases da cadeia de eliminação a indicadores.
Fase da cadeia de eliminação associada	Vincula as fases da cadeia de eliminação a objetos STIX.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_m2m_object_kill_chain_phase]	
Capacidade de malware associado [sn_ti_stix2_m2m_malware_capability]	Vincula o malware às suas capacidades.
Tipo de malware associado [sn_ti_stix2_m2m_malware_malware_type]	Vincula o malware aos seus tipos.
Observável associado [sn_ti_stix2_m2m_malware_observable]	Coleta todos os observáveis associados a um malware.
Observável associado [sn_ti_stix2_m2m_observed_data_observable]	Coleta todos os observáveis associados a dados observados.
Tipo de relatório associado [sn_ti_stix2_m2m_report_report_type]	Vincula relatórios de ameaças a seus tipos.
Função de agente da ameaça associada [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Vincula os agentes da ameaça às suas funções.
Tipo de agente da ameaça associada [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Vincula os agentes de ameaça aos seus tipos.
Tipo de ferramenta associada [sn_ti_stix2_m2m_tool_tool_type]	Vincula ferramentas a seus tipos.
Motivação de ataque [sn_ti_stix2_attack_motoration]	A Motivação de ataque molda a intensidade e a persistência de um ataque. Os Atores da ameaça e os Conjuntos de intrusão geralmente agem de uma maneira que reflete sua emoção ou situação subjacente, e isso informa aos defensores sobre a forma de ataque.
Padrão de ataque [sn_ti_stix2_attack_pattern]	Um tipo de TTP que descreve os métodos que os adversários usam para tentar comprometer os destinos.
Campanha [sn_ti_stix2_campaign]	Um agrupamento de comportamentos adversários que descreve um conjunto de atividades mal-intencionadas ou ataques (às vezes chamados de vagas) que ocorrem durante um período contra um conjunto específico de metas.
Linha de ação	Uma recomendação de um produtor de inteligência a um consumidor sobre

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_course_of_action]	as ações que ele pode realizar em resposta à inteligência.
Referência externa [sn_ti_stix2_external_reference]	Ponteiros para informações representadas fora do STIX.
Detecção de identidade [sn_ti_stix2_m2m_sighting_identity]	Coleta todas as identidades associadas a uma detecção.
Identidade [sn_ti_stix2_identity]	Indivíduos, organizações ou grupos reais (por exemplo, ACME, Inc.), bem como classes de indivíduos, organizações, sistemas ou grupos (por exemplo, o setor financeiro).
Referência externa do indicador [sn_ti_stix2_indicator_external_reference]	Representa referências externas associadas a indicadores.
Detecção do indicador [sn_ti_stix2_indicator_sighting]	Representa detecções de indicadores.
Tipo de infraestrutura [sn_ti_stix2_infrastructure_type]	Representa os vários tipos de infraestrutura.
Infraestrutura [sn_ti_stix2_infrastructure]	Um tipo de TTP que descreve todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados, destinados a oferecer suporte a alguma finalidade (por exemplo, servidores C2 usados como parte de um ataque, dispositivo ou servidor que fazem parte da defesa, servidores de banco de dados direcionados por um ataque e assim por diante).
Software instalado [sn_ti_stix2_m2m_malware_analysis_sw]	Coleta todos os softwares (tipos de software SCO) associados a uma análise de malware.
Conjunto de intrusão [sn_ti_stix2_intrusion_set]	Um conjunto agrupado de recursos e comportamentos adversários com propriedades comuns que se acredita ser orquestrado por uma única organização.
Fase da cadeia de eliminação [sn_ti_stix2_kill_chain_phase]	Representa as fases da cadeia de eliminação associadas a uma cadeia de eliminação.
Cadeia de eliminação [sn_ti_stix2_kill_chain]	Representa várias cadeias de eliminação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Local [sn_ti_stix2_location]	Representa uma localização geográfica fornecida por meio de STIX.
Análise de malware [sn_ti_stix2_malware_analysis]	Os metadados e resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.
Capacidade do malware [sn_ti_stix2_malware_capability]	Representa capacidades comuns que uma família ou instância de malware exibe.
Sistema operacional do malware [sn_ti_stix2_m2m_malware_operating_system]	Coleta todos os sistemas operacionais (tipos de software SCO) associados a malware.
Malware [sn_ti_stix2_malware]	Um tipo de TTP que representa código mal-intencionado.
Definição de marcação [sn_ti_stix2_marking_definition]	Representa requisitos de manipulação ou compartilhamento para objetos STIX.
Detecção de objeto [sn_ti_stix2_object_sighting]	Representa detecções de objetos STIX.
Relacionamento objeto-indicador [sn_ti_stix2_m2m_object_indicator]	Coleta todos os relacionamentos entre objetos STIX e indicadores STIX.
Relacionamento objeto-objeto [sn_ti_stix2_m2m_object]	Coleta todos os relacionamentos entre objetos STIX e outros objetos STIX, excluindo os indicadores.
Relacionamento objeto-observável [sn_ti_stix2_m2m_object_observable]	Coleta todos os relacionamentos entre observáveis STIX e objetos STIX.
Detecção de dados observados [sn_ti_stix2_m2m_sighting_observed_data]	Coleta todos os objetos de dados observados associados a uma detecção.
Dados observados [sn_ti_stix2_observed_data]	Transmite informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os STIX Cyber-Observable Objects (SCOs).
Tipo de relatório [sn_ti_stix2_report_type]	Representa a finalidade ou o assunto primário dos relatórios de ameaças.
Observável relatado [sn_ti_stix2_m2m_malware_analysis_observable]	Coleta todos os observáveis associados à análise de malware.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Objeto STIX V2 [sn_ti_stix2_object]	Tabela primária comum para objeto STIX.
Detecção de STIX V2 [sn_ti_stix2_sighting]	Tabela primária comum para tabelas de detecções STIX.
Função de agente da ameaça [sn_ti_stix2_threat_actor_role]	Representa funções que podem ser desempenhadas por agentes de ameaça.
Agente da ameaça [sn_ti_stix2_threat_actor]	Os agentes da ameaça são indivíduos, grupos ou organizações reais que operam com intenção mal-intencionada.
Grupo de ameaça [sn_ti_stix2_threat_grouping]	Agrupa todos os objetos STIX que compartilham algum contexto comum.
Anotação de ameaça [sn_ti_stix2_threat_note]	Fornece contexto e análise adicional não contida no objeto STIX correspondente.
Opinião sobre ameaças [sn_ti_stix2_threat_opinion]	Fornece avaliação da precisão das informações em um objeto STIX produzido por uma entidade diferente.
Relatório de ameaças [sn_ti_stix2_threat_report]	Relatórios são coleções de inteligência contra ameaças com foco em um ou mais tópicos, como uma descrição de um agente de ameaça, malware ou técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar inteligência de ameaças relacionada para publicar como uma história abrangente de ameaças cibernéticas.
Tipo de Ferramenta [sn_ti_stix2_tool_type]	As categorias de ferramentas que podem ser usadas para executar ataques.
Ferramenta [sn_ti_stix2_tool]	As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques.
Vulnerabilidade [sn_ti_stix2_vulnerability]	Representa fraqueza ou defeito nos requisitos, designs ou implementações da lógica computacional (exemplo de código) encontrada no software e em alguns componentes de hardware (exemplo de firmware). Eles podem ser explorados diretamente para afetar negativamente a confidencialidade,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	integridade ou disponibilidade desse sistema.

Definir Inteligência contra ameaças propriedades

Inteligência contra ameaças As propriedades permitem que você controle como diferentes aspectos do sistema funcionam, incluindo a configuração de chaves de API.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração** > **Propriedades**.
2. Defina as seguintes propriedades, conforme necessário.

Propriedades de Inteligência contra ameaças

Propriedade	Descrição
O nome do domínio para recuperar informações adicionais para endereços IP/URLs sn_ti.ip_lookup.web_site	O nome de domínio a ser usado para recuperar informações adicionais em seu banco de dados de IoC. Esta propriedade é usada pela inclusão de script `ThreatAdditionalInfo` para preencher informações adicionais no formulário Observáveis. Valor padrão: http://api.ipinfodb.com/v3/ip-country/ **Nota:** A API de terceiros do pinfodb.com está disponível sem custo extra e é usada em muitos programas de software comerciais. Se você substituí-lo por um nome de domínio diferente, também deverá fornecer a chave de API no próximo campo.
A chave de API a ser usada para o domínio, se houver sn_ti.ip_lookup.api_key	A chave de API a ser usada para recuperar informações adicionais em seu banco de dados de IoC. Esta propriedade é usada (junto com a propriedade sn_ti.ip_lookup.web_site) pela inclusão de script `ThreatAdditionalInfo` para preencher informações adicionais no formulário Observáveis.
Não execute a pesquisa automatizada de ameaças em um observável quando o	Opção para interromper a execução da pesquisa automatizada de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
observável estiver associado a um IoC ou for considerado mal-intencionado. sn_ti.scan_ioc_before_saging **Nota:** Você precisa definir a duração na próxima propriedade (sn_ti.scan_ioc_num_days).	ameaças em um observável quando o observável é mal-intencionado ou associado a um IoC pela duração configurada (em dias). Se você ainda precisar executar a pesquisa de ameaças para o observável, poderá fazê-lo manualmente. Valor padrão: sim
Duração (em dias) sn_ti.scan_ioc_num_days	Opção para definir a duração até a qual a pesquisa automatizada de ameaças do observável é ignorada. Valor padrão (em dias): 30
Não execute a pesquisa automatizada de ameaças em um observável se já estiver em execução. sn_ti.enable_threat_lookup_bypass **Nota:** Você precisa definir a duração na próxima propriedade (sn_ti.threat_lookup_bypass_times).	Se já houver um resultado de pesquisa de ameaças para um observável disponível, você terá a opção de ignorar a nova execução da pesquisa automatizada de ameaças para o mesmo observável até que a duração configurada seja aprovada. Valor padrão: não **Nota:** Se você estiver habilitando esta propriedade, certifique-se de adicionar um valor apropriado.
Duração (em minutos) sn_ti.threat_lookup_bypass_time	Opção para definir a duração após a qual a pesquisa automatizada de ameaças do observável pode ser executada novamente. Valor padrão (em minutos): 0
Defina uma duração de validade para substituições de usuário na descoberta de observável. sn_ti.enable_observable_finding_system_override **Nota:** Você precisa definir a validade na próxima propriedade (sn_ti.observable_finding_override_expiry).	Opção para definir uma duração de validade para substituições do usuário nas descobertas do observável. A descoberta de pesquisa de ameaças do observável não será alterada pelo sistema de base durante esta duração de validade. Valor padrão: Não. **Nota:** Se você estiver habilitando esta propriedade, certifique-se de adicionar um valor apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Validade (em minutos) sn_ti.observable_finding_override_expiry	Opção para definir o período de validade da descoberta do observável. Valor padrão (em minutos): nenhum
Quando um modo/método de ataque não tiver sido recebido de nenhuma origem pelo número de dias especificado, marque-o como inativo sn_ti.attack_mode_inactivate_days	Número de dias a partir do qual um modo/método de ataque foi recebido pela última vez para que o registro seja marcado como inativo. Valor padrão: 360 **Nota:** A caixa de seleção **Ativo** não está visível no formulário **Modo/método de ataque** por padrão. No entanto, você pode adicioná-lo. Quando os modos/métodos de ataque estão inativos, eles não podem ser selecionados em outros formulários.
Quando um indicador não tiver sido recebido de nenhuma origem pelo número de dias especificado, marcá-lo como inativo sn_ti.indicator_inactivate_days	Número de dias a partir do qual um indicador foi recebido pela última vez para o registro ser marcado como inativo. Valor padrão: 180 **Nota:** A caixa de seleção **Ativa** não está visível no formulário do **indicador** por padrão. No entanto, você pode adicioná-lo. Quando os indicadores estão inativos, eles não podem ser selecionados em outros formulários.
O tamanho máximo da carga (em MB) para um anexo STIX que pode ser analisado. sn_ti.stix.max_payload_size	Especifica o tamanho máximo da carga para o anexo STIX que você pode analisar. Valor-padrão: nenhum Valor máximo permitido: sem limite.
Tempo máximo em segundos que uma conexão HTTP de saída aguarda para obter dados de coleta de TAXII sn_ti.taxii.http.max_timeout	Especifica o tempo máximo que uma conexão HTTP de saída espera antes de buscar o próximo pacote de dados de coleta TAXII.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	Valor padrão: 300
Número máximo de objetos recuperados em uma chamada REST de um servidor TAXII (aplicável somente para TAXII versões 2.0 e 2.1) sn_ti.taxii.max_page_size	Especifica o número máximo de objetos recuperados em uma chamada REST do servidor TAXII para uma página. Valor padrão: 5000 Valor máximo permitido: 50.000
Número máximo de novas tentativas para uma chamada REST TAXII 2.X com falha sn_ti.taxii2.retry_count	Especifica o número máximo de novas tentativas para uma chamada REST TAXII com falha. Valor padrão: 3

3. Clique em **Salvar**.

Definir uma origem de ameaça

Você pode manter uma lista de Inteligência contra ameaças origens de ameaça. Cada origem inclui a capacidade de definir com que frequência uma origem é consultada. Você também pode executar uma origem de ameaça sob demanda para importar os dados necessários do Structured Threat Information eXpression (STIX).

Antes de Iniciar

Função necessária: sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

Inteligência contra ameaças emprega duas tecnologias para importar informações relacionadas a ameaças: STIX e TAXII (Trusted Automated Exchange of Indicator Information, troca automatizada confiável de informações do indicador).

O STIX fornece uma linguagem padronizada e estruturada para representar um amplo conjunto de informações de ameaças cibernéticas que inclui indicadores de atividade de comprometimento (IoC) (por exemplo, endereços IP e hashes de arquivo), bem como informações contextuais sobre ameaças, como modos/métodos de ataque, que, juntos, caracterizam de forma mais completa as motivações, capacidades e atividades de um adversário cibernético. Como tal, os dados do STIX fornecem informações valiosas sobre como sua organização pode se proteger melhor contra ameaças cibernéticas.

O Trusted Automated Exchange of Indicator Information (TAXII) é usado para facilitar a troca automatizada de informações sobre ameaças cibernéticas. O TAXII define um conjunto de serviços e trocas de mensagens que permitem o compartilhamento de informações acionáveis sobre ameaças cibernéticas entre organizações e limites de produto/serviço para detecção, prevenção e mitigação de ameaças cibernéticas. Os perfis TAXII podem ser configurados como repositórios para compartilhar informações no formato STIX. Cada perfil contém uma ou mais coleções ou feeds TAXII.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Origens** > **Origens de Ameaças**.
2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da origem da ameaça.
Aplicação	A aplicação que contém este registro.
Ativo	Marque esta caixa de seleção para ativar a origem da ameaça.
Avançado	Marque esta caixa de seleção para exibir os scripts nos campos **Script de fábrica de integração** e **Processador de relatório**.
Descrição	Uma descrição desta origem de ameaça.

4. Preencha os campos na seção **Programação**, conforme apropriado.

Campo	Descrição
Executar	A frequência com que você deseja que a integração seja executada: Diariamente, Semanalmente, Periodicamente e assim por diante. Conforme observado, os campos subsequentes são exibidos com base na configuração deste campo.
Dia	O dia em que você deseja que a integração seja executada. ◦ Se você selecionou **Semanalmente** no campo **Executar**, este campo exibirá os dias da semana. ◦ Se você selecionou **Mensal** no campo **Executar**, este campo exibirá os dias do mês.
Hora	A hora em que você deseja que a integração seja iniciada.
Intervalo de repetição	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá o número de dias e horas antes que a integração seja executada novamente.
Início	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá as datas e a hora a serem usadas como ponto de partida para atualizações periódicas.
Condicional	Selecione este campo se quiser adicionar parâmetros condicionais.
Condição	Se você marcou a caixa de seleção **Condicional**, insira as condições aqui.

5. Preencha os campos na seção **Detalhes da ameaça**, conforme apropriado.

Campo	Descrição
Indicador	O indicador a ser usado quando os dados não fornecem um explicitamente. Para listas de bloqueio, se vazias, um novo indicador será criado para cada observável.
Tipo de indicador	O tipo de indicador a ser usado para indicadores que são criados e os dados não fornecem explicitamente um tipo de indicador.
Modo/método de ataque	O modo/método de ataque a ser usado quando os dados não fornecem um explicitamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de Observável	O tipo de observável a ser usado para observáveis que são criados e os dados não fornecem explicitamente um tipo de observável.[SI1]
Ponderação	Insira um valor de peso para esta origem a ser usada no cálculo de confiança.

Nota: O uso dos campos **Indicador**, **Tipo**de indicador , **Modo/Método de ataque**e **Tipo de observável** é específico da implementação. O processador padrão, SimpleBlocklistProcessor, se comporta como as dicas das ferramentas descrevem. No entanto, uma origem de ameaça TAXII é totalmente orientada por dados. Qualquer processador de origem de ameaça personalizado seria capaz de usar sua própria estratégia. Esses campos são basicamente itens a serem expostos à integração/ processador e a implementação decide como usá-los.

6. Preencha os campos na seção **Detalhes da origem**, conforme apropriado.

Campo	Descrição
Endpoint	Insira a URL do endpoint do serviço web em que a origem da ameaça é acessada por Inteligência contra ameaças. Clique no ícone de cadeado para bloquear o URL.
Usar Mensagem REST	Se você precisar de uma mensagem REST para acessar a origem da ameaça, marque esta caixa de seleção. Os campos de **mensagemREST e método REST** se tornam obrigatórios.
Mensagem REST	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** para definir uma nova mensagem REST .
Método REST	Clique no ícone de pesquisa e selecione o método REST na lista ou clique em **Novo** para definir um novo método REST.
Script de integração	O script de integração padrão é **SimpleRESTSecurityDataIntegration**. Ele executa uma chamada REST simples, salva a resposta como um anexo e retorna o anexo para o processador. Este script atende às necessidades da maioria das organizações. Mas, se quiser, você pode clicar no ícone de pesquisa e selecionar um script de integração diferente ou definir um novo.
Script de fábrica de integração	Se a caixa de seleção **Avançado** estiver marcada, este campo exibirá o script real para construir o script de integração. Você pode editar o script conforme necessário. Essa capacidade é útil para implementações personalizadas. As integrações no sistema de base geralmente não precisam de nenhuma lógica de construtor personalizada.
Processador de relatórios	O script de integração padrão é **SimpleBlocklistProcessor**. Este script é um processador simples que aceita uma lista de bloqueios simples (simples, ou seja, um documento de coluna única com observáveis, como URLs ou endereços IP) e cria observáveis. Ele usa os vários campos de **Detalhes da ameaça** para determinar quais campos definir quando os observáveis forem criados.
Script de fábrica do processador	Se a caixa de seleção **Avançado** estiver marcada, este campo exibirá o script real para construir o processador. Você pode editar o script conforme necessário. Este script geralmente é útil para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	implementações personalizadas. As integrações no sistema de base geralmente não precisam de lógica de construtor personalizada.

7. Clique em **Enviar**.

Nota: Para obter mais informações sobre como configurar a paginação da origem da ameaça, consulte o artigo KB1213825 .

Criar um perfil TAXII

Você pode manter perfis TAXII para compartilhar informações no formato STIX. Cada perfil contém uma ou mais coleções ou feeds TAXII.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
2. Clique em **Nova**.
3. Preencha os seguintes campos conforme apropriado.

Campo	Descrição
Nome	O nome do perfil TAXII
Aplicação	A aplicação que contém este registro.
Usar mensagens REST como modelo	Se você precisar de uma mensagem REST para acessar o perfil TAXII, marque esta caixa de seleção.
Versão de TAXII	Especifique a versão TAXII. As versões do STIX compatíveis são 1.1, 2.0 e 2.1.
Descrição	Uma descrição deste perfil TAXII.

4. Preencha os campos na seção **Configuração do serviço de descoberta**, conforme apropriado.

Campo	Descrição
Endpoint do serviço de descoberta	O endpoint de descoberta autoriza os clientes a obter informações sobre um servidor TAXII e obter uma lista de raízes de API.
Usar Mensagem REST	Selecione esta opção se precisar de uma mensagem REST para acessar o perfil TAXII. Os campos **Mensagem REST do serviçode descoberta e Método REST do serviço de descoberta** se tornam obrigatórios.
Mensagem REST do serviço de descoberta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** para definir uma nova mensagem REST.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Método REST do serviço de descoberta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** para definir um novo método REST.

5. Preencha os campos na seção **Configuração do serviço de coleta**, conforme apropriado.

Campo	Descrição
Endpoint do serviço de informações de coleta	Uma coleção TAXII é uma interface para um repositório lógico de objetos CTI fornecidos por um servidor TAXII e é usada por clientes TAXII para enviar informações para o servidor TAXII ou solicitar informações do servidor TAXII. Um servidor TAXII pode hospedar várias coleções por raiz de API, e as coleções são usadas para trocar informações de solicitação-resposta.
Usar Mensagem REST	Selecione esta opção se precisar de uma mensagem REST para acessar o perfil TAXII. Os campos **Mensagem REST do Serviço de informações decoleta e Método REST do Serviço de informações de coleta** se tornam obrigatórios.
Mensagem REST do serviço de informações de coleta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** para definir uma nova mensagem REST.
Método REST de serviço de informações de coleta	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** para definir um novo método REST.

6. Clique em **Enviar**.

Repositório LOC

O repositório IoC contém objetos STIX, cada um desses objetos contém uma informação específica.

Ao combinar objetos STIX por meio de relacionamentos, você permite representações fáceis ou complexas de Inteligência contra ameaças cibernéticas (CTI).

Inteligência contra ameaças O é compatível com STIX versões 1.1, 2.0 e 2.1.

Modos e métodos de ataque

Os modos e métodos de ataque, às vezes chamados de Táticas, técnicas e procedimentos (TTPs), são representações de como os adversários cibernéticos se comportam. Eles caracterizam o que esses adversários fazem e como o fazem, em níveis crescentes de detalhe. Os modos e métodos de ataque se aplicam a STIX 1.1.

Por exemplo, um modo/método de ataque pode ser usar malware para roubar credenciais de cartão de crédito. Ou outra tática relacionada (em um nível inferior de detalhe) pode ser o envio de e-mails direcionados com anexos que contêm código malicioso, que é

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

executado após a abertura, captura informações de cartão de crédito de pressionamentos de tecla e usa http para se comunicar com um comando e servidor de controle para transferir informações.

Os modos e métodos de ataque se aplicam a STIX 1.1.

Definir um modo/método de ataque

Os modos e métodos de ataque são importados com os dados STIX, mas você pode adicionar novos modos/métodos, conforme necessário.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de classificação para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do modo/método de ataque. Se você não configurou ou ativou marcadores de classificação, esta lista suspensa não será exibida.
Título	Insira um nome descritivo para este modo/método de ataque.
Tipo de malware	Selecione o tipo de malware para este modo/método de ataque. Os tipos de malware disponíveis são recuperados do servidor do fornecedor como dados STIX.
Origem	Selecione a fonte de dados da ameaça para este modo/método de ataque. Algumas fontes de dados estão incluídas no sistema de base. Você pode criar novas fontes de dados conforme necessário.
Mecanismo de ataque	Selecione o mecanismo de ataque para este modo/método de ataque. Mecanismos de ataque representam as diferentes técnicas usadas para atacar um sistema. Os mecanismos de ataque disponíveis são recuperados do servidor do fornecedor como dados STIX.
Visto pela primeira vez	Esta data é recuperada do servidor do fornecedor como dados STIX.
Visto pela última vez	Esta data é recuperada do servidor do fornecedor como dados STIX.
Tipo de Ator da Ameaça	Selecione o tipo de agente da ameaça para este modo/método de ataque. Os tipos de agente de ameaça caracterizam agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo intenção presumida e comportamento observado ao longo do tempo. Os tipos de agentes de ameaça disponíveis são recuperados do servidor do fornecedor como dados STIX.
Descrição	Insira uma descrição do modo/método de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Manipulação	Insira instruções sobre como lidar com este modo/método de ataque.
Efeito pretendido	Insira o efeito pretendido deste tipo de ataque.

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**. Você pode exibir qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça.
Modo/método de ataque secundário	Lista os modos/métodos de ataque que são secundários do modo/método de ataque primário.
Tarefas Associadas	Lista as mudanças associadas ao modo/método de ataque primário.

Adicionar um IoC a um modo/método de ataque

Além de importar indicadores como dados STIX, você pode adicionar IoCs a um modo/método de ataque manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar um IoC.
3. Clique na lista relacionada **Indicadores** relacionados.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o IoC que você deseja adicionar.
6. Usando o slushbucket, adicione o IoC à lista de **Indicadores relacionados**.
7. Clique em **Salvar**.

Adicionar um método de modo de ataque relacionado

Além de importar modos/métodos de ataque como dados STIX, você pode adicionar manualmente modos/métodos de ataque relacionados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar um modo/método de ataque relacionado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique na lista relacionada ao **modo/método de ataque secundário**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o modo/método de ataque que você deseja relacionar ao atual.
6. Usando o slushbucket, adicione o modo/método de **ataque** à lista de modos/métodos de ataque secundário.
7. Clique em **Salvar**.

Adicionar tarefa associada a um modo/método de ataque

Além de importar tarefas associadas (como mudanças e incidentes) como dados STIX, você pode adicioná-las a um modo/método de ataque manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar uma tarefa associada.
3. Clique na lista relacionada **Tarefas associadas**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao modo/método de ataque.
6. Usando o slushbucket, adicione a tarefa à lista **Tarefas associadas**.
7. Clique em **Salvar**.

Indicadores de comprometimento

Indicadores de comprometimento (IoC) são artefatos observados em uma rede ou sistema operacional que provavelmente indicam uma invasão. IoCs típicos são assinaturas de vírus e endereços IP, hashes MD5 de arquivos de malware ou URLs ou nomes de domínio. O IoC se aplica a STIX 1.1 e 2.x.

Um IoC pode ser um único observável ou uma coleção de observáveis (por exemplo, uma única URL incorreta conhecida ou a presença de um arquivo específico e alguns valores de chave de registro específicos).

Depois que os IoCs são identificados em um processo de resposta a incidentes e perícia de computador, eles podem ser usados para detecção antecipada de futuras tentativas de ataque usando sistemas de detecção de intrusão e software antivírus.

O IoC se aplica a STIX 1.1 e 2.x.

Exibir um IoC

Os IoCs, às vezes chamados de indicadores, são normalmente recuperados de uma fonte de dados de ameaças como dados STIX. Se necessário, você também pode criar IoCs.

Antes de Iniciar
Função necessária: sn_ti.write

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Depois que o trabalho agendado tiver recuperado os dados de IoC da fonte de dados definida, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**. Os IoCs recuperados são listados.
2. Clique no IoC que você deseja exibir.
3. As informações a seguir são exibidas.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do IoC. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Título	Um nome descritivo para este indicador.
Visto pela primeira vez	A primeira data em que este indicador foi observado no sistema.
Visto pela última vez	A data mais recente em que este indicador foi observado no sistema.
Contagem encontrada	O número de vezes que o indicador foi encontrado.
Contagem originada	O número de vezes que o indicador foi importado de origens de ameaça definidas.
Anotações	Quaisquer anotações adicionais sobre o indicador. Este campo também pode conter pares de chave/valor JSON.

4. Você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Observáveis Relacionados	Lista os observáveis que estão vinculados ao indicador atual.
Modo/método de ataque relacionado	Lista modos/métodos de ataque relacionados que foram identificados como relacionados a este indicador.
Tipo associado	Lista outros tipos de indicador associados a este IoC.
Origens do indicador	Lista as origens deste indicador, junto com o nível de confiança da origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Tarefas Associadas	Lista todas as tarefas, mudanças e incidentes associados ao IoC.
Metadados do indicador	Se o campo **Anotações** contiver pares de chave/valor JSON válidos, eles serão analisados e exibidos. Se nenhum par de chave/valor JSON estiver presente ou se o JSON for inválido, esta lista relacionada não será exibida.
Anotações de segurança	
Referências externas do indicador	
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.

Adicionar um observável relacionado a um IoC

Além de importar observáveis como dados STIX, você pode adicionar observáveis relacionados a um IoC manualmente.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar um observável relacionado.
3. Clique na lista relacionada **Observáveis** relacionados.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o observável que você deseja relacionar com o IoC.
6. Usando o slushbucket, adicione o observável à lista de **observáveis relacionados**.
7. Clique em **Salvar**.

Adicionar um modo/método de ataque relacionado a um IoC

Além de importar modos/métodos de ataque relacionados como dados STIX, você pode adicionar modos/métodos de ataque relacionados a um IoC manualmente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar um modo/método de ataque relacionado.
3. Clique na lista **relacionada ao modo/método de ataque** relacionado.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o modo/método de ataque que você deseja relacionar com o IoC.
6. Usando o slushbucket, adicione o modo/método de ataque à lista de modo/método de **ataque relacionado**.
7. Clique em **Salvar**.

Identificar tipos de indicador associados

Se um IoC não tiver tipos de indicador associados definidos, ele rastreará todos os tipos de observáveis. No entanto, se você associar um ou mais tipos de indicadores a um IoC, isso limitará os tipos de observáveis que podem ser associados ao IoC.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja associar um tipo de indicador.
3. Clique na lista relacionada **Tipo associado**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o tipo de indicador que você deseja associar ao IoC.
6. Usando o slushbucket, adicione o tipo de indicador à lista **Tipo associado**.
7. Clique em **Salvar**.

Identificar origens de indicador

As origens de indicador são normalmente rastreadas automaticamente como parte do processo de importação de ameaças, mas mais origens podem ser adicionadas manualmente.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar fontes de indicador.
3. Clique na lista relacionada **Origens do indicador**.
4. Clique em **Editar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Conforme necessário, use os filtros para localizar a origem do indicador que você deseja associar ao IoC.
6. Usando o slushbucket, adicione a origem do **indicador à lista Origens** do indicador.
7. Clique em **Salvar**.

Adicionar tarefas associadas a um IoC

Além de importar tarefas associadas (como mudanças e incidentes) como dados STIX, você pode adicioná-las a um IoC manualmente.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no IoC ao qual você deseja adicionar uma tarefa associada.
3. Clique na lista relacionada **Tarefas associadas**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao IoC.
6. Usando o slushbucket, adicione a tarefa à lista **Tarefas associadas**.
7. Clique em **Salvar**.

Observáveis

Os observáveis representam propriedades com monitoramento de estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes . Os observáveis se aplicam a STIX 1.1 e 2.x.

Conjuntos de observáveis cibernéticos são úteis para identificar indicadores de comprometimento quando são combinados com informações contextuais que representam os comportamentos de ameaças cibernéticas.

Os observáveis se aplicam a STIX 1.1 e 2.x.

Definir um observável

Os observáveis são recuperados do servidor do fornecedor como dados STIX. No entanto, você pode criar observáveis, conforme necessário.

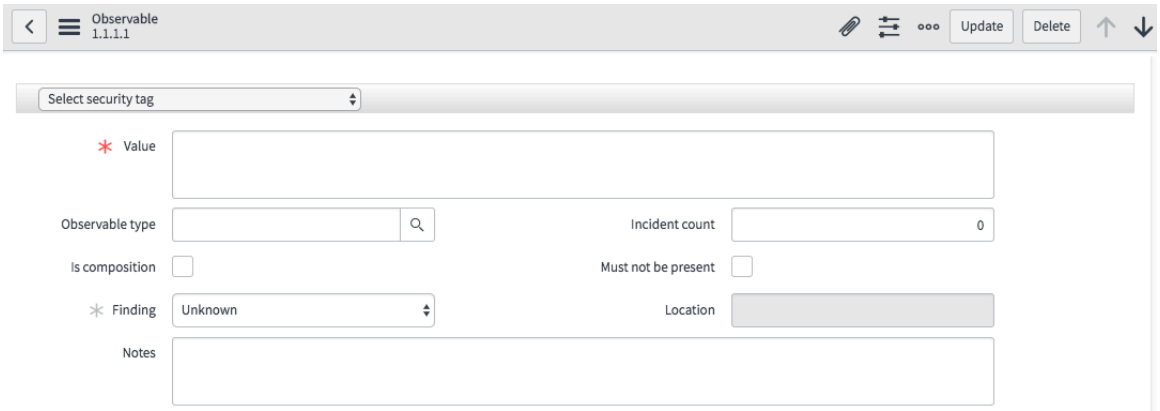
Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do observável. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável. **Nota:** Se uma verificação de ameaças em um endereço IP ou hash retornar malware ou alguma outra falha, o endereço IP ou o valor de hash será adicionado automaticamente à tabela Observável [sn_ti_observable]. Como tal, ele pode ser pesquisado no formulário Observáveis.
Tipo de observável	Selecione a classificação de observável, como um endereço IP ou hash de arquivo. Esses tipos de observável são definidos no módulo **Tipos de observável**.
Contagem de incidentes	O número de vezes que o valor do observável foi encontrado.
É composição	Este campo é exibido somente depois que o registro do observável foi salvo. Se o **tipo de observável** estiver definido como qualquer outra coisa que não seja **composição de observável**e este novo observável for uma composição, marque esta caixa de seleção. Se o **Tipo de observável** já estiver definido como **Composição de observável**, a caixa de seleção será marcada e será somente leitura. Uma composição de observável é um observável que contém observáveis secundários.
Descoberta	Selecione uma das seguintes propriedades:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Mal**-intencionado : indica que o observável é prejudicial à organização. ◦ **Suspeito**: indica que o observável pode ser prejudicial à organização. ◦ **Limpar**: indica que o observável não é prejudicial à organização. ◦ **Desconhecido**: indica que ainda não determinamos a descoberta do observável. ◦ Valor padrão: desconhecido. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças. **Nota:** Após um upgrade, os observáveis existentes são marcados como Mal-intencionados.
Operador	Este campo aparece somente quando a caixa de seleção **É composição** está marcada. Dependendo da sua configuração neste campo, os observáveis e seus secundários são considerados ao decidir se um indicador associado está presente. Defina este campo como **E** se todos os observáveis secundários precisarem estar presentes para que um indicador associado seja considerado presente. Defina como **OU** se algum dos observáveis secundários estiver presente para que um indicador associado seja considerado presente.
Não deve estar presente	Este campo é exibido somente depois que o registro do observável foi salvo. Se selecionado, este campo significa que a ausência do observável é o possível problema (por exemplo, uma chave de registro ausente).
Local	Usando as configurações em duas propriedades e uma definição de inclusão de script, você pode carregar Carregar mais dados de IoC neste campo.
Anotações	Insira anotações adicionais sobre o observável.

Tradução automática

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**. Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores que foram identificados pela origem da ameaça.
Tarefas Associadas	Lista as mudanças associadas ao observável.
Observáveis secundários	Lista os observáveis relacionados que foram identificados pela origem da ameaça.
Recursos correspondentes para IP	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Origens observáveis	Lista as origens deste observável, junto com o nível de confiança da origem.
Anotações de segurança	Lista as anotações de segurança adicionadas a este observável.

Adicionar um IoC relacionado a um observável

Além de importar observáveis como dados STIX, você pode adicionar observáveis relacionados a um IoC manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar um IoC relacionado.
3. Clique na lista relacionada **Indicadores** relacionados.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o indicador que você deseja relacionar com o observável.
6. Usando o slushbucket, adicione o indicador à lista de **Indicadores relacionados**.
7. Clique em **Salvar**.

Adicionar tarefas associadas a um observável

Além de importar tarefas associadas (como mudanças e incidentes) como dados STIX, você pode adicioná-las a um observável manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar uma tarefa associada.
3. Clique na lista relacionada **Tarefas associadas**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao observável.
6. Usando o slushbucket, adicione a tarefa à lista **Tarefas associadas**.
7. Clique em **Salvar**.

Adicionar um observável relacionado

Além de importar observáveis como dados STIX, você pode adicionar observáveis relacionados manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar um observável relacionado.
3. Clique na lista relacionada **Observáveis secundários**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o observável que você deseja relacionar ao atual.
6. Usando o slushbucket, adicione o observável à lista de **observáveis** secundários.
7. Clique em **Salvar**.

Carregar mais dados de IoC

Dependendo das configurações em duas propriedades e de uma definição de inclusão de script, você pode carregar informações de geolocalização para endereços IP e sites no formulário Observáveis. Com mais personalização, você também pode adicionar outras informações, como códigos de país e nomes de cidades.

Antes de Iniciar

As duas propriedades a seguir devem ser definidas:

- **O nome do domínio para recuperar informações adicionais para endereços IP/URLs** [sn_ti.ip_lookup.web_site]
- **A chave de API a ser usada para o domínio acima, se houver** [sn_ti.ip_lookup.api_key]

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no endereço IP ou URL do observável para o qual você deseja exibir mais dados de IoC.
   O campo **Local** mostra a geolocalização do IoC.
3. Clique no botão **Aprimorar dados** para carregar os dados de IoC adicionais.
4. Você também pode configurar o formulário Observável para adicionar outros campos relacionados ao local, como o código do país e o código da cidade.

> **Nota:** Para carregar mais informações relacionadas ao local, edite a inclusão de script **ThreatAdditionalInfo** e forneça a chave de API apropriada do site que fornece as informações adicionais.

Identificar origens de observável

Se um observável não tiver origens definidas, ele usará todos os tipos de origens. No entanto, se você adicionar uma ou mais origens de ameaça a um observável, isso limitará as origens usadas.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar origens de observável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique na lista relacionada **Origens do observável**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar a origem que você deseja associar ao observável.
6. Usando o slushbucket, adicione a origem do **observável à lista Origens** do observável.
7. Clique em **Salvar**.

Executar pesquisas em observáveis

Você pode executar pesquisas de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações de verificação executadas dependem daquelas que você ativou.

Antes de Iniciar

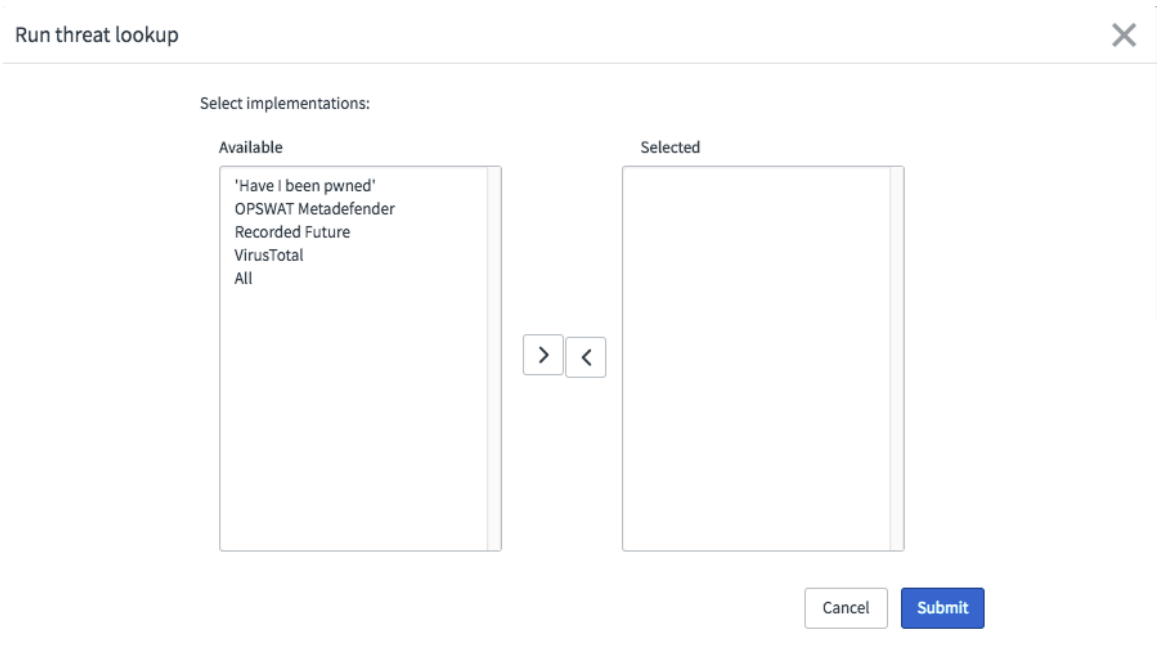
Antes de executar pesquisas, você deve ativar o plug-in Inteligência contra ameaças. Você também deve instalar o plug-in para uma ou mais das implementações de verificação:

- Integração do CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Operações de segurança Já foi pwned?
- VirusTotal

Função necessária: sn_ti.write

Procedimento

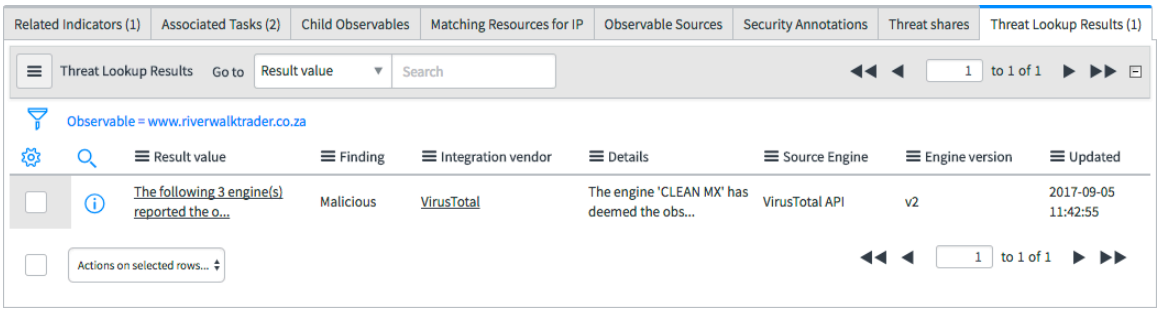
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Execute uma das seguintes etapas:
   - Para executar uma pesquisa em mais de um observável, selecione os observáveis, clique **em Ações nas linhas selecionadas**e selecione **Executar pesquisa de ameaças**.
   - Para executar uma pesquisa em um único observável, abra o registro do observável e clique no link relacionado **Executar pesquisa de ameaças**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione as implementações de pesquisa de ameaças que você deseja usar ou selecione **Todas** para executar pesquisas usando todas as implementações ativas e clique em **Enviar**.
   Uma mensagem indica que as pesquisas de ameaças foram iniciadas. O Integração de Operações de segurança - Fluxo de trabalho de pesquisa de ameaças executa e também executa os fluxos de trabalho de implementação das implementações de pesquisa de ameaças selecionadas. As pesquisas são realizadas e os resultados são gerados.
4. Quando as pesquisas forem concluídas, você poderá clicar na guia **Resultados da pesquisa de ameaças** para exibir os resultados.



Resultado da pesquisa de ameaças recentes: você também pode ver os resultados da pesquisa de ameaças mais recentes de cada fornecedor de integração ao clicar na guia **Resultado da pesquisa de ameaças recentes**.

Nota: A guia **Resultado da pesquisa de ameaças recentes** não faz parte do sistema de base.

Para habilitar esta guia, execute o seguinte:

a. Clique com o botão direito do mouse no cabeçalho do formulário.

b. Navegar até **Configurar** > **Listas relacionadas**.

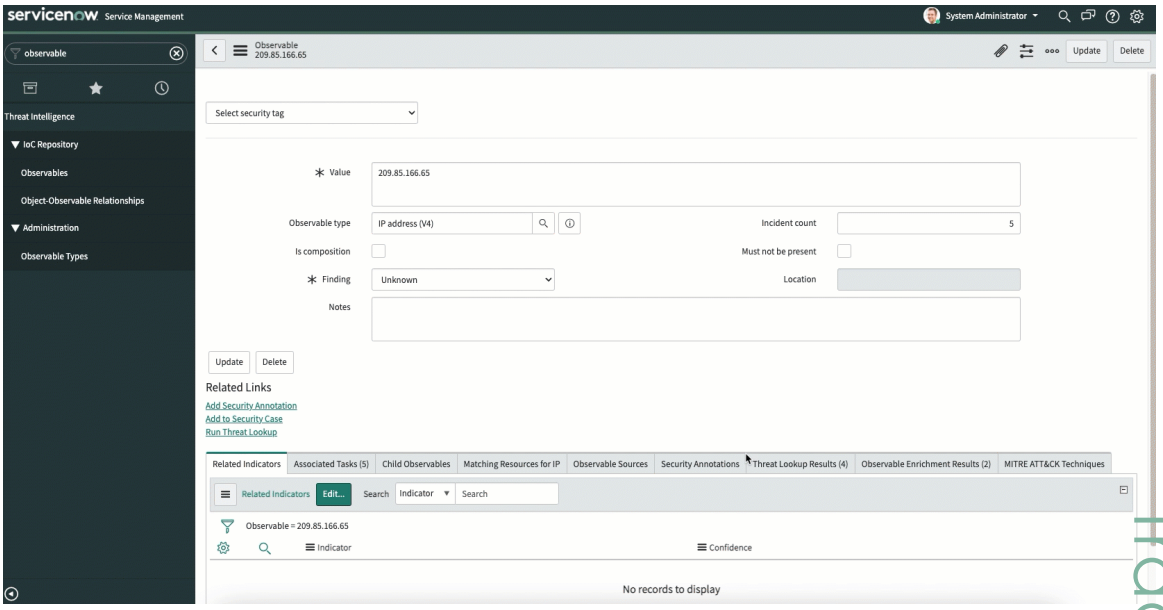
c. Localize **Resultados de pesquisa de ameaças recentes** na lista Disponível e mova-o para a lista Selecionada.

d. Clique em **Salvar**.

Tradução automática

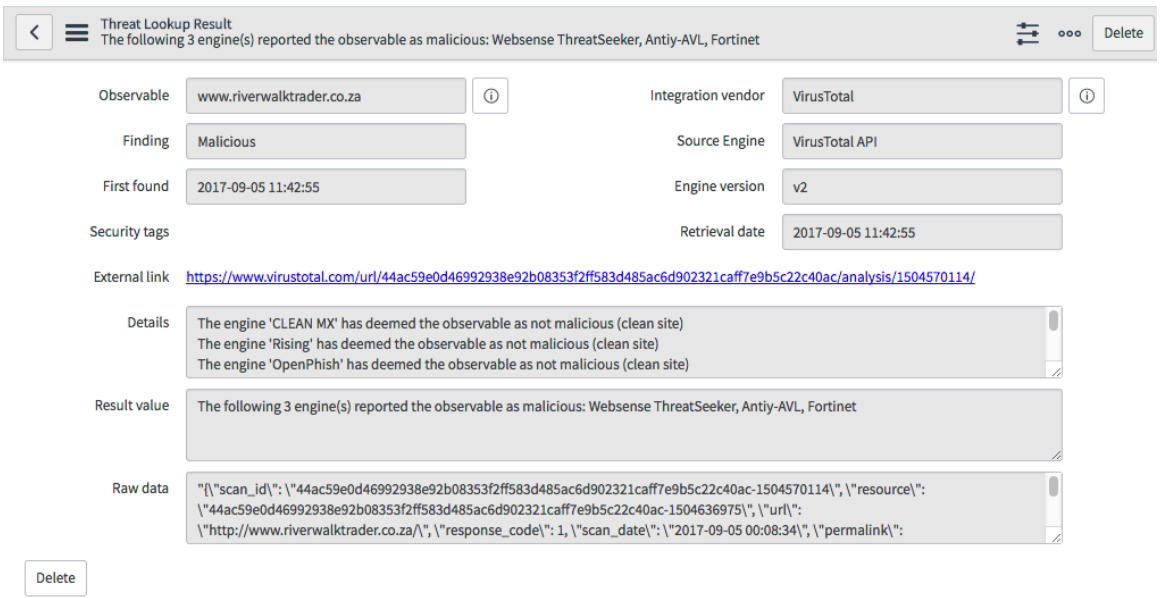
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Agora você pode exibir os resultados de pesquisa de ameaças recentes de cada fornecedor de integração na guia **Resultado de pesquisa de ameaças recentes**.



5. Para ver detalhes adicionais, incluindo resultados brutos de uma pesquisa específica, clique no **valor de Resultado**.

Nota: Quando as implementações VirusTotal ou OPSWAT Metadefender são usadas, os detalhes são consolidados, conforme mostrado abaixo.



Executar enriquecimento de ameaças em observáveis

Você pode executar o aprimoramento da inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações executadas dependem daquelas que você ativou.

Antes de Iniciar

Antes de executar o aprimoramento, você deve ativar o plug-in Inteligência contra ameaças. Você também deve instalar o plug-in para uma ou mais implementações de aprimoramento:

Tradução automática

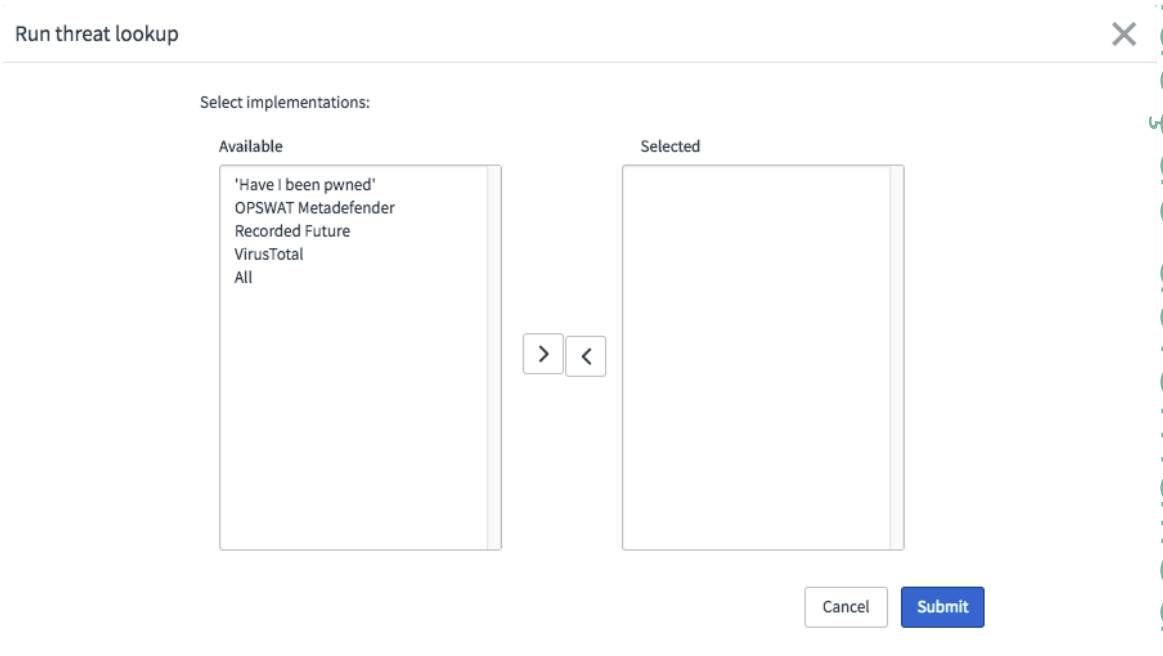
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração do CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Operações de segurança Já foi pwned?
- VirusTotal
- Quemé?

Função necessária: sn_ti.admin

Procedimento

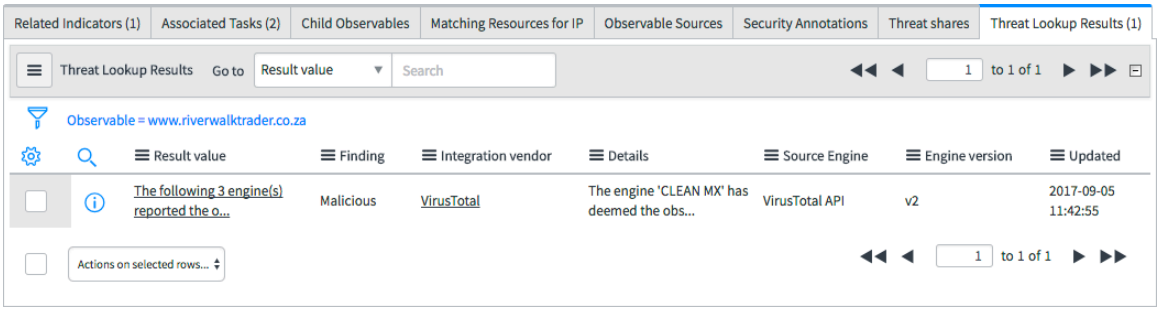
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Execute uma das seguintes etapas:
   - Para executar uma pesquisa em mais de um observável, selecione os observáveis, clique **em Ações nas linhas selecionadas**e selecione **Executar pesquisa de ameaças**.
   - Para executar uma pesquisa em um único observável, abra o registro do observável e clique no link relacionado **Executar pesquisa de ameaças**.



3. Selecione as implementações de pesquisa de ameaças que você deseja usar ou selecione **Todas** para executar pesquisas usando todas as implementações ativas e clique em **Enviar**.
   Uma mensagem indica que as pesquisas de ameaças foram iniciadas. O Integração de Operações de segurança - Fluxo de trabalho de pesquisa de ameaças executa e também executa os fluxos de trabalho de implementação das implementações de pesquisa de ameaças selecionadas. As pesquisas são realizadas e os resultados são gerados.
4. Quando as pesquisas forem concluídas, você poderá clicar na guia **Resultados da pesquisa de ameaças** para exibir os resultados.

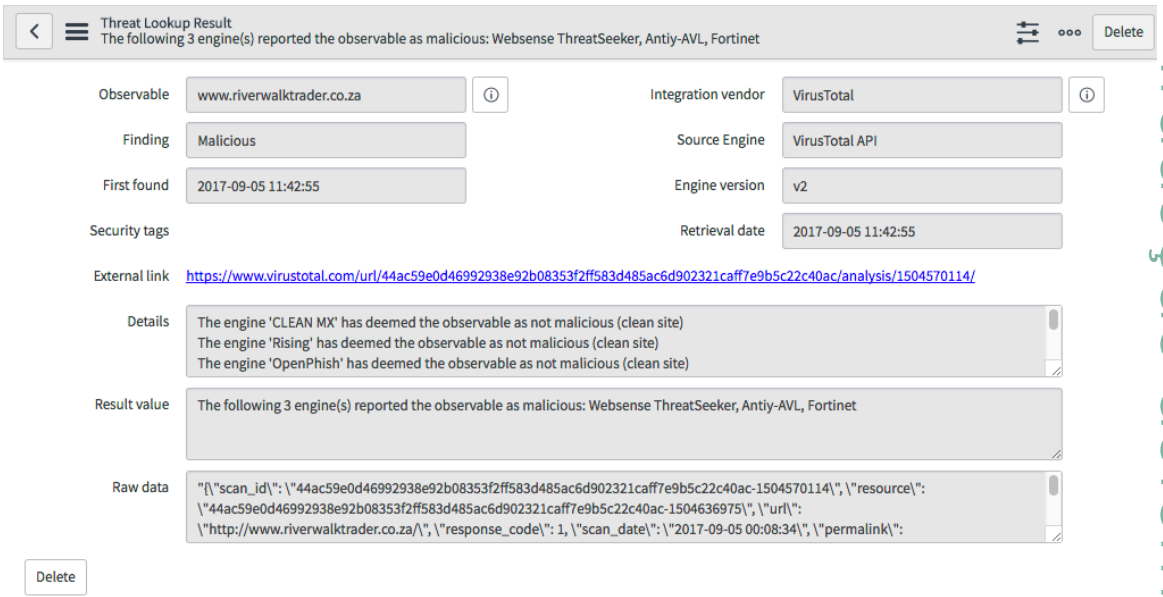
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para ver detalhes adicionais, incluindo resultados brutos de uma pesquisa específica, clique no **valor de Resultado**.

Nota: Quando as implementações VirusTotal ou OPSWAT Metadefender são usadas, os detalhes são consolidados, conforme mostrado abaixo.



Padrões de ataque

Padrões de ataque são um tipo de Táticas, técnicas e procedimentos (TTPs) que descrevem os métodos que os adversários tentam para comprometer os alvos. Os Padrões de ataque se aplicam ao STIX 2.x.

Padrões de ataque são usados para ajudar a categorizar os ataques. Eles generalizam ataques específicos para os padrões que seguem e fornecem informações detalhadas sobre como os ataques são realizados.

Por exemplo, o Spear Phishing é um tipo comum de ataque em que um invasor envia uma mensagem de e-mail cuidadosamente criada para uma parte com a intenção de fazer com que ela clique em um link ou abra um anexo para entregar malware. Os Padrões de ataque são mais específicos, como Spear Phishing por um agente de ameaça específico (exemplo - que o destino venceu uma contestação) também pode ser um padrão de ataque.

Definir um padrão de ataque

Defina um padrão de ataque para ajudar a categorizar os ataques.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Padrões de ataque**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Insira uma descrição do padrão de ataque.
Aliases	Nomes alternativos para identificar este padrão de ataque.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois
Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao padrão de ataque.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

Campanhas

Uma campanha é um agrupamento de comportamentos adversários. Esses comportamentos descrevem um conjunto de atividades ou ataques mal-intencionados que ocorrem ao longo do tempo contra um conjunto específico de destinos. As campanhas se aplicam ao STIX 2.x.

As campanhas geralmente têm objetivos bem definidos e podem fazer parte de um conjunto de intrusão.

As campanhas geralmente são atribuídas a um conjunto de intrusão e agentes de ameaça. Os agentes da ameaça podem reutilizar a infraestrutura conhecida do conjunto de intrusão ou podem configurar uma nova infraestrutura específica para conduzir essa campanha.

As campanhas têm um objetivo comum nos incidentes que causam, nas pessoas ou nos recursos que atingem e nos recursos que usam.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, um sindicato do crime ataque os executivos do ACME Bank. Eles usam uma variante específica de malware e novos servidores para obter informações secretas sobre uma futura fusão com outro banco.

Definir uma campanha

Defina uma campanha para agrupar comportamentos adversários.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Campanhas**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para esta campanha.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a campanha. Isso inclui sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta campanha.
Objetivo	O objetivo primário, objetivo, resultado desejado ou efeito pretendido da campanha. O que o agente da ameaça ou o conjunto de intrusão espera realizar com esta campanha.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à campanha.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Linhas de ação

Um curso de ação é uma ação realizada para impedir um ataque ou para responder a um ataque que está em andamento. O curso de ação se aplica ao STIX 2.x.

O curso de ações descreve respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls). Também pode descrever ações de nível superior, como treinamento de funcionários ou mudanças de política.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, um curso de ação para atenuar uma vulnerabilidade pode descrever a aplicação do patch que a corrige.

Definir um curso de ação

Defina um curso de ação para impedir um ataque ou responder a um ataque que está em andamento.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Linha de ação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para este curso de ação.
Ação	Para capturar cursos de ação estruturados ou automatizados.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o curso de ação, incluindo potencialmente sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao curso de ação.

Links relacionados	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados	Descrição
	é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Identidades

As identidades representam indivíduos, organizações ou grupos reais (ACME, Inc.) e classes de indivíduos, sistemas ou grupos (o setor financeiro). As identidades se aplicam ao STIX 2.x.

O SDO de identidade pode capturar informações básicas de identificação, informações de contato e os setores aos quais a identidade pertence. A identidade representa alvos de ataques, fontes de informações, criadores de objetos e identidades de agentes de ameaças.

Definir identidades

Defina identidades que representam indivíduos, organizações ou grupos reais.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Identidades**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para esta identidade. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Classe da identidade	O tipo de entidade que esta identidade descreve.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por exemplo, indivíduo ou organização.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a identidade, incluindo potencialmente sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Infraestrutura

O SDO de infraestrutura representa um tipo de táticas, técnicas e procedimentos (TTPs). Eles descrevem todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque. A infraestrutura se aplica ao STIX 2.x.

Os elementos de um ataque são representados por outros SDOs ou SCOs. No entanto, o SDO de infraestrutura representa um grupo nomeado de dados que constitui a infraestrutura.

Exemplos de infraestrutura incluem servidores C2 usados em um ataque, um dispositivo ou um servidor que faz parte de uma defesa ou servidores de banco de dados direcionados por um ataque.

Definir infraestrutura

Defina uma infraestrutura que são quaisquer sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Infraestrutura**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a infraestrutura.
Visto pela primeira vez	A hora em que esta infraestrutura foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta infraestrutura foi vista pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a infraestrutura, incluindo potencialmente sua finalidade, como ela está sendo usada, como ela se relaciona com outras atividades de inteligência capturadas em objetos relacionados e suas principais características.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aliases	Nomes alternativos para identificar esta infraestrutura.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais. Você também pode associar outros objetos à infraestrutura.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Observáveis Associados	Lista os observáveis associados a este objeto.
Infraestrutura associada	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Malware	Lista o código malicioso associado a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Conjunto de intrusão

Um conjunto de intrusão é um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns. Um conjunto de intrusão geralmente envolve uma única organização. O conjunto de intrusão se aplica ao STIX 2.x.

Um conjunto de intrusão pode capturar várias campanhas ou outras atividades. Essas atividades compartilham atributos que indicam um agente de ameaça comumente conhecido ou desconhecido.

A nova atividade pode ser atribuída a um conjunto de intrusão, mesmo se os agentes da ameaça por trás do ataque não forem conhecidos. Os agentes da ameaça podem passar de oferecer suporte a um conjunto de intrusão para oferecer suporte a outro ou podem oferecer suporte a vários conjuntos de intrusão.

Um conjunto de intrusão é o pacote de ataque inteiro e pode ser usado por um longo período em várias campanhas para atingir potencialmente várias finalidades.

Definir um conjunto de intrusão

Defina um conjunto de intrusão que é um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Conjunto de intrusão**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar o conjunto de intrusão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Visto pela primeira vez	A hora em que este conjunto de intrusão foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este conjunto de intrusão foi visto pela última vez executando atividades mal-intencionadas.
Motivação primária	O principal motivo, motivação ou finalidade por trás deste conjunto de intrusão. A motivação é o motivo pelo qual o Conjunto de Intrusão deseja atingir o objetivo (o que eles estão tentando alcançar). Por exemplo, uma intrusão definida com o objetivo de interromper o setor financeiro de um país pode ser motivada por um sentimento ideológico de aversão ao capital.
Nível de recurso	Esta propriedade especifica o nível organizacional no qual este conjunto de intrusão normalmente funciona, o que por sua vez determina os recursos disponíveis para uso em um ataque.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar este conjunto de intrusão.
Objetivos	Os objetivos de alto nível deste conjunto de intrusão, ou seja, o que eles estão tentando fazer. Por exemplo, eles podem ter a motivação de obter ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito. Para fazer isso, eles podem executar campanhas específicas que tenham objetivos detalhados, como comprometer os sistemas de ponto de venda em um grande varejo.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao conjunto de intrusão.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Motivações de ataque associadas	Lista todas as motivações secundárias pelas quais este conjunto de intrusão deseja alcançar.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Locais

Um local representa uma localização geográfica. Os locais são usados principalmente para fornecer contexto a outros SDOs. Os locais se aplicam ao STIX 2.x.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O local pode conter alguns ou todos os seguintes elementos: região (América do Norte), endereço cívico (Nova York, EUA), latitude e longitude.

O SDO do local pode estar relacionado a uma identidade ou conjunto de intrusão para indicar que a identidade ou o conjunto de intrusão está nesse local. Também pode estar relacionado a um malware ou padrão de ataque para indicar que a vítima está em um local específico.

Por exemplo, um Local pode ser usado em um relacionamento para descrever que o conjunto de intrusão Bourgeois Swallow se origina da Europa Oriental.

Pelo menos uma das seguintes propriedades ou conjuntos de propriedades deve ser fornecido:

- região
- país
- latitude e longitude

Definir local

Defina uma localização geográfica para fornecer mais contexto a outros SDOs.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Locais**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar o local.
Endereço	O endereço que este local descreve. Esta propriedade inclui todos os aspectos ou partes do endereço.
Cidade	A cidade em que este local está.
CEP	O código postal em que este local está.
Região	A região em que este local está.
País	O país em que este local está.
Latitude	A latitude do local em graus decimais. Números positivos descrevem latitudes ao norte do equador e números negativos descrevem latitudes ao sul do equador. O valor desta propriedade deve ser de -90,0 a 90,0, respectivamente.
Longitude	A longitude do local em graus decimais. Números positivos descrevem longitudes a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	leste do meridiano principal e números negativos descrevem longitudes a oeste do meridiano principal. O valor desta propriedade deve ser de -180,0 a 180,0, inclusive.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao local.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Malware

Malware é um tipo de TTP que representa código mal-intencionado. Refere-se a um programa que é inserido secretamente em um sistema. O malware se aplica ao STIX 2.x.

A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

O Malware SDO caracteriza, identifica e categoriza instâncias e famílias de malware a partir de dados derivados da análise. Este SDO captura informações detalhadas sobre como o malware funciona e o que ele faz.

Definir um malware

Defina um malware que representa um código mal-intencionado.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Malware**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome para identificar a instância ou família de malware, conforme especificado pelo produtor do SDO. Para uma família de malware, o nome deve ser definido.
Visto pela primeira vez	A hora em que esta instância ou família de malware foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta instância ou família de malware foi vista pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a instância ou família de malware, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta instância ou família de malware.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
É família	Especifica se o objeto representa uma família de malware ou uma instância de malware.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Capacidades associadas	Lista as capacidades identificadas e associadas a este objeto.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Observáveis Associados	Lista os observáveis associados a este objeto.
Malware associado	Lista o malware associado identificado com este objeto.
Sistemas operacionais associados	Os sistemas operacionais nos quais o objeto é executável. Isso se aplica a sistemas operacionais virtualizados, bem como aos que são executados em Bare Metal.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Análise de malware	Lista os registros de análise de malware associados a este objeto.
Observáveis relatados	Lista os observáveis relatados como parte deste objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Análise de malware

A análise de malware captura os metadados e os resultados de um malware. A análise de malware se aplica ao STIX 2.x.

A análise de malware inclui a análise estática ou dinâmica realizada em uma instância ou família de malware.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir análise de malware

Defina a análise de malware que captura os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Análise de malware**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar o conjunto de intrusão.
Versão do mecanismo de análise	A versão do mecanismo de análise ou produto (incluindo mecanismos AV) que foi usada para executar a análise.
Versão da definição de análise	A versão das definições de análise usadas pela ferramenta de análise (incluindo ferramentas AV).
Análise iniciada	A data e a hora em que a análise de malware foi iniciada.
Análise finalizada	A data e a hora em que a análise de malware foi encerrada.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Resultado	O resultado da classificação conforme determinado pelo scanner ou pelo processo de análise da ferramenta.
Nome do resultado	O resultado da classificação ou o nome atribuído à instância de malware pela ferramenta de verificação.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre os objetos associados à análise de malware.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Malware associado	Lista o malware associado identificado com este objeto.
Observáveis relatados	Lista os observáveis relatados como parte deste objeto.
Software instalado	Lista qualquer software não padrão instalado no sistema operacional usado para a análise dinâmica da instância ou família de malware.

Dados observados

Os Dados observados transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os Objetos cibernéticos (SCOs) STIX. Os dados observados se aplicam ao STIX 2.x.

Dados observados capturam uma única observação de uma única entidade (arquivo, conexão de rede), bem como a agregação de várias observações de uma entidade.

Você pode usar os Dados observados sozinhos (sem relacionamentos) para transmitir dados brutos coletados de qualquer origem. As origens incluem relatórios de analistas, áreas restritas e ferramentas de detecção baseadas em host e rede.

Por exemplo, Dados observados podem capturar informações sobre um endereço IP, uma conexão de rede, um arquivo ou uma chave de registro. Dados observados não são uma asserção de inteligência, são simplesmente as informações brutas sem qualquer contexto para o que isso significa.

Definir dados observados

Defina os dados observados que transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os STIX Cyber-observable Objects (SCOs).

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Dados observados**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Observado pela primeira vez	A hora inicial em que os dados foram vistos.
Última observação	A última vez em que os dados foram vistos.
Contagem de observações	O número de vezes que cada objeto observável cibernético foi visto. O valor deve ser um número inteiro de 1 a 999,999,999.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos dados observados.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Observáveis Associados	Lista os observáveis associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.

Agentes da ameaça

Os agentes da ameaça são indivíduos, grupos ou organizações que agem com intenção mal-intencionada. Os agentes da ameaça se aplicam ao STIX 2.x.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um agente de ameaça não é um conjunto de intrusão, mas pode oferecer suporte ou ser afiliado a vários conjuntos de intrusão, grupos ou organizações ao longo do tempo.

Os agentes da ameaça usam seus recursos e os recursos de um conjunto de intrusão para conduzir ataques e executar campanhas contra metas.

Você pode identificar os agentes da ameaça por seus motivos, capacidades, objetivos, nível de sofisticação, atividades anteriores, recursos aos quais eles têm acesso e sua função na organização.

Definir agentes da ameaça

Defina os agentes de ameaça que são indivíduos, grupos ou organizações que agem com intenção mal-intencionada.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Agentes da ameaça**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome para identificar a instância ou família de malware, conforme especificado pelo produtor do SDO. Para uma família de malware, o nome deve ser definido.
Visto pela primeira vez	A hora em que esta instância ou família de malware foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta instância ou família de malware foi vista pela última vez executando atividades mal-intencionadas.
Motivação primária	O principal motivo, motivação ou finalidade por trás deste agente da ameaça. A motivação é o motivo pelo qual o agente da ameaça deseja atingir o objetivo (o que ele está tentando alcançar). Por exemplo, um agente de ameaça com o objetivo de interromper o setor financeiro de um país pode ser movido por um sentimento de aversão ideológica ao capital.
Nível de recurso	O nível organizacional no qual este agente de ameaça normalmente trabalha, que por sua vez determina os recursos disponíveis para este agente de ameaça para uso em um ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o agente da ameaça, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Uma lista de outros nomes para identificar este agente da ameaça.
Objetivos	Os objetivos de alto nível deste agente da ameaça, ou seja, o que ele está tentando fazer. Por exemplo, eles podem ter a motivação de obter ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agente da ameaça.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Funções associadas	Lista as funções associadas ao agente da ameaça.
Motivações de ataque associadas	Lista as motivações de ataque associadas ao agente da ameaça.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Agrupamentos de ameaças

Um objeto de agrupamentos de ameaças afirma explicitamente que os objetos STIX referenciados têm um contexto compartilhado. Os agrupamentos de ameaças se aplicam ao STIX 2.x.

Um objeto de Agrupamentos de ameaças representa um conjunto de dados que, após análise suficiente, se desenvolve para transmitir um relatório de incidente ou ameaça como um objeto de relatório STIX. Por exemplo, um agrupamento pode ser usado para caracterizar uma investigação em andamento sobre um evento ou incidente de segurança.

Um objeto de agrupamentos de ameaças também pode ser usado para declarar que os objetos STIX referenciados estão relacionados a um processo de análise em andamento. Por exemplo, um analista de ameaças pode colaborar com outras pessoas em sua comunidade de confiança para examinar uma série de campanhas e indicadores.

O SDO de agrupamento de ameaças contém uma lista de referências a SDOs, SCOs e SROs, junto com uma declaração explícita do contexto compartilhado pelo conteúdo, uma descrição textual e o nome do agrupamento.

Definir agrupamentos de ameaças

Defina agrupamentos de ameaças como objetos que têm um contexto compartilhado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Grupos de ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome para identificar o agrupamento de ameaças.
Contexto	Uma descrição do contexto específico compartilhado pelo conteúdo referenciado pelo agrupamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição resumida que fornece detalhes e contexto sobre o agrupamento. Isso inclui sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois
Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agrupamento de ameaças.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos agrupados	Lista objetos agrupados como parte do agrupamento de ameaças.
Indicadores Agrupados	Lista os indicadores agrupados como parte do agrupamento de ameaças.
Observáveis agrupados	Lista observáveis agrupados como parte do agrupamento de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de marcação

O objeto de definições de marcação representa uma marcação específica.

As marcações de dados representam restrições, permissões e outras orientações sobre como os dados podem ser usados e compartilhados.

Por exemplo, os dados podem ser compartilhados com a restrição de que não devem ser compartilhados novamente ou que devem ser criptografados em repouso.

No STIX, as marcações de dados são especificadas usando o objeto de definição de marcação. Essas definições são aplicadas a objetos STIX usando marcações de objeto e a propriedades individuais de objetos STIX por meio de marcações granulares.

Definir definições de marcação

Defina definições de marcação que representam uma marcação de dados específica.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Definições de marcação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Definição	Especifique o objeto de marcação (por exemplo, TLP) ou alguma outra definição de marcação que tenha sido definida.
Tipo de definição	Identifica o tipo de definição de marcação - declaração ou TLP (Traffic Light Protocol).
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à definição de marcação.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
	Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos marcados	Listas de objetos marcados com a definição de marcação.
Indicadores marcados	Listas de indicadores marcados com a definição de marcação.

Anotações de ameaças

Uma anotação de ameaça transmite um texto informativo para fornecer análises adicionais não contidas nos objetos STIX, objetos de definição de marcação ou objetos de conteúdo de idioma aos quais a anotação está relacionada. As anotações de ameaça se aplicam ao STIX 2.x.

Por exemplo, um analista pode adicionar uma anotação a um objeto de campanha criado por outra organização. A anotação pode indicar que eles viram publicações relacionadas a essa campanha em um fórum de hackers.

As anotações geralmente são criadas por analistas humanos e são compostas de texto orientado por humanos. Elas contêm uma propriedade extra para capturar o autor que criou a anotação.

Definir anotações de ameaça

Defina anotações de ameaça que transmitem informações para fornecer contexto ou análise adicional que não está disponível em objetos existentes.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Anotações de ameaça**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Resumo	Especifique um breve resumo do conteúdo da anotação.
Conteúdo	Especifica o conteúdo da anotação.
Autores	Especifica o nome do autor (por exemplo, um analista).
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados às anotações de ameaça.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos associados	Listas de objetos aos quais as anotações de ameaça se aplicam.
Indicadores associados	Listas de indicadores aos quais as anotações de ameaça se aplicam.
Observáveis Associados	Lista os observáveis associados a este objeto.

Opiniões sobre ameaças

Uma Opinião é uma avaliação da precisão das informações em um Objeto STIX produzida por uma entidade diferente. As opiniões sobre ameaças se aplicam ao STIX 2.x.

A propriedade de opinião captura o nível de acordo ou desacordo usando uma escala fixa. A escala fixa também oferece suporte a um mapeamento numérico para permitir operações estatísticas consistentes entre opiniões.

Por exemplo, um analista de uma organização consumidora pode dizer que "discorda totalmente" de um objeto de campanha e fornecer uma explicação sobre o motivo.

As opiniões são subjectivas e a especificação não aborda a melhor forma de as interpretar.

Os analistas humanos criam opiniões e são compostos por texto orientado por humanos. Eles contêm uma propriedade extra para capturar o autor que criou a opinião.

Definir opiniões sobre ameaças

Defina opiniões de ameaças como uma avaliação da precisão das informações em um objeto STIX.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Opiniões sobre ameaças**.
2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Opinião	A opinião do produtor sobre o objeto STIX.
Explicação	A explicação do produtor sobre a opinião.
Autores	Especifica o nome do autor (por exemplo, um analista).
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à opinião de ameaça.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos associados	Lista de objetos aos quais a opinião de ameaça se aplica.
Indicadores associados	Lista de indicadores aos quais a opinião de ameaça se aplica.
Observáveis Associados	Lista os observáveis associados a este objeto.

Relatórios de ameaças

Relatórios de ameaças são coleções de inteligência contra ameaças com foco em um ou mais tópicos. Os relatórios de ameaças se aplicam ao STIX 2.x.

Os relatórios de ameaças incluem a descrição de um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar inteligência de ameaças relacionada para que ela possa ser publicada como uma história abrangente de ameaças cibernéticas.

O SDO do relatório de ameaças contém uma lista de referências a objetos STIX junto com uma descrição textual e o nome do relatório.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir relatórios de ameaças

Defina relatórios de ameaças que descrevem um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relatórios de ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Especifique um nome para identificar o relatório de ameaças.
Publicado	A data em que este relatório foi publicado oficialmente pelo autor do relatório.
Descrição	Uma descrição que fornece informações adicionais e contexto sobre o relatório.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos relatórios de ameaças.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Objetos relatados	Lista de objetos relatados no relatório de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Indicadores relatados	Listas de indicadores relatados no relatório de ameaças.
Observáveis relatados	Listas de observáveis relatados no relatório de ameaças.

Detecções

As vistas indicam que um indicador ou objeto foi visto. Os objetos podem ser um malware, uma ferramenta, um agente de ameaça e assim por diante.

As detecções rastreiam quem e o que é o alvo, como os ataques são realizados e para rastrear tendências no comportamento de ataque.

O objeto de relacionamento de detecção contém propriedades extras não presentes nos objetos de relacionamento genéricos. Essas propriedades extras representam dados específicos para relacionamentos de detecção.

Por exemplo, uma contagem ou representação de quantas vezes algo foi visto.

A detecção é capturada como um relacionamento porque você não pode ter uma detecção a menos que tenha algo que tenha sido avistado.

- O que foi detectado, como malware, campanha ou outro SDO
- Quem o avistou e/ou onde foi avistado, representado como uma identidade
- O que foi visto em sistemas e redes, representado como dados observados

Definir detecções do indicador

Defina detecções que denotam que um indicador foi visto.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Avistamentos do indicador**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Indicador	Identifica o indicador. Pesquise e selecione o indicador.
Contagem	O número de vezes que o objeto foi visto.
Visto pela primeira vez	A hora em que este objeto foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este objeto foi visto pela última vez executando atividades mal-intencionadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a detecção do indicador, incluindo potencialmente sua finalidade e suas principais características.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
É resumo	
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à detecção do indicador.

Listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Identidades	Lista de identidades associadas a este objeto.
Dados observados	Lista os dados observados associados a este objeto.

Definir detecções de objeto

Defina a detecção de objeto que descreve que um objeto (malware, ferramenta, agente de ameaça e assim por diante) foi visto.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Detecções de objeto**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Objeto	Identifica o objeto. Pesquise e selecione o objeto.
Contagem	O número de vezes que o objeto foi visto.
Visto pela primeira vez	A hora em que este objeto foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este objeto foi visto pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a detecção do objeto, incluindo potencialmente sua finalidade e suas características principais.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
É resumo	
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à detecção de objeto.

Listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Identidades	Lista de identidades associadas a este objeto.
Dados observados	Lista os dados observados associados a este objeto.

Ferramentas

As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques. As ferramentas se aplicam ao STIX 2.x.

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Por exemplo, ferramentas de acesso remoto (RDP) e ferramentas de verificação de rede (Nmap) são ferramentas que um agente de ameaça usa durante um ataque.

Definir ferramentas

Defina ferramentas como software legítimo que é usado para executar ataques.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Ferramentas**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a ferramenta.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a ferramenta, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta ferramenta.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao objeto da ferramenta.

Links e Listas Relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.

Vulnerabilidades

Uma vulnerabilidade é uma fraqueza ou um defeito em um componente de software ou hardware que os invasores exploram. As vulnerabilidades se aplicam ao STIX 2.x.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A fraqueza ou defeito está nos requisitos, designs ou implementações do código encontrado em um componente de software ou hardware. Essa fraqueza é explorada diretamente para afetar negativamente a confidencialidade, a integridade ou a disponibilidade desse sistema.

CVE é uma lista de vulnerabilidades e exposições de segurança da informação que fornece nomes comuns para problemas conhecidos publicamente [CVE].

Por exemplo, se um malware explorar CVE-2015-12345, um objeto de malware poderá ser vinculado a um objeto de vulnerabilidade que faz referência a CVE-2015-12345.

Definir vulnerabilidades

Defina vulnerabilidade como uma fraqueza ou defeito em um componente de software ou hardware que os invasores exploram.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Vulnerabilidades**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Nome	Insira um nome descritivo para identificar a vulnerabilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a vulnerabilidade, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar esta ferramenta.
ID da origem	Identificador exclusivo para este objeto na origem da ameaça.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao objeto de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links e Listas Relacionadas	Descrição
Mostrar relacionamentos	Abre o Visualizador STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

Relacionamentos

Use os objetos de relacionamento para vincular dois SDOs ou Objetos cibernéticos (SCOs) STIX para descrever como eles se relacionam entre si.

Os objetos de relacionamento STIX (SROs) representam tipos de relacionamentos entre vários objetos STIX. Os seguintes objetos de relacionamento estão disponíveis:

- **Relacionamento objeto-objeto**: este objeto define relacionamentos entre SDOs, exceto o objeto de indicador. Um exemplo de um relacionamento definido por objeto-objeto é que um padrão de ataque entrega um malware.
- **Relacionamento entre objeto e indicador**: este objeto define os relacionamentos entre o objeto do indicador e outros SDOs. Um exemplo de um relacionamento definido por objeto-indicador é quando um indicador detecta evidências de uma campanha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Relacionamento objeto-observável**: este objeto define relacionamentos entre SDOs e o objeto observável (SCO). Um exemplo de um relacionamento definido de objeto-observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.

Relacionamentos de objeto STIX

Objeto de relacionamento	Origem de exemplo	Exemplo de destino	Descrição de exemplo
Relacionamentos objeto-objeto	Padrão de ataque	Malware	Este relacionamento descreve que este padrão de ataque é usado para entregar esta instância de malware (ou família).
Relacionamentos objeto-indicador	Indicador	Padrão de ataque, Campanha, Infraestrutura, Conjunto de intrusão, Malware, Agente de ameaça, Ferramenta	Esse relacionamento descreve que o indicador pode detectar evidências do padrão de ataque, campanha, infraestrutura, conjunto de intrusão, malware, agente de ameaça ou ferramenta relacionada. A evidência pode não ser direta. Por exemplo, o indicador pode detectar evidências secundárias da campanha, como malware que é comumente usado por essa campanha específica.
Relacionamentos objeto-observável	Infraestrutura	Dados observados	Este relacionamento descreve que o indicador é criado com base em informações de um objeto de dados observado. Um exemplo de um relacionamento definido de objeto-observável é que uma infraestrutura consiste em objetos observáveis

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos de objeto STIX

Objeto de relacionamento	Origem de exemplo	Exemplo de destino	Descrição de exemplo
			cibernéticos que fornecem informações de um possível ataque.

Definir relacionamentos objeto-objeto

Defina relacionamentos entre SDOs, exceto o objeto de indicador.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto de origem	Selecione e defina o objeto de origem.
Tipo de objeto de origem	Define o tipo de objeto de origem.
Objeto de destino	Selecione e defina o objeto de destino.
Tipo de objeto de destino	Define o tipo de objeto de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identifica exclusivamente o objeto de origem.

4. Clique em **Enviar**.

Definir relacionamentos objeto-indicador

Defina relacionamentos entre o objeto do indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos entre objeto e indicador**.
2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto	Selecione e defina o objeto.
Tipo	Especifica o tipo de objeto com base no objeto selecionado.
Indicador	Selecione os indicadores de comprometimento.
Direção do relacionamento	Defina a direção do relacionamento, seja direta ou inversa.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identifica exclusivamente o objeto de origem.

4. Clique em **Enviar**.

Definir relacionamentos objeto-observável

Defina relacionamentos entre SDOs e o objeto observável (SCO).

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-observável**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto	Selecione e defina o objeto de origem.
Tipo	Insira um nome descritivo para identificar o tipo de objeto.
Observável	Selecione e defina o observável.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
ID da origem	Identifica exclusivamente o objeto de origem.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizador de STIX

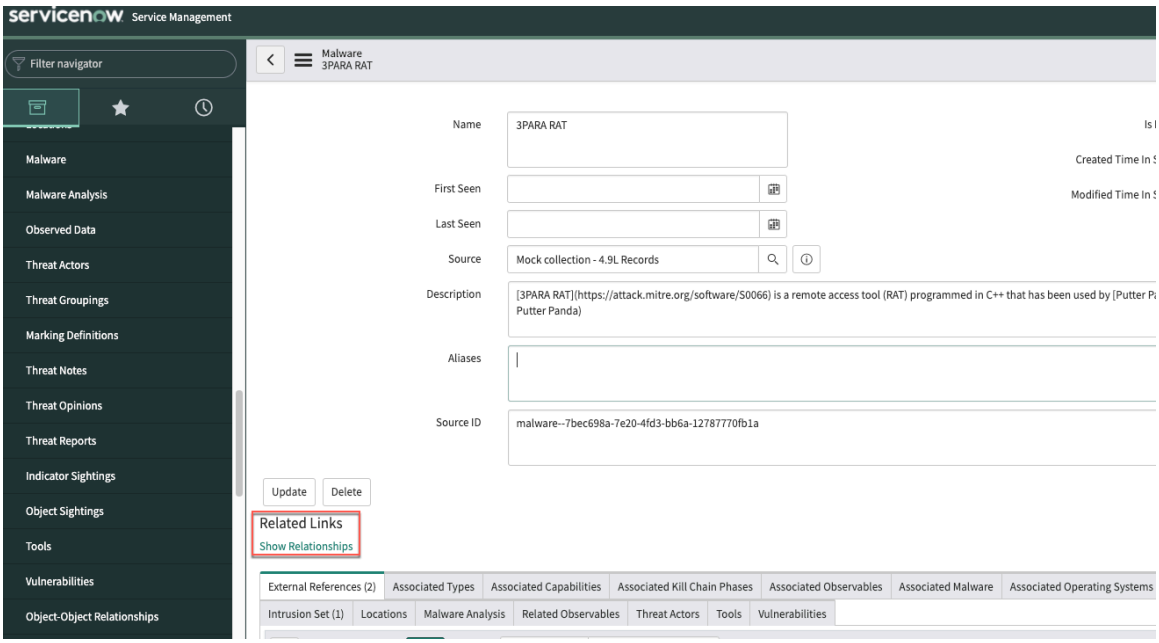
O STIX Visualizer representa visualmente a estrutura do objeto STIX e seu relacionamento.

Você pode obter mais informações sobre o objeto ou relacionamento selecionado no painel de detalhes.

O gráfico de relacionamento mostra os relacionamentos de um objeto e fornece contexto para você investigar. Você pode clicar em qualquer nó no gráfico para ver mais detalhes.

Nota: O Visualizador STIX está disponível para todos os SDOs, exceto os objetos Relatório e Dados observados.

Acessar Visualizador de STIX

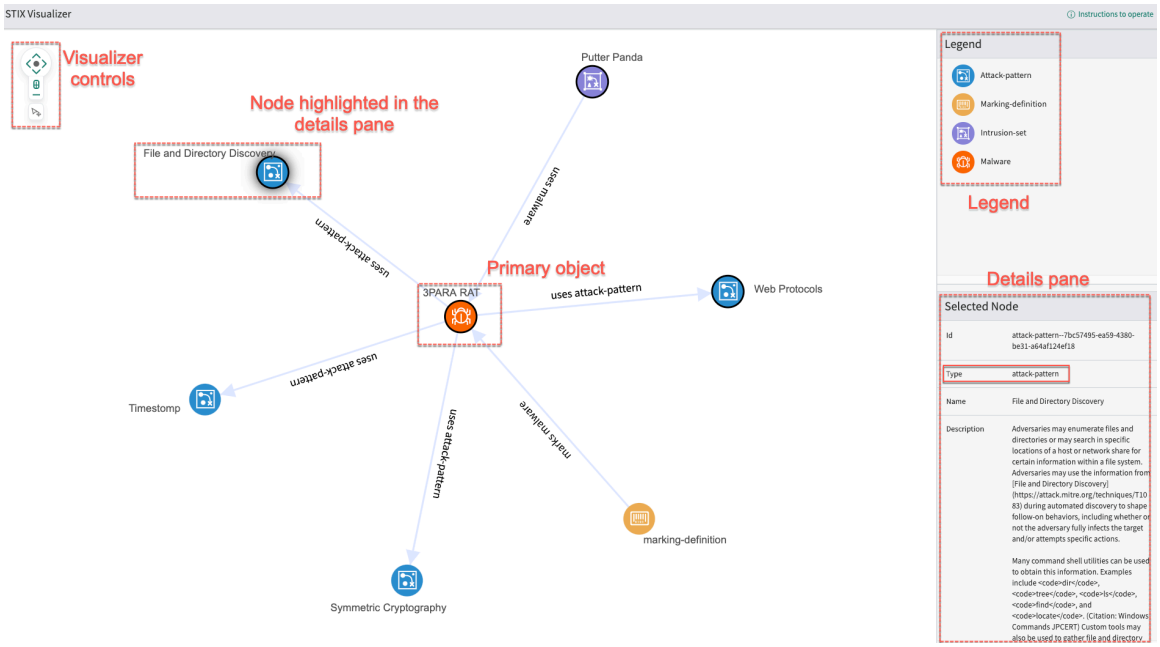


Clique em Mostrar relacionamentos na seção Links relacionados de qualquer um dos SDOs para exibir o Visualizador STIX.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir detalhes no visualizador do STIX



No Visualizador, você pode exibir o objeto e seu relacionamento, o que fornece contexto para você investigar mais. O Visualizador usa cores e ícones para ilustrar várias informações sobre os objetos.

Você pode ampliar um objeto, arrastar os nós ou fixá-los para enfocar um relacionamento específico.

Clique em qualquer objeto para abrir o painel de detalhes. No painel de detalhes, você pode obter mais informações associadas ao objeto.

MITRE-ATT&CK™ visão geral da estrutura

A estrutura MITRE-ATT&CK é uma base de conhecimento de táticas, técnicas e procedimentos comuns (TTP) que sua organização pode acessar para desenvolver modelos e metodologias de ameaças específicas contra ataques cibernéticos.

Visão geral

A estrutura MITRE de táticas, técnicas e conhecimento comum (ATT&CK) documenta e rastreia várias técnicas adversárias que são usadas durante diferentes fases de um ataque cibernético.

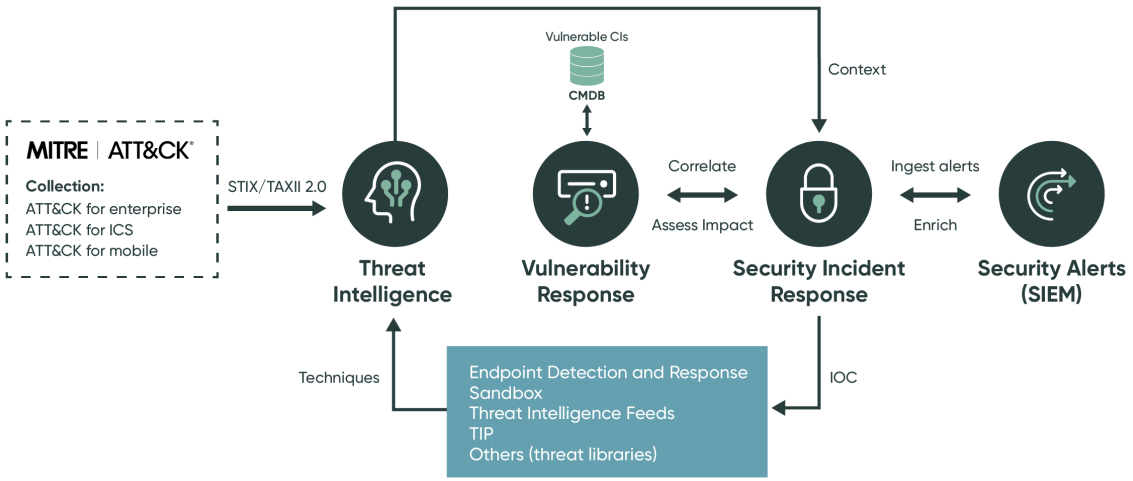
Ao usar a base de conhecimento da estrutura MITRE-ATT&CK, a comunidade de inteligência contra ameaças cibernéticas pode identificar rapidamente ameaças e coordenar respostas a ataques cibernéticos.

MITRE-ATT&CK e Operações de segurança

Consulte o diagrama a seguir para saber como as informações MITRE-ATT&CK fluem com aplicações Operações de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- O pré-carregado TAXII cliente se conecta ao servidor TAXII para ingerir as coletas de dados para Inteligência contra ameaças.
- As integrações existentes do Gerenciador de informações e eventos de segurança (SIEM) ingerem seus dados de ameaças (alertas e eventos), com TTPs relevantes e estão associadas a incidentes de segurança.
- Quando um IoC está associado a um incidente de segurança, Inteligência contra ameaças pesquisa automaticamente feeds de ameaças em busca de informações relevantes e envia IoCs para fontes de terceiros, como EDR, Sandbox ou TIP, para análise adicional.
- Se alguma origem de terceiros contiver as informações MITRE-ATT&CK, então Inteligência contra ameaças extrai as informações da técnica e aprimora os dados no repositório Inteligência contra ameaças para correlação e análise.
- MITRE-ATT&CK também compartilha informações de contexto de CVE para cada técnica. Sua equipe de segurança pode revisar as técnicas exploradas em Resposta a vulnerabilidades para determinar se seus ativos críticos para os negócios estão ameaçados.

MITRE-ATT&CK matrizes, táticas e técnicas

O núcleo da estrutura MITRE-ATT&CK é uma matriz de táticas e técnicas adversárias. A sequência das táticas representa o que um adversário está tentando realizar na fase de um incidente. Quando sua equipe de segurança entende essa sequência, você tem a oportunidade de antecipar o próximo movimento de um adversário e interromper a cadeia de eliminação. O ATT&CK consiste nas seguintes matrizes:

- Enterprise ATT&CK: descreve os comportamentos e ações que um adversário realiza para comprometer e operar em uma rede e nuvem corporativas.

  Nota: A matriz Pre ATT&CK foi descontinuada por MITRE e foi mesclada com a matriz Enterprise.

- ICS ATT&CK: descreve as ações que um adversário realiza enquanto opera em uma rede de Sistemas de controle industrial (ICS).
- Mobile ATT&CK: descreve os comportamentos e ações adversários que se concentram em dispositivos móveis.

As táticas representam o motivo de uma técnica ATT&CK. É o objetivo tático do adversário para executar uma ação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As técnicas representam como um adversário atinge um objetivo tático executando uma ação.

As técnicas podem ser associadas a mais de uma tática. Por exemplo, a manipulação de token de acesso é usada por um adversário para alcançar a tática de escalonamento de privilégios ou evasão de defesa.

Como usar uma abordagem baseada em intenção para respostas a incidentes

Uma resposta baseada em intenção usa uma estrutura de cadeia de eliminação dinâmica e contextual que pode ajudar sua organização a correlacionar incidentes de segurança e identificar um grande escopo de ataques. Sua equipe de segurança pode usar uma resposta baseada em intenção para entender como a organização está sendo ameaçada e o que o invasor pode fazer em seguida. Esse tipo de resposta permite prever o comportamento de um invasor para que você possa concentrar seus recursos com eficácia.

Usando Security Incident Response, sua equipe de segurança pode gerenciar o ciclo de vida de cada incidente de segurança, desde a análise até a contenção, concentrando-se em indicadores de comprometimento (IOCs), como endereços IP, hashes de arquivo e domínios.

Ao integrar Security Incident Response com a estrutura MITRE-ATT&CK, os incidentes de segurança são tratados como links em um ataque maior em toda a empresa.

Como sua organização pode se beneficiar de MITRE-ATT&CK em Operações de segurança

O uso da estrutura MITRE-ATT&CK pode ajudar sua organização a fazer o seguinte:

- Equipe os analistas de segurança com MITRE-ATT&CK táticas, técnicas e procedimentos (TTPs) para analisar e responder melhor aos incidentes de segurança.
- Automatize os fluxos de trabalho de incidentes usando o playbook para detectar e conter ameaças no contexto da estrutura MITRE-ATT&CK.
- Priorize indicadores de comprometimento e caça a ameaças com informações de MITRE-ATT&CK.
- Entenda a postura de segurança de alto nível da sua organização no contexto da estrutura MITRE-ATT&CK.

Administração do MITRE-ATT&CK

Você pode configurar, mapear fontes de dados, mapear a cobertura geral de detecção de técnica e manter o repositório MITRE-ATT&CK no Now Platform.

Introdução à estrutura MITRE-ATT&CK

Revise as informações a seguir antes de começar a configurar sua estrutura MITRE-ATT&CK.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform, Inteligência contra ameaçase Security Incident Response necessárias.	Estas funções são usadas nos recursos do MITRE-ATT&CK: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui as funções de administrador de incidentes de segurança (sn_si.admin) e administrador de inteligência contra ameaças (sn_ti.admin). • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.mitre_analyst — A função de analista MITRE foi introduzida para permitir a navegação cruzada dos recursos MITRE entre Security Incident Response e o suporte comum a Inteligência contra ameaças. Com esta função, você pode exibir o módulo Inteligência contra ameaças MITRE e o módulo Security Incident Response no modo somente leitura. • sn_si.read Para obter mais informações, consulte Configuração da Inteligência contra ameaças.
Verifique se as aplicações principais ServiceNow que são necessárias para oferecer suporte ao módulo MITRE-ATT&CK estão instaladas e ativadas.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas. • Threat Intelligence Support Common UI Components (sn_ti_seismic) - Versão 1.0 ou superior • Threat Intelligence Support Common - Versão 12.0 ou superior • Inteligência contra ameaças - Versão 12.0 ou superior • Security Incident Response - Versão 12.0 ou superior

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte obter direito de um produto ou aplicação das Operações de segurança e ativar uma aplicação da ServiceNow Store.
Domain Separation	Verifique a seção Domain Separation se você pretende separar dados, processos e tarefas administrativas.

Entenda o modelo de dados MITRE a STIX

Revise a terminologia usada por MITRE e STIX para usar e entender com eficiência a estrutura MITRE-ATT&CK™ no Now Platform.

MITRE objetos para STIX mapeamento

STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. O modelo de dados primário no módulo Inteligência contra ameaças são os objetos STIX. Enquanto os objetos MITRE são um subconjunto do modelo de dados primário STIX. Na estrutura MITRE-ATT&CK, MITRE fornece informações STIX] semelhantes com determinados rótulos e objetos.

MITRE para STIX mapeamento de objeto

Terminologia MITRE	**Terminologia** STIX
Técnica	Padrão de ataque
Mitigação	Linha de ação
Grupos	Conjuntos de intrusão
Malware	Malware
Ferramenta	Ferramenta

Estendendo dados no módulo Inteligência contra ameaças

Você pode manter uma lista de Inteligência contra ameaças origens de ameaças e importar os dados STIX necessários, que incluem um amplo conjunto de informações sobre ameaças cibernéticas. Você também pode usar os perfis TAXII para facilitar a troca automatizada de informações sobre ameaças cibernéticas.

Nota: Para obter mais informações, consulte definir uma origem de ameaça e criar um perfil TAXII.

Estendendo dados no módulo MITRE-ATT&CK

Você pode estender os objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica no repositório MITRE-ATT&CK.

Você pode criar um objeto e estabelecer um relacionamento entre uma técnica e o novo objeto no módulo Repositório do MITRE ATT&CK, mas não pode definir o tipo de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

relacionamento neste módulo. Para definir um tipo de relacionamento, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Se você mapear o tipo de relacionamento entre uma técnica existente e um objeto existente, deverá definir a técnica como o objeto de destino e o objeto como o objeto de origem. Para fazer isso, navegue até o **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Você pode criar um grupo e associá-lo a um padrão de ataque, mas no repositório do MITRE ATT&CK, você só pode estabelecer o relacionamento entre o grupo e o padrão de ataque. Para definir o tipo de relacionamento objeto a objeto, você deve fazer isso no Repositório de IoC.

Nota: Para obter mais informações, consulte estender MITRE-ATT&CK dados e repositório de IoC.

Domain Separation e MITRE-ATT&CK

Esta visão geral do Domain Separation pertence a MITRE-ATT&CK. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico.

Como o Domain Separation funciona com MITRE-ATT&CK

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com as funções sn_ti.admin necessárias no respectivo domínio.
- Replique o seguinte para cada domínio:
  - TAXII Coleções

    Nota:

    - Não ative as coleções no domínio global. Ative somente as coleções que estão replicadas e disponíveis em seu domínio.
    - Altere o campo **Executar como** nas coleções para o usuário com a função sn_ti.admin no respectivo domínio.

  - Definição de cobertura da técnica
  - Regra de extração da técnica
  - Regras de detecção – Mapeamentos do MITRE ATT&CK
  - Cobertura de mitigação
    - Copie todos os registros de definição de cobertura de mitigação.
    - Copie a calculadora de redução de cobertura ou crie uma nova calculadora para o respectivo domínio.
  - Grupo de ameaças - Definições do mapa térmico da técnica

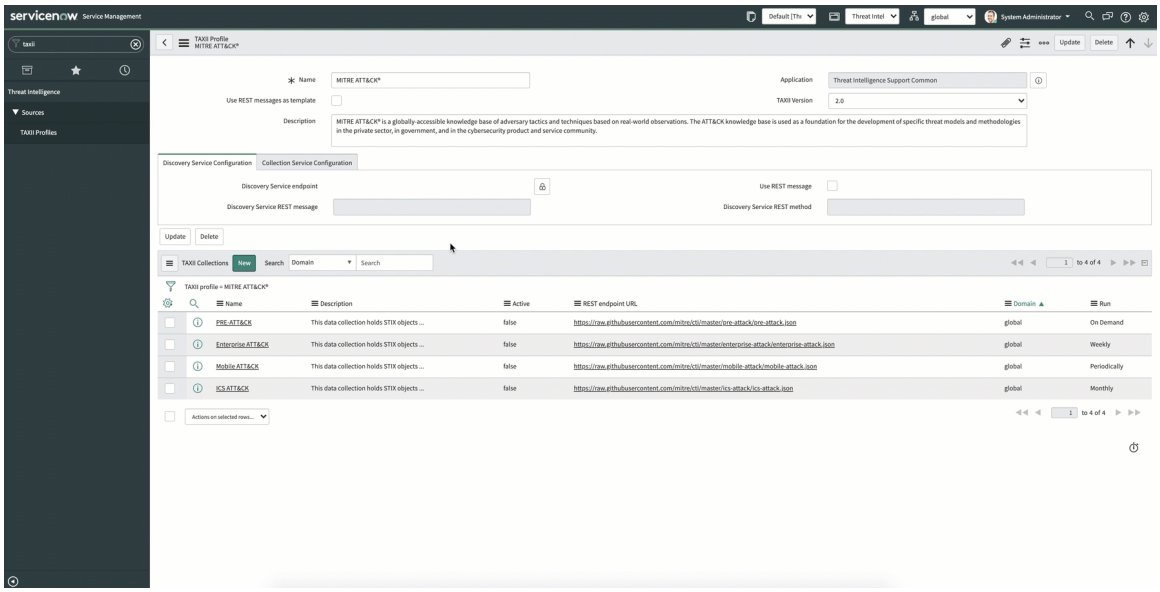
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Replicar coleta TAXII

1. Navegar até **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
2. Na barra de cabeçalho, use o seletor de domínio para selecionar seu domínio.
3. Selecione a coleção TAXII relevante para sua organização (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).
4. Clique com o botão direito do mouse na barra de cabeçalho e selecione **Inserir e permanecer**. A coleção TAXII duplicada é criada no domínio selecionado
5. Navegue de volta para o perfil TAXII do MITRE ATT&CK para exibir a coleção TAXII duplicada.

A ilustração a seguir mostra como selecionar o domínio TOP/Initech, replicar a coleção TAXII no domínio e verificar a coleção TAXII replicada.



Configurar a estrutura MITRE-ATT&CK™

Ative o perfil MITRE-ATT&CK e configure um trabalho agendado para que você possa configurar coleções MITRE-ATT&CK para detecção de ameaças em sua organização.

Antes de Iniciar

Função necessária: sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

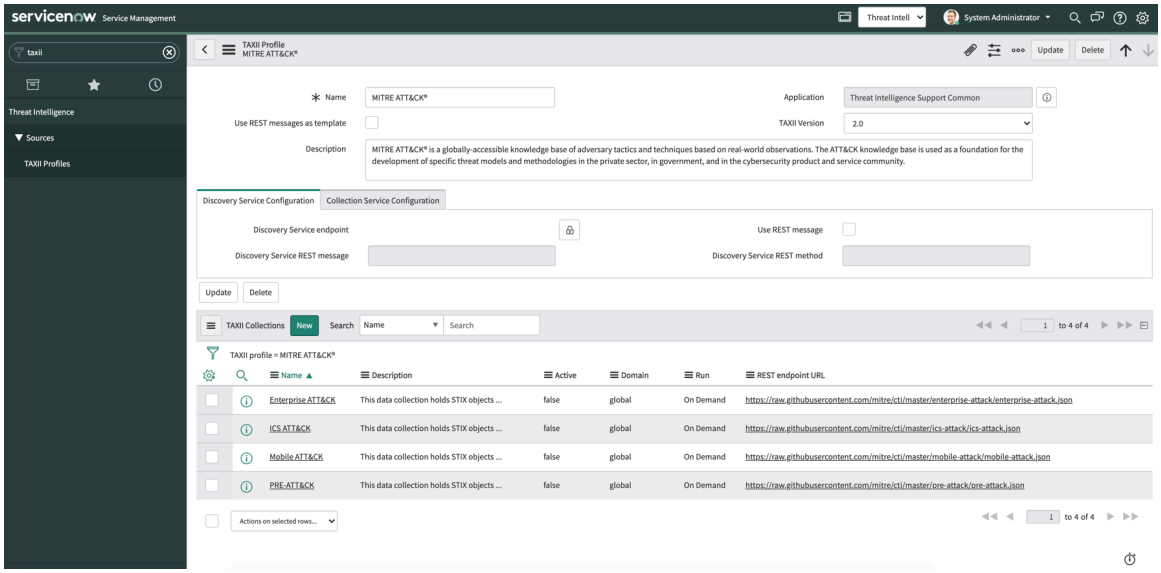
A Expressão de Informações de Ameaças Estruturadas (STIX™) é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. Usando dados STIX e perfis de Troca automatizada confiável de informações do indicador (TAXII™), as equipes de segurança podem usar informações compartilhadas de ameaças cibernéticas para isolar ameaças que foram identificadas anteriormente por sua empresa e de outras origens.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
   Você verá os perfis TAXII disponíveis.
2. Clique no perfil do **MITRE ATT&CK** fornecido com o sistema de base.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para ativar a coleção TAXII, defina a opção **Ativo** como verdadeira para a coleção TAXII que é relevante para sua organização (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).

Coleta TAXII	Descrição
Enterprise ATT&CK	Descreve os comportamentos e ações que um adversário realiza para comprometer e operar em uma rede e nuvem corporativas. **Nota:** A matriz Pre ATT&CK foi descontinuada por MITRE e foi mesclada com a matriz Enterprise.
ATT&CK móvel	Descreve os comportamentos e ações adversários que se concentram em dispositivos móveis.
ICS ATT&CK	Descreve as ações que um adversário realiza enquanto opera em uma rede de Sistemas de controle industrial (ICS).

4. Para atualizar periodicamente a coleção, defina a opção **Executar** conforme apropriado para sua organização.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, essa opção é definida como Sob demanda.

Nota:

a. As coleções são empacotadas como parte do plug-in Inteligência contra ameaças Core. Instalar ou atualizar o Threat Intelligence Support Common - Versão 12.0 ou superior e Threat Intelligence - Versão 12.0 ou superior garante que os dados de coleta sejam preenchidos automaticamente.

b. Ative a coleção TAXII somente para a coleção que você pretende usar em sua organização e desabilite as outras coleções. Por exemplo, se você pretende usar a matriz Enterprise ATT&CK, ative o Enterprise ATT&CK no nível de coleção TAXII e no nível de matrizes. Desabilite as outras matrizes Mobile ATT&CK e ICS ATT&CK na coleção TAXII e no nível Matrizes.

c. Nas listas relacionadas TAXII Coleções, se você selecionar a opção Executar como Diariamente, ocorrerá um erro e o padrão da opção será Sob demanda. Este erro ocorre porque a programação da atualização de dados MITRE-ATT&CK diária é restrita para otimizar a carga nos servidores MITRE. Além disso, MITRE atualiza os dados do ATT&CK apenas duas vezes por ano.

d. As coleções TAXII não são atualizadas a menos que você ative a coleção TAXII.

e. As atualizações das coleções existentes podem ser recuperadas do servidor MITRE, programando a frequência de "execução" em cada coleção.

f. As personalizações que você faz nos dados do repositório MITRE-ATT&CK (Malware, Grupo, Mitigação e Objetos de ferramenta para uma técnica) são salvas durante as atualizações programadas.

g. MITRE atualiza a MITRE-ATT&CK base de conhecimento em que alguns objetos são identificados como revogados ou descontinuados, novos objetos são adicionados ou objetos existentes são modificados. Se MITRE revogar qualquer tática ou técnica, esses objetos serão marcados como revogados no Now Platform. Os objetos revogados são mantidos no repositório, mas não estão disponíveis para uso no Now Platform.

O que Fazer Depois

Depois que a configuração do perfil TAXII é concluída, os dados do repositório MITRE-ATT&CK são importados em intervalos regulares para o Now Platform®. Você pode ver esses dados navegando até **Repositório do MITRE ATT&CK** > **Matrizes** e **Repositório do MITRE ATT&CK** > **Técnicas**.

Gerenciar matrizes

Gerencie as matrizes que foram importadas das coleções MITRE TAXII. Matrizes são uma coleção de táticas e técnicas. Você pode exibir as matrizes para revisar se suas coleções estão disponíveis no repositório MITRE-ATT&CK.

Antes de Iniciar

Nota: Revise e verifique se somente a matriz que você pretende usar em sua organização está definida como ativa e desabilite as outras matrizes. Por exemplo, se você pretende usar a matriz Enterprise ATT&CK, a matriz Enterprise ATT&CK será ativada no nível de coleta TAXII e no nível de matrizes. Desabilite as outras matrizes Mobile ATT&CK e ICS ATT&CK na coleção TAXII e no nível Matrizes.

Função necessária:

Tradução automática

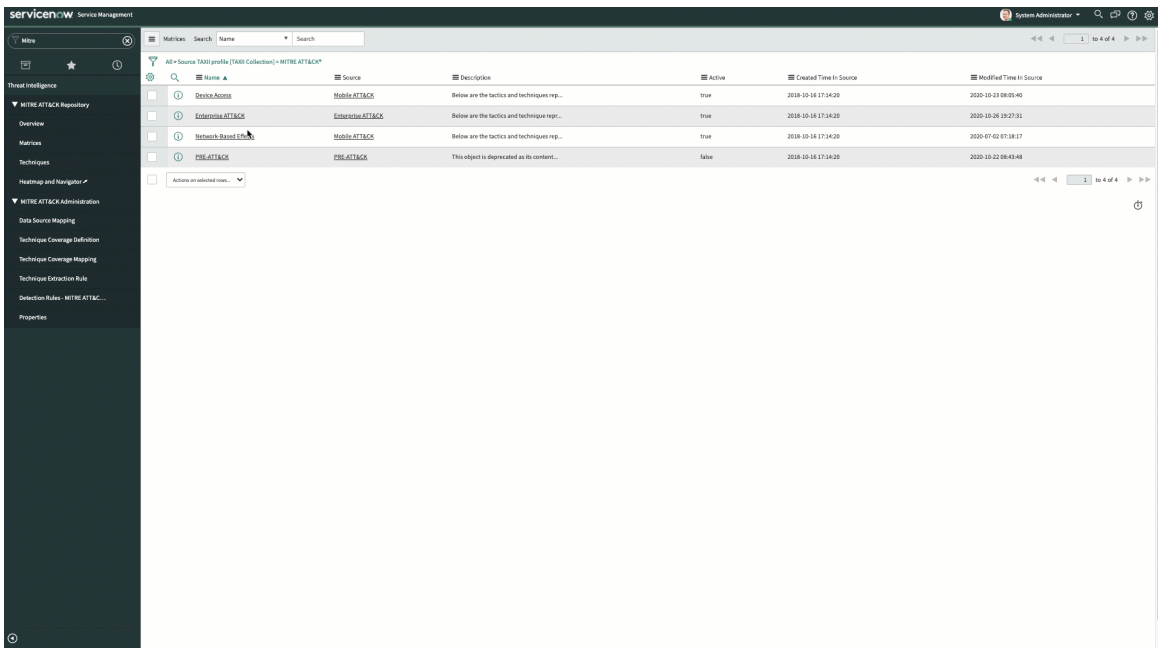
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Matrizes**.
   Todas as matrizes estão desabilitadas por padrão.
2. Para ativar uma matriz, aponte para **Ativo**, clique duas vezes e selecione **verdadeiro**.
3. Para exibir todas as informações associadas, clique em uma matriz.
4. Para exibir todas as táticas associadas a esta coleção, clique na guia **Táticas do MITRE**.
5. Para exibir detalhes adicionais e as técnicas associadas a uma tática selecionada, clique em uma tática.
6. Na guia **Técnicas do MITRE ATT&CK**, selecione uma técnica.
7. Nas listas relacionadas, exiba as associações que estão disponíveis para a técnica selecionada.

   Na ilustração a seguir, você pode ver o caminho de navegação da matriz Enterprise ATT&CK até a tática de acesso inicial (TA0001) e, em seguida, até a técnica de phishing (T1566). Na página Padrão de ataque - Técnica de phishing, você pode exibir a lista relacionada - Tática, Subtécnica, Grupo, Mitigação, Referências externas, Malware e Ferramentas.



O que Fazer Depois

Você pode estender as informações em alguns desses objetos de lista relacionados com base na técnica selecionada. Por exemplo, você pode adicionar novas informações para Grupo, Mitigação, Referências externas, Malware e Ferramentas.

Gerenciar técnicas

Gerencie as técnicas que foram importadas das coleções MITRE TAXII. As técnicas contêm várias maneiras que os invasores desenvolveram para empregar uma determinada tática.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode revisar e desativar técnicas que não são relevantes para sua organização. Em STIX, as técnicas são conhecidas como padrões de ataque.

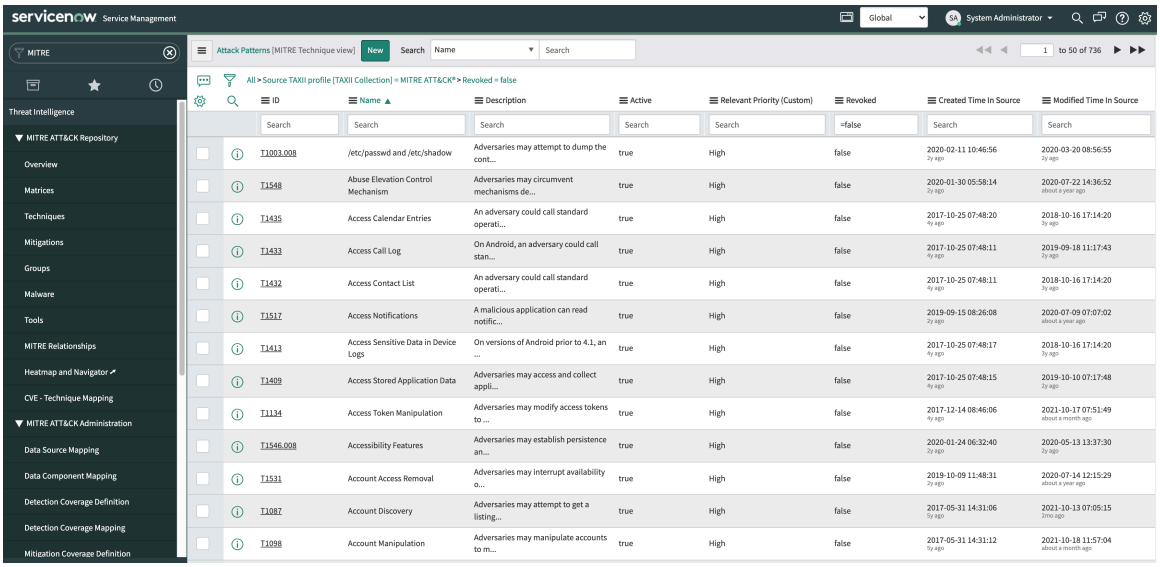
Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Técnicas**.



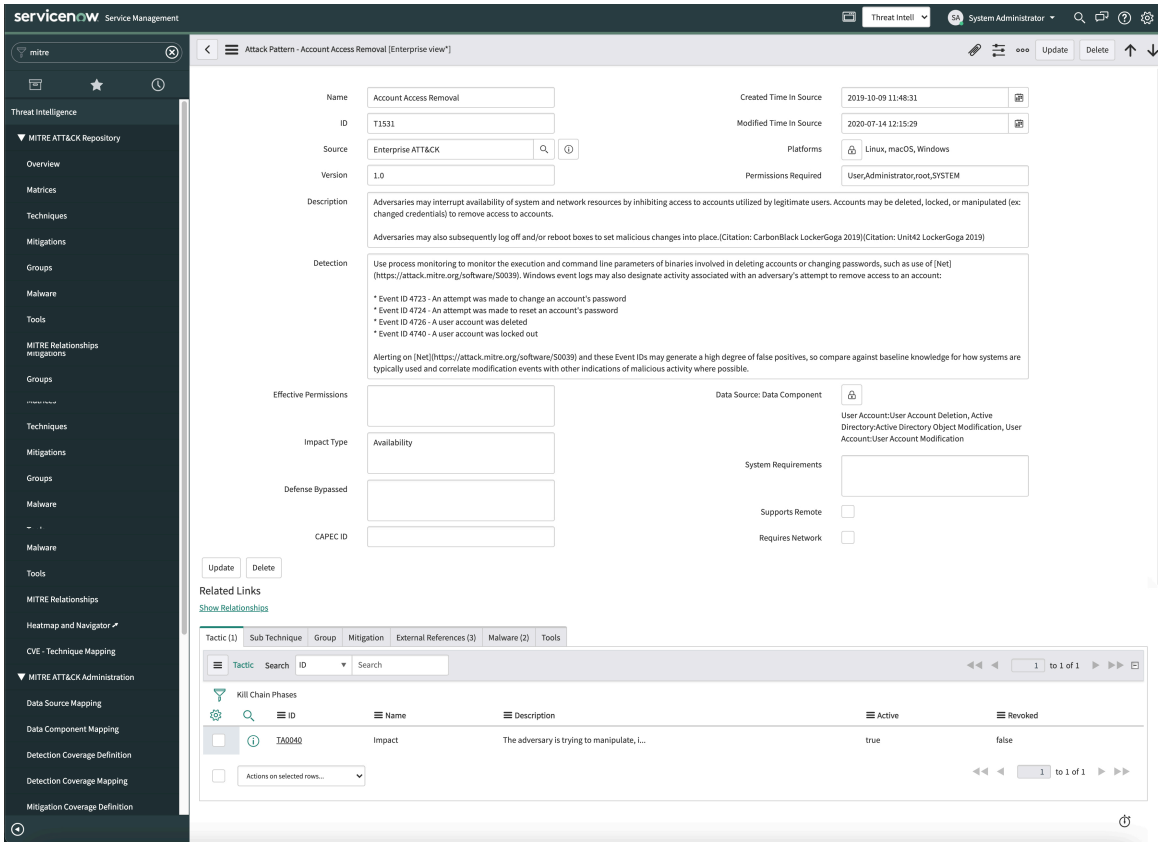
A lista de técnicas e subtécnicas agora está listada.

2. Para revisar e desativar técnicas que não são relevantes para sua organização, vá para a exibição de lista da técnica selecionada e, na coluna Ativa, atualize a configuração para **falso**e salve a configuração.
   Desative as técnicas que não são usadas por outros objetos no repositório MITRE-ATT&CK.
3. Para priorizar uma técnica, atribua uma prioridade no campo **Prioridade relevante (personalizada)**.
   A prioridade relevante do sistema de base está definida como nenhuma. O campo **Prioridade relevante (personalizado)** não é importado das coleções MITRE-ATT&CK TAXII, mas um campo personalizado introduzido no Now Platform. Você pode usar as informações de prioridade relevantes para filtrar e priorizar técnicas nos painéis, durante o mapeamento da fonte de dados ou ao analisar o mapa térmico.
4. Clique em uma técnica para exibir todas as informações associadas a ela.

   Na ilustração a seguir, você pode exibir os detalhes de cada técnica de remoção de acesso à conta, seu ID, origem e outras informações relacionadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: O elemento Fonte de dados: componente de dados introduzido por MITRE substitui o campo Fonte de dados anterior. O componente de dados fornece uma subcamada extra de contexto para as fontes de dados. Se o seu repositório MITRE-ATT&CK contiver as coleções TAXII antigas, você poderá exibir o campo Fonte de dados. Caso contrário, você pode exibir as fontes de dados com o contexto adicional de componentes de dados no campo Fonte de dados: componente de dados. Você pode exibir o novo campo de componente de dados somente quando a origem é Enterprise ATT&CK. Para obter mais informações, consulte mapeamento de componente de dados.

5. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Você pode estender as informações em alguns desses objetos de lista relacionados. Por exemplo, você pode adicionar novas informações para Grupo, Mitigação e Referências externas.

Gerenciar mitigações

Gerencie as mitigações que foram importadas das coleções MITRE TAXII. As mitigações permitem que você evite que um adversário execute com sucesso técnicas ou subtécnicas contra sua organização. Em STIX, as mitigações são conhecidas como cursos de ação.

Antes de Iniciar

Função necessária:

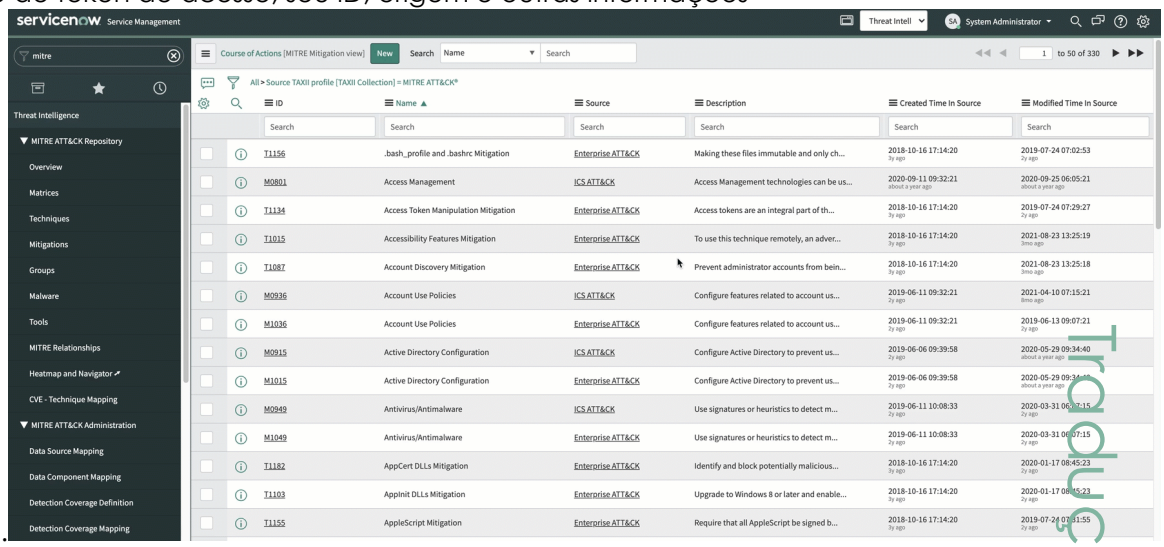
- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Mitigações**.
   As mitigações agora estão listadas.
2. Clique em uma mitigação para exibir todas as informações associadas.
   Na ilustração a seguir, você pode exibir os detalhes da mitigação da manipulação de token de acesso, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados de mitigações.

Gerenciar grupos

Gerencie os grupos que foram importados das coleções MITRE TAXII. Grupos são conjuntos de atividades de invasão relacionadas que são rastreados por um nome comum na comunidade de segurança. Os analistas rastreiam clusters de atividades usando vários termos, como grupos de ameaças, grupos de atividades, agentes de ameaças, conjuntos de intrusão e campanhas. Em STIX, os grupos são conhecidos como conjuntos de intrusão.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

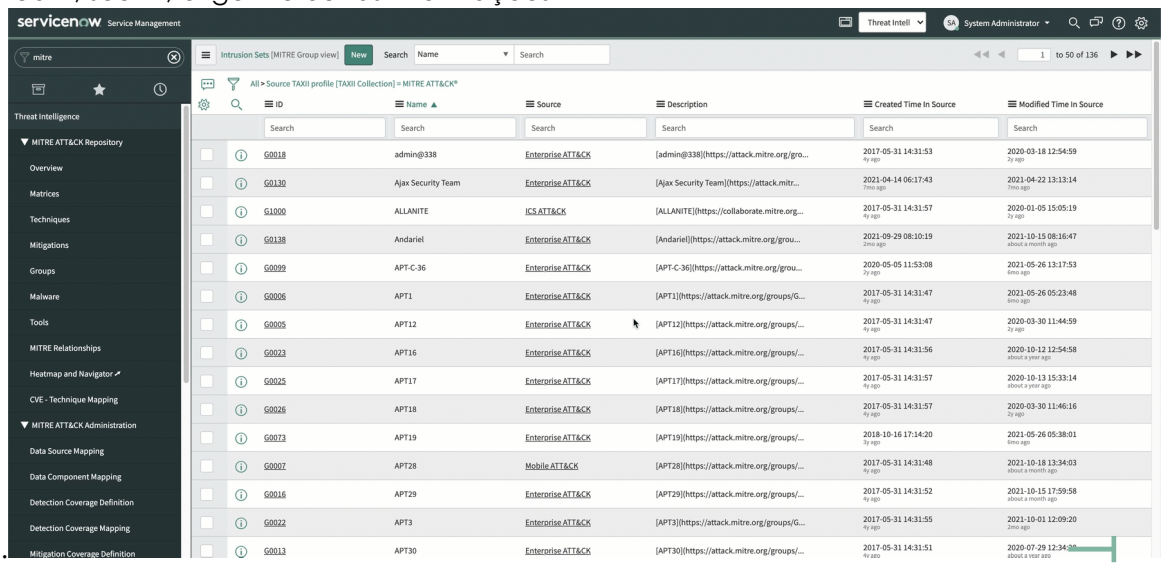
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Grupos**.
   Você pode exibir os grupos listados.
2. Clique em um grupo para exibir todas as informações associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do grupo Ajax Security Team, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

> **Nota:** Para associar os grupos de ameaças a um caso de segurança para uma investigação mais profunda, clique em **Adicionar ao caso de segurança**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados dos grupos.

Gerenciar malware

Gerencie as informações de malware que você importou das coleções MITRE TAXII. Malware é um tipo de TTP que representa código mal-intencionado. Refere-se a um programa que é inserido secretamente em um sistema. A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

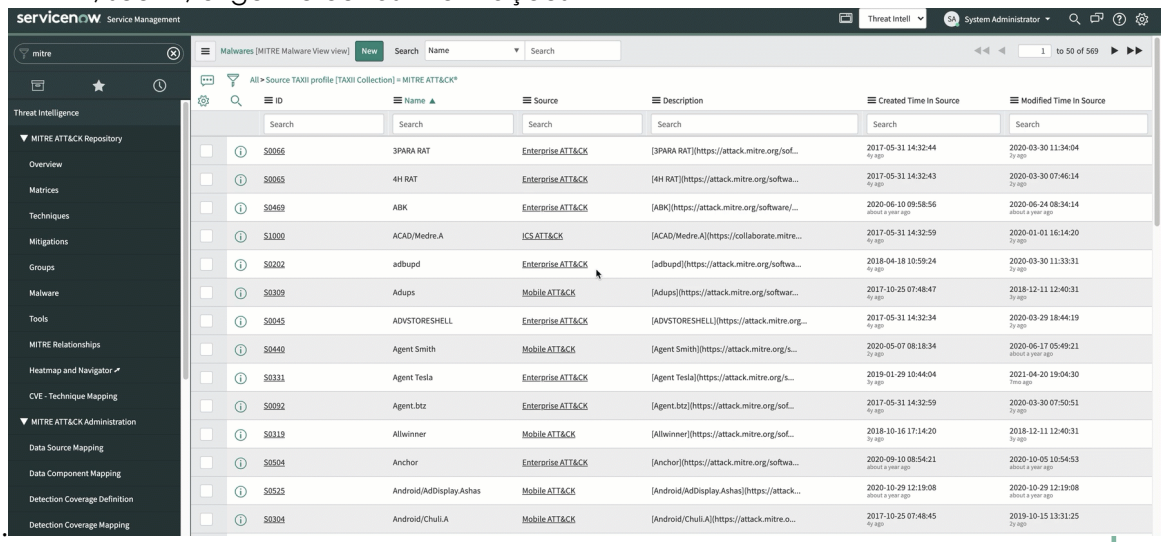
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Malware**.
   Você pode exibir os malwares listados.
2. Clique em um malware para exibir todas as informações associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do malware 3PARA RAT, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados de malware.

Gerenciar ferramentas

Gerencie as informações de ferramentas que você importou das coleções MITRE TAXII. As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Por Que e Quando Desempenhar Esta Tarefa

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

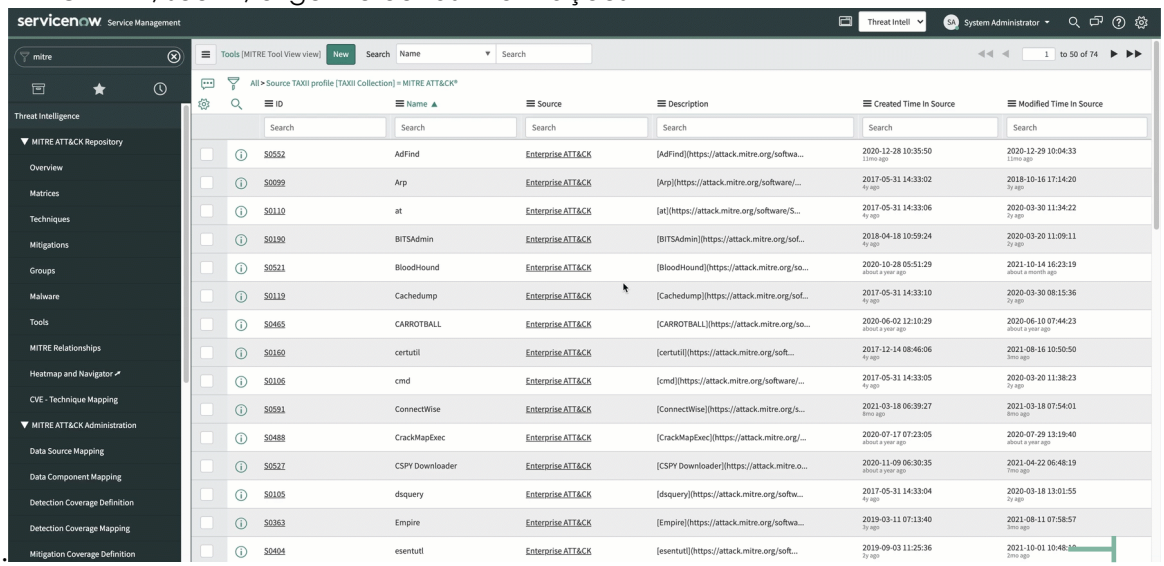
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Ferramentas**.
   Você pode exibir as ferramentas listadas.
2. Clique em uma ferramenta para exibir todas as informações associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes da ferramenta CARROTBALL, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados das ferramentas.

Gerenciar MITRE relacionamentos

Gerencie as informações de relacionamentos MITRE que você importou das coleções MITRE TAXII.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

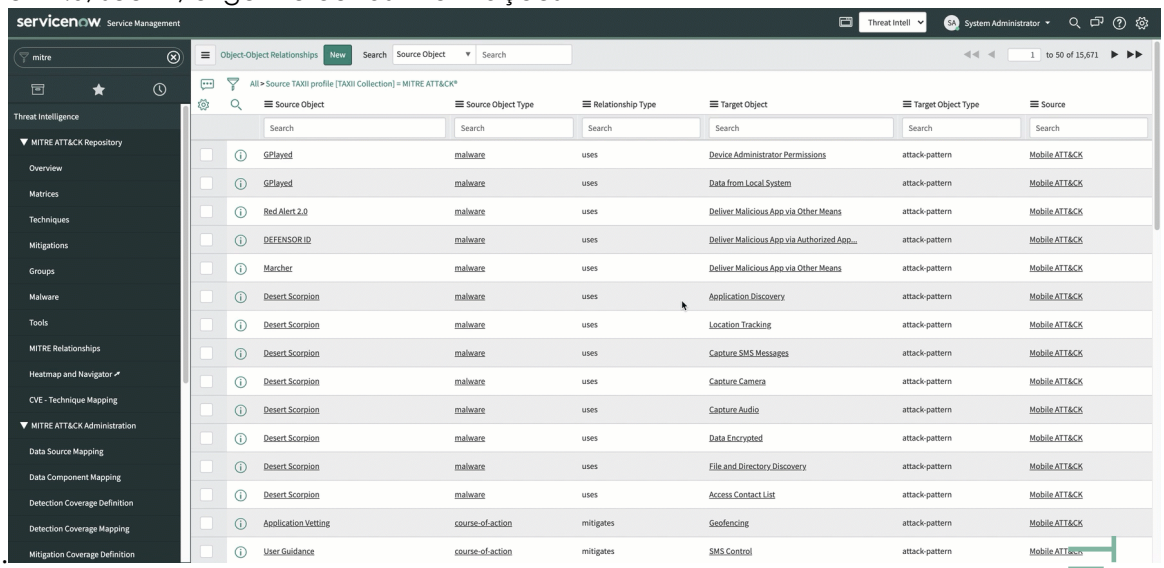
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Relações do MITRE**.
   Você pode exibir as ferramentas listadas.
2. Clique em um objeto de origem para exibir todas as informações associadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do objeto Red Alert 2.0, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados de relacionamentos do MITRE.

Gerenciar CVE e mapeamento de técnica

Gerencie o CVE e as informações de técnica que são mapeadas depois de importar as MITRE TAXII coleções.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Nota: O módulo **CVE-Technique Mapping** está disponível somente quando o produto Vulnerability Response está instalado em seu ambiente.

Por Que e Quando Desempenhar Esta Tarefa

Depois de importar as coleções MITRE TAXII, você pode exibir os CVEs em seu ambiente e o relacionamento deles com as técnicas MITRE-ATT&CK associadas. Você também pode criar associações com CVEs e os padrões de ataque.

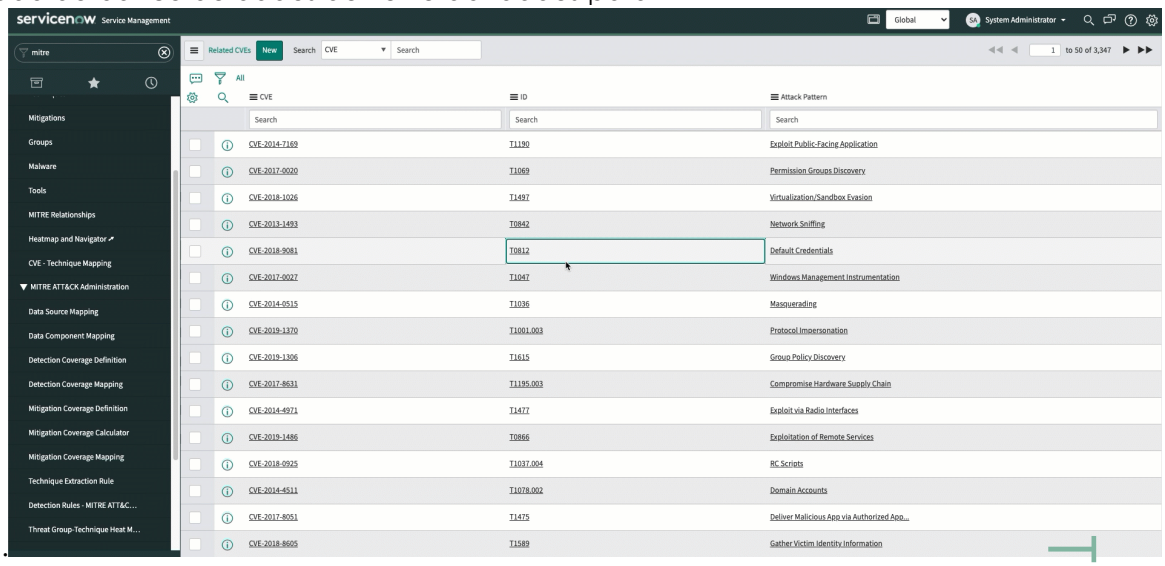
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **CVE - Mapeamento de técnica**.
   Você pode exibir os CVEs e as técnicas listados.
2. Clique em um CVE para exibir a entrada do banco de dados de vulnerabilidades.

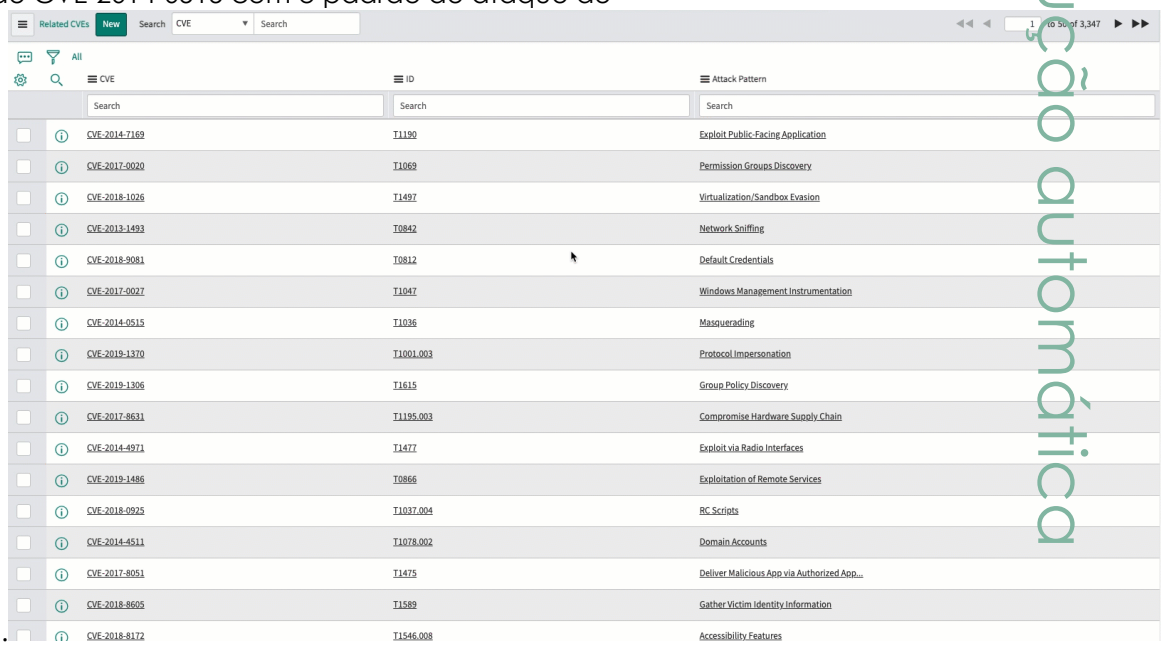
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes da lista de CVE e da entrada do banco de dados de vulnerabilidades para CVE-2014-7169.



3. Para adicionar uma entrada, clique em **Novo**, mapeie o CVE para um padrão de ataque e clique em **Enviar**.
   Na ilustração a seguir, uma nova entrada é criada pelo mapeamento de CVE-2014-0515 com o padrão de ataque de mascaramento.



Tradução automática

Estender os dados MITRE-ATT&CK

Estenda os dados do repositório MITRE-ATT&CK no Now Platform, aprimorando-os.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Por Que e Quando Desempenhar Esta Tarefa

Você pode estender os objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica no repositório MITRE-ATT&CK.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar um novo objeto e estabelecer um relacionamento entre uma técnica e o novo objeto no módulo Repositório do MITRE ATT&CK, mas não pode definir o tipo de relacionamento neste módulo. Para obter mais informações sobre como definir tipos de relacionamento, consulte relacionamentos objeto a objeto. Para definir um tipo de relacionamento, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

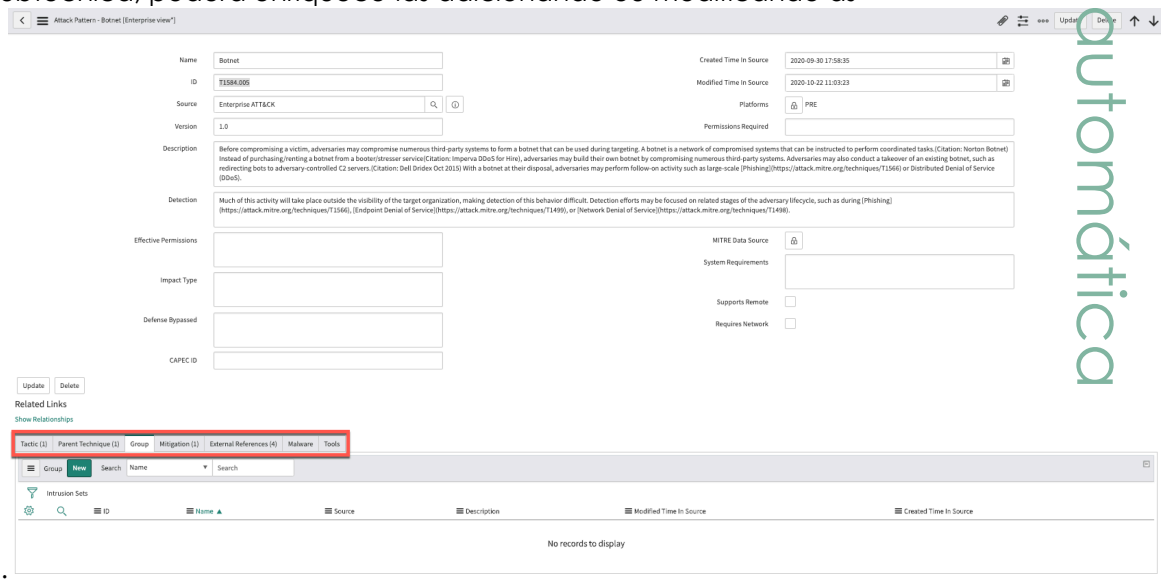
Se você mapear o tipo de relacionamento entre uma técnica existente e um objeto existente, deverá definir a técnica como o objeto de destino e o objeto como o objeto de origem. Para fazer isso, navegue até o **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Você pode criar um grupo e associá-lo a um padrão de ataque, mas no repositório do MITRE ATT&CK, você só pode estabelecer o relacionamento entre o grupo e o padrão de ataque. Para definir o tipo de relacionamento objeto a objeto, você deve fazer isso no Repositório de IoC.

Nota: Todas as personalizações feitas nos objetos são salvas durante as atualizações programadas.

Procedimento

1. Navegar até **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Técnicas**.
2. Clique em uma técnica ou subtécnica para exibir todas as informações associadas a esta técnica.
   Na ilustração a seguir, você pode ver que a técnica Botnet (T1584.005) não está associada a nenhum grupo. Se você tiver informações adicionais sobre uma técnica ou subtécnica, poderá enriquecê-las adicionando ou modificando as informações.

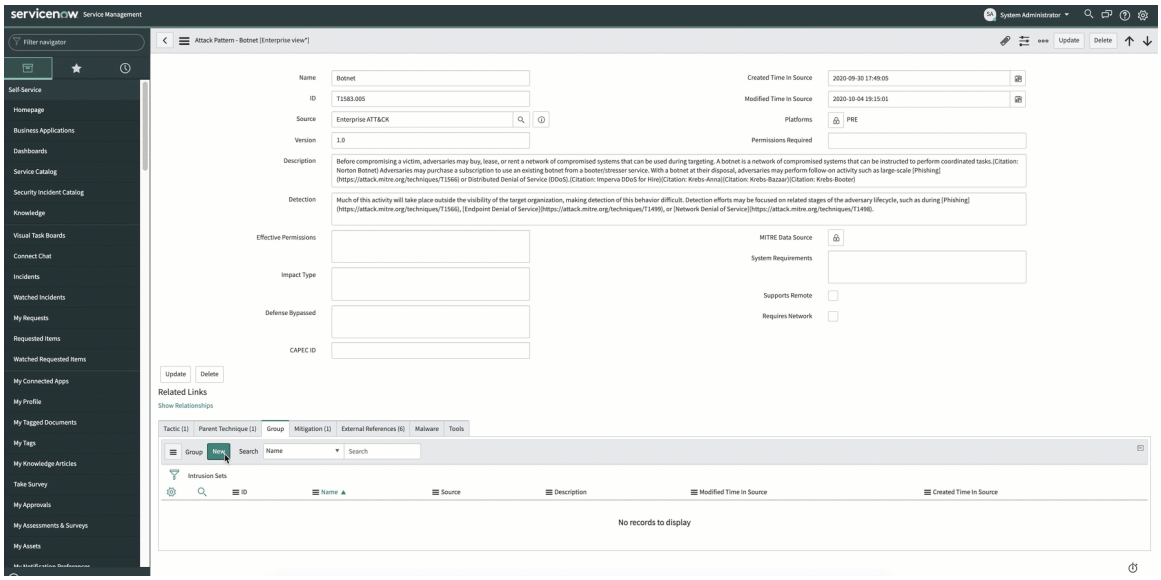


3. Clique em uma lista relacionada para aprimorar seus dados e associá-la a um novo grupo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, um grupo, Custom1, foi associado à subtécnica Botnet.



Definir a fonte de dados e o mapeamento da ferramenta de detecção

Defina a fonte de dados e o mapeamento da ferramenta de detecção para MITRE-ATT&CK táticas e técnicas. O mapeamento de fonte de dados fornece informações sobre a relevância e a disponibilidade das fontes de dados e as ferramentas de detecção para monitorar as fontes de dados em seu ambiente.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação, exclusão
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Você pode identificar as fontes de dados e as ferramentas de detecção de que sua organização precisa para detectar as técnicas com eficácia.

Por exemplo, se sua organização se concentrar em 5 técnicas, talvez você precise de 10 fontes de dados e 10 ferramentas de detecção para monitorar essas origens. Digamos que você identifique que sua organização não tem duas fontes de dados e cinco ferramentas de detecção. Este exercício fornece visibilidade sobre as fontes de dados, sua relevância para sua organização e para identificar lacunas na cobertura. Você também pode se concentrar em aprimorar seu ambiente com as fontes de dados e ferramentas de detecção corretas.

Todas as táticas, técnicas, ID e fontes de dados ativas são preenchidas automaticamente com base em seu TAXII perfil

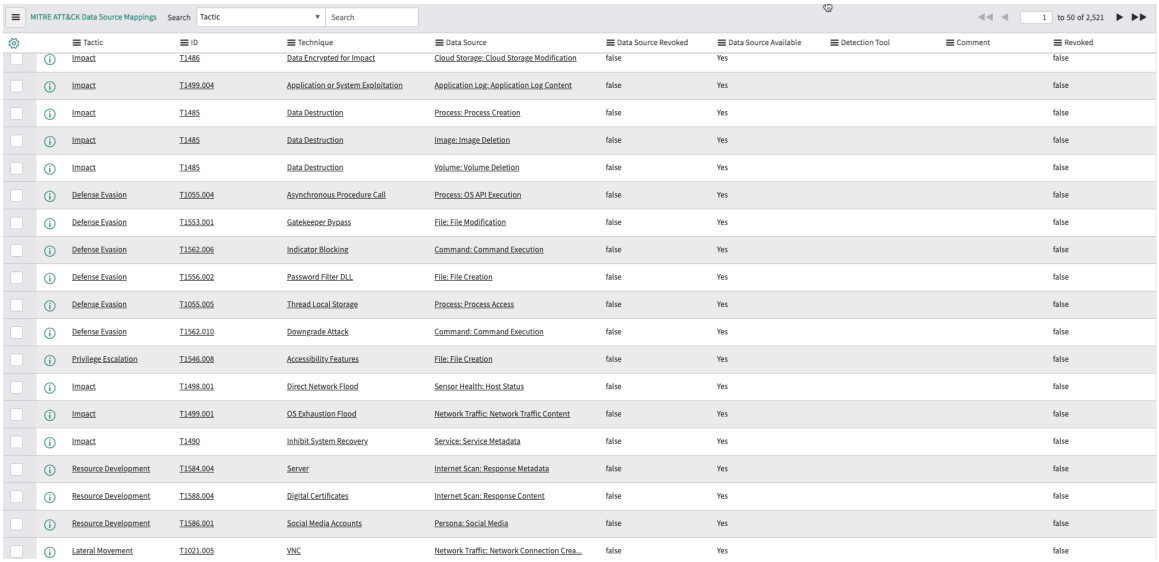
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de fonte de dados**.

   A ilustração a seguir mostra a lista de táticas, técnicas e seus IDs que foram preenchidos com base em suas atualizações de coleção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

Campo	Descrição
Tática	Objetivo do adversário ou o motivo para executar uma ação.
ID	Identidade exclusiva da técnica.
Técnica	Como um adversário atinge um objetivo tático executando uma ação.
Fonte de dados	Fonte de dados associada à técnica.
Fonte de dados revogada	A fonte de dados será revogada se definida como verdadeira, no entanto, o mapeamento da fonte de dados ainda será mantido. Se o valor da fonte de dados não for encontrado em MITRE, o valor de Fonte de dados revogada será marcado automaticamente como verdadeiro. O mapeamento da fonte de dados de um registro será revogado se a técnica e os relacionamentos da fonte de dados estiverem ausentes nos dados MITRE atualizados. Padrão: falso
Fonte de dados disponível	Disponibilidade da fonte de dados.
Ferramenta de detecção	Ferramenta que complementa a fonte de dados detectando as técnicas usadas. A ferramenta de detecção é mapeada com o sensor de alerta em SIR.
Revogado	O mapeamento da fonte de dados de um registro será revogado se a técnica e os relacionamentos da fonte de dados estiverem ausentes nos dados MITRE atualizados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Padrão: falso

2. Revise as fontes de dados listadas e modifique o valor no campo **Fonte de dados disponível** com base no seu ambiente.

3. **Nota:** Você não pode editar esta entrada na exibição de lista.

   No campo **Ferramenta de detecção**, siga estas etapas:

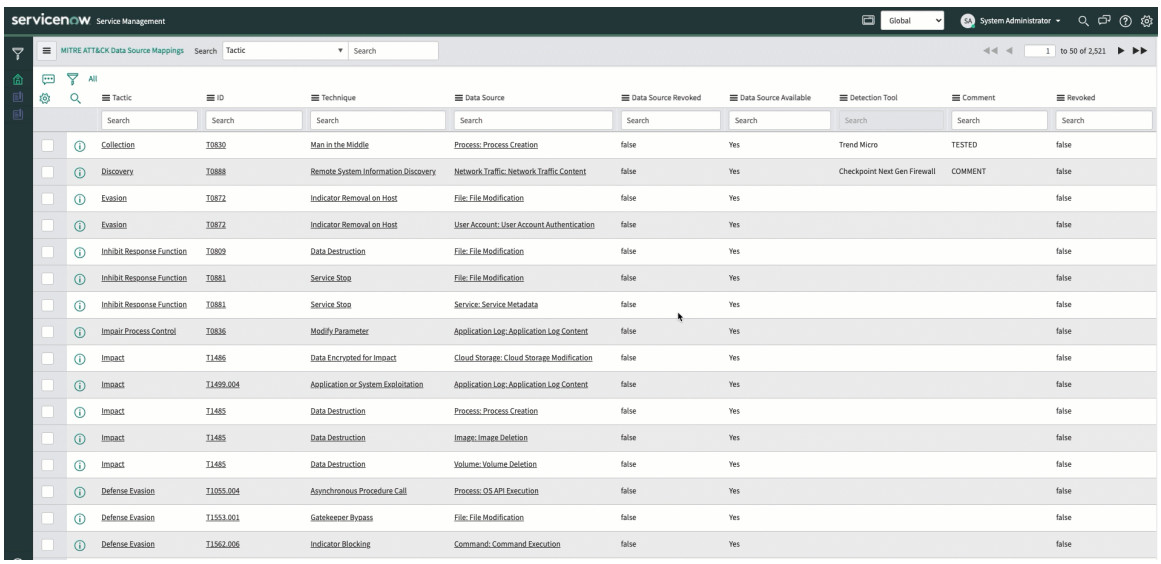
   a. Clique no ícone de informações e clique em **Abrir registro**.

   b. Desbloqueie a entrada **da Ferramenta de detecção**.

   c. Use a lista de pesquisa para selecionar uma ferramenta de detecção. Você pode selecionar várias ferramentas de detecção.

   d. Clique em **Atualizar**.

   Na ilustração a seguir, várias ferramentas de detecção foram adicionadas para monitorar a fonte de dados.



Definir a fonte de dados e o mapeamento do componente de dados

Use o Mapeamento de componente de dados se estiver usando as coleções TAXII mais recentes e quiser manter um relacionamento entre as fontes de dados, os componentes de dados e as várias técnicas. Mapeie as fontes de dados com o contexto adicional de componentes de dados que fornece uma subcamada extra de contexto para fontes de dados que permitem que você entenda melhor os comportamentos adversários em MITRE-ATT&CK.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação, exclusão
- sn_ti.read: acesso de leitura

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

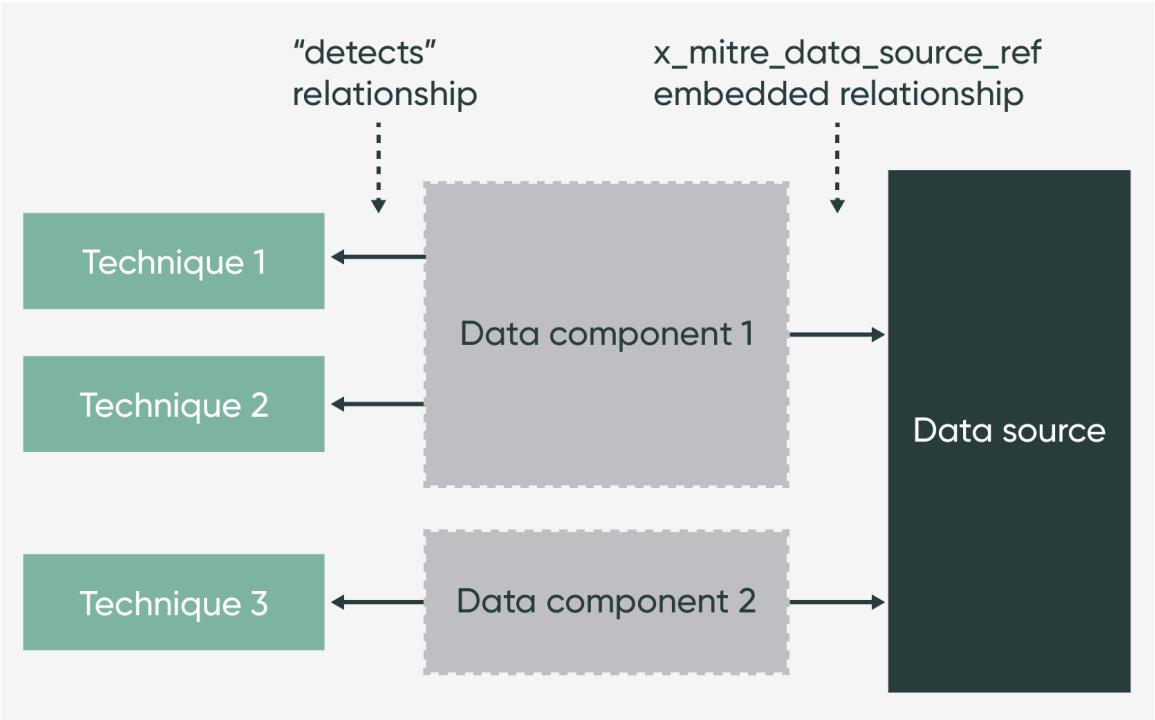
Por Que e Quando Desempenhar Esta Tarefa
O mapeamento das fontes de dados e dos componentes de dados fornece visibilidade sobre as fontes de dados ou componentes e as técnicas que são relevantes para sua organização.

Por exemplo, se sua organização se concentrar em 7 técnicas, talvez você precise de 5 fontes de dados e 10 componentes de dados para monitorar essas origens. Sua avaliação das ferramentas internas revela que sua organização não tem duas fontes de dados e quatro componentes de dados. Este exercício de mapeamento fornece visibilidade sobre as fontes de dados, componentes e técnicas, sua relevância para a sua organização e para identificar as lacunas na cobertura. Assim, você pode concentrar seu investimento nas fontes de dados e sensores de alerta corretos para detectar e mitigar ameaças adversas.

A estrutura MITRE-ATT&CK contém uma estrutura atualizada para as fontes de dados - Fonte de dados: Componente de dados. Esta nova forma de fonte de dados fornece um contexto extra para as fontes de dados. O objeto de fonte de dados apresenta o nome da fonte de dados, bem como detalhes importantes sobre os dados coletados (arquivo, processo, tráfego de rede e assim por diante) e valores ou propriedades específicas necessárias para detectar comportamentos adversários.

A ilustração a seguir mostra a representação da estrutura MITRE-ATT&CK STIX™ para fontes de dados e componentes de dados. Você pode ver as fontes de dados e os componentes de dados capturados como objetos STIX™ personalizados. A ilustração mostra que cada fonte de dados contém um ou mais componentes de dados e cada componente de dados detecta uma ou mais técnicas.

Estrutura geral de fontes de dados e componentes de dados



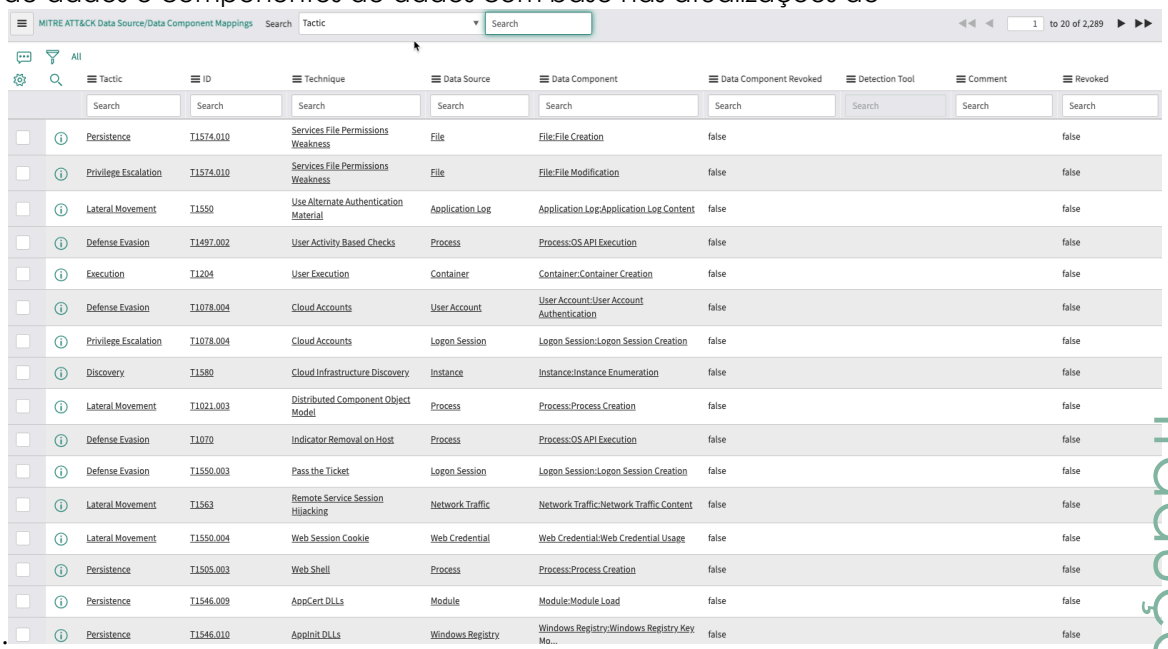
Você pode continuar usando o Mapeamento de fonte de dados se o seu repositório MITRE-ATT&CK contiver as coleções TAXII antigas e você tiver mapeado suas fontes de dados para várias técnicas. No entanto, use o Mapeamento de componente de dados se estiver usando as coleções TAXII mais recentes e quiser manter um relacionamento entre as fontes de dados, os componentes de dados e as várias técnicas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de componente de dados**.
   A ilustração a seguir mostra a lista de táticas, IDs e técnicas junto com as fontes de dados e componentes de dados com base nas atualizações de coleta.



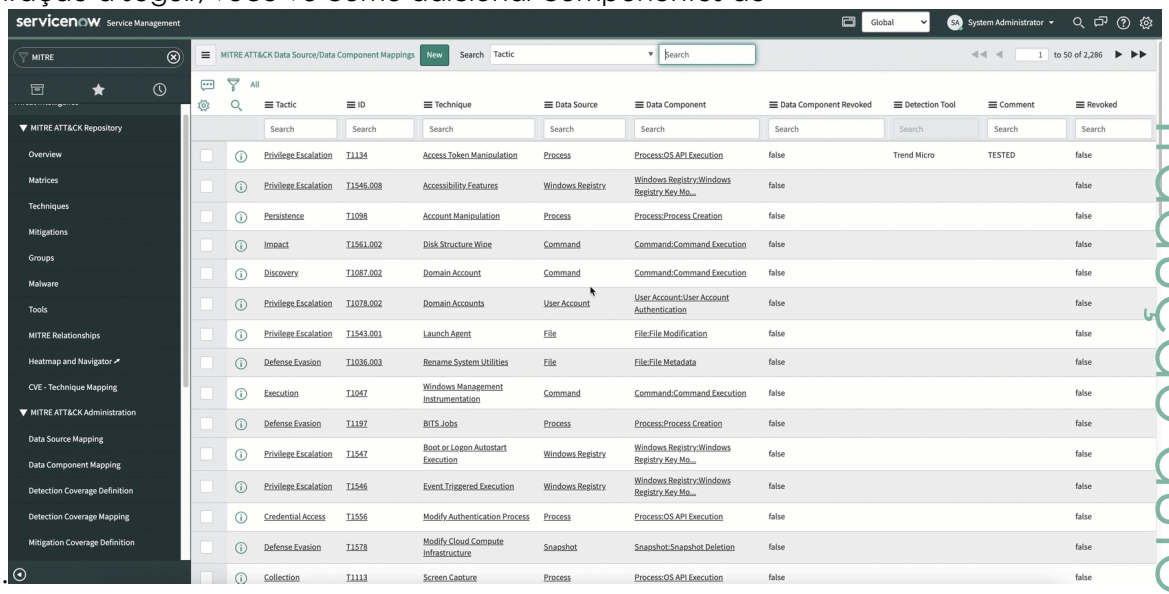
Campo	Descrição
Tática	Objetivo do adversário ou o motivo para executar uma ação.
ID	Identidade exclusiva da técnica.
Técnica	Como um adversário atinge um objetivo tático executando uma ação.
Fonte de dados	Fonte de dados associada à técnica.
Componente de dados	Componente de dados associado à fonte de dados. Um componente de dados só pode ter uma fonte de dados primária.
Componente de dados revogado	Identifica se o componente de dados foi revogado na base de conhecimento MITRE-ATT&CK.
Ferramenta de detecção	Ferramenta que complementa a fonte de dados detectando as técnicas usadas. A ferramenta de detecção é mapeada com o sensor de alerta em SIR.
Comentário	Descrição sobre a fonte de dados e o mapeamento do componente de dados.
Revogado	Identifica se o componente de dados para mapeamento de técnica foi revogado por MITRE-ATT&CK.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Revise as fontes de dados e os componentes de dados listados e modifique os valores com base no seu ambiente.
3. Siga estas etapas para adicionar um componente de dados.
   a. Navegar até **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Técnicas**.
   b. Clique em uma técnica que você deseja modificar a fonte de dados: informações do componente de dados.
   c. Desbloquear fonte de dados: componente de dados.
   d. Use a lista de pesquisa para selecionar MITRE-ATT&CK componentes de dados.
   e. Bloquear fonte de dados: componente de dados.
   f. Clique em **Atualizar**.

Na ilustração a seguir, você vê como adicionar componentes de dados.



Tradução automática

Definir a cobertura de detecção da técnica

Defina a cobertura de detecção de técnica que sua organização deve medir e detectar técnicas adversárias específicas.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: acesso de gravação
- Função necessária: sn_ti.read: acesso de leitura

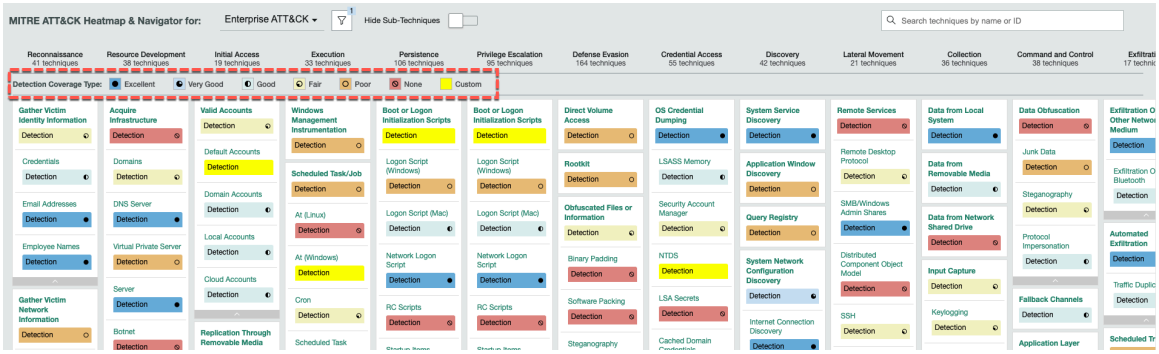
Por Que e Quando Desempenhar Esta Tarefa

As definições de cobertura de técnica são usadas no mapeamento geral de detecção de técnica. Você pode usar a cobertura da técnica do sistema de base. A cobertura da técnica do sistema de base consiste nos tipos de cobertura Nenhum, Ruim, Justo, Bom, Muito Bom e Excelente. A cobertura da técnica do sistema de base também está associada a cores predefinidas. Você pode personalizar as entradas e cores do tipo de cobertura ou criar suas próprias entradas. Por exemplo, você pode modificar os tipos de cobertura do sistema de base para Não aplicável, Cobertura parcial e Cobertura completa. Como alternativa, você também pode criar medidas numéricas para os tipos de cobertura, como 0-25%, 25-50% e 50-100%. O tipo de modificações feitas na cobertura do sistema de base não está limitado aos exemplos compartilhados.

As personalizações feitas no tipo de cobertura e na cor são usadas no mapeamento geral de detecção de técnica e também no mapa térmico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você modificar a definição de cobertura do sistema de base, os ícones de tipo de cobertura não serão exibidos com as técnicas no mapa térmico. O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que a cobertura de detecção de técnica definida pelo sistema de base e as cores de cobertura. No entanto, se você excluir campos existentes da cobertura de detecção de técnica geral, o mapa térmico não exibirá os ícones de tipo de cobertura.



Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição de cobertura de detecção**.
2. Revise as entradas de detecção de técnica geral e personalize as entradas para seu ambiente.

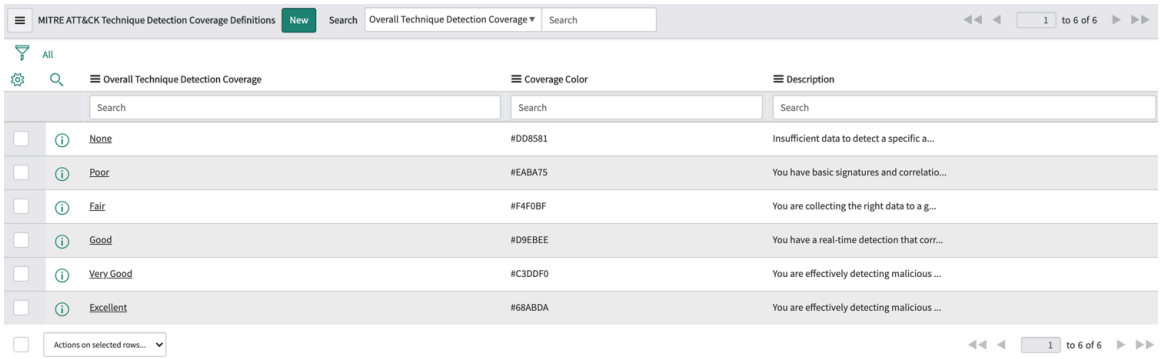
Definição de cobertura de detecção

Campo	Descrição
Cobertura geral de detecção de técnica	Nome da cobertura geral de detecção da técnica. A cobertura da técnica do sistema de base consiste em Nenhum, Ruim, Razoável, Bom, Muito Bom ou Excelente.
Cor da cobertura	Cor atribuída à pontuação de cobertura de detecção. A cor que você define é usada para a cobertura de detecção de técnica no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB (A).
Descrição	Cobertura geral de detecção da técnica. Consulte a definição do sistema de base na Definição de pontuação.

A ilustração a seguir mostra a lista Definição de cobertura de detecção.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para adicionar uma entrada, clique em **Novo**, conclua as entradas e clique em **Enviar**.

MITRE-ATT&CK Definição de pontuação

Defina o sistema de pontuação MITRE-ATT&CK da sua organização para que você possa medir a eficácia com que sua organização pode detectar técnicas adversárias específicas.

Definição de pontuação

Pontuação	Mapeamento de pontuação	Descrição
Nenhum(a)	0	Dados insuficientes para detectar uma técnica adversária específica.
Ruim	1	As assinaturas básicas e as regras de correlação estão em vigor para detectar técnicas adversárias específicas. A detecção de ameaças não é em tempo real e cobre apenas um número mínimo de aspectos de uma técnica. Por exemplo, a busca ocorre somente em um endpoint de cada vez. Sua organização ainda pode ter milhares ou centenas de eventos que os coletores devem revisar e correlacionar com outros eventos para encontrar exceções. O número de falso-positivos é alto.
Justo	2	Coletando os dados corretos em grande parte e a qualidade dos dados é justa. Por exemplo, sua organização pode estar começando a adicionar logs do Sysmon, ETW, logs do PowerShell e assim por diante. No entanto, a detecção de ameaças ainda não é em tempo real. Sua organização pode não ter todas as ferramentas certas para agregar e analisar os dados com eficácia. Os Caçadores devem executar consultas manualmente e correlacionar para analisar os dados com precisão. O número de falso-positivos é alto.
Boa	3	Detecção em tempo real que correlaciona e integra vários dados em seus endpoints. A detecção de ameaças cobre muitos aspectos dos procedimentos de uma técnica. Seus adversários podem ignorar a detecção com evasão e ofuscação. Sua organização pode identificar facilmente falsos positivos e filtrá-los.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de pontuação

Pontuação	Mapeamento de pontuação	Descrição
		Sua organização usa técnicas básicas de ciência de dados para analisar os dados no repositório central.
Muito Bom	4	Detecte com eficácia técnicas mal-intencionadas em tempo real e cubra a maioria dos aspectos dos procedimentos de uma técnica. A possibilidade de seus adversários ignorarem a detecção com métodos de evasão e ofuscação é mais difícil do que no nível Bom. Sua organização pode identificar facilmente falsos positivos e filtrá-los. Sua organização usa técnicas avançadas de ciência de dados para detectar técnicas adversárias.
Excelente	5	Detecte com eficácia técnicas mal-intencionadas em tempo real e cubra todos os aspectos dos procedimentos de uma técnica. Sua organização tem uma boa compreensão do seu ambiente com a automação e a qualidade de dados corretas. A possibilidade de seus adversários ignorarem a detecção com métodos de evasão e ofuscação não é possível neste nível. O número de falso-negativos é baixo.

Mapear sua cobertura de detecção de técnica para uma técnica

Mapeie sua cobertura geral de detecção de técnica com a técnica que permite que sua organização detecte técnicas adversárias específicas.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: acesso de gravação
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar a cobertura de detecção de técnica para obter uma visão geral da cobertura geral de detecção de técnica da sua organização. Por exemplo, se um adversário estiver atacado sua organização, você verá o tipo de cobertura que tem para detectar as técnicas do invasor.

A técnica e o ID são preenchidos automaticamente para todas as coleções e técnicas que você ativou. O tipo de cobertura e a definição de pontuação que você definiu estão disponíveis para como uma opção que você pode selecionar na cobertura de detecção de técnica geral.

Você pode mapear a cobertura geral de detecção da técnica com a técnica para concluir o mapeamento. Você pode associar uma técnica a apenas uma cobertura de detecção de técnica geral.

O mapeamento de cobertura de detecção de técnica que você define é usado na visualização de cobertura no mapa térmico.

Tradução automática

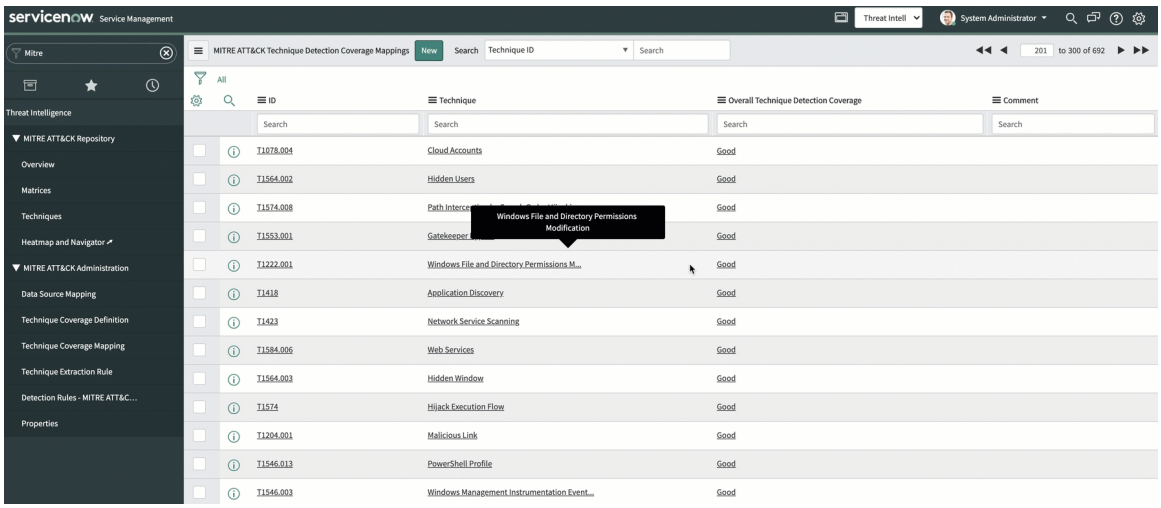
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você pode chegar à cobertura geral de detecção da técnica usando cálculos específicos da sua organização. Você pode usar qualquer produto de Simulação de violação e ataque (BAS), o Repositório de análise cibernética (CAR) ou qualquer outro método conforme necessário para definir a definição de pontuação e usá-lo neste procedimento para o mapeamento de cobertura de detecção de técnica geral.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de cobertura de detecção**.

   Nesta ilustração, você vê que a subtécnica Contas em nuvem (T1078.004) tem cobertura excelente na organização e que a Cobertura de detecção de técnica geral está mapeada para **Excelente**.



2. Revise cada técnica e mapeie a cobertura geral de detecção da técnica com base na definição de cobertura de detecção e na disponibilidade de cobertura da sua organização.

Definir a cobertura de mitigação

Defina a cobertura de mitigação para cada mitigação associada a uma técnica para que você tenha visibilidade de como sua organização pode impedir os ataques que acontecem devido a uma técnica específica.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

As definições de cobertura de mitigação são usadas na mitigação geral e no mapeamento de cobertura de técnica. Você pode usar a cobertura de mitigação do sistema de base. A cobertura de mitigação do sistema de base consiste nos tipos de cobertura Nenhum, Ruim, Justo, Bom, Muito Bom e Excelente. A cobertura de mitigação do sistema de base também está associada a cores predefinidas e porcentagens de cobertura. Você pode personalizar os tipos de cobertura (adicionar ou remover tipos de cobertura), porcentagens de cobertura para limites inferiores e limites superiores e cores ou criar sua cobertura de mitigação personalizada.

As personalizações feitas nos tipos de cobertura, cores ou porcentagens são usadas no mapeamento de cobertura de mitigação e também no mapa térmico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

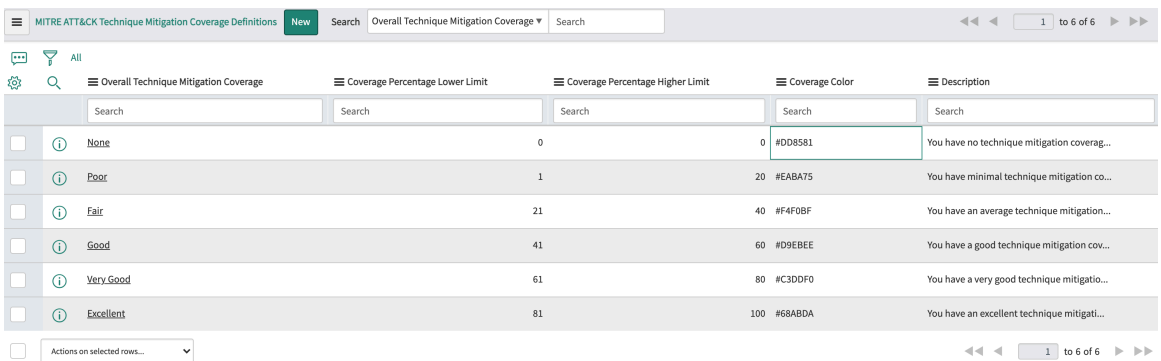
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição de cobertura de mitigação**.
2. Revise as entradas de detecção de mitigação e personalize as entradas para seu ambiente.

Definição de cobertura de mitigação de técnica

Campo	Descrição
Cobertura geral de mitigação da técnica	Nome da cobertura de mitigação da técnica. A cobertura de mitigação do sistema de base consiste em Nenhum, Ruim, Razoável, Bom, Muito Bom ou Excelente.
Limite Inferior da Percentual de Cobertura	O limite percentual inferior da cobertura de mitigação. Defina os valores numéricos entre 0 e 100.
Limite superior da porcentagem de cobertura	O limite percentual mais alto da cobertura de mitigação. Defina os valores numéricos entre 0 e 100.
Cor da cobertura	Cor atribuída à pontuação de cobertura de detecção. A cor que você define é usada para a cobertura de mitigação da técnica no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB (A).
Descrição	Cobertura geral de detecção de mitigação. Consulte a definição do sistema de base na definição de cobertura de mitigação da técnica.

Nota: Certifique-se de não sobrepor os intervalos de porcentagem de cobertura se personalizar os limites de porcentagem (inferior ou superior). Por exemplo, se um registro de cobertura tiver os intervalos de 0 a 20, o próximo registro consecutivo deverá ter o intervalo de limite inferior de 21 ou superior para evitar a sobreposição do intervalo percentual de cobertura.

A ilustração a seguir mostra a lista de definição de cobertura de mitigação.



3. Para adicionar uma entrada, clique em **Novo**, conclua as entradas e clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de cobertura de mitigação de técnica

Defina a cobertura de mitigação da sua organização para que você possa medir e detectar com eficácia técnicas adversárias específicas.

Definições de cobertura de mitigação da técnica do MITRE ATT&CK

Cobertura geral de mitigação da técnica	Limite Inferior da Percentual de Cobertura	Limite superior da porcentagem de cobertura	Cor da cobertura	Descrição
Nenhum(a)	0	0	#DD8581	Você não tem cobertura de mitigação de técnica e seus controles de defesa não têm capacidade de impedir um ataque em nenhum cenário.
Ruim	1	20	#EABA75	Você tem cobertura mínima de mitigação de técnica. As chances de um ataque são muito altas e seus controles de defesa podem impedir um ataque em 0 a 20% dos cenários.
Justo	21	40	#F4F0BF	Você tem uma cobertura de mitigação de técnica média. As chances de um ataque são altas e seus controles de defesa podem impedir um ataque em 21 a 40 por cento dos cenários.
Boa	41	60	#D9EBEE	Você tem uma boa cobertura de mitigação de técnica. No entanto, as chances de um ataque são

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de cobertura de mitigação da técnica do MITRE ATT&CK

Cobertura geral de mitigação da técnica	Limite Inferior da Percentual de Cobertura	Limite superior da porcentagem de cobertura	Cor da cobertura	Descrição
				relativamente altas e seus controles de defesa podem impedir um ataque em 41 a 60 por cento dos cenários.
Muito Bom	61	80	#C3DDF0	Você tem uma cobertura de mitigação de técnica muito boa. As chances de um ataque são baixas e seus controles de defesa podem impedir um ataque em 61 a 80 por cento dos cenários.
Excelente	81	100	#68ABDA	Você tem uma excelente cobertura de mitigação de técnica e as chances de um ataque usando essa técnica são muito baixas e seus controles de defesa podem impedir um ataque em 81 a 100 por cento dos cenários.

Mapear sua cobertura de mitigação para uma técnica

Mapeie sua cobertura de mitigação com a técnica que permite detectar a estratégia de mitigação geral da sua organização.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: acesso para gravação e exclusão
- Função necessária: sn_ti.read: acesso de leitura

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

As mitigações permitem que você evite que um adversário execute com sucesso técnicas ou subtécnicas contra sua organização. Cada técnica MITRE-ATT&CK contém mitigações que você pode implantar em sua organização para reduzir a chance de ser atacado. Você pode usar a cobertura de mitigação para obter uma visão geral da estratégia de mitigação geral da sua organização. Por exemplo, se um adversário estiver atacado sua organização, você verá o tipo de cobertura que tem para atenuar as técnicas do invasor.

A técnica e as informações de mitigação são preenchidas automaticamente para todas as coleções e técnicas que você ativou. A definição de cobertura de mitigação que você definiu está disponível para seleção na cobertura de mitigação da técnica.

Você pode identificar mitigações que são relevantes para sua organização. Se uma mitigação for relevante, você poderá definir se as estratégias de mitigação foram implantadas. Você pode especificar se as estratégias são aplicadas como parte da política SOC da sua organização. Você também pode identificar se sua organização tem ferramentas preventivas para mitigar as técnicas de um invasor e mapear todos os controles de segurança que sua organização implantou para minimizar os riscos à segurança. Preencha a cobertura de mitigação (porcentagem) para cada um dos registros.

Depois de mapear as informações para cada uma das técnicas, a calculadora de cobertura de mitigação preenche automaticamente a Cobertura de mitigação da técnica calculada. Para calcular a cobertura de mitigação geral para qualquer técnica, os registros de mapeamento de mitigação da técnica devem estar ativos e relevantes para a organização. Os registros que estão inativos e não são relevantes não são considerados para o cálculo da cobertura geral de mitigação da técnica. Com base nos valores em Cobertura de mitigação de técnica calculada e na definição de coberturade mitigação , sua Cobertura de mitigação de técnica geral (calculada) é preenchida.

As personalizações feitas nos tipos de cobertura, cores ou porcentagens são usadas no mapeamento de cobertura de mitigação e também no mapa térmico.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de cobertura de mitigação**.
2. Revise cada técnica para o mapeamento de mitigação e atualize a **Cobertura de mitigação (porcentagem)** para calcular a disponibilidade de cobertura da sua organização.

Mapeamentos de cobertura de mitigação de técnica

Campo	Descrição
ID	Identidade exclusiva da técnica. Os IDs são preenchidos automaticamente para todas as coleções e técnicas que você ativou.
Técnica	Como um adversário atinge um objetivo tático executando uma ação. As informações da técnica são preenchidas automaticamente para todas as coleções e técnicas que você ativou.
Mitigação	Mitigações que permitem impedir que um adversário execute com sucesso técnicas ou subtécnicas contra sua organização. As informações de mitigação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

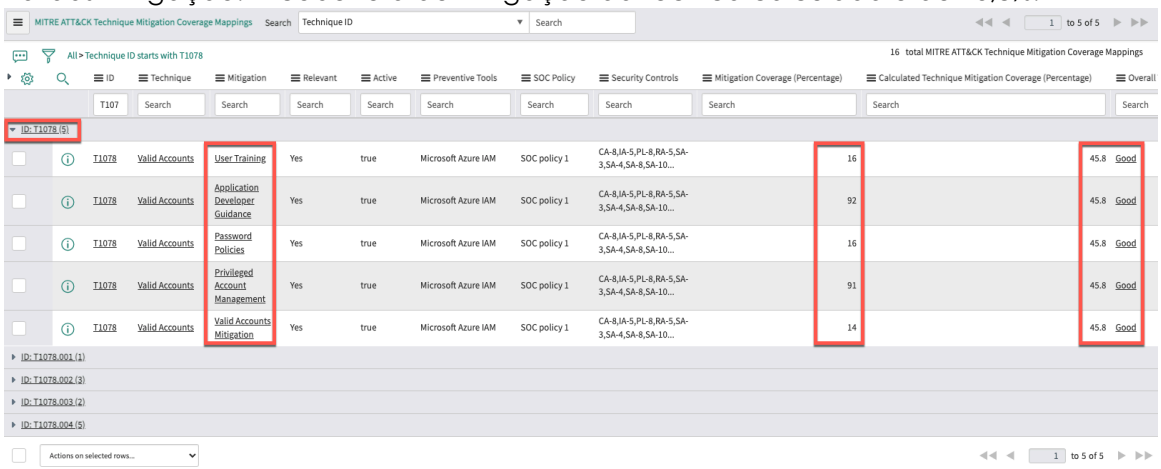
Campo	Descrição
	são preenchidas automaticamente para todas as coleções e técnicas que você ativou.
Relevante	Opção para especificar se a mitigação é relevante para sua organização.
Ativo	Opção para especificar se as estratégias de mitigação são implantadas em sua organização. Esta é uma opção necessária para calcular a cobertura de mitigação da técnica.
Ferramentas preventivas	Opção para especificar se sua organização tem ferramentas preventivas para atenuar as técnicas de um invasor.
Política SOC	As políticas de SOC que definem as estratégias de mitigação em sua organização.
Controles de segurança	Os controles de segurança da sua organização contêm as estratégias de mitigação para minimizar os riscos à segurança.
Cobertura de mitigação (porcentagem)	Um sistema de pontuação para calcular a cobertura de mitigação da técnica. Defina valores numéricos entre 0 e 100. Esta é uma opção necessária para calcular a cobertura de mitigação da técnica.
Cobertura de mitigação da técnica calculada (porcentagem)	A cobertura de mitigação da técnica calculada em porcentagem. Este valor é determinado com base na fórmula definida na calculadora de cobertura de mitigação.
Cobertura geral de mitigação da técnica (calculada)	A cobertura geral de mitigação da técnica. Este valor é determinado com base na cobertura de mitigação definida para sua organização.
Comentário	Descrição sobre a técnica e o mapeamento da cobertura de mitigação.
Revogado	A técnica para o mapeamento de cobertura de mitigação foi revogada.

Nesta ilustração, você vê que a técnica Contas válidas tem cinco mitigações associadas, cada uma com uma cobertura de mitigação de 16 para treinamento do usuário, 92 para orientação do desenvolvedor de aplicações e 16 para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

políticas de senha, 91 para gestão de contas privilegiadas e 14 para contas válidas mitigação. A cobertura de mitigação da técnica calculada é de 45,8%.



Calculadora de cobertura de mitigação da técnica geral

A cobertura de mitigação da técnica geral é determinada com base na fórmula definida na calculadora de cobertura de mitigação.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

- Você pode definir como ativa apenas uma calculadora de cobertura de mitigação por domínio.
- A calculadora de cobertura de mitigação do sistema de base é uma calculadora média.
- Quaisquer personalizações no script da calculadora devem garantir que a saída final seja um valor numérico entre 0 e 100.
- A definição de cobertura de mitigação é aplicada com base no intervalo da saída final.

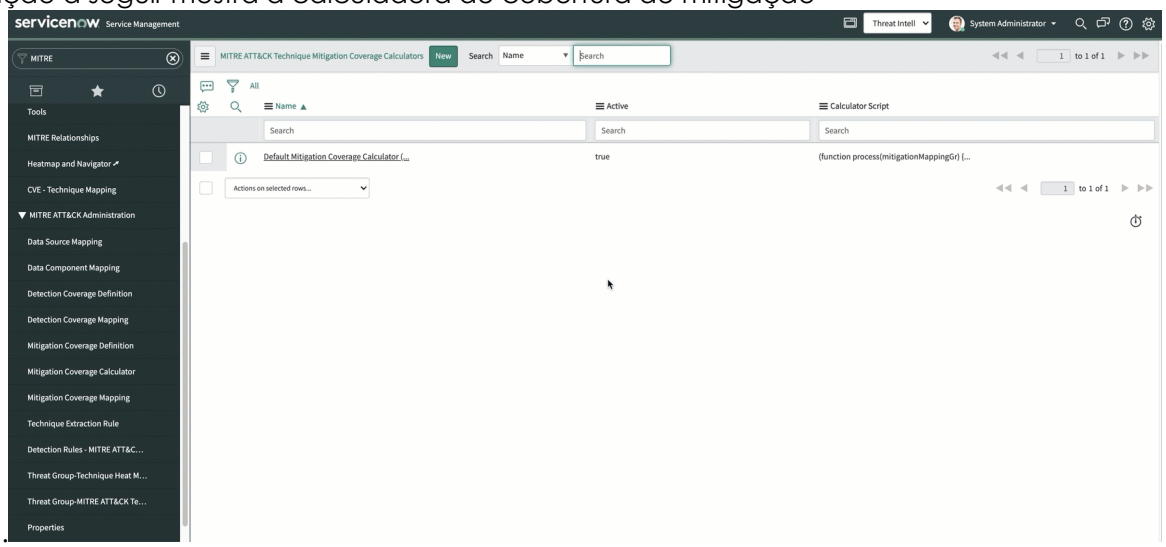
Procedimento

Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Calculadora de cobertura de mitigação**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra a calculadora de cobertura de mitigação padrão.



Criar e mapear regras de detecção

Crie regras de detecção e mapeie-as em relação às táticas e técnicas. Com este mapeamento, você pode ver a cobertura das regras de detecção em sua organização.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

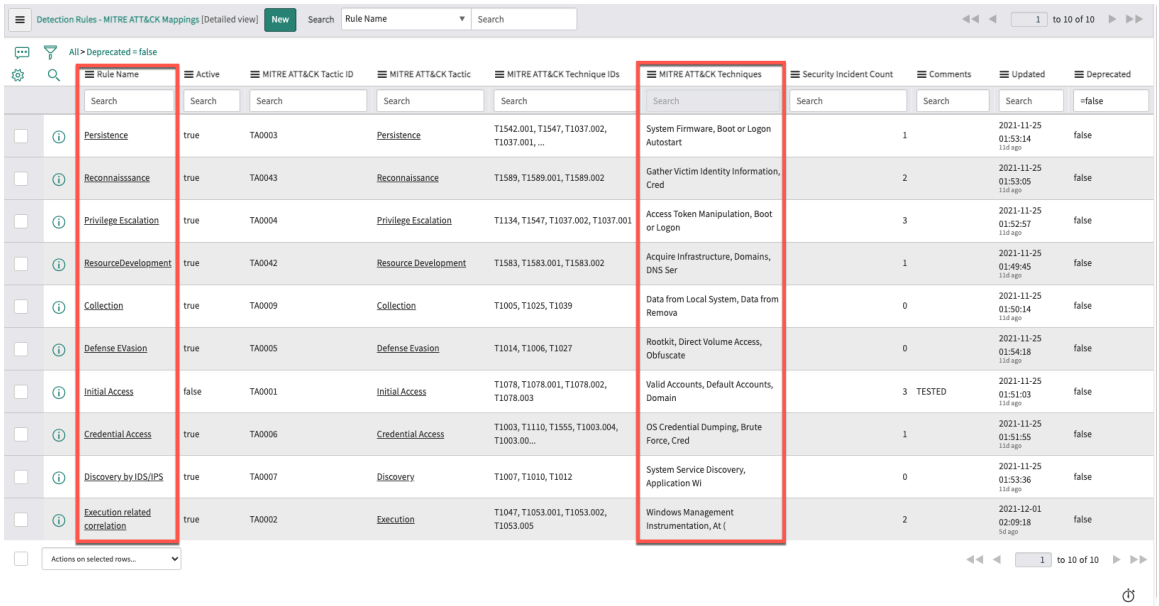
O mapeamento de regras de detecção permite que sua organização veja quais regras de detecção estão disponíveis para identificar técnicas específicas.

A finalidade primária do mapeamento é fornecer visibilidade se sua organização tiver as regras de detecção necessárias para identificar quando um alerta ou evento é acionado como resultado de um ataque de um adversário usando uma técnica específica.

Por exemplo, veja a ilustração a seguir que mostra uma lista das regras de detecção mapeadas para várias técnicas. Você também pode exibir essas informações em o MITRE-ATT&CK navegador.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você não pretende usar as regras de extração automática de SIEM do sistema de base, habilite o acúmulo automático de MITRE-ATT&CK TTPs com base no mapeamento da regra de detecção. Você pode preencher o alerta ou a regra de evento que aciona o incidente de segurança no campo Nome da regra de alerta. Você também pode preencher o campo Nome da regra de alerta usando integração de SIEM, análise de e-mail, criação manual etc. Para obter mais informações, consulte Acumular MITRE-ATT&CK informações das regras de detecção.

Nota:

O recurso de regras de detecção foi atualizado para incluir o mapeamento de uma única tática para várias técnicas. Anteriormente, era possível mapear uma única tática com uma única técnica. Se você estiver atualizando o plug-in Inteligência contra ameaças da versão 12.0.4 para uma versão superior, revise os pontos a seguir antes de usar as regras de detecção no módulo MITRE-ATT&CK.

- Você encontrará vários registros mesclados em um único registro se os campos - nome da regra, sensor de alerta, origem, categoria, subcategoria e MITRE-ATT&CK tática forem comuns.
- Os registros antigos são marcados como verdadeiros na coluna obsoleta e falsos na coluna ativa.
- Os novos registros mesclados estão disponíveis para uso e são marcados como falsos na coluna obsoleta e verdadeiros na coluna ativa.
- Depois de verificar o upgrade e exibir que todas as suas regras de detecção foram migradas com sucesso, você pode excluir os registros antigos marcados como verdadeiros na coluna descontinuado.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regras de detecção - Mapeamentos do MITRE ATT&CK**.
2. Use um dos seguintes métodos para criar sua regra de detecção:
   Método 1: criar regras de detecção manualmente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

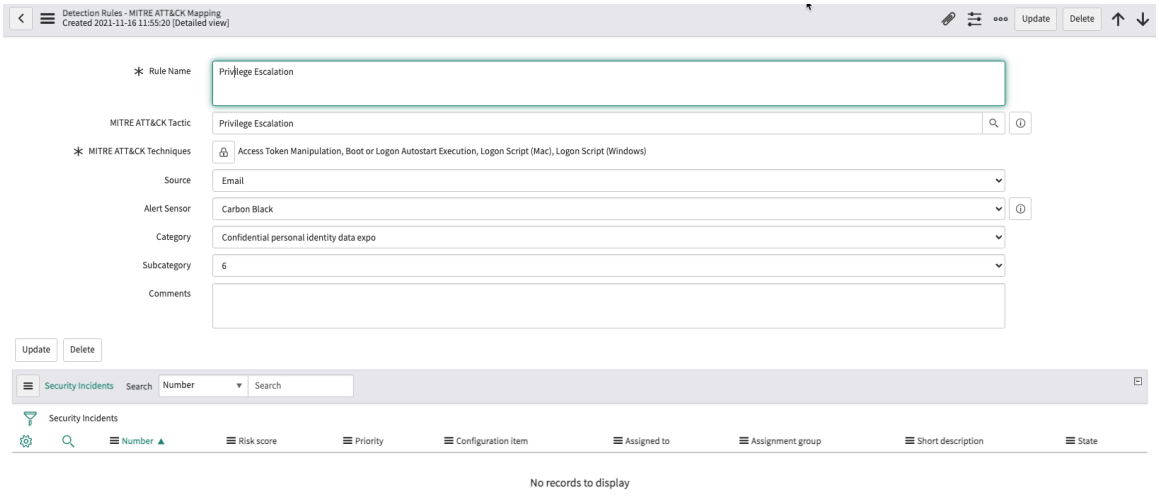
a. Clique em **Novo** e no formulário, preencha os campos.

Regras de detecção - MITRE-ATT&CK Mapeamento

Campo	Descrição
Nome de Regra	Nome da regra de detecção.
MITRE-ATT&CK Tática	Relevante MITRE-ATT&CK tática.
MITRE-ATT&CK Técnicas	Relevante MITRE-ATT&CK técnica. Você pode selecionar várias técnicas para uma única tática.
Origem	Origem do incidente de segurança, como e-mail, firewall, monitoramento de rede e assim por diante.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbon Black, CrowdStrike, McAfee e assim por diante.
Subcategoria	Subcategoria que define melhor o problema.
Categoria	Categoria que identifica o tipo de problema de segurança.
MITRE-ATT&CK Técnica	Relevante MITRE-ATT&CK técnica. Você pode selecionar várias técnicas para uma única tática.
Contagem de incidentes de segurança	O número de incidentes de segurança aos quais as técnicas são anexadas. Essa contagem aparece quando você habilita o acúmulo de MITRE-ATT&CK informações automaticamente de regras de alerta para incidentes de segurança.
Preterido	O mapeamento da regra de detecção está obsoleto.
Ativo	Opção para especificar se a regra de detecção está ativa e implantada em seu ambiente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



b. Clique em **Enviar**.

Método 2: importar e criar regras de detecção.

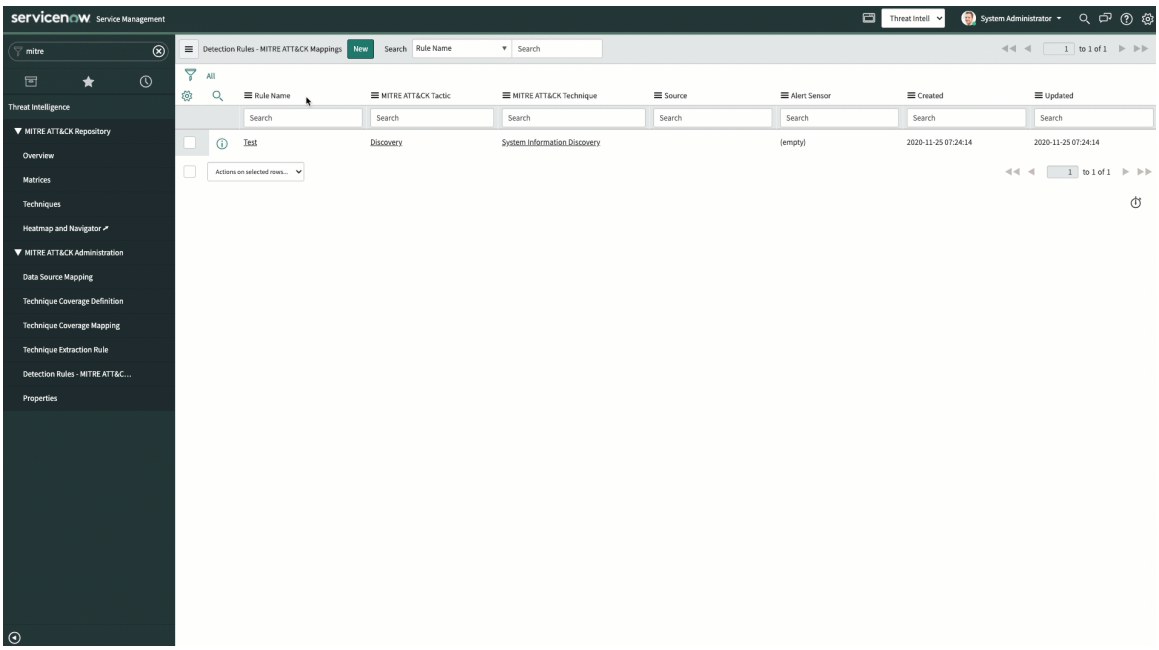
a. Clique com o botão direito do mouse no cabeçalho da coluna Nome da regra.

b. Na lista, clique em **Importar**.

c. Clique **em Criar modelo do Excel**.

d. Clique em **Download** após a conclusão da exportação. Um modelo do Excel com o nome de arquivo sn_ti_alert_rules_mitre_attack_technique_mapping é baixado para o seu computador.

Na ilustração a seguir, você vê como exportar o modelo do Excel, preencher os detalhes na planilha, carregar o arquivo, visualizar os campos e importá-los de volta para o Now Platform.



e. Abra a planilha, selecione a segunda guia da folha e revise o que você inseriu. No formulário, preencha os campos e salve o arquivo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

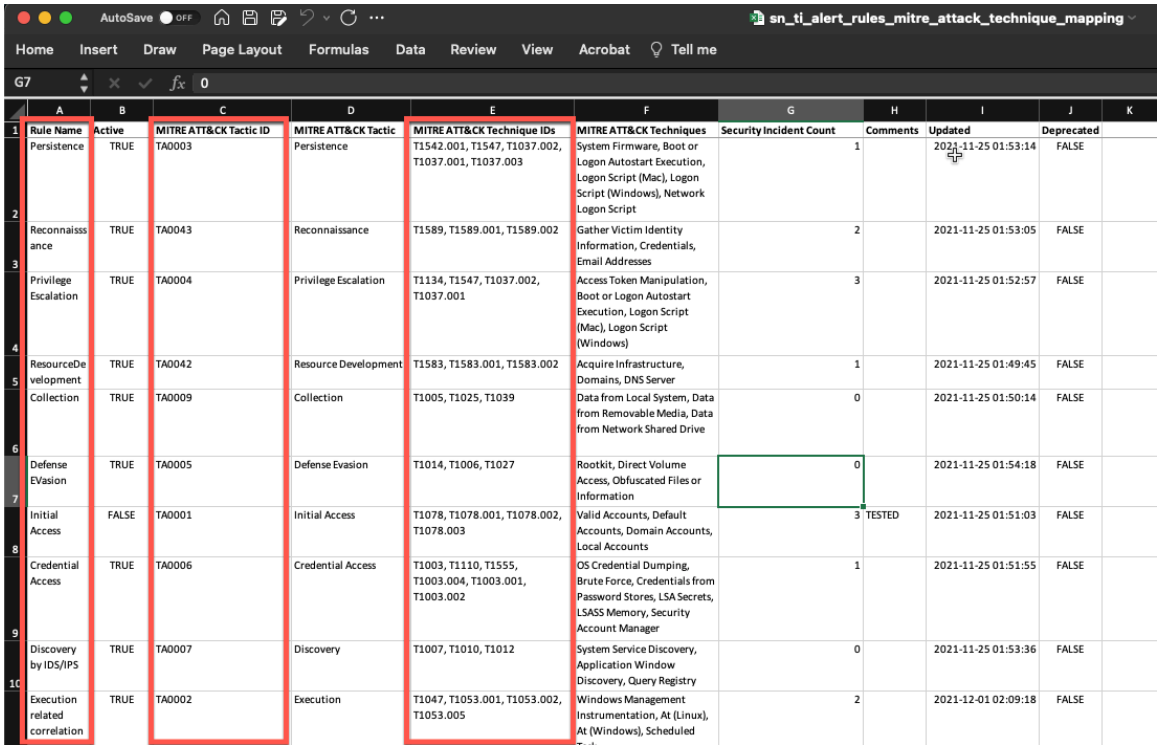
Importar modelo

Campo	Descrição
Nome de Regra	Nome da regra de detecção.
Ativo	Opção para especificar se a regra de detecção está ativa e implantada em seu ambiente.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbon Black, CrowdStrike, McAfee e assim por diante.
Categoria	Categoria que identifica o tipo de problema de segurança.
Comentários	Descrição sobre a regra de detecção.
Preterido	O mapeamento da regra de detecção está obsoleto.
MITRE-ATT&CK IDs de técnica	MITRE-ATT&CK ID de técnica, como T1546.008, para Recursos de acessibilidade.
MITRE-ATT&CK ID da tática	MITRE-ATT&CK ID de tática, como TA0003, para persistência.
Contagem de incidentes de segurança	O número de incidentes de segurança aos quais as técnicas são anexadas. Esta contagem aparece quando você habilita o acúmulo de MITRE-ATT&CK informações automaticamente de regras de alerta para incidentes de segurança e a regra de detecção está ativa.
Origem	Origem do incidente de segurança, como e-mail, firewall, monitoramento de rede e assim por diante.
Subcategoria	Subcategoria que define melhor o problema.
MITRE-ATT&CK Tática	Relevante MITRE-ATT&CK tática.
MITRE-ATT&CK Técnica	Relevante MITRE-ATT&CK técnica.

A ilustração a seguir mostra o modelo de planilha. Os campos obrigatórios são realçados em vermelho - Nome da regra, MITRE-ATT&CK ID da tática e MITRE-ATT&CK ID da técnica.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

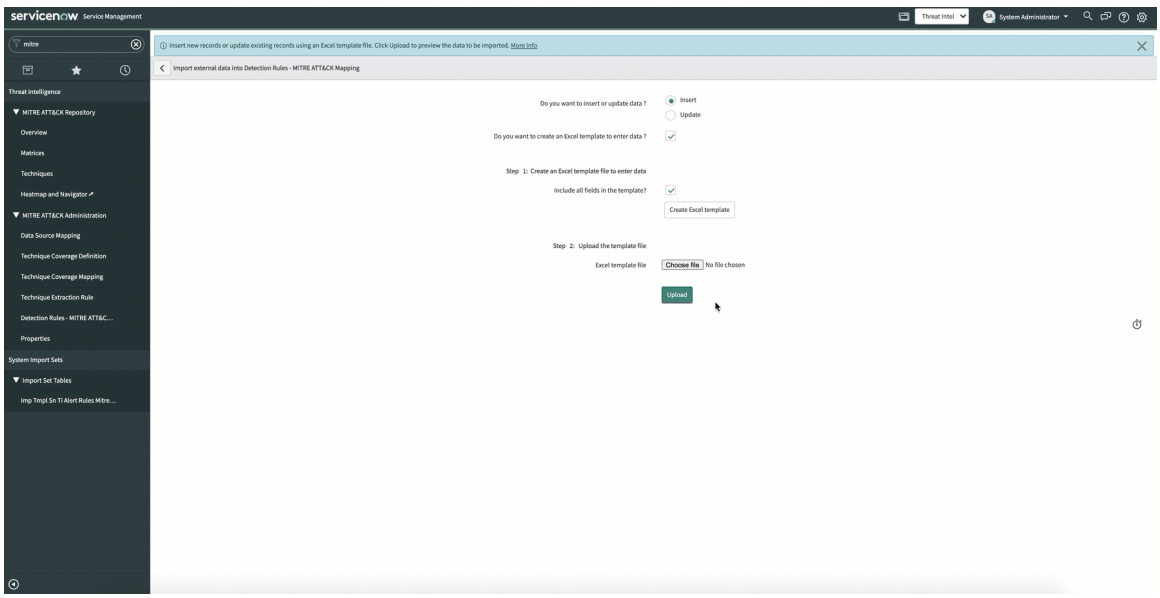
f. Clique **em Escolher arquivo** e selecione a planilha no seu computador.

g. Clique em **Carregar**.

h. Clique **em Visualizar dados importados**.

i. Visualize os mapeamentos e clique em **Concluir importação**.

A ilustração a seguir mostra como carregar a planilha, visualizar os dados, revisar os erros e concluir o processo de importação do mapeamento da regra de detecção.



Regras de técnica de extração automática para importar informações de MITRE-ATT&CK

Use as regras de extração automática do sistema de base para importar as informações MITRE-ATT&CK de quaisquer integrações de terceiros existentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar regras de extração automática de pesquisa de ameaças

Use as regras de extração automática de pesquisa de ameaças para importar as informações MITRE-ATT&CK de quaisquer integrações de terceiros Inteligência contra ameaças existentes.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Quando qualquer integração Inteligência contra ameaças, como Sandbox ou TIP, for compatível com a estrutura MITRE-ATT&CK e se as informações MITRE-ATT&CK forem analisadas em cada nível de integração, as informações serão exibidas em cada registro de resultado de pesquisa de ameaças. No entanto, nem todas as integrações Inteligência contra ameaças analisam as informações MITRE-ATT&CK. A regra de extração automática global de pesquisa de ameaças pode extrair MITRE-ATT&CK informações de todas as Inteligência contra ameaças integrações.

Você pode optar por acumular as informações MITRE-ATT&CK automaticamente dos resultados da pesquisa de ameaças para um incidente de segurança. Para o acúmulo automático de resultados de pesquisa de ameaças para incidentes de segurança, habilite a propriedade do sistema. Como alternativa, você pode acumular as informações manualmente para cada pesquisa de ameaça individual.

O sistema base Inteligência contra ameaças extrai automaticamente as MITRE-ATT&CK informações da carga bruta de integrações de terceiros para o registro de resultado da pesquisa de ameaças, se a integração Inteligência contra ameaças fornecer MITRE-ATT&CK informações, como a técnica ou a tática.

Se as informações de MITRE-ATT&CK não estiverem disponíveis no campo de carga bruta do registro de pesquisa de ameaças, você deverá definir sua própria regra para extração automática da integração de terceiros.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regra de extração da técnica**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de extração de técnica

Campo	Descrição
Nome	Nome da regra de extração automática.
Tipo de Regra	Tipo de regra de extração automática. Selecione **Pesquisa de ameaças**.
Ignorar extração automática	A configuração que, por padrão, está desmarcada. Esta configuração permite a extração automática de MITRE-ATT&CK técnicas.
Mecanismo de Origem	Mecanismo de origem.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Global	Configuração do mecanismo de origem. Quando você define o mecanismo de origem como **Global**, a extração é executada em todos os resultados de integração de pesquisa de ameaças.
Descrição	Descrição da regra de extração automática.
Método de processo	Regex ou um método de script que você especifica para vincular as informações da técnica da carga bruta.
Extração de Regex	Opção que você especifica para o **Campo de destino** ao usar o método de extração regex. Regex é o padrão.
Extração de script	Processo selecionado ao executar um script. O script revisa o seguinte: ◦ ThreatLookupResultSysId:sys_id do registro do resultado da pesquisa de ameaças ◦ sourceName: nome da origem da pesquisa de ameaças.
Extração de tática	Opção que você especifica para extrair informações relacionadas à tática da carga bruta. Se uma carga útil contiver informações relacionadas a táticas e técnicas específicas, você poderá extrair e anexar as informações ao incidente de segurança.

4. Clique em **Enviar**.

Usar regras de extração automática de SIEM

Use as regras de extração automática de SIEM para importar as informações MITRE-ATT&CK de quaisquer integrações de terceiros SIEM existentes Operações de segurança.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

A regra de extração de técnica está disponível para todas as integrações de SIEM do sistema base Operações de segurança, como Splunk, IBM QRadar e ArcSight. Quando o Now Platform ingere dados de alerta ou evento dessas integrações de SIEM e eles contêm MITRE-ATT&CK informações, o Now Platform processa a carga bruta e extrai automaticamente as MITRE-ATT&CK informações.

Se o seu Now Platform contiver integrações de SIEM do sistema de base, isso significa que as regras de extração de técnica já foram criadas no módulo MITRE-ATT&CK. Você deve revisar e modificar as regras conforme necessário.

Habilite a regra de extração automática de SIEM ou a regra de alerta de cada vez.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

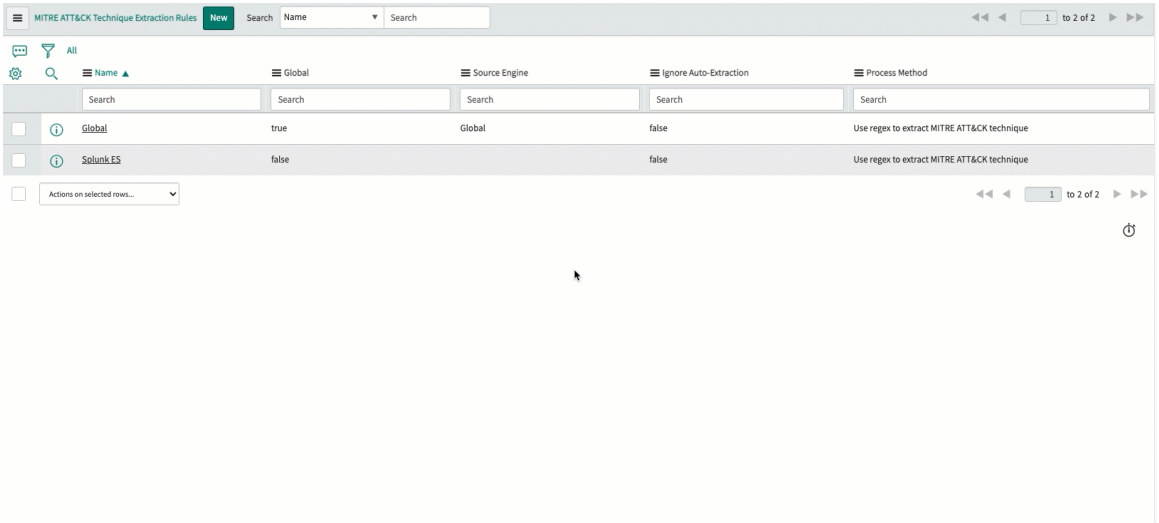
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regra de extração da técnica**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de extração de técnica

Campo	Descrição
Nome	Nome da regra de extração automática.
Tipo de Regra	Tipo de regra de extração automática. Selecione **SIEM**.
Ignorar extração automática	A configuração que, por padrão, está desmarcada. Esta configuração permite a extração automática de MITRE-ATT&CK técnicas.
Importar Tabela	Tabela de importação que é mapeada automaticamente para integrações de SIEM do sistema de base. Revise este campo para outras integrações de SIEM para as informações de MITRE-ATT&CK e mapeie de acordo.
Importar campo	Campo de importação que é mapeado automaticamente para integrações de SIEM do sistema de base. Revise este campo para outras integrações de SIEM para as informações de MITRE-ATT&CK e mapeie de acordo.
Descrição	Regra de extração automática.
Método de processo	Regex ou um método de script que você especifica para vincular as informações da técnica da carga bruta.
Extração de Regex	Opção que você especifica para o **Campo de destino** ao usar o método regex. A extração de Regex é o método de processo padrão.
Extração de script	Método de processo de script que você usa se quiser personalizar como as informações MITRE-ATT&CK são extraídas.
Extração de tática	Opção que você especifica para extrair informações relacionadas à tática da carga bruta. Se uma carga útil contiver informações relacionadas a táticas e técnicas específicas, você poderá extrair e anexar as informações ao incidente de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você vê um exemplo da regra de extração da técnica Splunk Enterprise SIEM na exibição do formulário. Esta regra é semelhante a todas as outras regras de extração da técnica SIEM.



4. Clique em **Enviar**.

Revisar grupo de ameaças e mapeamento de técnicas MITRE-ATT&CK

Revise o grupo de ameaças e as informações de mapeamento de objeto para objeto de técnicas que são importadas das coleções MITRE TAXII. Este mapeamento permite que você exiba o grupo de técnicas e o mapeamento de técnica correspondente.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

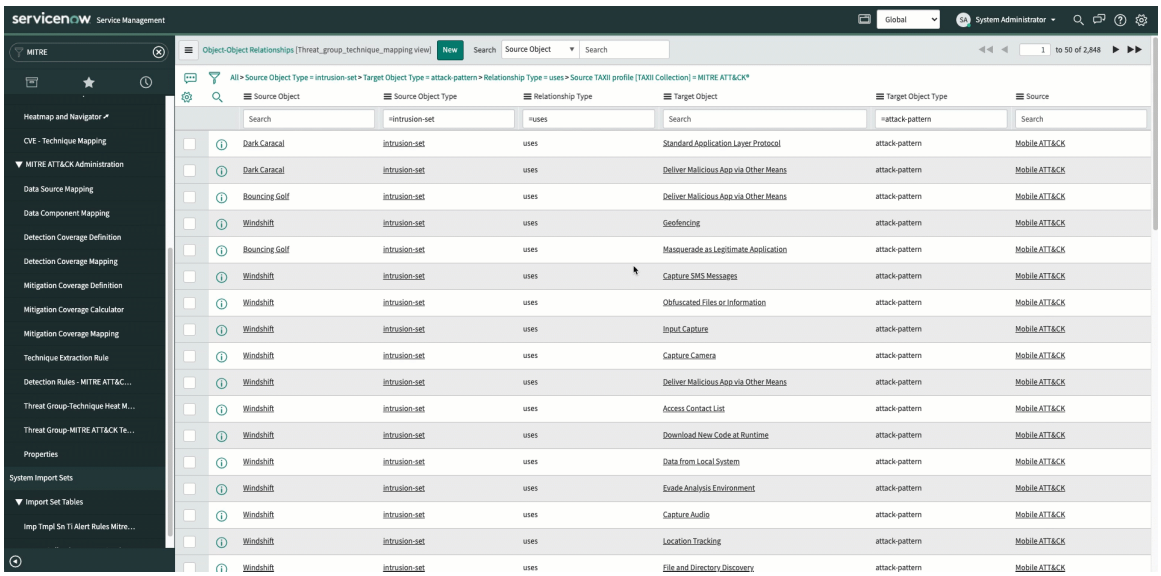
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Grupo de ameaças - Técnicas do MITRE ATT&CK**.
2. Clique com o botão direito do mouse no **Objeto de origem** e selecione **Agrupar por objeto de origem** para exibir todos os padrões de ataque associados a um grupo de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra o grupo de ameaças admin@338 e os vários padrões de ataque adotados por esse grupo de ameaças que fazem parte da origem de ataque empresarial.



Grupo de ameaças para definição do mapa térmico da técnica

Defina o grupo de ameaças para definir o mapa térmico da técnica para que, no mapa térmico, você possa medir e detectar os padrões de ataque que os grupos de ameaças estão usando para atacar sua organização. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um grande número de invasores.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação
- sn_ti.read: acesso de leitura

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição do mapa térmico da técnica de grupo de ameaças**.
2. Revise o grupo de ameaças para definição do mapa térmico da técnica e personalize as entradas para o seu ambiente.

Definições do mapa térmico da técnica de grupo de ameaças

Campo	Descrição
Número de grupos de ameaças (intervalo mínimo)	O número mínimo de grupos de ameaças que usam uma técnica específica.
Número de grupos de ameaças (intervalo máximo)	O número máximo de grupos de ameaças que usam uma técnica específica. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um grande número de invasores.
Cor do mapa térmico	Cor atribuída à categoria do grupo de ameaças. A cor que você define é usada

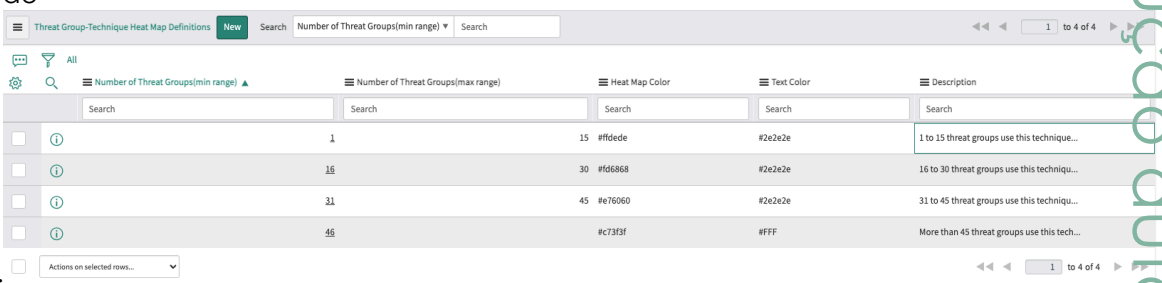
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	para realçar a categoria do grupo de ameaças no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB (A).
Cor do texto	Cor atribuída ao texto do grupo de ameaças. A cor que você define é usada para destacar os grupos de ameaças no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB (A).
Descrição	Descrição sobre o intervalo e a definição do grupo de ameaças.

Nota: Certifique-se de não sobrepor os intervalos de contagem de grupos de ameaças se personalizar o intervalo de grupos de ameaças (mínimo ou máximo).

A ilustração a seguir mostra o grupo de ameaças para a lista de definições de mapa térmico de



técnica.

3. Para adicionar uma entrada, clique em **Novo**, conclua as entradas e clique em **Enviar**.

Revise as MITRE-ATT&CK propriedades do sistema

Revise os valores de propriedade do sistema MITRE-ATT&CK.

Antes de Iniciar

Função necessária: sn_ti.admin, sn_si.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Propriedades**.
2. No formulário, preencha os campos.

MITRE-ATT&CK Formulário de propriedades

Campo	Descrição
Acumular informações do MITRE ATT&CK automaticamente dos observáveis para o incidente de segurança [sn_ti.rollup_mitre_att&ck_technique_observable_si]	Acúmulo de MITRE-ATT&CK informações de observáveis para o incidente de segurança. Para obter mais informações, consulte Associar informações do MITRE ATT&CK a observáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Valor padrão: sim
Acumular informações do MITRE ATT&CK automaticamente dos resultados da pesquisa de ameaças para o incidente de segurança [sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	Acúmulo de MITRE-ATT&CK informações dos resultados da pesquisa de ameaças para o incidente de segurança. Para obter mais informações, consulte Extração automática de pesquisa de ameaças. Valor padrão: sim
Acumular informações do MITRE ATT&CK automaticamente de regras de alerta para incidentes de segurança [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	Acúmulo de MITRE-ATT&CK informações de TTP automaticamente de regras de alerta para incidentes de segurança. Para obter mais informações, consulte regras de detecção de mapa. Valor padrão: não
Acumular informações do MITRE ATT&CK automaticamente de incidentes de segurança secundários para incidentes de segurança primários [sn_ti.rollup_mitre_att&ck_technique_child_si_v]	Acumule MITRE-ATT&CK informações automaticamente de incidentes de segurança secundários para o incidente de segurança primário. Valor padrão: sim
A habilitação desta propriedade permite o mapeamento de campos de incidente de segurança, como categoria e subcategoria, com regras de detecção na tabela "Regras de detecção - mapeamento MITRE ATT&CK" [sn_ti.enable_category_mapping_with_alert_rule]	Categoria e subcategoria na página de mapeamento Regras de detecção - MITRE ATT&CK. Valor padrão: não
Tempo (em horas) para calcular "CVE - Contagem de VUL" [sn_ti.time_to_calculate_cve_vits_count]	O tempo programado em horas para calcular as informações de CVE e VUL. Valor padrão: 24

3. Clique em **Salvar**.

Usando MITRE-ATT&CK para detectar e analisar ameaças

Use a estrutura MITRE-ATT&CK] nos módulos Inteligência contra ameaças e SIR para detectar e analisar ameaças à sua organização.

Associar MITRE-ATT&CK™ informações a incidentes de segurança

Associe as MITRE-ATT&CK táticas e técnicas ao incidente de segurança para obter uma melhor análise de incidentes e ameaças de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Adicione as MITRE-ATT&CK informações de táticas e técnicas ao incidente de segurança para que você possa correlacionar suas informações de incidente de segurança e ameaça para uma análise melhor. Por exemplo, sua organização pode estar recebendo informações relacionadas a táticas, técnicas e procedimentos (TTP) de fontes de terceiros, como Inteligência contra ameaças relatórios ou outras fontes fora de Security Incident Response. Em seguida, você adiciona essas informações novamente a SIR para obter melhor correlação e análise de ameaças.

Você pode optar por acumular as informações MITRE-ATT&CK automaticamente dos resultados da extração automática de pesquisa de ameaças, de observáveis ou de um incidente de segurança secundário para um incidente de segurança. Para acúmulo automático de incidentes de segurança, habilite a propriedade do sistema. Como alternativa, você pode acumular as informações manualmente para cada pesquisa de ameaça individual ou observável.

Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique no link relacionado **Associar técnica do MITRE ATT&CK**.
   O painel Associar técnica do MITRE ATT&CK é exibido.

   Esta ilustração mostra como navegar até a lista relacionada e procurar Associar MITRE-ATT&CK Técnica, revisar o Enterprise ATT&CK de origem, adicionar um Impacto de tática e adicionar uma técnica Desligamento/reinicialização do sistema.

   Associar informações do MITRE ao incidente de segurança
4. Selecione **Origem**.

   Nota: Somente as coleções e matrizes que foram ativadas aparecem na lista de origem.

   As táticas e técnicas associadas à origem estão disponíveis para seleção. Você também pode associar várias origens.
5. Selecione a **Tática** e as **Técnicas**.
6. Opcional: Revise as informações com base na relevância com o incidente de segurança e faça o seguinte:
   - Para remover completamente a associação, clique no ícone da lixeira. Clicar neste ícone exclui a origem e suas táticas e técnicas associadas.
   - Para remover uma tática, clique no ícone de menos ao lado da tática.
   - Para remover uma técnica, clique no ícone x ao lado da técnica.
7. Clique em **Salvar**.

Resultados

As informações MITRE-ATT&CK estão associadas ao incidente de segurança. Agora você pode exibir as informações associadas no **cartão MITRE ATT&CK**.

Associar MITRE-ATT&CK informações a incidentes de segurança encerrados

Agora você pode associar MITRE-ATT&CK táticas e técnicas aos incidentes de segurança encerrados para obter uma melhor análise de ameaças e incidentes de segurança.

Associar informações do MITRE ao incidente de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o cartão MITRE-ATT&CK para ver informações relacionadas em um incidente de segurança

Você pode usar o cartão MITRE-ATT&CK para ver as informações relacionadas a MITRE-ATT&CK em um incidente de segurança.

Depois que as informações são acumuladas de uma pesquisa de ameaças, um observável ou uma integração de SIEM, elas são adicionadas ao incidente de segurança. Em seguida, as informações agregadas são apresentadas no cartão MITRE-ATT&CK. O **cartão MITRE ATT&CK** fornece duas exibições:

- Exibição do navegador: esta exibição, que é semelhante ao navegador MITRE-ATT&CK, mostra todas as técnicas que foram adicionadas manualmente ou acumuladas das tabelas de pesquisa de observáveis ou ameaças. **Mostrar origem das técnicas** exibe a origem da técnica se ela tiver sido acumulada manualmente ou por meio de uma origem. **Mostrar ID** exibe o ID da técnica.

  A ilustração a seguir mostra como navegar até a exibição do navegador **de cartões do MITRE ATT&CK**. Ao clicar em qualquer um dos links disponíveis, as informações são abertas no módulo Inteligência contra ameaças.

  Cartão do MITRE ATT&CK: exibição do navegador e exibição de lista

- Exibição de lista: esta exibição mostra os dados em um formato de lista ou tabela. Você pode ver todos os dados distribuídos em diferentes tabelas e grupos nesta exibição.

  A ilustração a seguir mostra como navegar até a exibição de lista de cartões do MITRE ATT&CK. Ao clicar em qualquer um dos links disponíveis, as informações são abertas no módulo Inteligência contra ameaças.

Associar MITRE-ATT&CK informações a observáveis

Associe MITRE-ATT&CK táticas e técnicas a um observável para obter uma melhor análise de incidentes e ameaças de segurança em um nível granular.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Alguns SIEMs podem fornecer MITRE-ATT&CK informações com eventos, alertas ou observáveis. Para associar as informações MITRE-ATT&CK em um nível granular, você pode adicionar as informações a um observável.

Você pode optar por acumular as informações MITRE-ATT&CK automaticamente dos observáveis para um incidente de segurança. Para o acúmulo automático de observáveis para incidentes de segurança, habilite a propriedade do sistema. Como alternativa, você pode acumular as informações manualmente para cada observável.

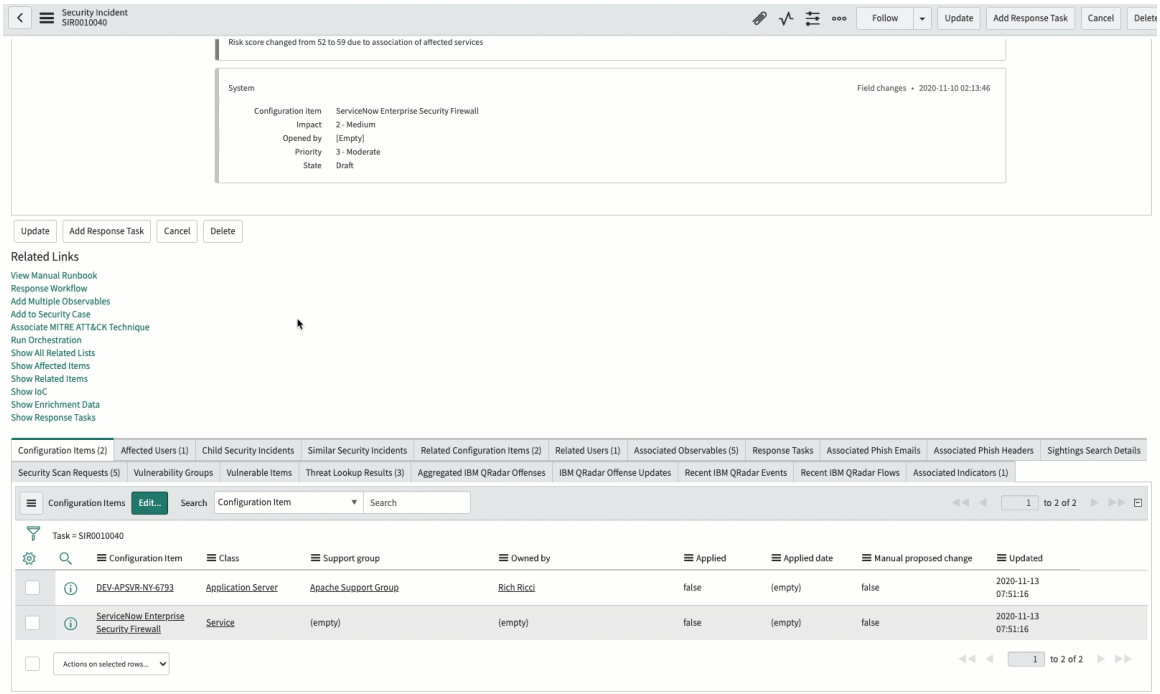
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Aponte para o observável que você deseja associar, clique com o botão direito do mouse e selecione **Associar técnica do MITRE ATT&CK**.

   Na ilustração a seguir, você pode ver como navegar na lista relacionada até **Associar técnica do MITRE ATT&CK**, revisar a origem e adicionar uma tática e uma técnica.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



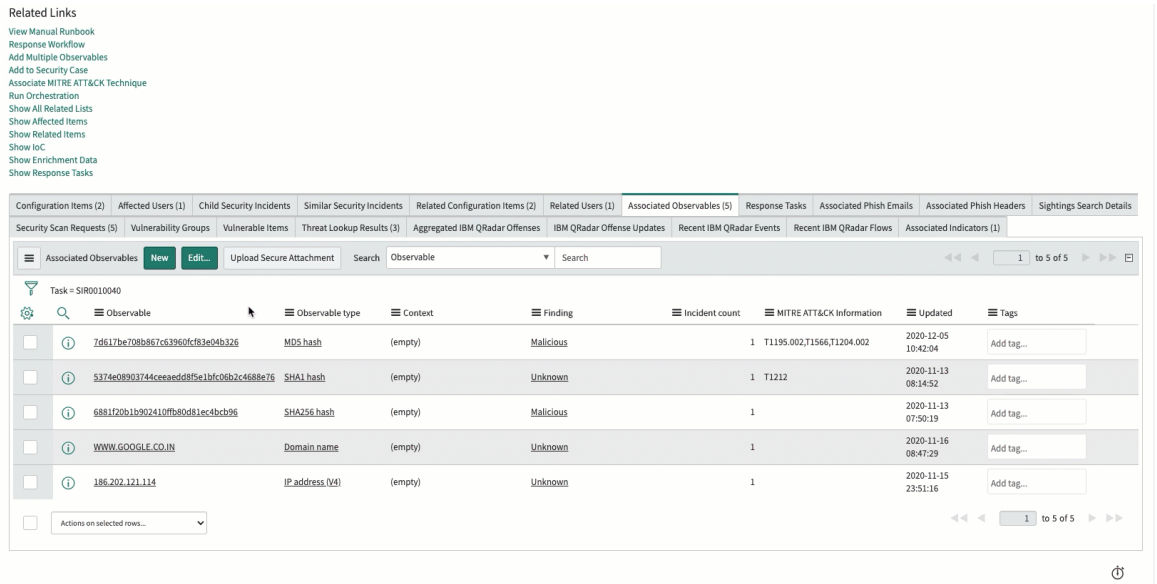
5. Nas listas de origens, revise a **Origem**.

   Nota: Somente as coleções e matrizes que foram ativadas aparecem na lista de origem.

6. Revise a **Tática** e as **Técnicas**e adicione ou remova-as com base na relevância com o observável.
7. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem na coluna MITRE-ATT&CK Informações na lista relacionada de observáveis.
8. Selecione o observável e, no menu Ações, clique em **Acumular informações do MITRE ATT&CK no SI**.
   Se você tiver habilitado acúmulo automático de MITRE-ATT&CK informações de observáveis para incidente de segurança, as informações serão acumuladas automaticamente. Se você não habilitou o acúmulo automático, será necessário fazer isso manualmente.

   A ilustração a seguir mostra como selecionar um observável e acumular as informações MITRE-ATT&CK para um incidente de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Para ter uma exibição agregada das técnicas associadas aos observáveis, selecione dois ou mais observáveis na lista e, no menu **Ações** na lista de linhas selecionadas, clique em **Mostrar informações do MITRE ATT&CK**.

Resultados
Uma exibição agregada das informações do MITRE ATT&CK para os observáveis selecionados é exibida.

Associar MITRE-ATT&CK informações ao caso de segurança

Associe MITRE-ATT&CK táticas e técnicas a um caso de segurança para melhorar a gestão de casos de segurança e a análise de ameaças em um nível granular.

Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Selecione o caso de segurança que você deseja aprimorar com as informações do MITRE-ATT&CK.
3. Na lista relacionada, clique em **Associar técnica do MITRE ATT&CK**.

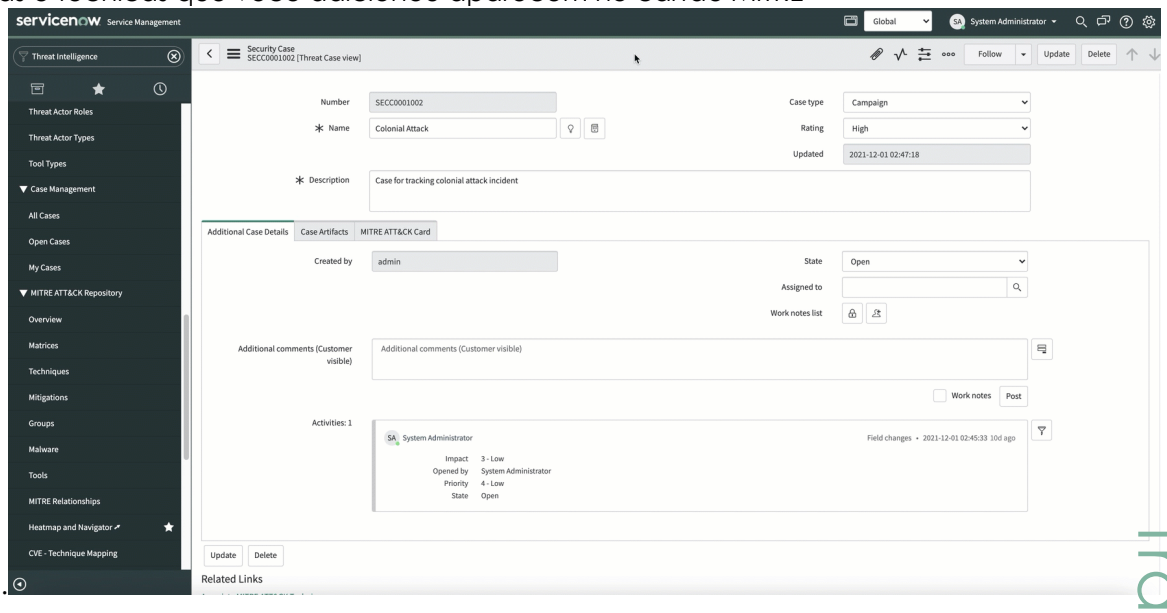
   Na ilustração a seguir, você pode ver como navegar na lista relacionada até **Associar técnica do MITRE ATT&CK**, revisar a origem e adicionar uma tática e uma técnica.

4. Nas listas de origens, revise a **Origem**.
5. Revise a **Tática** e as **Técnicas**e adicione ou remova-as com base na relevância do caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem no cartão MITRE-ATT&CK.



Acumular MITRE-ATT&CK informações usando os resultados da pesquisa de ameaças

Se você não habilitou o acúmulo automático de informações de MITRE-ATT&CK, poderá fazer isso manualmente.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

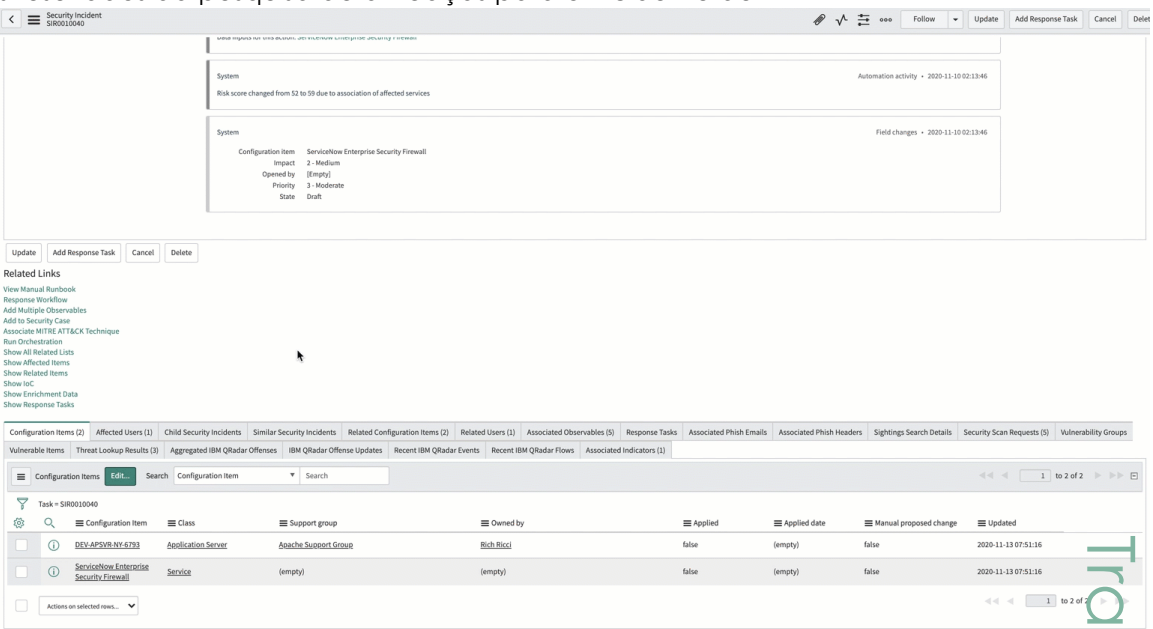
Se você tiver habilitado acúmulo automático de MITRE-ATT&CK informações dos resultados da pesquisa de ameaças ao incidente de segurança, as informações serão acumuladas automaticamente. Se você não habilitou o acúmulo automático, poderá fazer isso manualmente.

Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Resultados da pesquisa de ameaças**.
4. Selecione o observável e, no menu Ações, clique em **Acumular informações do MITRE ATT&CK no SI**.
   Você pode selecionar vários observáveis e acumular as informações.
5. Clique em **Recarregar** para confirmar as mudanças.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra como selecionar um observável e acumular os resultados da pesquisa de ameaças para o incidente de segurança.



Você pode exibir o cartão MITRE-ATT&CK para confirmar que os resultados da pesquisa de ameaças foram acumulados para o incidente de segurança.

Acumular MITRE-ATT&CK informações das regras de detecção

Habilite o acúmulo de MITRE-ATT&CK informações das regras de detecção para os incidentes de segurança para obter uma melhor análise de ameaças e incidentes de segurança.

Antes de Iniciar

Função necessária: nenhuma

Certifique-se de ter realizado o seguinte:

- Habilite a propriedade Acumular informações do MITRE ATT&ACK automaticamente das regras de alerta para a propriedade de incidentes de segurança no módulo Propriedades. Por padrão, esta opção está desabilitada. Para obter mais informações, consulte Revisão das propriedades do sistema MITRE-ATT&CK.
- Execute o mapeamento de regras de detecção para MITRE-ATT&CK TTPs no módulo Mapeamento de regras de detecção – MITRE ATT&CK TTP. O nome da regra de detecção deve corresponder ao nome da regra de alerta que aciona o incidente de segurança. Para obter mais informações, consulte Criar e mapear regras de detecção.

Por Que e Quando Desempenhar Esta Tarefa

Se você não pretende usar as regras de extração automática de SIEM do sistema de base, habilite o acúmulo automático de MITRE-ATT&CK TTPs com base no mapeamento da regra de detecção. Você pode preencher o alerta ou a regra de evento que aciona o incidente de segurança no campo Nome da regra de alerta. Você também pode preencher o campo Nome da regra de alerta usando integração de SIEM, análise de e-mail, criação manual e assim por diante.

Procedimento

1. Navegar até **Administração do MITRE ATT&CK** > **Propriedades**.
2. Habilite a propriedade Acumular informações do MITRE ATT&ACK automaticamente das regras de alerta para a propriedade de incidentes de segurança e clique em **Salvar**.

Tradução automática

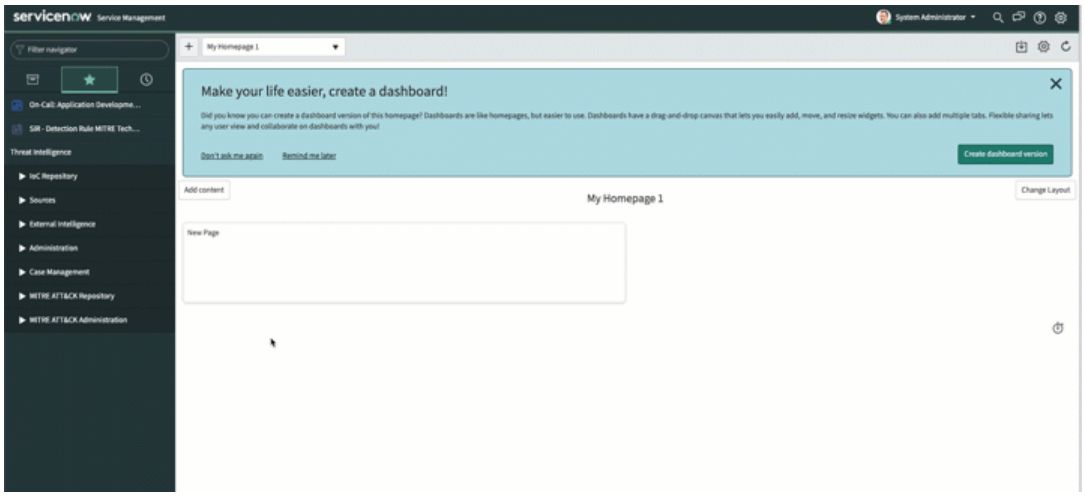
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, esta opção está desabilitada.

3. Você precisa preencher o campo Nome da **regra de alerta** do incidente de segurança com as regras de alerta necessárias.

   Nota: Certifique-se de adicionar o nome exato da regra de alerta. Para adicionar várias regras, você precisa adicionar as regras usando um separador de vírgulas.

4. Clique com o botão direito do mouse no formulário e clique em **Salvar**.
   Se o valor do nome da regra de alerta no incidente de segurança corresponder a um registro no módulo Regra de detecção - Mapeamento de TTP do MITRE ATT&CK, as técnicas e táticas correspondentes associadas à regra de alerta serão vinculadas ao incidente de segurança automaticamente.



5. Abra o incidente de segurança, selecione o **cartão MITRE ATT&CK** e valide se as técnicas foram acumuladas.
6. Habilite a opção **Mostrar origem das técnicas** para exibir a origem das técnicas.
   A origem das técnicas deve ser Regra de detecção.

Acumular MITRE-ATT&CK informações de incidentes de segurança secundários

Se você não habilitou o acúmulo automático de informações de MITRE-ATT&CK, poderá fazer isso manualmente.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Se você tiver habilitado acúmulo automático de MITRE-ATT&CK informações de incidentes de segurança secundários, as informações serão acumuladas automaticamente. Se você não habilitou o acúmulo automático, poderá fazer isso manualmente.

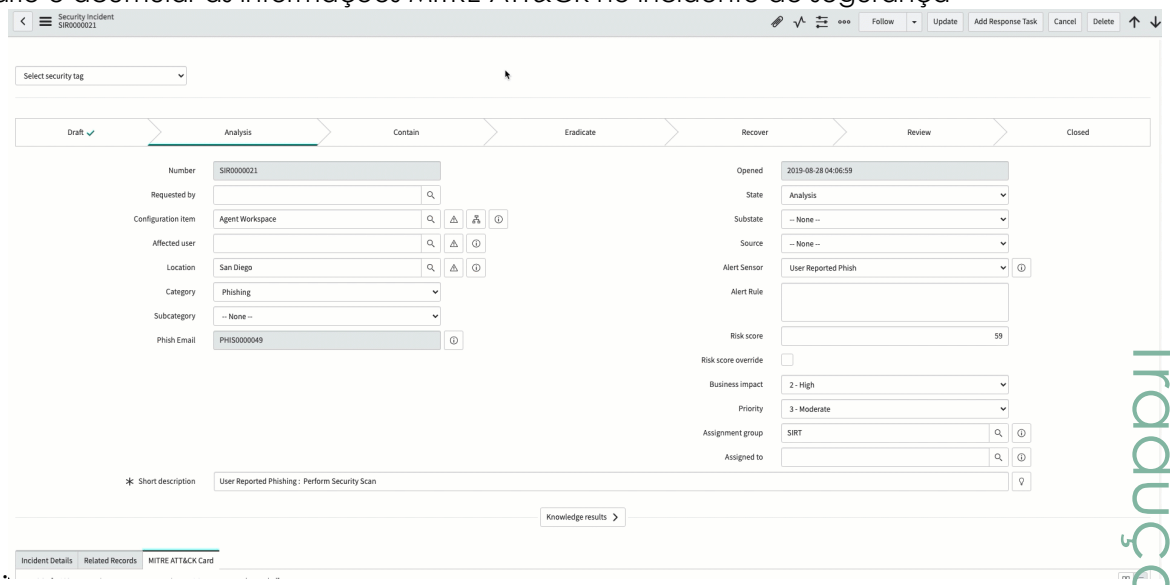
Procedimento

1. Navegar até **Todos** > **Incidentes** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança primário que você deseja aprimorar com as informações secundárias MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Incidentes de segurança secundários**.
4. Selecione o incidente de segurança secundário e, no menu Ações, clique em **Acumular informações do MITRE ATT&CK no SI**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode clicar em **Mostrar informações do MITRE ATT&CK** para exibir as informações do MITRE do incidente de segurança secundário antes de acumular as informações do MITRE ATT&CK.

5. Clique em **Recarregar** para confirmar as mudanças.
6. Clique no **cartão do MITRE ATT&CK** para exibir a origem das técnicas.
   A ilustração a seguir mostra como selecionar o incidente de segurança secundário e acumular as informações MITRE-ATT&CK no incidente de segurança primário.



   Você pode exibir o cartão MITRE-ATT&CK para confirmar que as informações do incidente de segurança secundário MITRE-ATT&CK foram acumuladas no incidente de segurança primário.

Executar análise de link e caça a ameaças usando MITRE-ATT&CK filtros específicos

Correlacione e execute a análise de link de observáveis, incidentes de segurança e MITRE-ATT&CK informações relacionadas para que sua organização possa começar a procurar ameaças.

Antes de Iniciar

Função necessária: sn_ti.mitre_analyst, sn_si.read

Por Que e Quando Desempenhar Esta Tarefa

Depois de associar os incidentes de segurança às informações MITRE-ATT&CK, você pode usar os filtros específicos MITRE-ATT&CK para caçar ameaças. Use os filtros MITRE-ATT&CK com os filtros Security Incident Response existentes para correlacionar e executar a análise de link.

Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Clique em **Atualizar lista personalizada** para adicionar as MITRE colunas.
3. Selecione uma condição de filtro para que você possa exibir MITRE informações e associações relacionadas a incidentes ou observáveis de segurança:
   - MITRE-ATT&CK Grupo adversário
   - MITRE-ATT&CK Fonte de dados
   - MITRE-ATT&CK Procedimento (malware)
   - MITRE-ATT&CK Procedimento (ferramentas)

Tradução automática

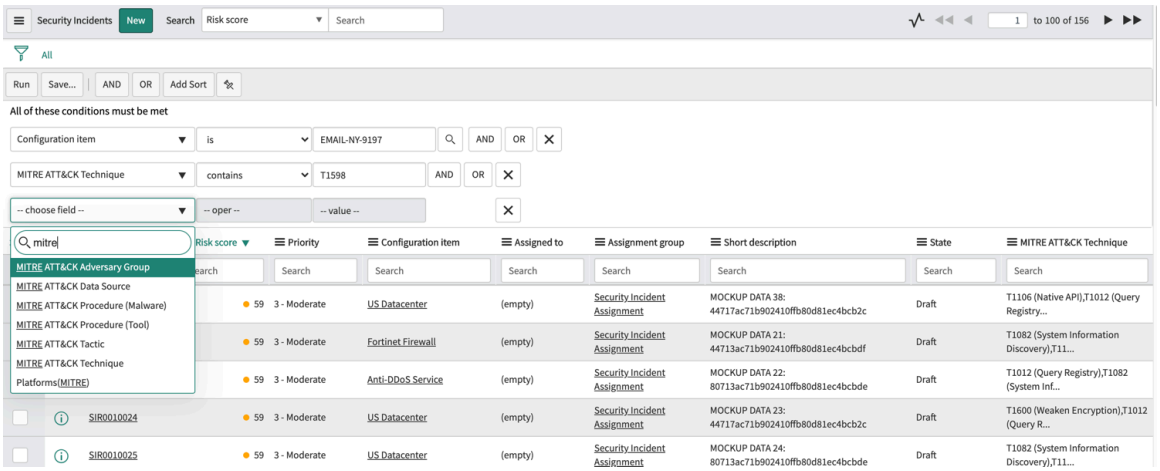
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- MITRE-ATT&CK Tática
- MITRE-ATT&CK Técnica

4. Crie uma condição de filtro com base nos critérios acima e clique em **Executar** para executar uma análise de link ou correlação entre incidentes de segurança, observáveis e MITRE-ATT&CK informações relacionadas.

   Nota: Os dados MITRE-ATT&CK são armazenados como uma cadeia de caracteres e você só pode usar **contém** como o operador para condições de filtro.

   Por exemplo, se você quiser revisar se um item de configuração (IC) está comprometido, selecione um IC. Em seguida, você correlaciona o IC com as técnicas que estão presentes adicionando um MITRE-ATT&CK ID de técnica. Você pode continuar a criar seus critérios de filtro para correlacionar as informações e para a detecção de ameaças.



MITRE-ATT&CK mapa térmico e navegador

Você pode usar o mapa térmico MITRE-ATT&CK e o navegador para navegação básica e para visualizar a cobertura geral de detecção da técnica.

Visão geral do mapa térmico MITRE-ATT&CK e do navegador

Você pode usar o navegador com os filtros primários para navegação básica e observação de matrizes ATT&CK. O mapa térmico destaca o espetro da cobertura de detecção, incluindo os pontos cegos em que sua organização não tem cobertura. Isso está disponível depois de mapear a cobertura de detecção da técnica.

Com o mapa térmico e o navegador, você pode:

- Identifique com rapidez e eficiência as capacidades de detecção da sua organização e destaque lacunas na cobertura de detecção da técnica.
- Procure ameaças e execute a correlação de ameaças usando recursos associados.

Acessar o mapa térmico e o navegador MITRE-ATT&CK

Acesse o mapa térmico MITRE-ATT&CK e o navegador para que você possa visualizar a matriz que permite usar o ATT&CK.

Antes de Iniciar
Função necessária: sn_ti.read, sn_ti.mitre_analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode revisar o mapa térmico, usar os filtros para correlacionar e executar a análise de link de MITRE-ATT&CK, informações, observáveis e incidentes de segurança em sua organização.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Mapa térmico e navegador**.
   O mapa térmico e o navegador são abertos em uma nova guia.
2. Selecione a origem para preencher o mapa térmico.

   Nota: Somente as coleções e matrizes que foram ativadas aparecem na lista de origem.

   Na ilustração a seguir, você vê como navegar até o mapa térmico e o navegador e como selecionar a origem, que é o Enterprise ATT&CK neste exemplo.

   Navegue até e selecione a origem para preencher o mapa térmico
3. Use a caixa de pesquisa para encontrar rapidamente uma tática ou técnica específica usando seu nome ou ID.

   A ilustração a seguir mostra como pesquisar uma tática, técnica ou qualquer informação contida nelas. Use a pesquisa para detalhar rapidamente uma tática ou técnica específica.
4. Clique em **Filtros** e selecione um filtro entre os filtros Primário ou Avançado.
5. Clique em **Aplicar** e controle os filtros da seguinte forma:
   - Para salvar seus filtros, crie uma exibição personalizada. Você pode criar e salvar três exibições personalizadas.
   - Para remover os filtros selecionados, clique em **Restaurar filtros padrão** para carregar a exibição salva padrão.
   - Para limpar todos os filtros e a exibição existente, clique em **Limpar todos os filtros**.

   Nota: As exibições que você salva são específicas para um usuário.
6. Clique **em Ocultar subtécnicas** para remover todas as subtécnicas da exibição do mapa térmico.
   Se uma técnica tiver subtécnicas, você poderá clicar no ícone de expansão para exibir as subtécnicas.

Como usar as exibições personalizadas

As exibições personalizadas no mapa térmico e no navegador MITRE-ATT&CK ajudam a salvar e exibir seus filtros favoritos na próxima vez que você acessar o mapa térmico.

Nota: Você pode criar e salvar três exibições personalizadas para cada coleção MITRE-ATT&CK por usuário.

Criar uma exibição

Depois de selecionar os filtros necessários nos filtros Primário ou Avançado, clique no botão de reticências (…) no cabeçalho Filtros e selecione **Criar uma nova exibição**. Insira o nome de exibição personalizado e **Salvar exibição**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibições padrão

Clique **em Salvar como uma exibição padrão** para carregar diretamente a exibição na próxima vez que você acessar o mapa térmico. Você pode definir uma exibição padrão para cada uma das coleções.

Nota: Se você estiver atualizando o plug-in Inteligência contra ameaças de uma versão mais antiga, a exibição padrão existente da versão antiga aparecerá como uma exibição personalizada.

A ilustração mostra como criar uma exibição personalizada no mapa térmico

Atualizar uma exibição

Você pode fazer atualizações em uma exibição personalizada existente modificando os filtros Primário ou Avançado necessários. Selecione uma exibição personalizada, atualize os filtros conforme necessário e clique no botão de reticências (...) no cabeçalho Filtros e selecione **Atualizar exibição** para salvar os filtros.

Esta ilustração mostra como atualizar uma exibição personalizada.

Gerenciar exibições personalizadas

Use as caixas de seleção ao lado de cada exibição personalizada para aplicar o filtro de exibição personalizado selecionado.

Clique no botão de reticências (…) ao lado de cada nome de exibição personalizado para controlar as exibições personalizadas da seguinte forma:

- Defina uma exibição padrão.
- Remova uma exibição personalizada como a exibição padrão. Isso não exclui a exibição personalizada.
- Renomeie a exibição personalizada.
- Exclua a exibição personalizada.

Esta ilustração mostra como gerenciar exibições personalizadas.

Exportar uma exibição salva

Para exportar as exibições personalizadas salvas para arquivos JSON, clique nas reticências (...) no cabeçalho Filtros e selecione **Exportar exibições salvas**. Clique no ícone de download da exibição personalizada que você deseja baixar para o computador local.

Esta ilustração mostra como exportar exibições personalizadas.

Importar uma exibição

Você pode importar somente arquivos JSON. Para importar as exibições personalizadas, clique no botão de reticências (...) no cabeçalho Filtros e selecione **Importar exibição (json)**.

Revise as seguintes condições ao importar exibições:

- Você só pode importar o formato de arquivo JSON.
- Você pode importar apenas uma exibição ou arquivo por vez.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você não pode importar se já tiver três exibições personalizadas em seus filtros. Exclua uma exibição personalizada e importe uma exibição.
- Você não pode importar uma exibição com um nome de exibição personalizado existente. Renomeie uma exibição antes de importar.

Esta ilustração mostra como importar uma exibição.

Navegador com filtros primários

Use os filtros primários para filtrar técnicas no navegador MITRE-ATT&CK. As informações no repositório MITRE-ATT&CK estão disponíveis para seleção.

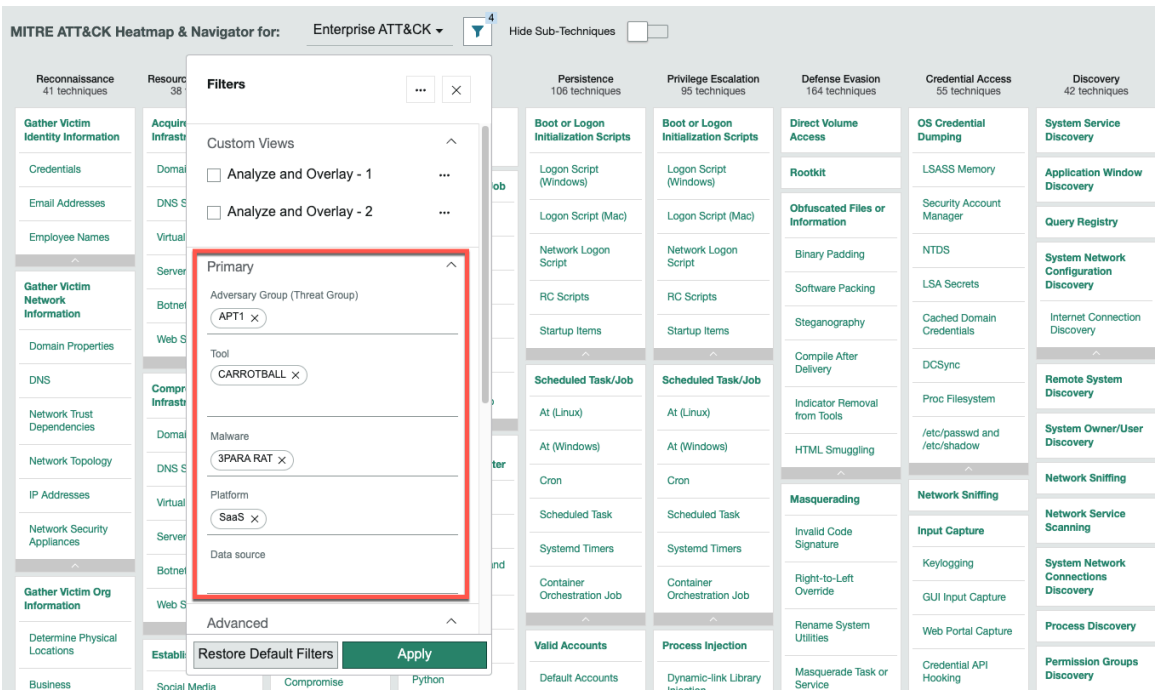
Filtrar	Descrição
Grupo adversário (grupo de ameaça)	Conjuntos de atividades de intrusão relacionadas que são rastreadas por um nome comum na comunidade de segurança. Grupos podem significar vários grupos de ameaças, grupos de atividades, agentes de ameaça, conjuntos de intrusão e campanhas. Você pode adicionar vários grupos ao filtro **Grupo adversário (grupo de ameaças)**. Por exemplo, você adiciona APT1 e AT12, pois ambos são grupos de ameaças atribuídos à China. Embora ambos os grupos possam ter como destino origens diferentes, eles podem usar técnicas semelhantes.
Ferramenta	Software legítimo que é usado por agentes de ameaça para executar ataques. Você pode entender como os agentes de ameaça executam campanhas se souber como e quais ferramentas são usadas por agentes de ameaça. As ferramentas incluem software que não é encontrado em um sistema empresarial e software que está disponível como parte de um sistema operacional que já está presente em um ambiente, como utilitários do Microsoft Windows. Por exemplo, gsecdump é um descarregador de credenciais disponível publicamente que o grupo adversário do APTI1 usa para obter hashes de senha e segredos LSA (Autoridade de Segurança Local) dos sistemas operacionais Microsoft Windows.
Malware	Software comercial, personalizado de código fechado ou de código aberto que se destina a ser usado para fins mal-intencionados por adversários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtrar	Descrição
	Os exemplos são PlugX, CHOPSTICK e assim por diante
Plataforma	Táticas e técnicas que representam MITRE-ATT&CK em uma plataforma específica. Por exemplo, MITRE-ATT&CK é compatível com estas plataformas na matriz Enterprise ATT&CK: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Rede.
Fonte de dados	Fontes de dados que você está coletando em seu ambiente e usando para detectar MITRE-ATT&CK técnicas. Os exemplos são monitoramento de dll e extensões de navegador.

A ilustração a seguir mostra todos os filtros primários disponíveis no navegador MITRE-ATT&CK.



Como usar um mapa térmico com recursos primários e avançados

Você pode usar um mapa térmico com filtros avançados para executar uma análise correlacionando incidentes de segurança com MITRE-ATT&CK informações.

Exibir IDs de técnica

Você pode exibir os MITRE-ATT&CK IDs de técnica com os nomes das técnicas ao selecionar o filtro **Exibir IDs de técnica**.

Exibir IDs de técnica em um mapa térmico

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir técnicas relevantes por prioridade

Para filtrar as técnicas com base em sua prioridade relevante no navegador, selecione **Filtrar por filtro de prioridade relevante da técnica** e selecione a **Prioridade relevante** no menu. Você pode atribuir várias prioridades para filtragem. Você também pode apontar para as técnicas no mapa térmico para saber a prioridade da técnica.

As informações de prioridade relevantes são baseadas na priorização que você definiu no campo Prioridade relevante de técnicas.

Esta ilustração mostra a filtragem por prioridade relevante.

Exibir cobertura de detecção de técnica

Para exibir a cobertura geral de detecção de técnica no mapa térmico, selecione o filtro **Exibir cobertura de detecção de técnica**. O mapa térmico destaca o espetro visual da cobertura de detecção, incluindo os pontos cegos onde você não tem cobertura. A definição de pontuação do sistema de base e as cores foram definidas na cobertura de detecção da técnica. As informações foram extraídas automaticamente da cobertura geral de detecção da técnica.

Por exemplo, as áreas do mapa térmico marcadas em vermelho indicam falta de detecção. As áreas marcadas em azul indicam a presença de capacidades de detecção completas. As áreas marcadas em laranja, amarelo e azul claro refletem capacidades de detecção parcial.

- A visualização de cores é baseada na definição da técnica e na codificação de cores que você define.
- A visualização de cobertura é baseada no mapeamento de cobertura de detecção de técnica que você define.
- Se você modificar a definição de cobertura do sistema de base, os ícones de tipo de cobertura não serão exibidos com as técnicas no mapa térmico.

> **Nota:** O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que a cobertura de detecção de técnica definida pelo sistema de base e as cores de cobertura.

Nesta ilustração, você vê a cobertura de detecção de técnica para todas as técnicas e subtécnicas e o tipo de cobertura com suas cores e ícones.

Cobertura de detecção da técnica de mapa térmico

Exibir cobertura de mitigação da técnica

Para exibir a cobertura geral de mitigação da técnica no mapa térmico, selecione o filtro Exibir cobertura de mitigação da técnica. O mapa térmico destaca o aspecto visual da cobertura de mitigação, incluindo áreas que você não tem cobertura. A cobertura de mitigação, as cores e os intervalos percentuais foram definidos na Definição de cobertura de mitigação. As informações são extraídas da Cobertura de mitigação da técnica geral.

Por exemplo, as técnicas realçadas em vermelho indicam nenhuma cobertura de mitigação, laranja indica cobertura de mitigação ruim e azul indica cobertura de mitigação excelente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

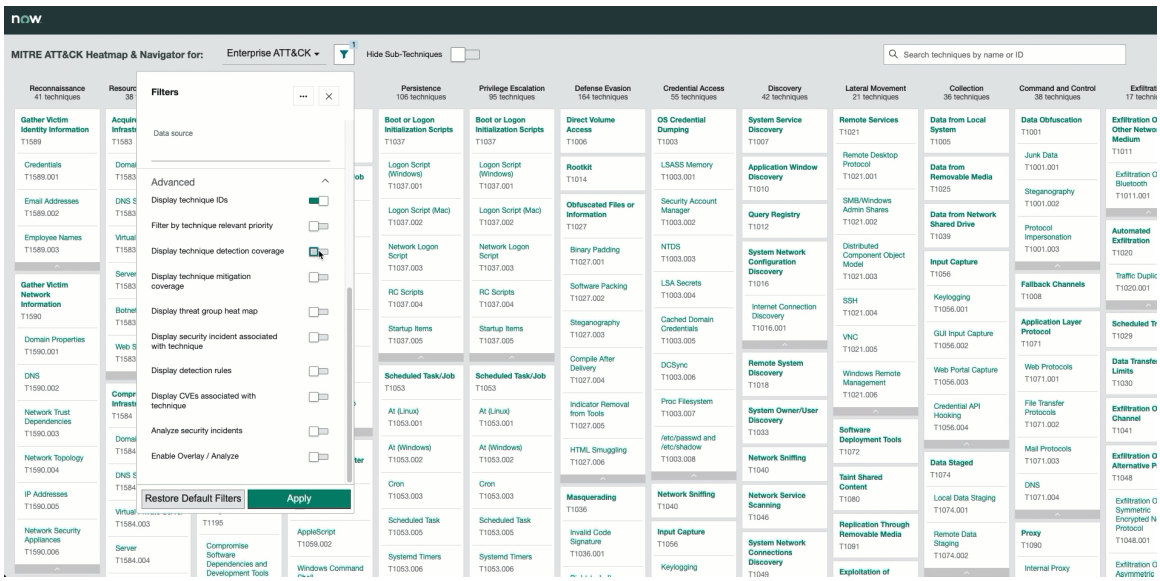
- A visualização de cores é baseada na definição de mitigação de técnica e na codificação de cores que você define.
- A visualização da cobertura é baseada no mapeamento de cobertura de mitigação da técnica que você define.
- Se você modificar a definição de cobertura de mitigação do sistema de base, os ícones do tipo de cobertura de mitigação não serão exibidos com as técnicas no mapa térmico.

> **Nota:** O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que a cobertura de mitigação da técnica definida pelo sistema de base e as cores de cobertura.

Esta ilustração mostra o mapa térmico de cobertura de mitigação da técnica

Exibir cobertura de detecção e mitigação

Você pode usar os filtros de cobertura de detecção e mitigação de técnica juntos para obter informações sobre a relevância da detecção de técnica e reduzir a cobertura para sua organização.



Esta ilustração mostra como usar os filtros de detecção e mitigação juntos.

Exibir grupo de ameaças

Para exibir o grupo de ameaças para informações de técnica no mapa térmico, selecione **Exibir mapa térmico do grupo de ameaças**. Você pode medir o número de grupos de ameaças que estão usando uma técnica específica. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um grande número de invasores. Os intervalos do grupo de ameaças e as cores do mapa térmico foram definidos na definição do mapa térmico de técnica de grupo de ameaças.

- A visualização de cores do mapa térmico e do texto é baseada no grupo de ameaças para definição do mapa térmico da técnica.
- A visualização do intervalo do grupo de ameaças se baseia no mapeamento do grupo de ameaças para a técnica.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você não pode usar o filtro **Exibir mapa térmico de grupo de ameaças** quando a cobertura de detecção de técnica ou a cobertura de mitigação de técnica estão habilitadas. Esta ilustração mostra as informações do grupo de ameaças no mapa térmico.

Exibir incidentes de segurança associados à técnica

Para exibir as técnicas que são exploradas com frequência em sua organização e que resultaram em incidentes de segurança, clique em **Exibir incidente de segurança associado à técnica**. Você pode exibir mais informações sobre cada um dos incidentes de segurança associados ao clicar no link que abre em uma nova janela para análise. Incidentes de segurança associados a uma técnica.

- Prioridade: selecione **Prioridade do incidente de segurança** para filtrar pela prioridade do incidente de segurança.
- Intervalo de datas: selecione o **Intervalo de datas do incidente de** segurança para filtrar problemas de segurança pelo intervalo de datas.
- Falsos-positivos: selecione **Filtrar incidentes de segurança** com falso-positivos para remover problemas com falso-positivos. A seleção deste filtro reduz o número de incidentes de segurança que você vê no mapa térmico.

Quando você usa este filtro com o filtro **Exibir cobertura de detecção de técnica**, ele fornece uma visão sobre a relevância da cobertura de detecção de técnica para sua organização até a data selecionada.

Por exemplo, ao ativar os dois filtros, você pode ver que na tática de evasão de defesa, a técnica de Mascaramento não tem cobertura. Quando você observa mais detalhadamente, a técnica de Mascaramento está relacionada à Tarefa ou Serviço de Mascaramento, que também tem um incidente de segurança associado a ele. Isso mostra que há uma lacuna na cobertura de detecção de técnica para a técnica de Mascaramento e você pode revisar a cobertura de detecção de técnica geral.

Exibir regras de detecção

Para ver se você tem regras de detecção definidas para uma técnica específica, clique em **Exibir regras de detecção**. Você também pode ver cada regra de detecção associada com sua definição.

Essas informações são baseadas no mapeamento de regras de detecção que você definiu. Exibir regras de detecção associadas.

Exibir CVEs associados à técnica

Para exibir as informações de CVEs e vulnerabilidades comuns (CVE) associadas a cada uma das técnicas, clique em **Exibir CVEs associadas à técnica**. As informações de CVE para técnica são baseadas nas informações disponíveis no módulo Mapeamento de técnica de CVE. Isso fornece informações sobre vulnerabilidades conhecidas e permite que você saiba se adversários podem explorar sua organização.

Importante: O mapa térmico foi aprimorado para exibir somente os CVEs relevantes associados aos VITs

Para exibir VITs associados a CVEs e técnicas, selecione **Exibir VITs associados a CVE e técnicas**. Além disso, para filtrar ainda mais as técnicas sem VITs, selecione **Ocultar técnicas sem VITs**. As informações de CVE e VIT exibidas são obtidas do produto Resposta a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades em seu ambiente. Você pode exibir a lista filtrada de CVEs e VITs no mapa térmico e navegar até cada CVE ou VIT para cada técnica do mapa térmico.

Nota:

- A **técnica Exibir CVEs associados à** está disponível somente quando o produto Resposta a vulnerabilidades está instalado em seu ambiente.
- As informações de VIT e CVE são calculadas com base no trabalho agendado definido em MITRE-ATT&CK propriedades. O trabalho de programação do sistema de base está definido para 24 horas.

Ao usar este filtro com o filtro **Exibir incidente de segurança associado à técnica**, você pode saber se as vulnerabilidades conhecidas causaram incidentes de segurança em sua organização.

Você pode exibir mais informações sobre cada CVE para analisar se o CVE é relevante para sua organização. Para fazer isso, exiba os itens de vulnerabilidade. Se os itens de vulnerabilidade forem criados, você poderá exibir mais informações sobre qualquer informação de IC associada no módulo Resposta a vulnerabilidades. Você também pode revisar a gravidade e a prioridade para tomar decisões informadas. Revise os CVEs para tomar decisões fundamentadas.

Analisar incidentes de segurança

Para analisar incidentes de segurança e revisar as técnicas usadas por um adversário para um ataque, clique em **Analisar incidentes de segurança**. Você pode adicionar vários incidentes de segurança para análise usando cadeias de caracteres separadas por vírgulas.

Este filtro ajuda a analisar um incidente de segurança. Você pode saber por que o incidente ocorreu, quais técnicas foram exploradas, se algum agente de ameaça conhecido estava envolvido, se os agentes de ameaça usaram uma sequência específica para um ataque e assim por diante. Como é possível analisar vários incidentes de segurança ao mesmo tempo, você pode correlacionar as informações para ver se elas estão relacionadas ou se são um incidente isolado. Se os incidentes de segurança estiverem relacionados e você observar um padrão, poderá revisar o andamento deles na cadeia de eliminação para interromper o ataque ou para formar uma estratégia de defesa para sua organização.

Ao usar o filtro **Analisar incidentes de segurança** com filtros primários, como um **grupo adversário**, você pode correlacionar se adversários conhecidos estiverem envolvidos. Por exemplo, quando vários incidentes de segurança estão sendo analisados, as técnicas associadas aos incidentes de segurança estão presentes na forma de uma cadeia de eliminação. Ao sobrepor as informações com o adversário, você notará uma sobreposição entre as técnicas associadas ao incidente de segurança e as técnicas associadas ao adversário. Somente as informações da técnica sobreposta serão mostradas se ambos os filtros estiverem habilitados.

Analisar incidentes de segurança

Usando sobreposição para analisar incidentes de segurança e grupos adversários

Use o filtro **Habilitar sobreposição/analisar** para exibir o comportamento do adversário e analisar um ou mais dos incidentes de segurança e correlacionar as informações para ver se um ataque é um incidente isolado ou um ataque coordenado por um adversário conhecido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, agora você pode exibir os incidentes de segurança e o comportamento da cadeia de eliminação de ameaças adversárias na mesma exibição. Esta exibição fornece informações de sobreposição que informam sobre o ataque e o comportamento adversário conhecido. Isso permite que você analise se este é um ataque isolado ou um ataque coordenado por um adversário conhecido.

Habilitar o filtro de análise de sobreposição ignora todos os filtros primários, exceto o filtro **Grupo adversário**, e ignora o filtro avançado **Filtrar por prioridade relevante de técnica** ao gerar uma exibição.

Depois de habilitar o filtro de análise de sobreposição, use a paleta de cores para atribuir cores para o seguinte:

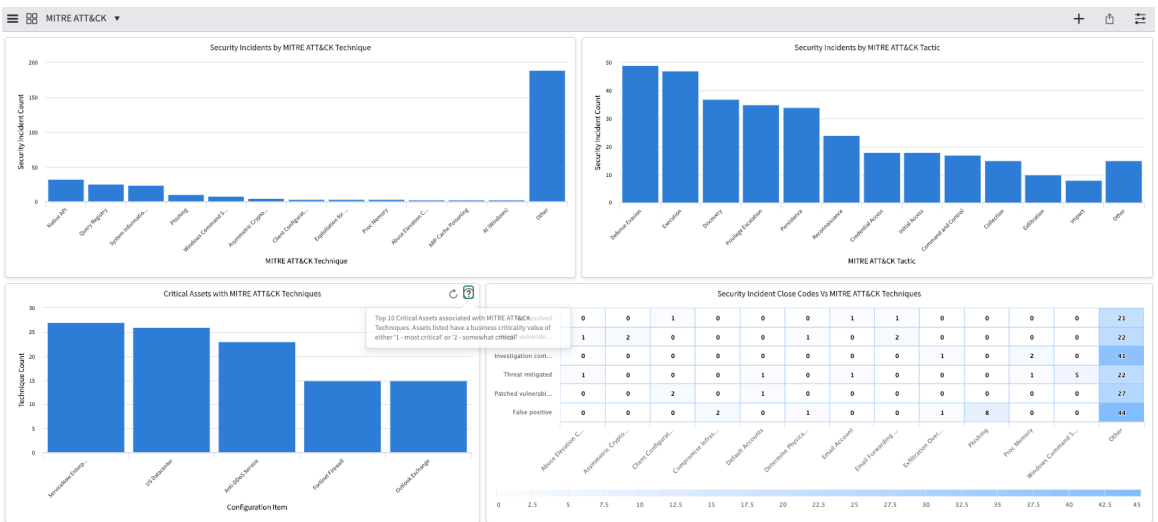
- Analisar incidente de segurança
- Grupo adversário
- Sobreposição

A ilustração a seguir mostra que o grupo adversário APT18 está distribuído em várias técnicas e táticas na cadeia de eliminação. A análise também mostra que há três técnicas que se sobrepõem ao grupo adversário e aos incidentes de segurança que você está rastreando. Esta ilustração mostra as informações de sobreposição de adversários e incidentes de segurança.

Como usar o painel MITRE-ATT&CK

O painel MITRE-ATT&CK fornece uma exibição executiva da cobertura, táticas e técnicas da fonte de dados que são usadas em sua organização.

O módulo MITRE-ATT&CK Visão geral exibe MITRE-ATT&CK informações sobre incidentes de segurança, incluindo tendências e relatórios. Você pode clicar em qualquer parte de um widget (barra, ponto de dados, tabela e assim por diante) para exibir os dados específicos dessa parte.



Use o painel MITRE-ATT&CK para ver seus dados relacionados à segurança

Use o painel MITRE-ATT&CK para obter uma visão geral da cobertura, das táticas e das técnicas da fonte de dados usadas em sua organização.

Antes de Iniciar

Função necessária: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

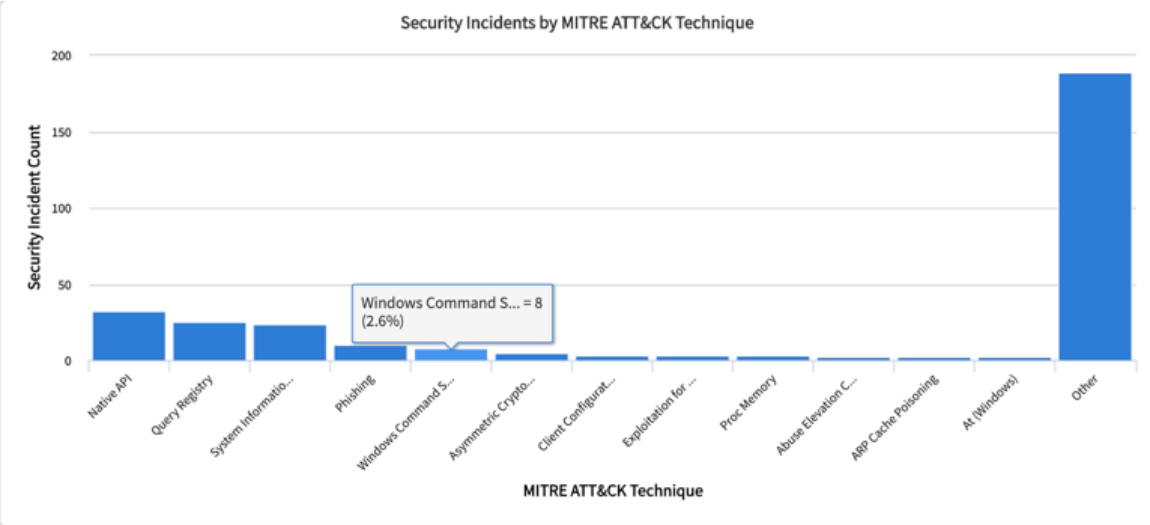
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Visão geral**.
2. Clique em qualquer um dos seguintes widgets para ver detalhes adicionais:
   - Incidentes de segurança por MITRE-ATT&CK técnica
   - Incidentes de segurança por MITRE-ATT&CK tática
   - Ativos críticos com MITRE-ATT&CK técnicas
   - Códigos de fechamento de incidente de segurança versus técnicas MITRE-ATT&CK
   - Técnicas do MITRE-ATT&CK por cobertura de detecção
   - Técnicas MITRE-ATT&CK por cobertura de mitigação
   - Grupos de ameaças por técnica MITRE-ATT&CK
   - CVEs por técnica MITRE-ATT&CK

Widgets do MITRE-ATT&CK

O módulo MITRE-ATT&CK Visão geral consiste em widgets que permitem correlacionar as informações MITRE-ATT&CK com as informações do incidente de segurança em seu ambiente.

Exemplo de incidentes de segurança pela técnica MITRE-ATT&CK

Neste exemplo, o widget Incidentes de segurança por técnica **do MITRE ATT&CK** exibe as técnicas por incidente de segurança no ambiente de uma organização nos últimos 90 dias.

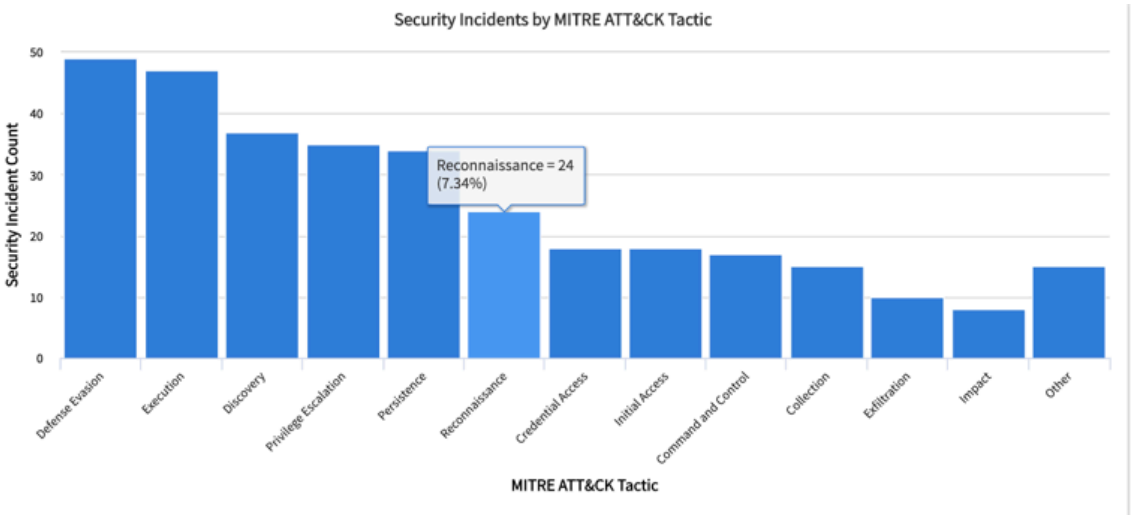


Exemplo de incidentes de segurança por tática MITRE-ATT&CK

Neste exemplo, o widget **Incidentes de segurança por tática do MITRE ATT&CK** exibe as principais táticas por incidente de segurança no ambiente de uma organização nos últimos 90 dias.

Tradução automática

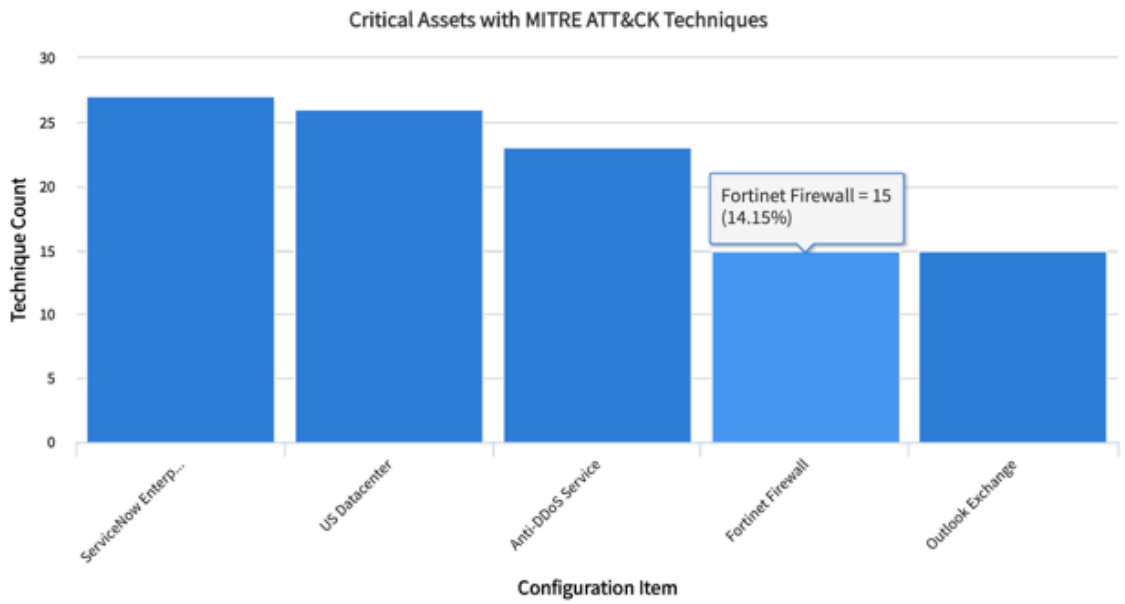
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de ativos críticos com MITRE-ATT&CK técnicas

Neste exemplo, o widget **Ativos críticos com técnicas MITRE ATT&CK** exibe os 10 principais ativos críticos que estão associados às técnicas MITRE-ATT&CK. Os ativos têm uma criticalidade de negócio de 1 (mais crítico) ou 2 (um pouco crítico).

Este relatório permite que uma organização veja os tipos e o número de técnicas usadas na execução de ataques contra os ativos críticos.



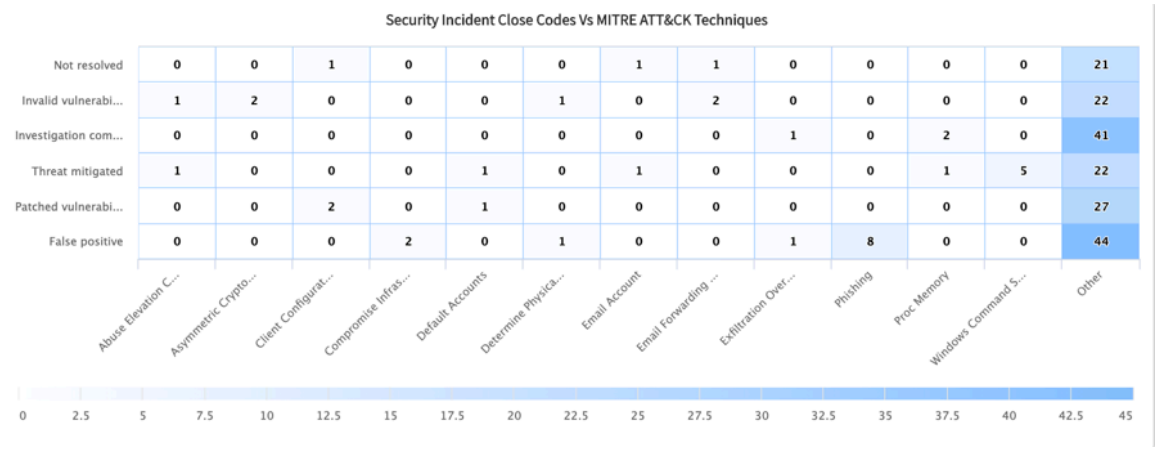
Exemplo de códigos de fechamento de incidente de segurança versus técnicas MITRE-ATT&CK

Neste exemplo, o widget Códigos de fechamento de incidentes de segurança **versus técnicas** *MITRE-ATT&CK* exibe os códigos de fechamento de incidentes de segurança que foram mapeados em relação às principais técnicas identificadas no ambiente de uma organização.

O eixo x exibe as principais técnicas que foram usadas para realizar ataques contra a empresa e o eixo y exibe os códigos encerrados.

Tradução automática

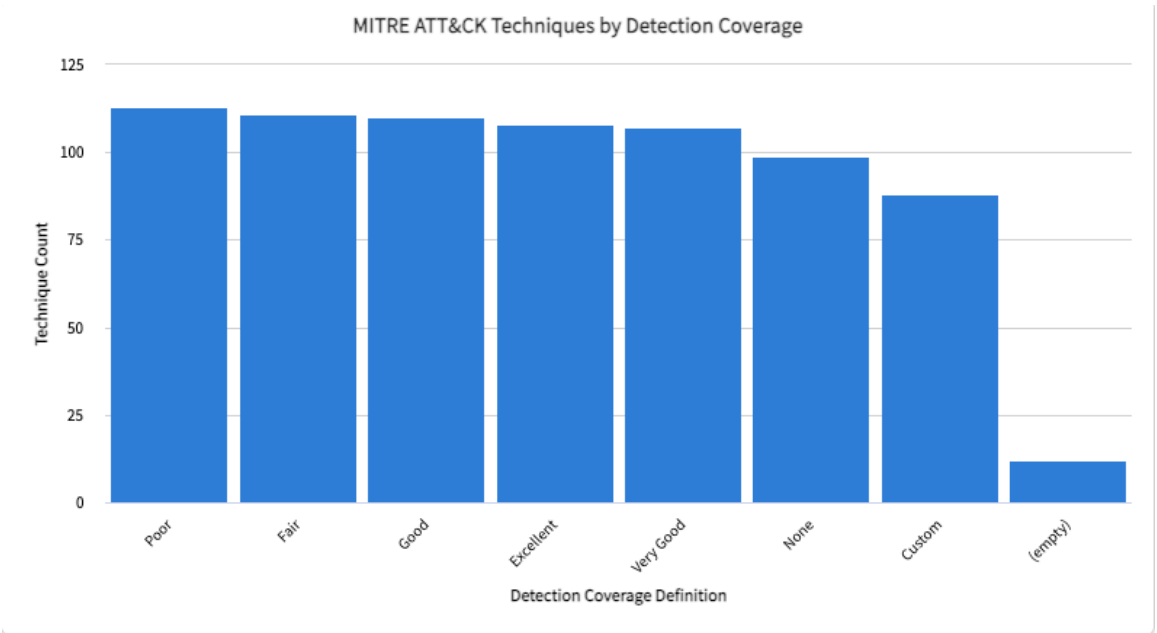
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de cobertura de detecção por MITRE-ATT&CK técnicas

Neste exemplo, o widget **Técnicas MITRE-ATT&CK por cobertura de detecção** exibe a contagem de técnicas pela cobertura de detecção em seu ambiente.

O eixo x exibe a contagem de técnicas e o eixo y exibe os tipos de cobertura de detecção.



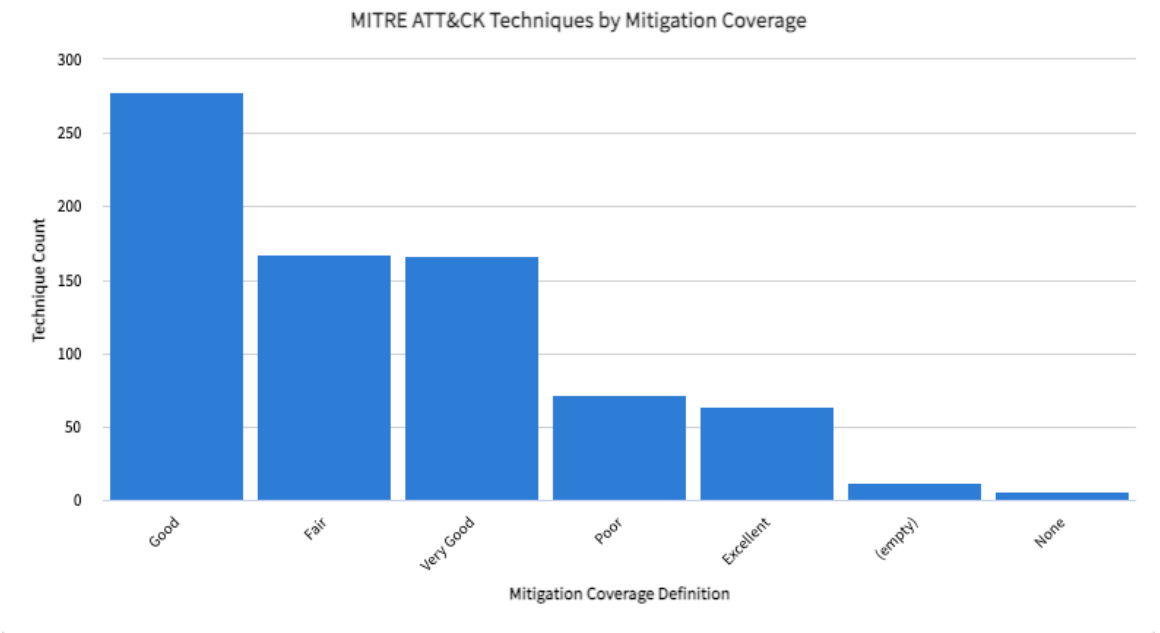
Exemplo de cobertura de mitigação por MITRE-ATT&CK técnicas

Neste exemplo, o widget **Técnicas MITRE-ATT&CK por cobertura de mitigação** exibe a contagem de técnicas pela cobertura de mitigação em seu ambiente.

O eixo x exibe a contagem de técnicas e o eixo y exibe os tipos de cobertura de mitigação.

Tradução automática

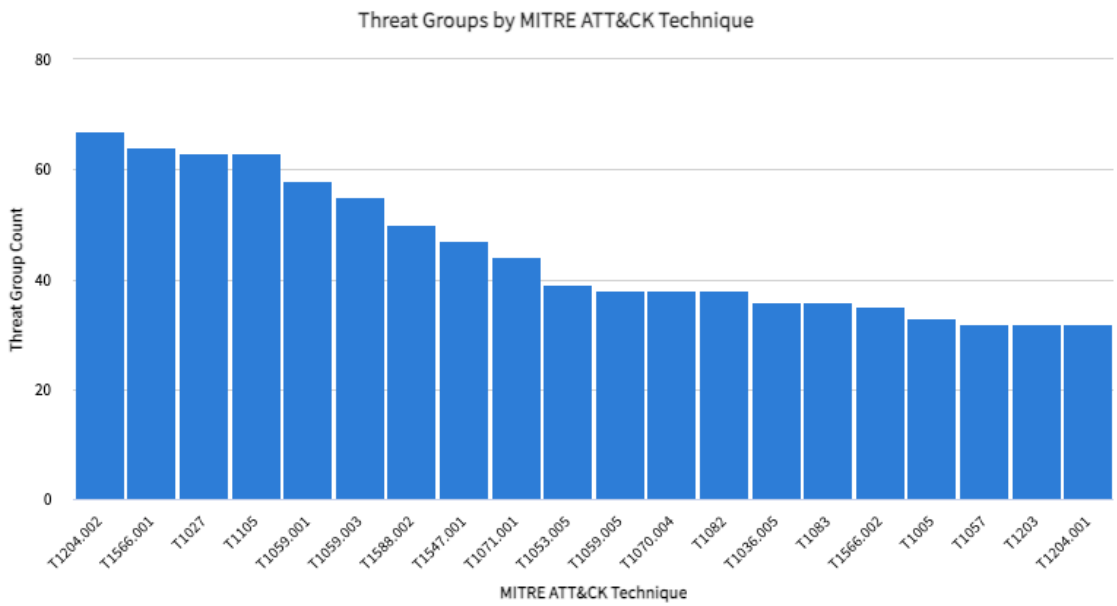
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de grupos de ameaças por MITRE-ATT&CK técnicas

Neste exemplo, o widget **Grupos de ameaças por técnica MITRE-ATT&CK** exibe as técnicas pela contagem de grupos de ameaças. Este widget exibe 20 técnicas com a maior contagem de grupos de ameaças.

O eixo x exibe a contagem de grupos de ameaças e o eixo y exibe as MITRE-ATT&CK técnicas.



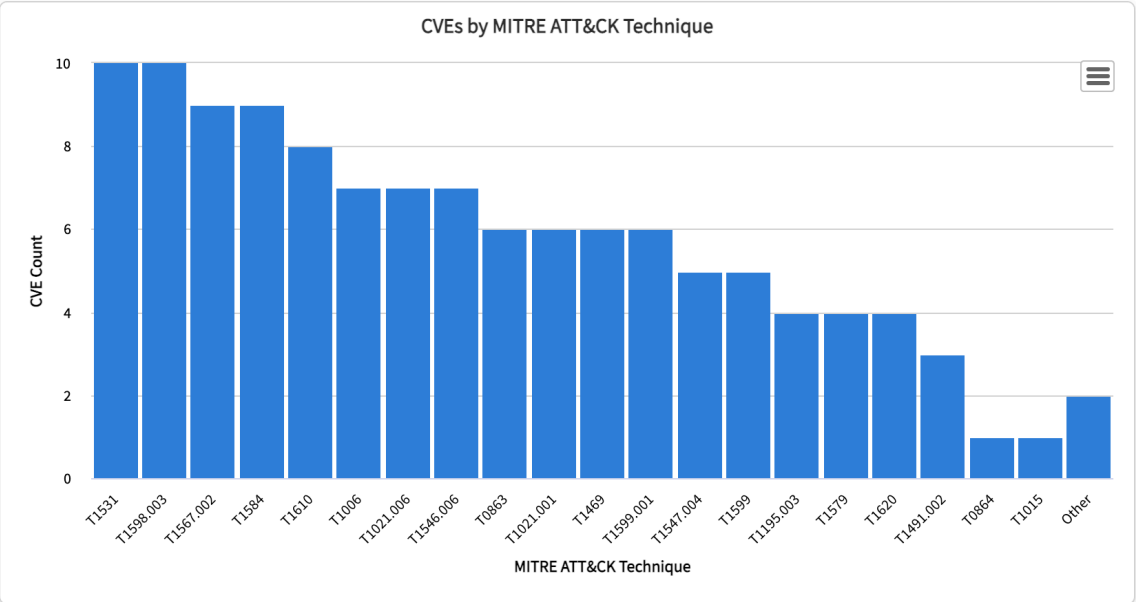
Exemplo de CVEs por MITRE-ATT&CK técnicas

Neste exemplo, o widget **CVEs por técnica MITRE-ATT&CK** exibe as técnicas com a contagem de CVE relevante em seu ambiente.

O eixo x exibe a contagem de CVE relevante e o eixo y exibe as técnicas MITRE-ATT&CK.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Administração do Inteligência contra ameaças

O sistema de base Inteligência contra ameaças está pronto para uso na ativação. Você pode adicionar registros a determinados módulos no menu da aplicação Administração, mas a maioria já está preenchida com informações padrão do setor.

As seguintes aplicações estão disponíveis no módulo **Administração** da barra de navegação Inteligência contra ameaças :

Aplicações de administração de Inteligência contra ameaças

Aplicação	Descrição
Propriedades	Inteligência contra ameaças As propriedades permitem que você controle como diferentes aspectos do sistema funcionam, incluindo a configuração de chaves de API.
Mecanismos de Ataque	Este módulo organiza os padrões de ataque hierarquicamente, com base em mecanismos que são empregados com frequência ao explorar uma vulnerabilidade.
Motivações de ataque	Este módulo lista as possíveis motivações de ataque que moldam a intensidade de um ataque por um agente de ameaça ou conjunto de intrusão.
Métodos de descoberta	Este módulo descreve como os incidentes de segurança são descobertos.
Feeds	Este recurso foi descontinuado.
Tipos de Indicador	Este módulo é usado para caracterizar indicadores de ameaças cibernéticas compostos por padrões que identificam determinadas condições observáveis, bem como informações contextuais sobre o significado dos padrões e como e quando eles são aplicados.
Tipos de infraestrutura	Este módulo lista as classificações possíveis de infraestrutura.
Efeitos Pretendidos	Esta aplicação é usada para expressar o efeito pretendido de um agente de ameaça.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de administração de Inteligência contra ameaças

Aplicação	Descrição
Capacidades do malware	Este módulo lista os possíveis recursos do malware.
Tipos de malware	Este módulo lista as possíveis classificações de malware.
Notificações	Este módulo é usado para criar notificações por e-mail . Isso envolve especificar quando eles são enviados, quem os recebe e o que eles contêm.
Tipos de observável	Este módulo lista as classificações possíveis de um observável, como um endereço IP ou hash de arquivo.
Tipos de relatório	Este módulo lista as classificações possíveis de relatórios de ameaças.
Funções de agente da ameaça	Este módulo lista as funções que os agentes de ameaça desempenham.
Tipos de Agente da Ameaça	Este módulo caracteriza agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo a intenção presumida e o comportamento observado ao longo do tempo.
Calculadoras descobertas de pesquisa de ameaças	Este módulo calcula as descobertas com base nas respostas recebidas. Para integrações de terceiros que fornecem os resultados calculados, a calculadora de descoberta de pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças.
Tipos de Ferramentas	Este módulo lista a possível classificação de ferramentas.

Calculadoras descobertas de pesquisa de ameaças

A Calculadora de descoberta de pesquisa de ameaças ajuda a calcular as descobertas observáveis com base nas respostas recebidas.

Você pode criar uma Calculadora de descoberta de pesquisa de ameaças para sua integração e usar um script para determinar como deseja identificar as várias descobertas de observáveis. A Calculadora de descoberta de pesquisa de ameaças inclui um script de exemplo que vem com o sistema de base, que você pode usar para identificar as descobertas observáveis ou pode modificar este script de acordo com seus requisitos.

Para integrações de terceiros que fornecem os resultados calculados, a Calculadora de descoberta de pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema de base.

Acumular resultados de pesquisa de ameaças

Quando você tem vários resultados de pesquisa de ameaças para um observável de vários fornecedores de integração, os resultados de pesquisa de ameaças recentes de todos os fornecedores são considerados e as descobertas gerais do observável são marcadas da seguinte forma:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descobertas de pesquisa de ameaças de acúmulo

Descoberta de observável mais recente	Descoberta observável geral
Mal-intencionado	Se um dos fornecedores de integração relatar o observável como malicioso, a descoberta geral do observável será marcada como mal-intencionada.
Suspeito	Se nenhum dos fornecedores de integração relatar o observável como malicioso, um deles o relatará como suspeito e a descoberta geral do observável será marcada como suspeita.
Limpar	Se todos os fornecedores de integração relatarem o observável como Limpo, a descoberta geral do observável será marcada como Limpo.
Desconhecido	Se nenhum dos fornecedores de integração relatar o observável como malicioso ou suspeito e um deles o relatar como desconhecido, a descoberta geral do observável será marcada como desconhecida.

Como usar calculadoras de descoberta de pesquisa de ameaças

Use a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis da sua integração.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração** > **Calculadoras descobertas de pesquisa de ameaças**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Campo	Descrição
Fornecedor de pesquisa de ameaças	Nome do fornecedor de pesquisa de ameaças.
Tipo de Observável	Especifique a classificação do tipo de observável ao qual o script se aplica. Por exemplo, endereço IP ou hash de arquivo e assim por diante. O script se aplica a todos os observáveis se você não selecionar nenhum tipo de observável.
Script de descoberta	Editor de script para determinar como você deseja identificar as várias descobertas observáveis. A Calculadora de descoberta de pesquisa de ameaças contém um script de exemplo com o sistema de base. Você pode usar este script para determinar as des-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	cobertas observáveis ou pode modificar este script de acordo com seus requisitos.

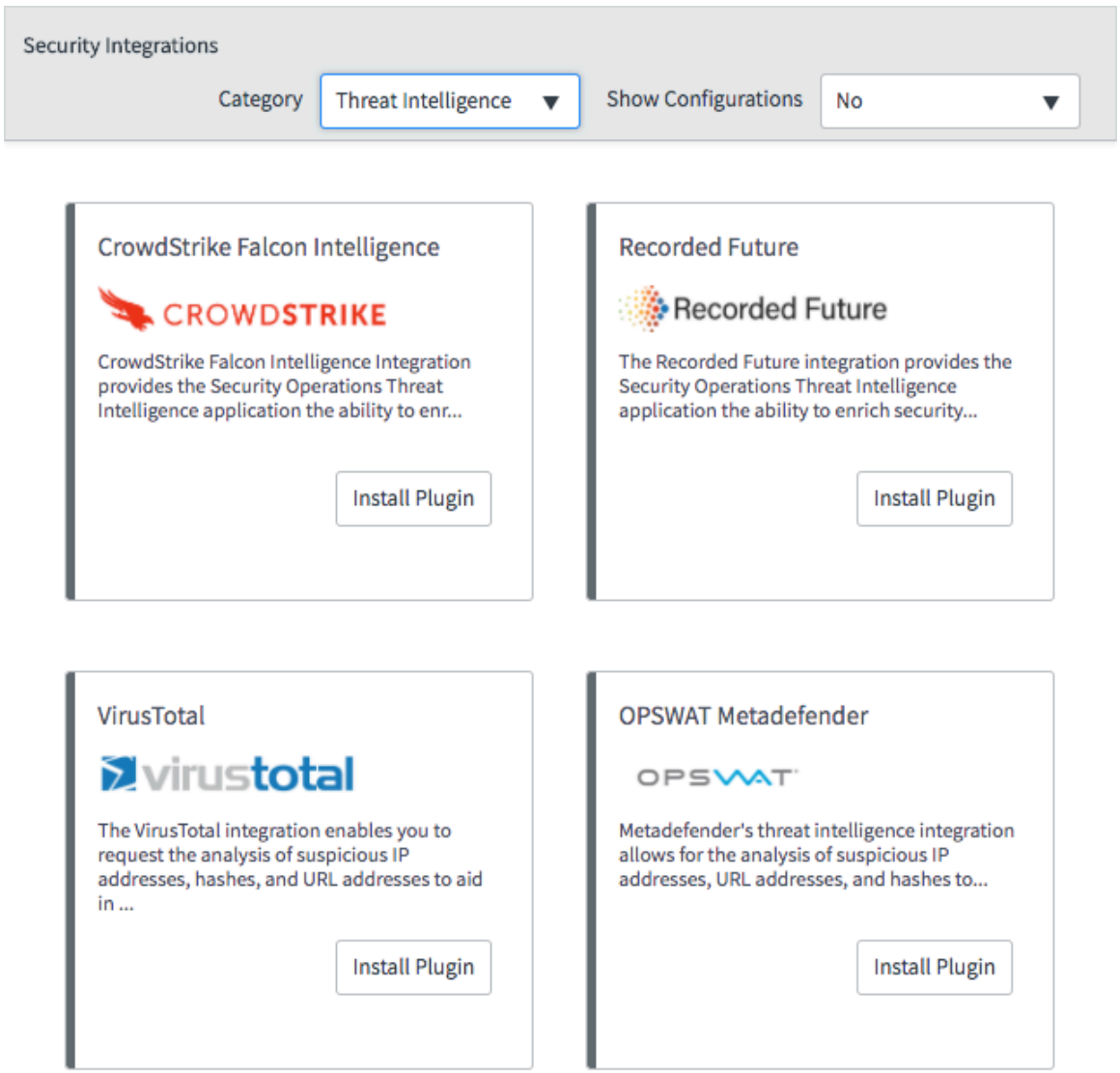
4. Clique em **Atualizar**.

Integrações do Inteligência contra ameaças

O sistema base Inteligência contra ameaças inclui integrações com pacotes de software de detecção de malware de terceiros. Esta seção fornece instruções para ativar os plug-ins e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.

Configurações de Integração

O sistema base inclui uma série de "cartões" para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que tenham dependências de Operações de segurança plug-ins. Os cartões de integração podem ser exibidos selecionando **Operações de segurança** > **Configurações de Integração**.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode filtrar as integrações visíveis usando o menu suspenso **Categoria**. O menu suspenso **Mostrar configurações** permite que você veja várias instâncias de implementações que permitem sua criação.

Botões em cartões de integração

Os cartões de integração exibem botões diferentes, dependendo do estado atual da integração e da origem do cartão.

Botão	Descrição
Instalar Plug-in	Clique neste botão para instalar o plug-in aplicável para ativar a integração. Depois que o plug-in é instalado, o botão muda para **Configurar**.
Configurar	Clique neste botão para inserir informações para configurar a integração. Para algumas integrações, pode ser necessário inserir chaves de API ou URLs adquiridos do site da integração de terceiros.
Novo	Certas integrações, como Carbon Black e IBM QRadar, permitem que você defina várias implementações da mesma integração. Para essas integrações, clique em **Novo** depois que o plug-in for ativado. Os cartões permitem instalar plug-ins (quando aplicável) e configurar as implementações para uso.
Abrir página	No sistema base, sua instância executa uma consulta na ServiceNow Store para todas as aplicações que tenham dependências de Operações de segurança plug-ins. Quando esses aplicativos são encontrados e os plug-ins do aplicativo associados são ativados, os cartões de integração deles são exibidos com os outros cartões de integração de segurança. Clique em **Abrir página** para acessar o site da aplicação de terceiros para configurar a integração. Depois de concluir a configuração, o botão **Abrir página** mudará para **Configurar**.

Integração do CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence aprimora Inteligência contra ameaças com dados para incidentes de segurança e observáveis associados.

Explorar

- CrowdStrike Falcon Intelligence visão geral da integração
- Integrações do Security Incident Response

Configurar

Ativar e configurar a integração CrowdStrike Falcon Intelligence

Usar

- Executar pesquisas em observáveis
- Pesquisa de ameaças - CrowdStrike Falcon Intelligence fluxos

Desenvolver

- ServiceNow Operações de segurança diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Fazer ou responder a perguntas na comunidade das Operações de segurança
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

CrowdStrike Falcon Intelligence visão geral da integração

CrowdStrike Falcon Intelligence fornece inteligência de segurança cibernética que se integra facilmente com Operações de segurança.

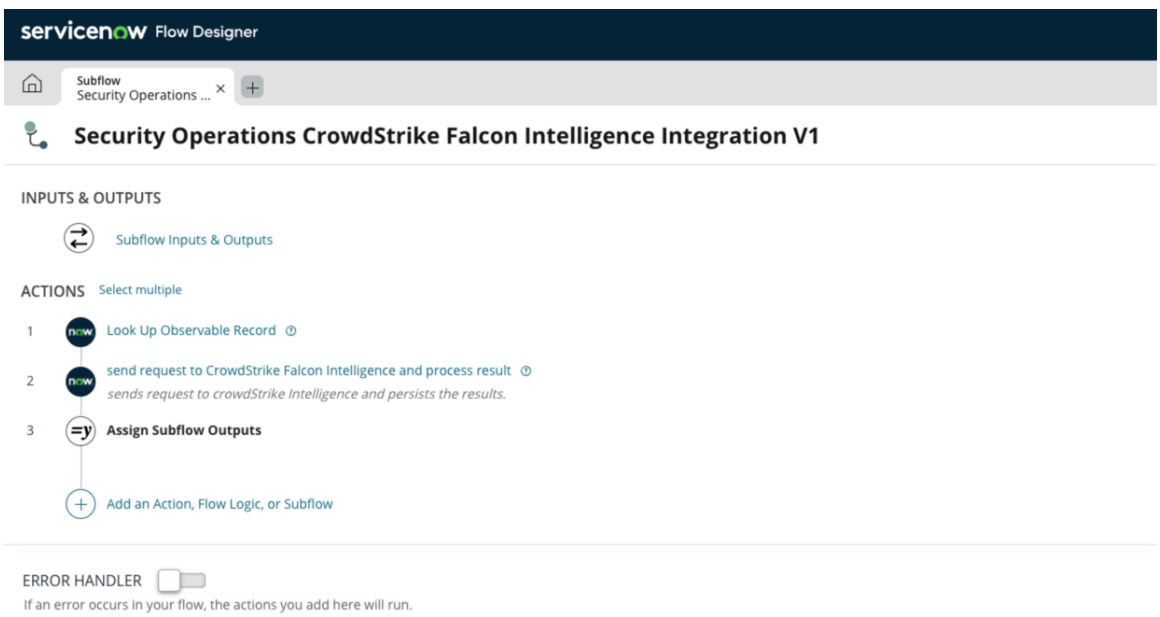
Nota: O plug-in Inteligência contra ameaças é necessário para implementar a integração CrowdStrike Falcon Intelligence.

Pesquisa de ameaças - CrowdStrike Falcon Intelligence fluxos

O Flow Designer de pesquisa de ameaças - CrowdStrike Falcon Intelligence executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por CrowdStrike Falcon Intelligence, eles serão verificados quanto a malware e os resultados serão retornados.

Este fluxo é acionado pelo Integração de Operações de segurança - Capacidade de pesquisa de ameaças quando você publica um ou mais observáveis em uma lista de observação e a implementação do CrowdStrike Falcon Intelligence está selecionada. Depois de serem publicadas, as listas de observação podem ser visualizadas no software CrowdStrike Falcon Host.

Função necessária: administrador



Para obter informações sobre as atividades usadas por este Flow Designer, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar e configurar a integração CrowdStrike Falcon Intelligence

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo a integração CrowdStrike Falcon Intelligence. Antes de poder usar o CrowdStrike Falcon Intelligence, você deve baixá-lo do ServiceNow Store e adicionar a chave de API e o ID apropriados.

Antes de Iniciar

Função necessária: administrador

- O plug-in Inteligência contra ameaças deve ser instalado e ativado para que você possa usar a integração CrowdStrike Falcon Intelligence.
- Obtenha o ID do cliente de API e o segredo do cliente de API no seu perfil CrowdStrike Falcon Intelligence.
- Se você estiver atualizando a integração CrowdStrike Falcon Intelligence de uma versão anterior, deverá excluir a configuração existente e definir uma nova configuração. A integração é compatível com a autenticação OAUTH2. Esta atualização requer que você insira o **ID do cliente de API** e o **segredo do cliente** de API para autenticar e concluir a configuração.
- Nos CrowdStrike Falcon Intelligence**Escopos de API**do portal, habilite a configuração **Leitura** para **Indicadores (Falcon X)** ou **IOCs (Indicadores de Compromisso)**.

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão CrowdStrike Falcon Intelligence, clique em **Configurar**.
4. No formulário, preencha os campos para concluir a configuração:

CrowdStrike Falcon Intelligence Configuração

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
ID do cliente da API	O ID de cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Intelligence.
Segredo do cliente de API	A chave secreta do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Intelligence.

5. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
Depois de configurado, CrowdStrike Falcon Intelligence pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Informações relacionadas

Executar pesquisas em observáveis

Integração de Have I been pwned?

A integração Operações de segurança Have I been pwned? permite que você envie pesquisas em nomes de domínio e endereços de e-mail para determinar se os dados pessoais do usuário foram comprometidos por violações de dados.

Explorar Integrações do Security Incident Response	**Configurar** • Configuração de integração de Operações de segurança Have I been pwned? • Ativar a integração das Operações de segurança Have I been pwned?
Usar Executar pesquisas em observáveis Pesquisa de ameaças - Have I been pwned? fluxo	**Desenvolver** • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Configuração de integração de Operações de segurança Have I been pwned?

Have I been pwned? é um recurso gratuito usado para avaliar se alguém pode ter sido colocado em risco devido a sua conta on-line ter sido comprometida ou "pwned" em uma violação de dados. Ele se integra facilmente com Operações de segurança.

Antes de poder usar a integração Have I been pwned?, você deve ativar o plug-in. Se necessário, você também pode atualizar sua certificação SSL X509.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os plug-ins Security Incident Response, Inteligência contra ameaçase Operações de segurança Have I been pwned? são necessários para implementar a integração Operações de segurança Have I been pwned?.

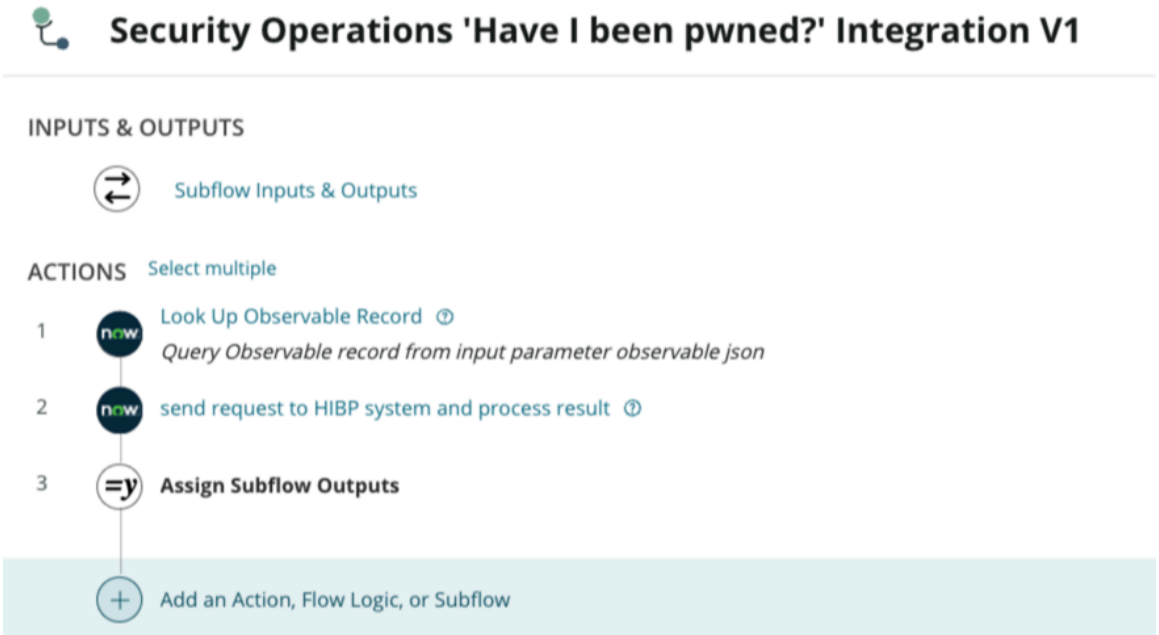
Pesquisa de ameaças - Have I been pwned? fluxo

O fluxo Pesquisa de ameaças - Have I been pwned? executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por Have I been pwned?, eles serão verificados quanto a malware e os resultados serão retornados.

Função necessária: sn_si_admin

Este fluxo é acionado pelo Integração de Operações de segurança - Capacidade de pesquisa de ameaças quando você executa uma pesquisa de ameaças em um ou mais observáveis e a implementação Have I been pwned? é selecionada. Para obter mais informações, consulte Executar pesquisas em observáveis.

Fluxo de I Been Pwned



Para obter informações sobre as atividades usadas por este fluxo, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Ativar a integração das Operações de segurança Have I been pwned?

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo a integração Operações de segurança Have I been pwned?. Antes de poder usar a integração Have I been pwned?, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser instalado e ativado para que você possa usar a integração Operações de segurança Have I been pwned?.

Função necessária: sn_si_admin

Procedimento

Baixe a integração do ServiceNow Store.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta integração oferece suporte a uma API aberta e não requer configuração adicional. Have I been pwned? agora pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Informações relacionadas

Executar pesquisas em observáveis

Atualizar seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor de terceiros ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.
   a. Insira a URL do endpoint na barra de endereço do navegador.
      Por exemplo: `https://<3rdparty>/`.
   b. Clique no ícone de cadeado na linha de endereço.
   c. Clique em **Mais informações** e na guia **Segurança**.
   d. Clique em **Exibir certificado** e na guia **Detalhe**.
   e. Clique em **Exportar** para salvar o PEM no sistema de arquivos local.
   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
      Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.
2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou na área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os outros campos no registro são gerados automaticamente.

Nota: Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Como substituir um certificado SAML expirando .

MISP integration for Security Operations

Com MISP integration for Security Operations, você pode investigar incidentes de segurança com pesquisas de detecções, aprimoramento de observável e criar ou atualizar eventos em MISP. Usando MISP, você pode investigar ataques direcionados com mais rapidez, melhorar a taxa de detecção e reduzir o número de falso-positivos em seu ambiente.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

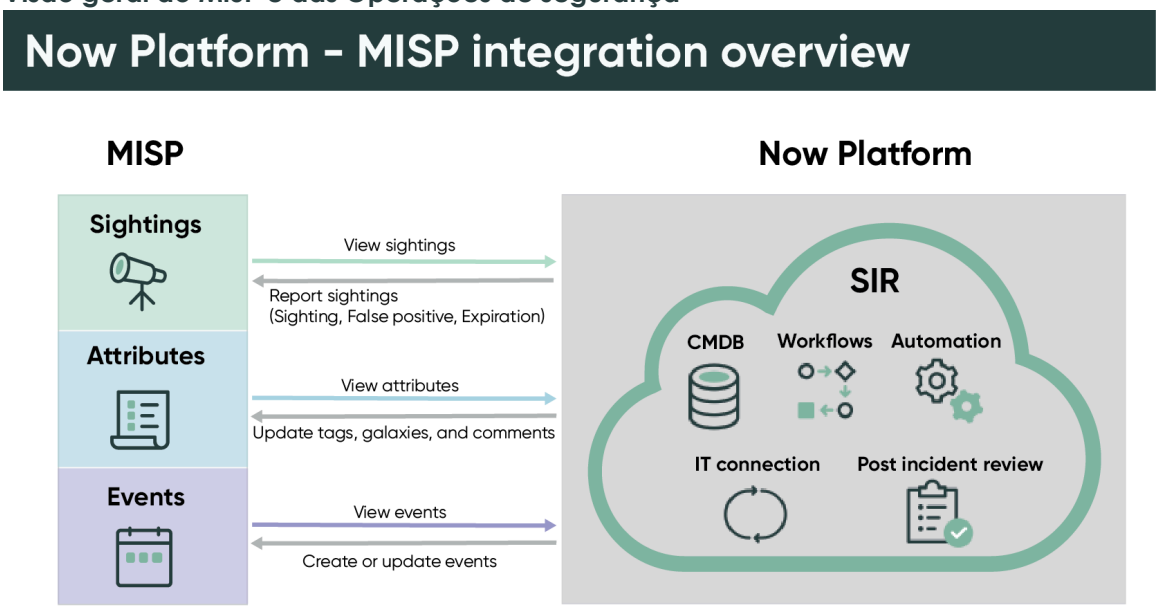
MISP Visão geral

MISP, que significa Malware Information Sharing Platform, permite que você troque e compartilhe inteligência contra ameaças e Indicadores de Compromisso (IoCs) sobre os ataques e malware direcionados em sua comunidade de membros confiáveis. Você também pode compartilhar MISP informações com comunidades privadas ou abertas. Ao trocar MISP informações, você pode investigar ataques direcionados com mais rapidez, melhorar a taxa de detecção e reduzir o número de falso-positivos em seu ambiente.

MISP e Operações de segurança

Consulte o exemplo a seguir para saber como as informações MISP fluem com as aplicações Operações de segurança.

Visão geral do MISP e das Operações de segurança



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

Esta integração inclui o que você pode fazer com os recursos principais MISP :

- Conectar-se a privados e públicos MISP instâncias.
- Oferece suporte à pesquisa de detecções manual e automática de observáveis.
- Executar pesquisa de detecções na gestão de casos.
- Relatar ou atualizar detecções para um atributo:
  - Relatar um observável como uma detecção (global)
  - Relatar um observável como falso-positivo (global)
  - Relatar um observável como expirado
- Suporte ao enriquecimento observável manual e automático. Os resultados incluem o atributo MISP e as informações de evento associadas aos observáveis.
- Aprimoramento de atributo em MISP, que inclui adicionar ou atualizar marcadores, galáxiasou comentários.
- Criação de eventos no MISP de SIR: oferece suporte à criação manual e automática de eventos em MISP de SIR.
- Atualize um evento [MISP de SIR, o que inclui adicionar ou atualizar marcadores, galáxiasou atributos.
- Adicionar observáveis associados a incidentes de segurança como atributos a um MISP evento.
- Extração automática MITRE-ATT&CK™ informações de MISP atributos e associe as informações a SIR incidentes de segurança.
- Adicionar automaticamente SIR MITRE-ATT&CK™ informações como galáxias para um MISP evento.

Conceitos-chave

Esta integração inclui os seguintes conceitos-chave que você deve saber:

- MISP é uma plataforma de inteligência contra ameaças (TIP). Você usa TIPs para coletar, correlacionar, categorizar, compartilhar e integrar dados de ameaças à segurança em tempo real para oferecer suporte à priorização de ações e ajudar na prevenção, detecção e resposta de ataques.
- MISP é uma Gestão de inteligência contra ameaças (TIM). Você usa TIMs para transformar dados de ameaças em inteligência contra ameaças por meio de contexto e para priorizar automaticamente as ameaças por pontuação e relevância definidas pelo usuário.
- MISP Camada de dados
  - Eventos são encapsulamentos para informações vinculadas contextualmente.
  - Atributos são pontos de dados individuais, que podem ser indicadores ou dados de suporte.
  - Os objetos são compostos de atributo de modelo personalizado.
  - Referências de objeto são os relacionamentos entre os outros blocos de construção.
  - Detecções são ocorrências específicas de tempo de um ponto de dados detectado.
- MISP Camada de contexto

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Marcadores são rótulos anexados a eventos ou atributos e podem vir de taxonomias.
  - Clusters de galáxias são itens da base de conhecimento que você pode usar para rotular eventos ou atributos que vêm de galáxias.
  - Os relacionamentos de cluster denotam relacionamentos predefinidos entre clusters.
- Os indicadores contêm um padrão que você pode usar para detectar atividades cibernéticas suspeitas ou mal-intencionadas.
- Os atributos em MISP podem ser indicadores de rede (endereço IP), indicadores de sistema (uma cadeia de caracteres na memória) ou até mesmo detalhes de contas bancárias. Os atributos em MISP são conhecidos como observáveis em outros SIEMs ou formatos como STIX.
  - Um tipo descreve o atributo. Por exemplo, MD5 ou um URL.
  - A categoria de atributo descreve um atributo. Por exemplo, uma entrega de carga.
  - Um marcador IDS determina se um atributo pode ser usado automaticamente para detecção.

Nota: Para obter mais informações sobre conceitos MISP, consulte o site de documentação do MISP.

Como sua organização pode se beneficiar do MISP integration for Security Operations

Os analistas de segurança devem obter e manter a conscientização da situação do cenário de ameaças, o que significa que eles devem consolidar e integrar manualmente uma quantidade enorme de dados de ameaças. Coletar, consolidar e integrar esses dados leva um tempo valioso, o que torna mais lenta a detecção e a análise de ameaças. MISP integration for Security Operations permite que os analistas detectem mais ameaças e respondam mais rapidamente, integrando a inteligência de segurança MISP em uma instância Now Platform existente.

Ao usar o MISP integration for Security Operations, sua organização pode realizar as seguintes ações:

- Permita que seus analistas de segurança respondam rapidamente e com o contexto correto.
- Melhore a eficiência da sua equipe de segurança automatizando os fluxos de incidentes para detectar e conter ameaças.
- Reduza o tempo de pesquisa manual e permita que os analistas de segurança operacionalizem e selecionem indicadores de dentro do Now Platform.

Conheça esta integração

Identificador do documento	Título do documento
MISP site de documentação	Site de documentação do MISP
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Administração do MISP

Você pode configurar a integração MISP no Now Platform para executar uma pesquisa de detecções, aprimoramento de observável e para criar e atualizar eventos no MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comece com MISP integration for Security Operations

Revise as informações a seguir antes de configurar seu MISP integration for Security Operations.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform, Inteligência contra ameaçase Security Incident Response necessárias.	As funções a seguir são usadas nos recursos MISP no Now Platform: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui as funções de administrador de incidentes de segurança (sn_si.admin) e administrador de inteligência contra ameaças (sn_ti.admin). • sn_si.admin e sn_ti.admin podem configurar a integração e configurar os perfis de criação de eventos automáticos MISP. • sn_sec_misp.write — A função de analista MISP tem permissões de leitura e gravação para MISP dados que incluem os dados de evento e atributo. Para obter mais informações, consulte Configuração da Inteligência contra ameaças.
Atribua as funções de usuário MISP necessárias.	Revise MISP funções de usuário e as permissões necessárias para usar o MISP integration for Security Operations. **Nota:** Para obter mais informações sobre as funções de usuário em MISP, consulte a seção Funções no site de documentação do MISP .
Verifique se você está usando MISP versão 2.4.137 ou posterior.	O MISP integration for Security Operations é testado com um mínimo MISP versão 2.4.137 .
Verifique se as aplicações principais ServiceNow que são necessárias para oferecer suporte ao módulo MISP estão instaladas e ativadas.	Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• Security Incident Response • Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) • Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest) Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte obter direito de um produto ou aplicação das Operações de segurança e ativar uma aplicação da ServiceNow Store.
Domain Separation	Verifique a seção Domain Separation se você pretende separar dados, processos e tarefas administrativas.

MISP funções e permissões do usuário

Revise as funções de usuário necessárias na integração MISP integration for Security Operations.

Permissões de enriquecimento observável e pesquisa de detecções

Nota:

- Todas as **ServiceNow** capacidades de integração de MISP precisam das permissões básicas para **gerenciar eventos da organização** e **acesso à chave de autenticação**. Verifique se você tem essas permissões básicas antes de prosseguir.
- Para adicionar galáxias locais, o usuário que configura a integração deve pertencer à organização host do servidor MISP correspondente.

Capacidade do MISP	Marcador	Editor de marcadores
Aprimoramento de observável (somente leitura)	#	#
Pesquisa de detecções (somente leitura)	#	#

Relatar permissões de detecção

Capacidade do MISP	Criador de detecções
Relatar vista	#

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Permissões de atributo e evento

Capacidade do MISP	Marcador	Editor de marcadores
Editar marcadores de evento/atributo	#	#
Editar galáxias de evento/ atributo	#	#
Editar comentários de atributo	#	#
Adicionar novo atributo ao evento	#	#
Criar evento no MISP	#	#

Instalar e configurar o MISP integration for Security Operations

Instale e configure o MISP integration for Security Operations a partir do ServiceNow Store em sua instância Now Platform para que você possa começar a investigar incidentes de segurança usando os dados MISP.

Antes de Iniciar

Certifique-se de ter instalado os certificados SSL válidos no servidor MISP.

Função necessária: sn_si.admin

Procedimento

1. Baixe o MISP integration for Security Operations do ServiceNow Store e instale-o.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco MISP -SIR/TI Integration e clique em **Configurar**.
4. No formulário, preencha os campos.

MISP - Formulário de configuração de integração de SIR/TI

Campo	Descrição
Nome	Nome da configuração da instância MISP.
MISP URL do servidor	URL do servidor MISP que serve como endpoint REST para o servidor MISP.
Chave de API	Chave de API configurada para sua conta de usuário no servidor MISP. A chave de API corresponde ao **Authkey** no servidor MISP.
Implantação no Local	Opção que você pode selecionar se o servidor MISP for implantado em uma instância no local. Ao selecionar a opção **Implantação no local**, você deve usar o MID Server para se conectar ao servidor MISP.
Aplicação de MID	Campo de cadeia de caracteres que identifica o nome da aplicação MID usada para se comunicar com MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este campo é obrigatório quando você seleciona a opção **Implantação no** local. Para obter informações sobre como configurar o MID Server para sua aplicação, consulte Configuração de um MID Server para cada aplicação

5. Clique em **Enviar**.

Resultados
Depois de validar e enviar a configuração com sucesso, a integração MISP - SIR/TI será salva na página Integrações de segurança como um bloco.

Revisar as configurações de integração MISP

Revise as configurações de MISP integration for Security Operations e modifique as propriedades do sistema padrão para adequá-las ao seu ambiente.

Antes de Iniciar
Função necessária: sn_si.admin, sn_ti.admin

Procedimento
1. Navegar até **Todos** > **Integração MISP** > **Configurações de integração**.
2. Modifique as seguintes configurações conforme necessário.

Configurações de integração de MISP

Nome da propriedade		Descrição
Aprimoramento de Observável	Tempo (em horas) antes de buscar novos dados	Tempo em horas antes que você possa buscar novos dados. Tipo: inteiro Valor padrão: 24
Pesquisa de detecções	Executar pesquisa de detecções automaticamente quando novos observáveis forem associados ao incidente de segurança	Pesquisa de detecções que é executada sempre que um novo observável está associado a um incidente de segurança. Valor padrão: sim
	Intervalo de pesquisa (em dias) para pesquisa de detecções no MISP	Número de dias em que os dados de pesquisa de detecções são pesquisados em MISP. Use esta opção somente para o recurso de pesquisa de detecções automática. Valor padrão: 90

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade		Descrição
Sincronização de dados	Período de intervalo (em minutos) para que os marcadores sejam obtidos e sincronizados com o MISP	MISP marcadores que são buscados no momento da configuração da integração. Depois que os dados estão no Now Platform, esta propriedade define a frequência na qual os dados com o servidor MISP são sincronizados. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
	Período de intervalo (em minutos) para atualizar galáxias MISP de origens configuradas	MISP galáxias que são buscadas no momento da configuração da integração. Depois que os dados estão no Now Platform, esta propriedade define a frequência na qual os dados com o servidor MISP são sincronizados. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
	Período de intervalo (em minutos) para que as organizações sejam obtidas e sincronizadas com o MISP	MISP organizações que são buscadas no momento da configuração da integração. Depois que os dados estão no Now Platform, esta propriedade define a frequência na qual os dados com o servidor MISP são sincronizados. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
MITRE™ Extração de técnica	Acumular MITRE-ATT&CK técnicas automaticamente dos Resultados de enriquecimento observável do MISP (Tags) para o incidente de segurança	Acúmulo de MITRE-ATT&CK informações de MISP resultados de aprimoramento observáveis (marcadores) para o incidente de segurança. Valor padrão: sim
	Acumular MITRE-ATT&CK técnicas automaticamente dos Resultados de enriquecimento observável	Acúmulo de MITRE-ATT&CK informações dos MISP resultados de aprimoramento observáveis

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade		Descrição
	do MISP (Galaxies) para o incidente de segurança	(galáxias) para o incidente de segurança. Valor padrão: sim

Nota:

- Para usar os recursos de extração da técnica [MITRE™ em MISP, você deve habilitar o MITRE-ATT&CK recurso no Inteligência contra ameaças módulo.
- O MISP integration for Security Operations apresenta duas regras de extração da técnica do sistema base MITRE-ATT&CK para galáxias MISP - MISP e marcadores MISP. Para obter mais informações sobre regras de extração automática em MITRE-ATT&CK, consulte regras de técnica de extração automática para importar informações do MITRE-ATT&CK.

3. Clique em **Salvar**.

Resultados
Suas configurações de integração modificadas são salvas e aplicadas.

Configurar MISP pesquisas de detecções

Configure o Now Platform para fazer pesquisas de detecções para observáveis na instância MISP. Com essas informações, você pode determinar com que frequência as ameaças ocorrem.

Antes de Iniciar

- Revise MISP função e permissões do usuário que são necessários para usar os MISP recursos bidirecionais.
- Função necessária: sn_si.admin, sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho Integração de Operações de segurança - Pesquisa de detecções executa as pesquisas de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra capacidades de implementação, cria as consultas baseadas nas configurações de pesquisa de detecções e executa as pesquisas baseadas no fluxo de trabalho configurado.

O MISP integration for Security Operations fornece um perfil de pesquisa de detecções do sistema de base que permite configurar pesquisas de detecções automáticas. Com este perfil, você pode acessar as informações de detecções de observáveis relacionadas de uma organização e também ver as detecções externas de outras organizações.

Procedimento

1. Navegar até **Todos** > **Integração MISP** > **Configuração de pesquisa de detecções**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Configuração de pesquisa de detecções

Campo	Descrição
Nome	Nome do perfil de capacidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisa salva	Configuração de pesquisa que é salva quando você seleciona esta opção. As consultas de configuração de pesquisa salvas são consultas de exemplo. Você pode substituí-los pelos parâmetros do seu ambiente e criar configurações adicionais de pesquisa salva conforme necessário.
Origem da pesquisa de detecções	Origem da pesquisa de detecções. Selecione o armazenamento de log MISP como a origem.
Ativo	Opção que habilita a configuração de pesquisa salva. Somente configurações de pesquisa ativas podem executar uma pesquisa de detecções.
Tipo de observável	Tipo de observável, como endereço IP, valor de hash, URL e nome de domínio.
Máximo de observável por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa.
Pesquisar	Cadeia de caracteres de pesquisa padrão que é `$(observable)`. No entanto, você define sua própria consulta de pesquisa especificando os parâmetros compatíveis com armazenamento de log MISP.

4. Clique em **Enviar**.

Resultados
Você criou um perfil de configuração de pesquisa de detecções MISP.

Configurar como um evento automático é criado

Configure o Now Platform para criar automaticamente eventos em MISP.

Antes de Iniciar

- Revise MISP função e permissões do usuário que são necessários para usar os MISP recursos bidirecionais.
- Função necessária: sn_si.admin, sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Integração MISP** > **Perfis automáticos de criação de evento**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de nome

Campo	Descrição
Nome	Nome do perfil de criação automática de eventos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Breve descrição sobre o perfil. Uma descrição mais detalhada é compartilhada por meio dos atributos na próxima fase da criação do evento.
Ordem	Ordem do perfil quando as condições de acionamento são atendidas. O padrão é 100. Deixe esta configuração no padrão. Se você criar vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O perfil com o número mais baixo tem a prioridade mais alta.
Origem	MISP origem para a criação do evento.
Ativo	Opção que indica se o perfil está ativo ou inativo. A opção está desmarcada por padrão para indicar que o perfil está desativado. Este perfil não está ativo até que você conclua todas as etapas de configuração do perfil e clique em **Concluir**.

4. Clique em **"Continuar"**.

Configurar condições do gatilho de evento

Configure as condições do gatilho de evento em Now Platform para que você possa acionar automaticamente um evento em MISP quando as condições forem atendidas.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

1. No formulário Condições do gatilho, preencha os detalhes que podem acionar um evento.
   Você pode criar uma lógica composta fornecendo as condições do gatilho que são baseadas em campos de incidente de segurança ou campos observáveis. Você também pode criar eventos em MISP se os observáveis não tiverem um evento correspondente em MISP. Você pode optar por criar uma lógica composta usando uma combinação das três condições de gatilho - Acionar com base em campos de incidente de segurança, Acionar com base em campos observáveis e Criar evento de MISP, se um observável não tiver eventos correspondentes no MISP. Se você selecionar vários gatilhos, poderá juntá-los usando a condição E. Considere criar um perfil com novas condições se você precisar usar a condição OU.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Condições do gatilho de evento

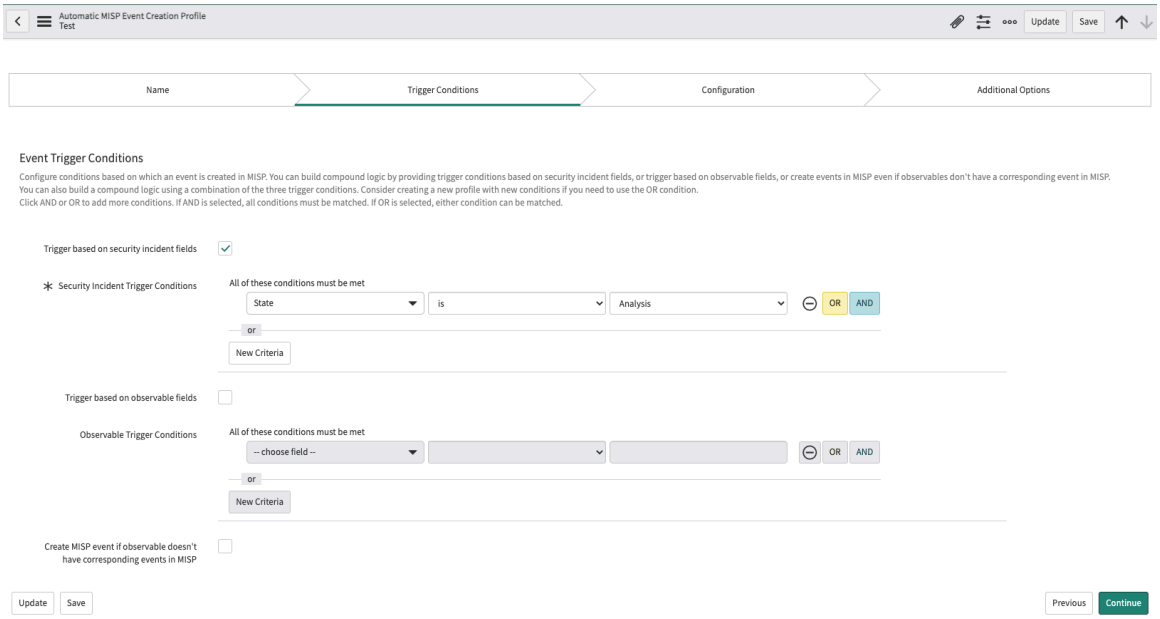
Campo	Descrição
Acionar com base nos campos de incidente de segurança	MISP evento que você pode criar se todas as condições do gatilho de incidente de segurança forem atendidas.
Condições do gatilho de incidente de segurança	Filtros na primeira linha que você pode definir usando as listas e os campos do construtor de condições. Para adicionar mais condições, clique em AND ou OR. Se E for selecionado, todas as condições deverão ser atendidas. Se OU for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**.
Acionar com base em campos observáveis	MISP evento que você pode criar se todas as condições do gatilho observável forem atendidas.
Condições do gatilho observáveis	Filtros na primeira linha que você pode definir usando as listas e os campos do construtor de condições. Para adicionar mais condições, clique em AND ou OR. Se E for selecionado, todas as condições deverão ser atendidas. Se OU for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**.
Criar evento MISP se o observável não tiver eventos correspondentes no MISP	MISP evento que você pode criar se um observável não tiver eventos correspondentes em MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições do gatilho de evento

O exemplo a seguir mostra as condições do gatilho de evento conforme você configura o perfil de criação de eventos MISP.



2. Clique em **"Continuar"**.

Mapear os campos de evento MISP

Mapeie os campos de evento MISP no Now Platform para que as informações do incidente de segurança estejam disponíveis quando os eventos MISP forem criados.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

1. No formulário, preencha os campos.

Formulário de mapeamento de campo de evento de MISP padrão

Campo	Descrição
Informações do evento	Informações de evento que são criadas automaticamente a partir de Now Platform Security Incident Response. O campo **Informações do evento** oferece suporte a variáveis de substituição usando ${SIR FIELD LABEL}$. Durante a criação de um evento, essas variáveis são substituídas pelos valores reais do campo de incidente de segurança. A variável de substituição ${URL}$ é substituída pela URL do incidente de segurança.
Distribuição	Opção que controla quem pode exibir este evento depois que o evento é publicado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos e a configuração mais restritiva vence. As opções de distribuição são as seguintes: ◦ Somente sua organização: permite que somente membros da sua organização exibam este evento. O evento pode ser extraído para outra instância por um dos membros da sua organização, onde somente a sua organização pode ter acesso para exibi-lo. Eventos com esta configuração não são sincronizados. ◦ Somente esta comunidade: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo sua própria organização, organizações neste servidor MISP e organizações que executam servidores MISP que são sincronizados com este servidor. Quaisquer outras organizações que se conectem aos seus servidores vinculados estão impedidas de exibir o evento. ◦ Comunidades conectadas: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo todas as organizações neste servidor MISP, todas as organizações nos servidores MISP que são sincronizados com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que está a dois saltos de distância. Quaisquer outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância estão impedidas de exibir o evento. ◦ Todas as comunidades: compartilha o evento com todas as MISP comunidades.
Nível de ameaça	Campo que indica o nível de risco do evento. Você pode categorizar os incidentes em três categorias de ameaça diferentes (baixa, média, alta). Este campo também pode ser deixado como indefinido. A seguir estão as opções: ◦ Baixo: malware geral em massa ◦ Médio: ameaças persistentes avançadas (APT) ◦ Alto: APTs sofisticados e ataques de dia 0

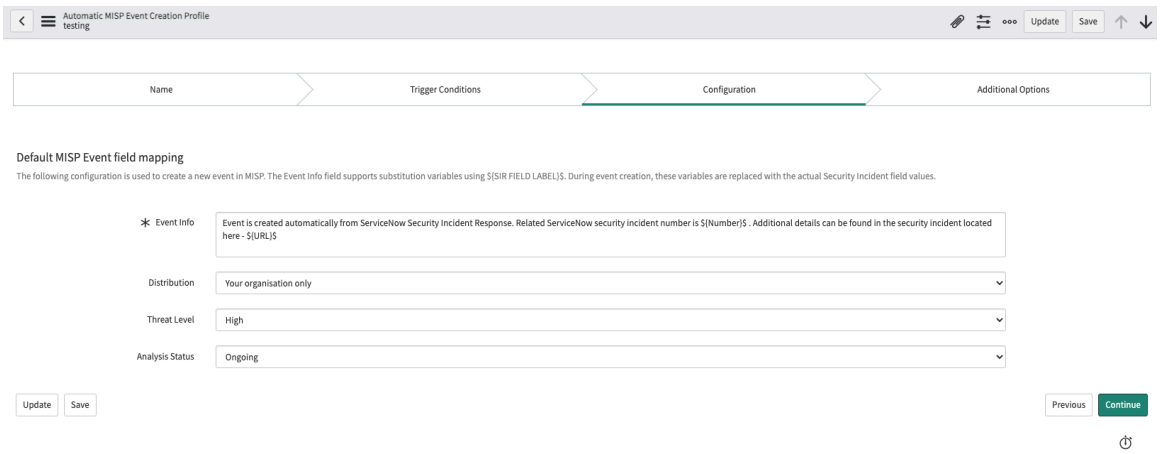
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status da análise	Fase atual da análise do evento, com as seguintes opções possíveis: ◦ Inicial: a análise está apenas começando ◦ Em andamento: a análise está em andamento ◦ Concluído: a análise está concluída

O exemplo a seguir mostra o formulário que você pode usar para criar um evento no MISP.

Mapeamento de campo de evento MISP padrão



2. Clique em **"Continuar"**.

Mapear ou associar SIR observáveis como atributos a MISP eventos

Mapeie os tipos de observável Security Incident Response para os tipos de atributo MISP, porque os tipos de atributo MISP e os observáveis SIR podem ser diferentes.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Por Que e Quando Desempenhar Esta Tarefa

O MISP integration for Security Operations fornece um mapeamento do sistema de base que você usa ao adicionar SIR observáveis como atributos a um evento MISP.

Você pode optar por modificar o mapeamento do sistema de base para se adequar ao seu ambiente. Por exemplo, você pode mapear vários observáveis SIR para apenas um tipo de atributo MISP. Se algum tipo de observável não estiver mapeado, o **outro** MISP tipo de atributo será selecionado por padrão.

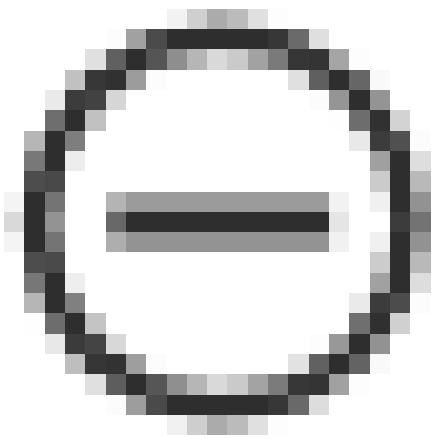
Procedimento

1. No formulário Opções adicionais, mapeie os tipos de atributo SIR e observável MISP.
2. Mapeie os tipos de observável Security Incident Response para os tipos de atributo MISP, conforme descrito na tabela a seguir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento do observável de SIR e tipo de atributo do MISP

Campo	Descrição
Adicionar todos os observáveis associados como atributos	Opção que você habilita para adicionar observáveis disponíveis em um incidente de segurança a um evento MISP como atributos. Esta opção habilita o mapeamento na seção Tipo de observável para mapeamento de tipo de atributo.
Tipo de observável para mapeamento de tipo de atributo	Opção para mapear os tipos de observável SIR para os tipos de atributo MISP. Por exemplo, você pode mapear o número CVE em SIR para o atributo de vulnerabilidade em MISP. Você pode adicionar um tipo de observável SIR a apenas um tipo de atributo MISP. O sistema de base fornece um mapeamento dos tipos de observável SIR para os tipos de atributo MISP. Se algum tipo de observável SIR não estiver mapeado para um tipo de atributo MISP, o observável será mapeado para o **outro** tipo de atributo em MISP. Para adicionar um novo mapeamento, clique em **Adicionar tipo de observável**, pesquise o tipo de observável SIR e mapeie para o tipo de atributo MISP correspondente. Clique no ícone  para remover a associação de mapeamento de atributo SIR e MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Para obter mais informações sobre os tipos de atributo MISP, consulte a documentação do MISP .
Filtrar observáveis com base em marcadores de segurança	Opção para filtrar os observáveis com base nos marcadores de segurança selecionados. Marcadores de**segurança**: adicione marcadores para filtrar os observáveis. Por exemplo, se você estiver adicionando um marcador chamado "Bloquear contra compartilhamento" ou "TLP: branco", se um dos observáveis tiver algum desses marcadores associados, esses observáveis não serão adicionados como um atributo ao evento de MISP durante o MISP criação de eventos.
Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada	Opção que permite que você saiba que se um observável for marcado como mal-intencionado em SIR, o atributo correspondente em MISP terá o sinalizador de IDS habilitado. Se o sinalizador IDS não estiver definido, o atributo será considerado como informações contextuais e não será usado para detecção automática de intrusão.

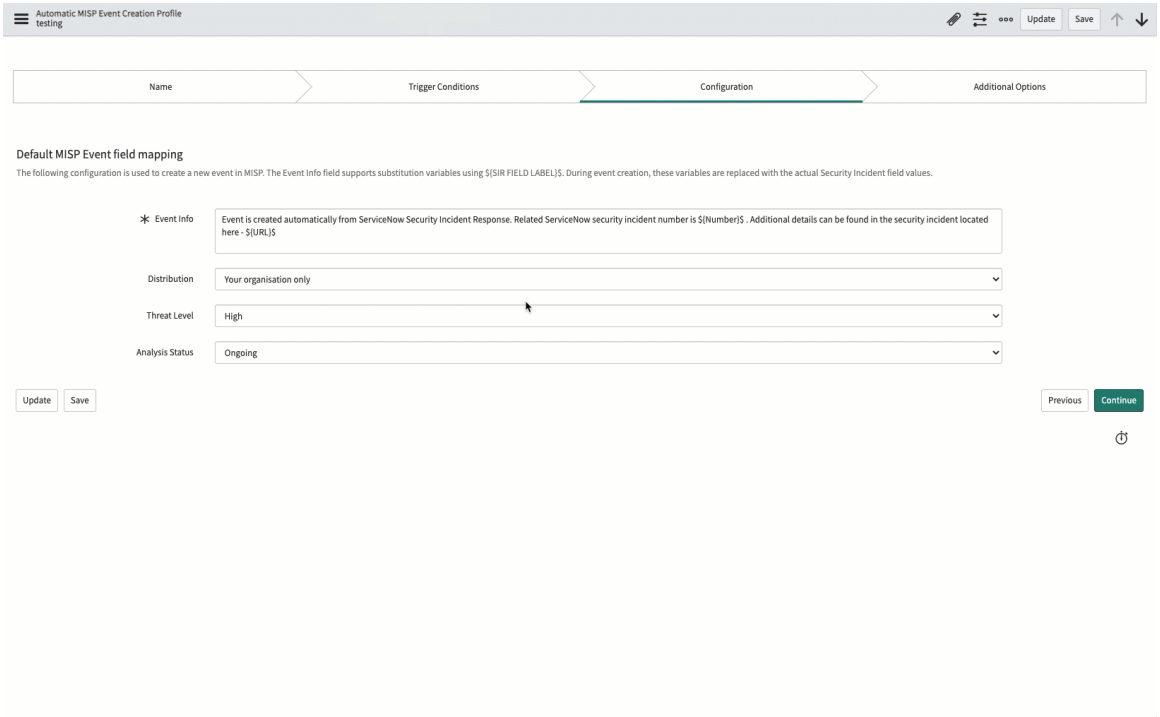
O exemplo a seguir mostra como navegar até a página de opções adicionais. Nesta página, você pode habilitar os observáveis SIR e o mapeamento de tipos de atributo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MISP, adicionar novos tipos de observável SIR, como a rede IPV6 e a rede IPV4, e mapeá-los para o endereço IP de domínio do tipo de atributo MISP.

Mapeamento de SIR observáveis e MISP tipos de atributo



Sincronizar MITRE-ATT&CK informações com MISP eventos

Sincronize as informações [MITRE-ATT&CK com os atributos MISP para obter uma melhor análise de ameaças e incidentes de segurança.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

No formulário Opções adicionais, revise as opções para sincronizar as informações MITRE-ATT&CK com os atributos MISP.

Formulário Opções avançadas

Campo	Descrição
Sincronizar técnicas de incidente de segurança MITRE-ATT&CK™ como galáxias locais para o evento MISP	Opção para sincronizar as técnicas Now Platform SIR de incidente de segurança MITRE-ATT&CK™ como galáxias locais no evento MISP. **Nota:** Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do servidor MISP correspondente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Sincronizar técnicas de incidente de segurança MITRE-ATT&CK™ como galáxias globais para o evento MISP	Opção para sincronizar as técnicas Now Platform SIR de incidente de segurança MITRE-ATT&CK™ como galáxias globais no evento MISP.

Resultados
Você criou um perfil que permite criar automaticamente eventos em MISP a partir de Now Platform. Agora você pode exibir os eventos na lista relacionada Eventos de MISP associados.

Adicionar marcadores de MISP a eventos

Adicione marcadores de MISP aos eventos de MISP criados.

Antes de Iniciar
Função necessária: sn_sec_misp.write

Procedimento
1. No formulário Opções adicionais, navegue até **Selecionar marcadores MISP para adicionar à seção de eventos** na exibição do formulário.
2. Revise as opções para adicionar marcadores aos eventos criados.

Formulário Opções avançadas

Campo	Descrição
Adicionar marcadores ao evento MISP criado	Opção que permite adicionar automaticamente marcadores de MISP aos eventos criados na ServiceNow.
Marcadores (local)	Os marcadores selecionados serão adicionados como marcadores locais ao evento MISP.
Marcadores (global)	Os marcadores selecionados serão adicionados como marcadores globais ao evento MISP.

3. Clique em **Salvar**.

Resultados
Adicionar marcadores de MISP ajuda na classificação do evento.

MISP dados do evento

Você pode revisar os dados do evento MISP para ver informações detalhadas sobre os eventos MISP.

MISP dados do evento na exibição de lista

Acessar a exibição de lista em **MISP** > **Dados do evento de MISP**.

Use a exibição de lista para obter uma visão geral rápida dos dados do evento MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de lista de eventos de MISP

Campo	Descrição
ID de Evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para o servidor MISP.
Informações	Descrição resumida do evento.
Análise	Fase atual da análise do evento com as seguintes opções possíveis: • Inicial: a análise está apenas começando • Em andamento: a análise está em andamento • Concluído: a análise está concluída
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média e alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: • Baixo: malware geral em massa • Médio: ameaças persistentes avançadas (APT) • Alto: APTs sofisticados e ataques de dia 0
Marcadores MISP	Marcadores associados ao evento MISP.
Galáxias MISP	Galáxias associadas ao evento MISP.
Organização do proprietário	Organização proprietária do evento na instância MISP. Este campo está visível somente para os administradores.
Organização do criador	Organização que criou o evento na instância MISP.
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Hiperlink de evento MISP	Link para o evento MISP que está armazenado no servidor MISP.
Origem do MISP	MISP origem em que o evento é criado.

MISP dados do evento na exibição do formulário

Use a exibição de formulário para obter informações detalhadas sobre os eventos MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição do formulário de eventos de MISP

Campo	Descrição
ID de Evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para o servidor MISP.
UUID	ID que identifica exclusivamente eventos e atributos.
Organização do criador	Organização que criou o evento na instância MISP.
Organização do proprietário	Organização proprietária do evento na instância MISP. Este campo está visível somente para os administradores.
Usuário do criador	Usuário que criou o evento em MISP.
Última mudança	Data em que o evento foi modificado pela última vez.
Origem do MISP	MISP origem em que o evento é criado.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez no servidor MISP.
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média e alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: • Baixo: malware geral em massa • Médio: ameaças persistentes avançadas (APT) • Alto: APTs sofisticados e ataques de dia 0
Análise	Fase atual da análise do evento com as seguintes opções possíveis: • Inicial: a análise está apenas começando • Em andamento: a análise está em andamento • Concluído: a análise está concluída
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Publicado	Status que indica se o evento foi publicado ou não. A publicação permite que os atributos do evento sejam usados para todas as exportações qualificadas e notifique os usuários que assinaram os alertas de evento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição do formulário de eventos de MISP

Campo	Descrição
Hiperlink de evento MISP	Link para o evento MISP que está armazenado no servidor MISP.
Informações	Descrição resumida do evento.
Marcadores (local)	Marcadores que estão disponíveis na instância MISP da organização host para habilitar a marcação para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa marcadores locais. Os marcadores locais são sempre removidos antes de serem sincronizados com outras MISP instâncias e comunidades de compartilhamento.
Marcadores (global)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outras MISP instâncias e comunidades de compartilhamento. Ao adicionar marcadores globais a instâncias MISP, você pode modificar eventos.
Galáxias (local)	Galáxias que estão disponíveis na instância MISP da organização host para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa galáxias locais. Essas galáxias locais são sempre eliminadas antes de serem sincronizadas com outras MISP instâncias e comunidades de compartilhamento.
Galáxias (global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras MISP instâncias e comunidades de compartilhamento. Ao adicionar galáxias globais, MISP, você pode modificar eventos.

Tradução automática

Eventos MISP associados

Você pode usar a exibição de lista de eventos MISP associados para exibir os eventos que foram criados manual ou automaticamente no contexto de um incidente de segurança.

Eventos de MISP associados

Campo	Descrição
Incidente de segurança	SIR incidente de segurança. Clique no incidente de segurança para exibir o incidente de segurança.
Evento MISP	MISP ID do evento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Eventos de MISP associados

Campo	Descrição
	Clique no evento MISP para exibir o evento MISP no Now Platform.
Origem do MISP	MISP origem em que o evento é criado. Clique na origem MISP para exibir a origem.
Modo de criação de evento	Status que indica se o evento foi criado manualmente ou automaticamente com o perfil de criação de eventos. Clique no evento MISP para exibir o evento MISP associado.
Perfil de criação automática de evento	Perfil de criação de eventos usado para criar o evento automático. Clique no perfil para exibir o perfil de criação automática de eventos de MISP.

MISP informações do usuário

Você pode usar a página de informações do usuário MISP para exibir todos os usuários associados ao Now Platform MISP integration for Security Operations.

Informação do usuário de MISP

Campo	Descrição
Origem	Origem MISP da conta do usuário.
ID do Usuário	ID do usuário que é atribuído pelo servidor MISP quando uma conta de usuário é criada.
E-mail do Usuário	Endereço de e-mail de um usuário. Somente administradores da organização podem ver os endereços de e-mail dos usuários da própria organização.
Organização	Organização à qual um usuário pertence.
Nome da Função	Nome da função que define os privilégios de usuário atribuídos a um usuário. Para obter mais informações sobre funções em MISP, consulte a documentação do MISP .
ID de Função	ID da função do usuário em MISP. Por exemplo, Perm Admin, Perm Audit ou Perm Tagger e assim por diante.
Permissão	Permissões que um usuário tem. As permissões que estão disponíveis no MISP são as seguintes:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informação do usuário de MISP

Campo	Descrição
	• Somente Leitura • Gerenciar eventos próprios • Gerenciar eventos da organização • Gerenciar Publicar eventos da organização
Permissão de vista	Permissão que habilita um usuário a realizar pesquisas de detecções.
Permissão do tagger	Permissão que habilita um usuário a marcar.

Separação de domínios e MISP

Separação de domínios é compatível com MISP. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico.

Como o Domain Separation funciona com MISP

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com as funções necessárias no seu domínio.
- Execute os procedimentos MISP integration for Security Operations no seu domínio.

Solução de problemas de integração de MISP

Esta seção aborda dicas importantes de solução de problemas que podem ajudá-lo a resolver problemas comuns que podem ser encontrados ao configurar ou executar a integração de MISP.

Problemas de SSL

Ao se conectar por meio da integração de MISP, certifique-se de ter instalado um certificado de CA válido no servidor MISP, que não tenha expirado. Você pode importar RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Para obter mais informações, consulte Instalar e configurar o MISP integration for Security Operations e MISP funções e permissões do usuário.

Usando MISP para investigar e analisar ameaças

Você pode usar os dados MISP] no módulo Now Platform Inteligência contra ameaças e no módulo Now Platform SIR para investigar e analisar ameaças à sua organização.

Pesquisas de detecções em MISP

Você pode executar pesquisas de detecções em observáveis na instância MISP para determinar com que frequência determinados tipos de ataques, como ataques de phishing

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ou comunicações com um IP ou URL mal-intencionado, ocorrem em sua rede. Cada ocorrência é considerada uma detecção.

Detecções em MISP

As vistas indicam que um indicador, objeto ou atributo foi visto e sua validade foi confirmada. Detecções em MISP é um sistema que permite responder a atributos em um evento. Ele foi projetado para fornecer um método fácil para os usuários confirmarem que viram um determinado atributo, dando a ele mais confiabilidade. Você pode visualizar um atributo várias vezes.

Nota: Os observáveis são conhecidos como atributos no MISP.

Alguns atributos são considerados falso-positivos, o que significa que não são detecções válidas. Outros atributos são válidos por apenas uma determinada duração, como uma campanha de phishing que é executada por apenas uma semana. Você pode atribuir uma data de vencimento aos atributos que são válidos por uma determinada duração, mas cada organização pode atribuir apenas uma data de vencimento válida a um atributo.

As detecções criadas em MISP por usuários de organizações marcadas como locais no servidor MISP correspondente são conhecidas como detecções internas. As detecções criadas em MISP por usuários de organizações marcadas como remotas no servidor MISP correspondente são conhecidas como detecções externas.

Pesquisas de detecções em SIR

O fluxo de trabalho Integração de Operações de segurança - Pesquisa de detecções executa a pesquisa de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra capacidades de implementação, cria as consultas baseadas nas configurações de pesquisa de detecções e executa as pesquisas baseadas no fluxo de trabalho configurado.

As pesquisas de detecções ajudam os analistas a determinar a predominância de uma ameaça ao longo do tempo. Você pode selecionar observáveis individuais ou múltiplos e o intervalo de datas para sua pesquisa de um incidente de segurança. Os resultados são incluídos nas listas relacionadas Detecçõesde incidentes de segurança, Resultadosda pesquisa de detecções e Detalhes da pesquisa de detecções.

Ao começar a analisar um incidente, você pode configurar seu Now Platform para executar automaticamente uma pesquisa de detecções ou executar manualmente uma pesquisa de detecções de observável para identificar outros usuários em sua organização que foram afetados pelo mesmo ataque de phishing.

Habilitar pesquisas de detecções automáticas no MISP

Habilite a pesquisa de detecções em MISP para ser executada automaticamente para que o fluxo de trabalho Integração de Operações de segurança - Pesquisa de detecções seja acionado sempre que novos observáveis forem associados a um incidente de segurança.

Antes de Iniciar

Verifique se o Perfil de configuração de pesquisa de detecções para MISP está ativo.

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Se você habilitar a capacidade de pesquisa de detecções seja executada automaticamente no MISP configuração de integração, a pesquisa de detecções em MISP será acionada quando novos observáveis forem associados a um incidente de segurança.

Tradução automática

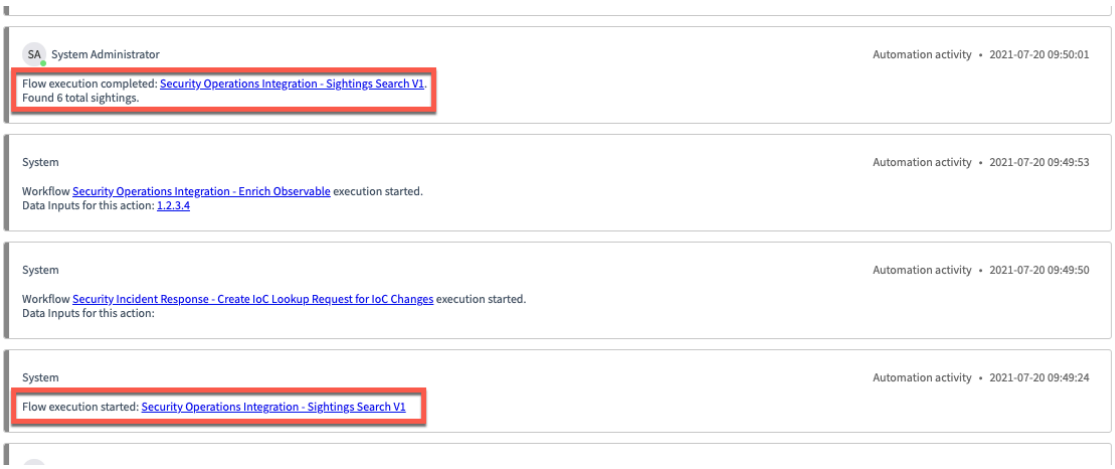
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, a opção **Executar pesquisa de detecções automaticamente quando novos observáveis estão associados ao incidente de segurança** está habilitada.

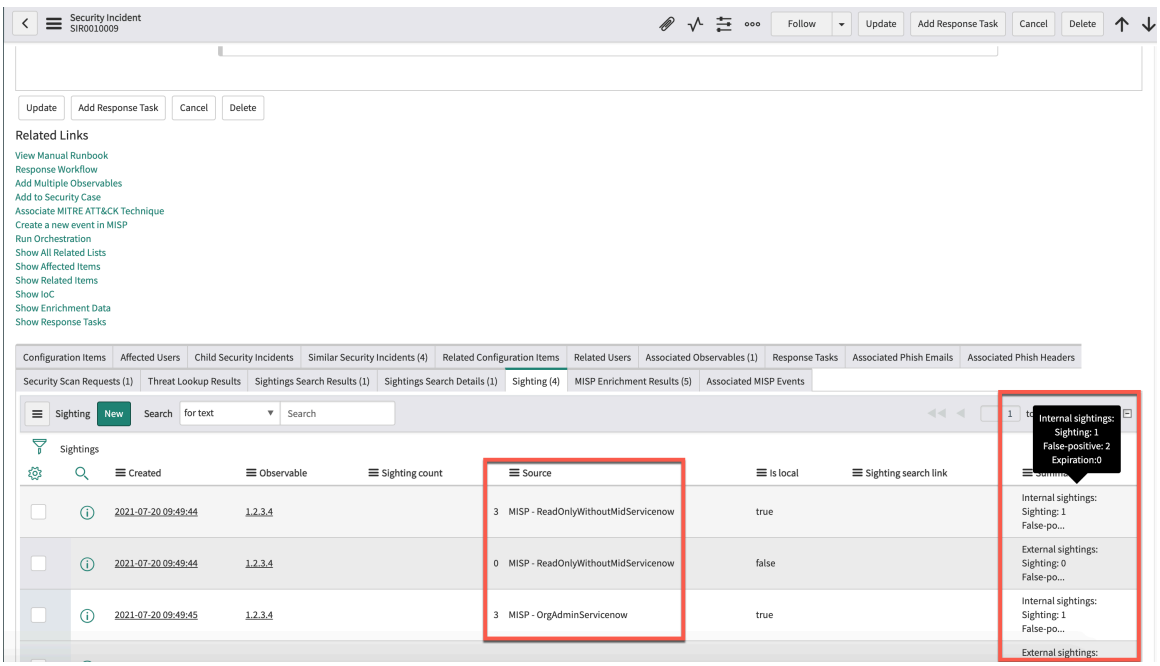
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis que você deseja exibir nos dados de pesquisa de detecções MISP.
3. Revise as anotações de trabalho depois que novos observáveis forem associados ao incidente de segurança.
   Uma anotação de trabalho é publicada quando o fluxo de trabalho Integração de Operações de segurança - Pesquisa de detecções é acionado.

   O exemplo a seguir mostra a seção de anotações de trabalho.



4. Exiba as informações agregadas de observáveis que são vistos em todos os eventos (global) e categorizados por suas detecções internas ou externas após a conclusão da execução do fluxo de trabalho.
   Exiba as informações nas listas relacionadas Detecções, Resultados da pesquisa de detecções e Detalhes da pesquisa de detecções.O exemplo a seguir mostra o registro de pesquisa de detecções que foi criado na lista relacionada Detecções.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de pesquisa de detecções

Campo	Descrição
Criação	Data e hora em que o registro de pesquisa de detecções foi criado.
Observável	Observável pesquisado pela consulta.
Contagem de detecções	Contagem de detecções internas e externas.
Origem	Origem do observável. Se o observável for de uma organização MISP, o registro será precedido pelas palavras `MISP`.
É local	Status se a detecção foi relatada por um usuário interno.
Link de pesquisa de detecção	Link de pesquisa de detecções na instância MISP.
Resumo	Tipo de detecções associadas ao registro. Os três tipos de Detecções são Detecção, Falso-positivo e Expiração. A coluna Resumo aparece somente quando o MISP integration for Security Operations está instalado. Se forem exibidas origens diferentes de MISP, a entrada da coluna Resumo estará vazia para esse registro.

Executar uma pesquisa de detecções manual em MISP

Selecione observáveis individuais ou múltiplos e execute uma pesquisa de detecções manual na aplicação Now Platform MISP integration for Security Operations para determinar a predominância de uma ameaça ao longo do tempo.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja executar a pesquisa de detecções MISP.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione o observável e, no menu Ações, clique em **Executar Pesquisa de detecções**.
   Você pode selecionar vários observáveis para uma pesquisa de detecções.
   A caixa de diálogo Executar pesquisa de detecções é aberta.
5. Especifique o intervalo de datas para pesquisar os dados de pesquisa de detecções.

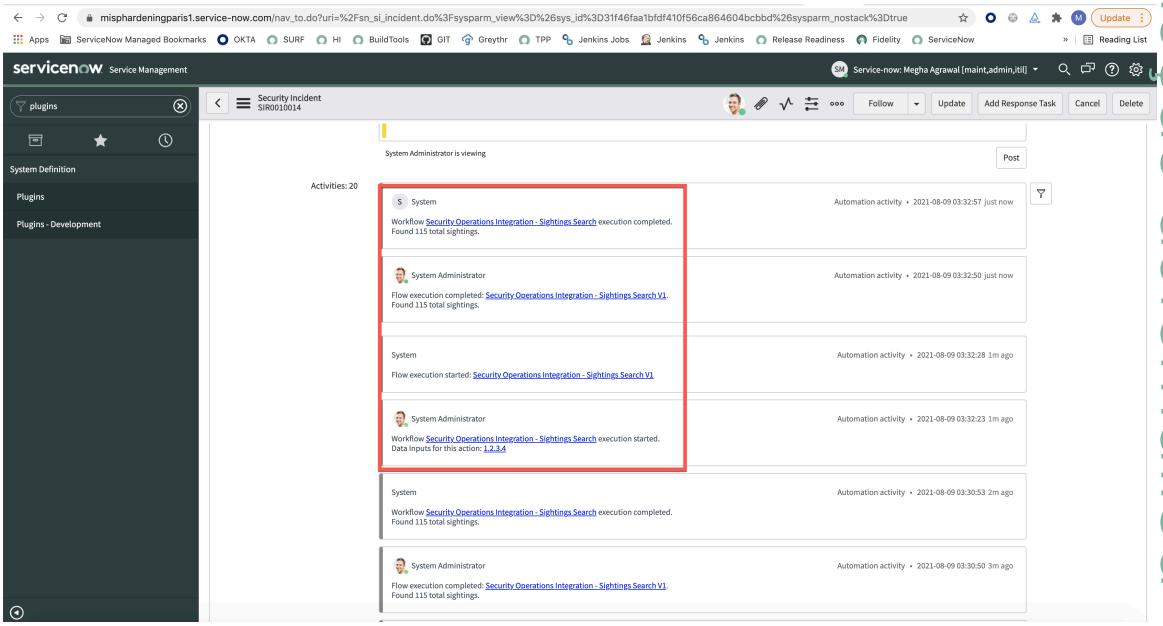
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caixa de diálogo Executar pesquisa de detecções

Campo	Descrição
Último	Número de horas ou dias anteriores à criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.
entre	Intervalo de datas a serem pesquisadas. As datas padrão são as seguintes: ◦ A data e a hora em que o incidente foi criado. ◦ A data e a hora que são sete dias antes da abertura do incidente.

6. Clique em **Pesquisar**.
   O exemplo a seguir mostra os resultados da pesquisa de detecções manual nas anotações de trabalho.



Resultados

Um registro de pesquisa de detecções é criado. Depois que a execução do fluxo de trabalho for concluída, você poderá exibir as informações agregadas de observáveis que são vistos em todos os eventos (global) e categorizados por suas detecções internas ou externas. Os dados agregados e de detecções associados são exibidos no incidente de segurança nas listas relacionadas Detecções, Resultadosda pesquisa de detecções e Detalhes da pesquisa de detecções.

Relatar detecções para MISP

Relate detecções de dados de ameaças para que você possa reagir a falsos positivos em seus dados e aumentar sua conscientização quando ocorrer uma ameaça positiva verdadeira. Você também pode adicionar uma data de expiração para um observável ou atributo específico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O MISP integration for Security Operations permite que você relate detecções para MISP globalmente em todos os eventos. Para relatar uma detecção para um evento específico, você deve usar a instância MISP e relatar a detecção localmente.

Para relatar uma detecção para MISP, o observável ou o atributo deve estar disponível na instância MISP.

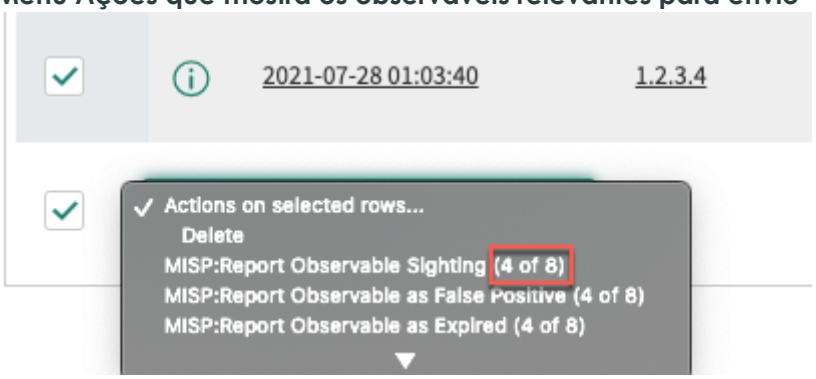
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja relatar as detecções para MISP.
3. Clique **em Mostrar todas as listas relacionadas** e na lista relacionada Detecções.
4. Selecione o observável e, no menu Ações, selecione uma das seguintes opções.

Opção	Descrição
MISP: relatar detecções de observável	Relate o observável como avistado para MISP. Se o observável estiver associado a vários eventos, ele será atualizado em todos os eventos.
MISP: relatar observável como falso-positivo	Relate o observável como um falso-positivo para MISP.
MISP: relatar observável como expirado	Relate o observável como expirado para MISP.

Se você selecionar observáveis que não são específicos de uma origem MISP, o menu Ações mostrará a contagem de origens MISP relevantes. O exemplo a seguir mostra quatro de oito observáveis como relevantes para MISP.O exemplo a seguir mostra o menu de ações e os observáveis relevantes para envio.

Menu Ações que mostra os observáveis relevantes para envio



5. Opcional: Se você selecionou a opção **MISP: Relatar detecções de observável**, preencha os campos da caixa de diálogo Relatar detecções de observável ao MISP.

Tradução automática

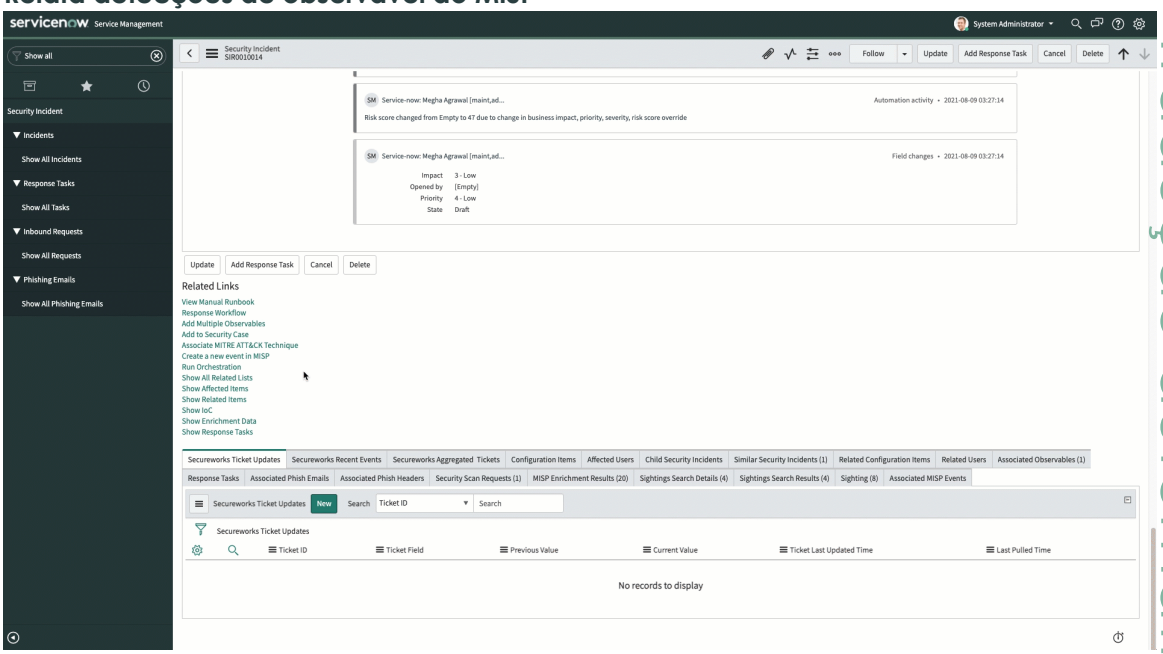
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caixa de diálogo Relatar vista observável para MISP

Campo	Descrição
Origem	Campo de origem que corresponde à origem MISP da detecção.
Data	Campo de data que corresponde à data em que o observável foi avistado. Se a data estiver vazia, a data e hora atuais serão preenchidas em MISP.

O exemplo a seguir mostra como navegar até a lista relacionada Detecções no incidente de segurança. Nessa lista, você pode selecionar um observável e relatar a detecção de observável para MISP. A mensagem de sucesso mostra que a detecção foi enviada com sucesso para MISP.

Relata detecções de observável ao MISP



a. Clique **em Relatar detecções**.

6. Opcional: Se você selecionou a opção **MISP: Relatar observável como falso-positivo**, preencha os campos da caixa de diálogo Relatar observável como falso-positivo para MISP.

Caixa de diálogo Relatar observável como falso-positivo para MISP

Campo	Descrição
Origem (opcional)	Campo de origem que corresponde à origem MISP. Use este campo para declarar o observável como um falso-positivo.
Data	Campo de data que corresponde à data em que o observável foi identificado como um falso-positivo. Se a data estiver vazia, a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	data e hora atuais serão preenchidas em MISP.

a. Clique **em Relatar falso-positivo**.

7. Opcional: Se você selecionou a opção **MISP: Relatar observável como expirado**, preencha os campos da caixa de diálogo Relatar expiração do observável para MISP.

Caixa de diálogo Relatar expiração do observável ao MISP

Campo	Descrição
Origem	Campo de origem que corresponde à origem MISP. Use este campo para definir um observável como expirado.
Data	Campo de data que corresponde à data em que o observável expirou. Se a data estiver vazia, a data e hora atuais serão preenchidas em MISP.

a. Clique **em Relatar expiração**.

Resultados

As detecções foram atualizadas com sucesso para o servidor MISP.

Aprimoramento de observável em MISP

Ao aprimorar os observáveis com informações adicionais de várias MISP origens durante as investigações de resposta do incidente, você pode conter as ameaças identificadas.

Habilitar enriquecimento automático de observável em MISP

Habilite o enriquecimento automático de observáveis no Now Platform MISP quando novos observáveis estiverem associados ao incidente de segurança.

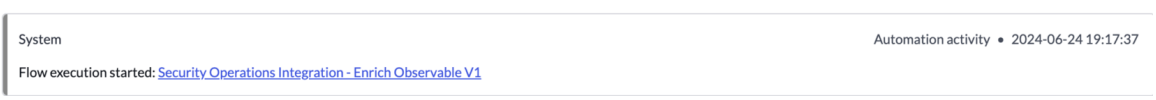
Antes de Iniciar

- Habilite a propriedade do sistema Security Incident Response para a opção **Habilita ou Desabilita o trabalho agendado, Pesquisar observáveis de incidentes de segurança** para acionar a capacidade de aprimoramento do observável em SIR.
- Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja aprimorar os dados do observável em MISP.
3. Revise as anotações de trabalho depois que novos observáveis forem associados ao incidente de segurança.

   O exemplo a seguir mostra que uma anotação de trabalho é publicada quando o fluxo Integração de Operações de segurança - Aprimorar observável é acionado.



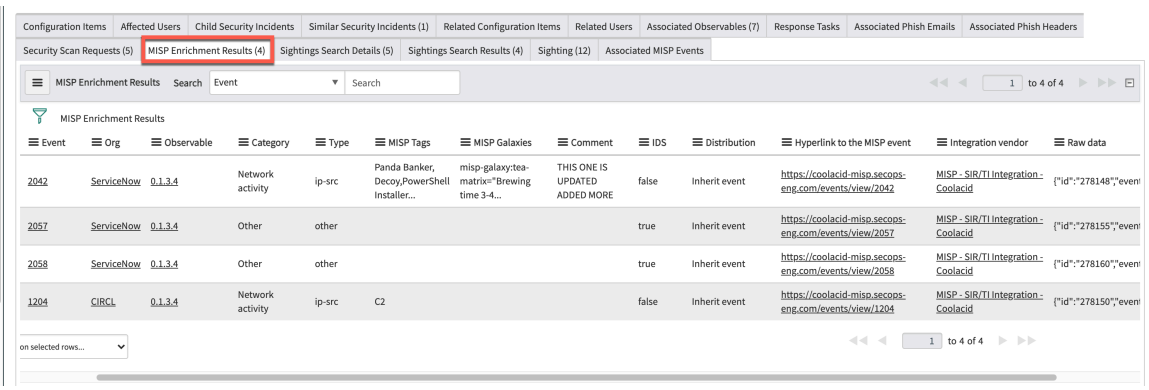
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na lista relacionada MISP Resultados de aprimoramento do incidente de segurança, exiba os resultados de aprimoramento após a conclusão da execução do fluxo.

Nota: Você deve configurar para que a lista relacionada MISP Resultados de aprimoramento apareça nas listas relacionadas a incidentes de segurança. Para obter mais informações, consulte configuração de lista relacionada.

O exemplo a seguir mostra os resultados de aprimoramento no MISP.



A tabela a seguir mostra os resultados de aprimoramento do MISP.

Resultados de enriquecimento de MISP

Campo	Descrição
Evento	ID do evento. Clique em Abrir para exibir o registro na instância Now Platform.
Organização	Organização que criou originalmente o evento.
Observável	Observável que está associado ao evento.
Categoria	Categoria do atributo. Exiba a lista de categorias na documentação do MISP .
Tipo	Tipo do atributo. Exiba a lista de tipos na documentação do MISP .
Marcadores MISP	Lista de marcadores associados ao atributo MISP.
Galáxias MISP	Lista de galáxias associadas ao atributo MISP.
Comentário	Comentário contextual para descrever melhor o atributo. Esses comentários não são usados para correlação e são exclusivamente informativos.
IDS	Indicador de comprometimento, o que permite que ele seja incluído em todas as exportações qualificadas.
Distribuição	Distribuição do atributo depois que ele é publicado. Um atributo pode ter um nível de distribuição diferente do evento. Em qualquer um dos casos, o nível de distribuição mais baixo é usado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hiperlink para o evento MISP	Link para o evento MISP, que está armazenado no servidor MISP.
Fornecedor de integração	Fornecedor de integração que fornece os dados para enriquecimento.
Dados brutos	Dados brutos associados ao atributo MISP.

Executar um aprimoramento de observável manual em MISP

Selecione observáveis individuais ou múltiplos e execute um aprimoramento de observável manual para que você possa aprimorar observáveis com informações adicionais de várias MISP origens.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Função necessária: sn_si.analyst

Procedimento

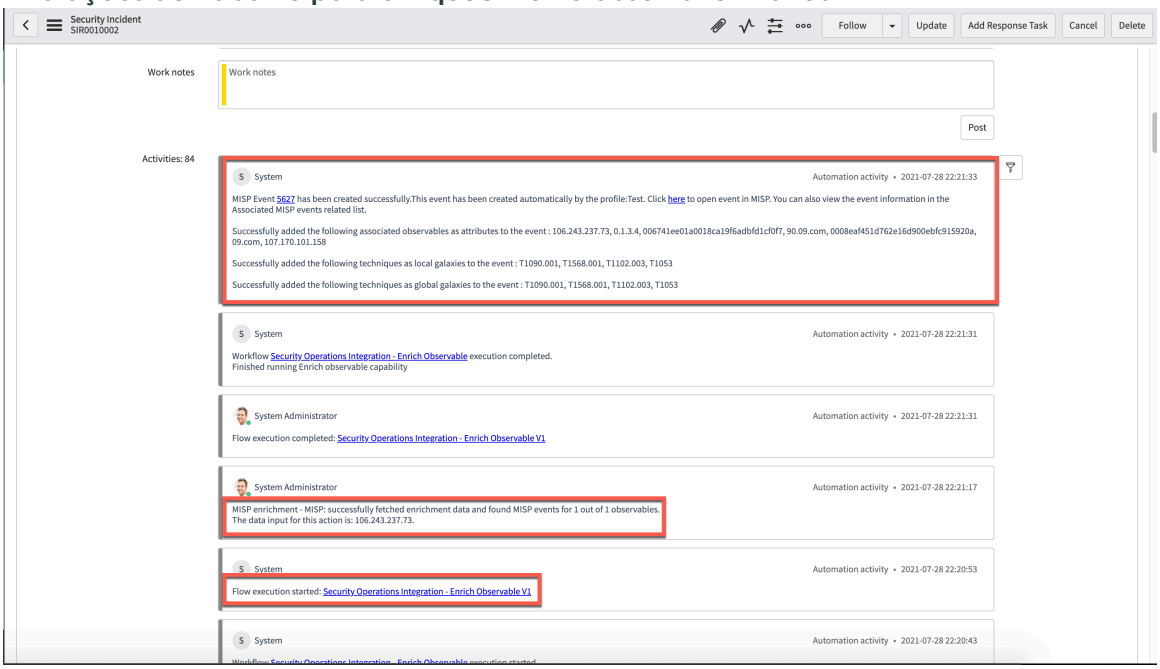
1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja executar o aprimoramento.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione o observável e, no menu Ações, clique em **Executar aprimoramento de observável**.
   Você pode selecionar vários observáveis para uma pesquisa de detecções.
   A caixa de diálogo Executar aprimoramento de observável é exibida.
5. Selecione uma origem MISP e, na coluna Selecionada, selecione uma implementação para aprimorar os observáveis selecionados.
6. Clique em **Enviar**.
   Uma anotação de trabalho mostra que o fluxo de trabalho Integração de Operações de segurança - Aprimorar observável foi acionado. Os fluxos de trabalho de implementação associados são executados para realizar o aprimoramento. Você pode exibir as anotações de trabalho no incidente de segurança para exibir o status.

   O exemplo a seguir mostra como exibir as anotações de trabalho para um aprimoramento de observável manual.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anotações de trabalho para enriquecimento observável manual



A mensagem de aprimoramento lista o evento criado. Você pode exibir o evento na instância Now Platform ou na instância MISP e exibir os detalhes do registro na guia Resultados de aprimoramento do MISP.

Adicionar ou remover marcadores dos atributos MISP

Adicione ou remova marcadores em MISP para classificar eventos ou atributos. Você pode usar a marcação globalmente para habilitar sua classificação ou usar marcadores localmente quando não quiser que os eventos MISP sejam modificados durante a classificação.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Verifique se o atributo que você está editando pertence à mesma organização que o usuário MISP.
- Observe que os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis, atributos ou eventos aos quais você deseja adicionar os marcadores.
3. Clique **em Mostrar todas as listas relacionadas** e na lista relacionada de Resultados de aprimoramento do MISP.
4. Clique no ícone de ⓘ ao lado de um registro e clique em **Abrir registro**.
   O exemplo a seguir mostra como revisar os **resultados de aprimoramento do MISP** e como abrir um registro de aprimoramento MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de resultado de aprimoramento do MISP
Abrindo o registro de resultado de aprimoramento do MISP

5. Revise o registro de resultado de aprimoramento do MISP.

Resultado do aprimoramento de MISP

Campo	Descrição
Observável	
Evento	ID do evento atribuído pelo servidor MISP quando o evento foi criado ou importado pela primeira vez para MISP. Visualize o evento ou clique no registro para exibir os dados do evento na página MISP Dados do evento.
Organização	Organização que criou o atributo MISP.
Categoria	Categoria do atributo que você adiciona ao evento específico em MISP. Você pode selecionar uma opção como referência interna, atividade de rede, fraude financeira e assim por diante.
Tipo	Tipo de atributo MISP.
Fornecedor de integração	Fornecedor de integração que fornece os dados para o aprimoramento do observável.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez para MISP.
IDS	Status de um observável marcado como mal-intencionado em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
Distribuição	Controles de opção de distribuição, como quem pode exibir este evento depois que ele é publicado. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos e a configuração mais restritiva vence. As opções de distribuição são as seguintes: ◦ Somente sua organização: permite que somente membros da sua organização exibam este evento. O evento pode ser extraído para outra instância por um dos membros da sua organização, onde somente a sua organização tem acesso para exibi-lo. Eventos com esta configuração não são sincronizados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Somente esta comunidade: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo sua própria organização, organizações neste servidor MISP e organizações que executam servidores MISP que são sincronizados com este servidor. Quaisquer outras organizações conectadas a esses servidores vinculados estão impedidas de exibir o evento. ◦ Comunidades conectadas: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo todas as organizações neste servidor MISP, todas as organizações em servidores MISP que são sincronizados com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que está a dois saltos de distância). Quaisquer outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância estão impedidas de exibir o evento. ◦ Todas as comunidades: compartilha o evento com todas as MISP comunidades, o que permite que o evento fique disponível gratuitamente.
Hiperlink para o evento MISP	Link para o evento MISP que está armazenado no servidor MISP.
Dados brutos	Detalhes brutos do registro de dados de aprimoramento do observável.
Comentário	Comentários que você adiciona aos atributos. Esses comentários são apenas para fins informativos e não são usados para correlação.
Marcadores (local)	Marcadores que estão disponíveis na instância MISP da organização host para habilitar a marcação para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa marcadores locais. Esses marcadores são sempre removidos antes de serem sincronizados com outras MISP instâncias e comunidades de compartilhamento.
Marcadores (global)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outras MISP instâncias e comunidades de compartilhamento. Ao adicionar marcadores globais a instâncias MISP, você modifica eventos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Galáxias (local)	Galáxias que estão disponíveis na instância MISP da organização host para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa galáxias locais. Essas galáxias são sempre eliminadas antes de serem sincronizadas com outras MISP instâncias e comunidades de compartilhamento.
Galáxias (global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras MISP instâncias e comunidades de compartilhamento. Quando você adiciona galáxias globais, os eventos MISP são modificados.

6. Para editar um marcador local ou global, clique no ícone de edição ícone de em uma das seguintes opções:

   - **Marcadores (local)**
   - **Marcadores (global)**

7. Na caixa de diálogo Marcadores de atributo do MISP, insira o nome do marcador para pesquisar e adicioná-lo.
8. Clique **em Atualizar marcadores para atributo MISP**.

   O exemplo a seguir mostra que, ao clicar no ícone de edição dos marcadores locais, você pode pesquisar e adicionar os marcadores C3, Adware, C2 e Botnet 3101 e atualizar o servidor MISP com os marcadores. A mensagem de confirmação mostra que todos os marcadores foram atualizados em MISP.

   Adicionar marcadores locais no atributo MISP.
   Os marcadores são atualizados com sucesso no servidor MISP.
9. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Adicionar ou remover galáxias de um evento ou atributo MISP

Adicione ou remova galáxias em MISP para que você possa classificar esses objetos como um cluster em MISP e anexá-los a eventos ou atributos MISP.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do servidor MISP correspondente.
- Observe que os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Clique no ícone de edição Ícone de em uma das seguintes opções.

- **Galáxias (local)**
- **Galáxias (global)**

2. Na caixa de diálogo Galáxias de eventos do MISP, preencha os detalhes.

Caixa de diálogo Galáxias de eventos do MISP

Campo	Descrição
ID de Evento	ID do evento atribuído pelo servidor MISP quando o evento foi criado ou importado pela primeira vez para MISP.
Namespace	Namespace onde a galáxia está armazenada. Você pode usar namespaces para agrupar galáxias semelhantes.
Galáxias	Galáxia em que você armazena as informações do cluster.
Clusters	Informações sobre os clusters na galáxia.

3. Clique **em Atualizar galáxias para atributo MISP**.
   O exemplo a seguir mostra que, ao clicar no ícone de edição das galáxias locais, você pode selecionar o namespace descontinuado, selecionar a galáxia Ataque empresarial - padrão de ataque e adicionar as informações do cluster. Depois que as informações da galáxia forem atualizadas, você poderá exibir a mensagem de sucesso.

   Como adicionar informações da galáxia no MISP por meio da Now Platform

4. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Resultados
As informações da galáxia foram atualizadas com sucesso no servidor MISP.

Adicionar comentários ao atributo MISP

Adicione comentários para os atributos MISP. Os comentários adicionados são apenas para fins informativos e não são usados para correlação de dados MISP.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Verifique se o atributo que você está editando pertence à mesma organização que o usuário MISP.
- Função necessária: sn_sec_misp.write

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Clique no ícone de edição Ícone de no campo Comentário.
2. Insira seu comentário no campo Comentário do atributo.
3. Clique **em Atualizar comentário para atributo MISP**.
   O exemplo a seguir mostra que, ao clicar no ícone de edição ao lado do campo de comentário, você pode adicionar um comentário e atualizar o atributo MISP. Depois que o comentário for atualizado, você poderá exibir a mensagem de sucesso.

   Adição de informações da galáxia no MISP por meio da Now Platform.

4. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Resultados
O comentário foi atualizado com sucesso no servidor MISP.

Como gerenciar eventos no MISP

Você pode criar eventos em MISP automaticamente ou manualmente a partir de Now Platform. Você também pode editar os dados do evento em MISP a partir de Now Platform.

Como verificar eventos criados automaticamente no MISP

Você pode verificar os eventos criados automaticamente depois de configurar o perfil de criação de eventos em sua instância Now Platform.

Perfil de criação automática de eventos

A configuração do perfil de criação automática de eventos é feita pelas funções de usuário sn_si.admin ou sn_ti.admin no **Integração MISP** > **Perfis automáticos de criação de evento** módulo.

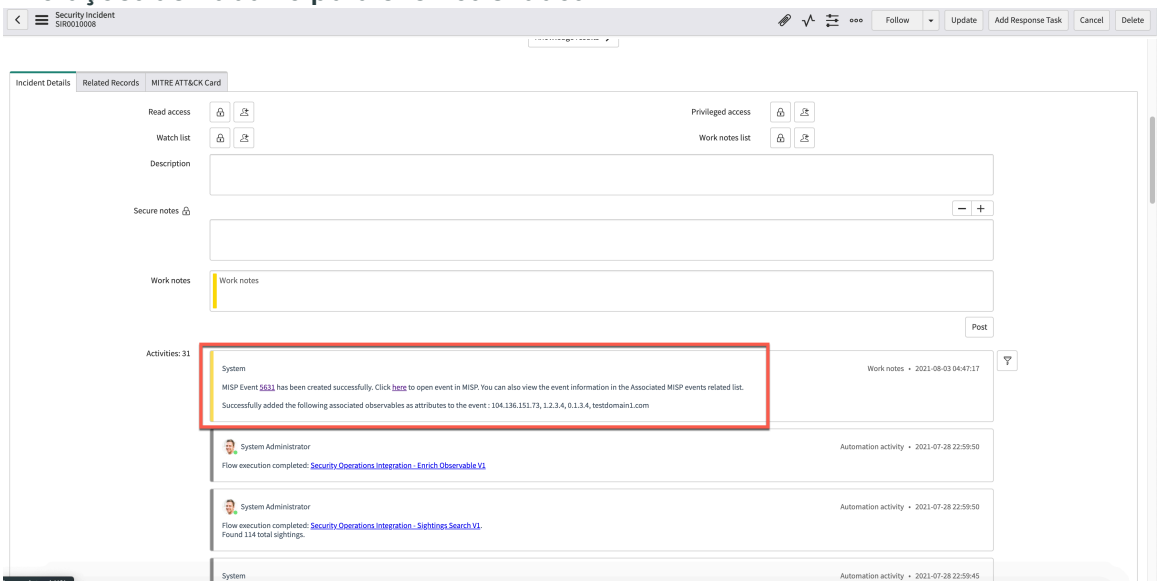
Exibição dos dados do evento MISP

Você pode exibir os eventos criados das seguintes maneiras:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

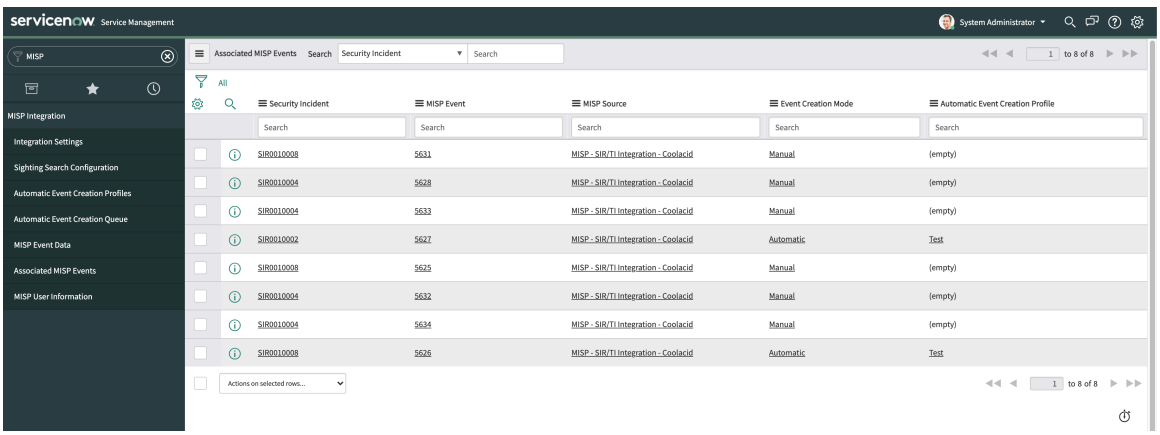
- Exiba as anotações de trabalho dos eventos criados. Você pode exibir os detalhes do evento na instância Now Platform e também como ele aparece no servidor MISP, conforme mostrado no exemplo a seguir.

Anotações de trabalho para eventos criados



- Clique na lista relacionada Eventos de MISP associados. Aqui, você pode exibir o evento em relação ao incidente de segurança e aos recursos MISP, conforme mostrado no exemplo a seguir.

Lista de eventos associados

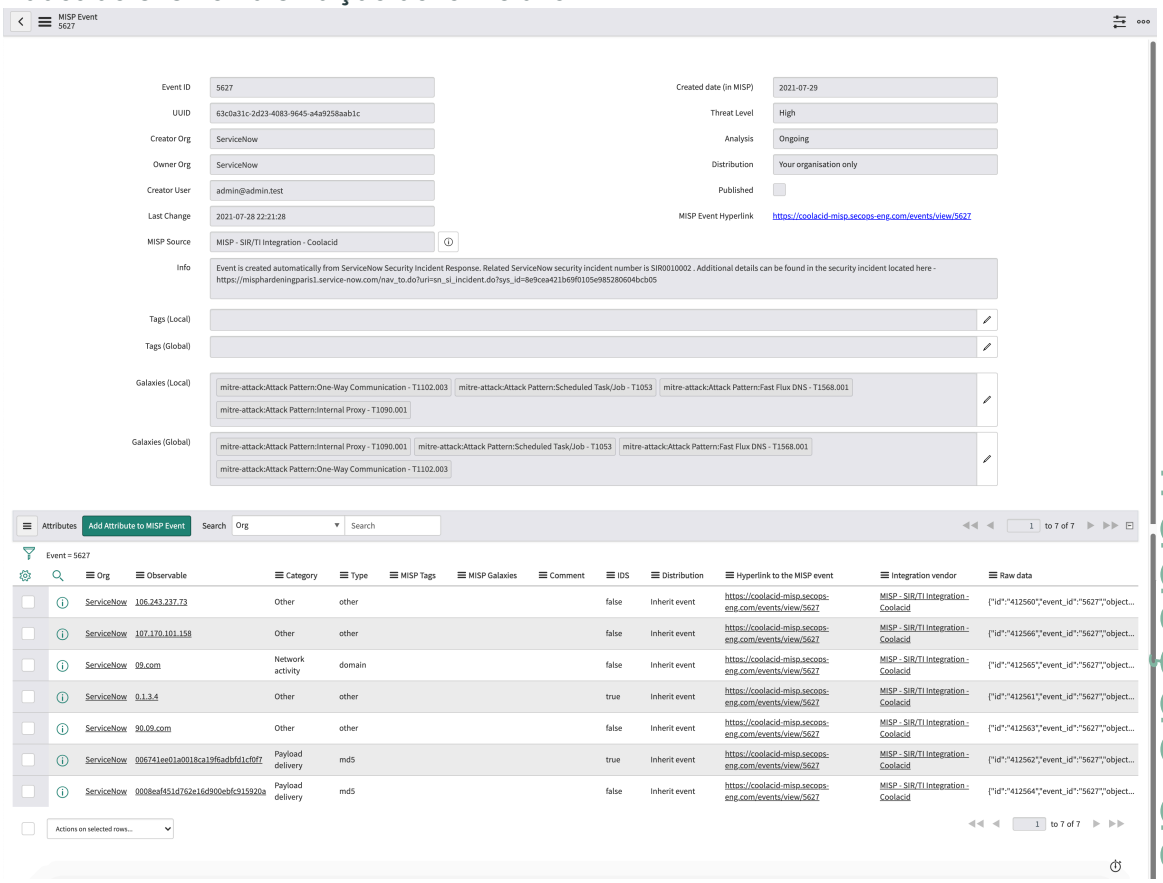


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Exiba os dados do evento MISP na exibição do formulário para revisar as informações detalhadas sobre os eventos MISP, conforme mostrado no exemplo a seguir.

Dados do evento na exibição do formulário



Criar manualmente um evento no MISP

Crie eventos manualmente em MISP a partir de Now Platform para capturar informações relacionadas ao contexto representadas como atributos e objetos.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja criar um evento.
3. Clique **em Criar um novo evento no MISP**.
4. Na caixa de diálogo Criar um novo evento no MISP, preencha os detalhes.

Criar um evento na caixa de diálogo do MISP

Campo	Descrição
Data	Data de criação do evento em MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Informações do evento	Informações de evento que são criadas automaticamente a partir de Now Platform Security Incident Response.
Nível de ameaça	Nível de risco do evento. Você pode categorizar os incidentes em três categorias de ameaça diferentes (baixa, média, alta). Este campo também pode ser deixado como indefinido. A seguir estão as opções: ◦ Baixo: malware geral em massa ◦ Médio: ameaças persistentes avançadas (APT) ◦ Alto: APTs sofisticados e ataques de dia 0
Origem	MISP origem para a criação do evento.
Distribuição	Opção que controla quem pode exibir este evento depois que o evento é publicado. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos. A configuração mais restritiva vence. As opções de distribuição são as seguintes: ◦ Somente sua organização: permite que somente os membros da sua organização exibam este evento. O evento pode ser extraído para outra instância por um dos membros da sua organização, onde somente a sua organização tem acesso para exibi-lo. Eventos com esta configuração não são sincronizados. ◦ Somente esta comunidade: permite

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo sua própria organização, organizações neste servidor MISP e organizações que executam servidores MISP que são sincronizados com este servidor. Quaisquer outras organizações conectadas a servidores vinculados estão impedidas de exibir o evento. ◦ Comunidades conectadas: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo todas as organizações neste servidor MISP, todas as organizações em servidores MISP que são sincronizados com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que está a dois saltos de distância. Quaisquer outras organizações conectadas aos servidores vinculados que estão a dois saltos deste servidor estão impedidas de exibir o evento. ◦ Todas as comunidades: compartilha o evento com todas as MISP comunidades.
Análise	Fase atual da análise do evento com as seguintes opções possíveis:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo		Descrição
		◦ Inicial: a análise está apenas começando ◦ Em andamento: a análise está em andamento ◦ Concluído: a análise está concluída
Opções avançadas	Adicionar observáveis associados do SIR como atributos ao evento MISP	Opção para adicionar observáveis disponíveis em um incidente de segurança a um evento MISP como atributos. Esta opção habilita o **sinalizador Definir atributo IDS quando a descoberta do observável for mal-intencionada**.
	Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada	Observável marcado como mal-intencionado em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
	Filtrar observáveis com base em marcadores de segurança	Opção para filtrar os observáveis com base nos marcadores de segurança selecionados. Esta opção fornece a capacidade de distinguir e gerenciar os eventos de MISP na inteligência contra ameaças. Marcadores de**segurança**: adicione marcadores para filtrar os observáveis. Por exemplo, se você estiver adicionando um marcador chamado "Bloquear contra compartilhamento" ou "TLP: branco", se um dos observáveis tiver algum desses marcadores associados, esses observáveis não serão adicionados como um atributo ao evento de MISP durante o MISP criação de eventos.
	Sincronizar técnicas de incidente de segurança do MITRE ATT&CK como	Opção para sincronizar as técnicas Now Platform SIR de incidente de segurança

Tradução automática

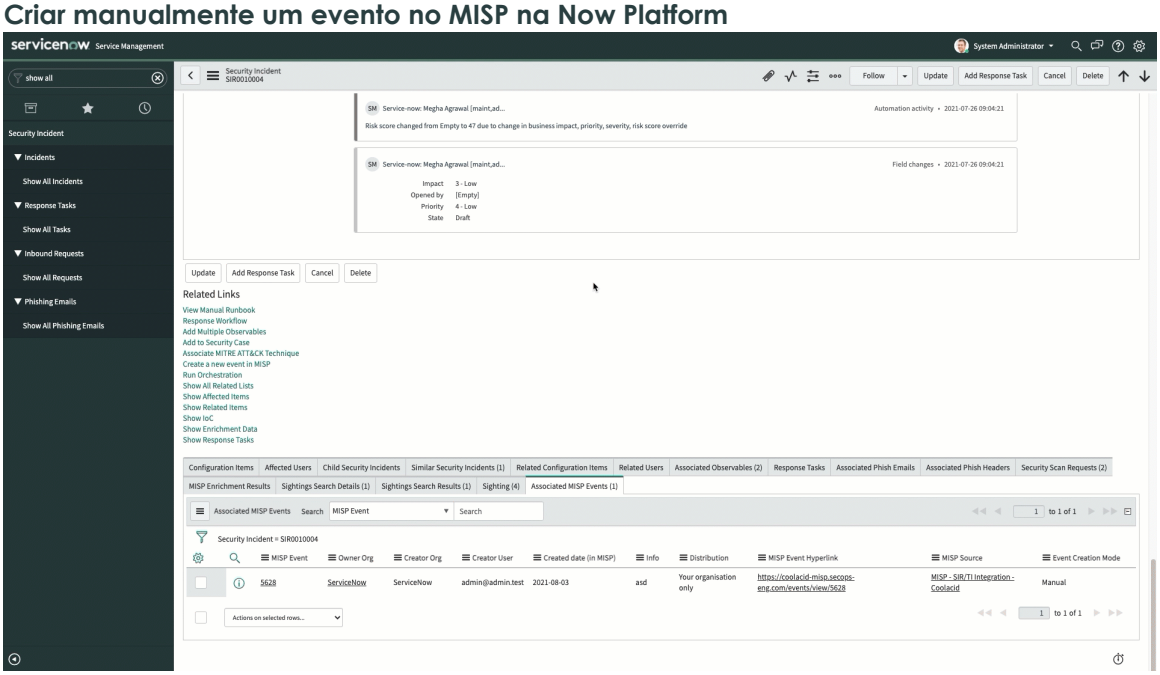
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo		Descrição
	galáxias locais para o evento de MISP	MITRE-ATT&CK™ como galáxias locais no evento MISP.
	Sincronizar técnicas de incidente de segurança MITRE ATT e CK como galáxias globais para evento MISP	Opção para sincronizar as técnicas Now Platform SIR de incidente de segurança MITRE-ATT&CK™ como galáxias globais no evento MISP.
	Adicionar marcadores ao evento MISP	Opção que permite adicionar marcadores de MISP aos eventos criados na ServiceNow. Esta opção exibe as seguintes opções: ◦ **Local (marcadores):** os marcadores selecionados serão adicionados como marcadores locais ao evento de MISP. ◦ **Global (marcadores):** os marcadores selecionados serão adicionados como marcadores globais ao evento de MISP.

5. Clique **em Criar novo evento MISP**.

   O exemplo a seguir mostra que, ao criar um evento em MISP, você pode exibir os resultados no incidente de segurança. Você também pode exibir as anotações de trabalho, o evento na instância Now Platform e o evento no servidor MISP, conforme mostrado no exemplo a seguir.

Criar manualmente um evento no MISP na Now Platform



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir os resultados das seguintes maneiras:

- Uma mensagem de sucesso aparece na parte superior da página do incidente de segurança. Você pode exibir os detalhes do evento na instância Now Platform e também como ele aparece no servidor MISP.
- Nas anotações de trabalho, você pode exibir a mensagem de sucesso com mais detalhes. Você também pode exibir os detalhes do evento na instância Now Platform e como ele aparece no servidor MISP.
- Na lista relacionada Eventos de MISP associados, você pode exibir o evento em relação ao incidente de segurança e aos recursos MISP.

Adicionar atributos a um evento MISP

Adicione atributos a um evento, como tipo, categoria e outras informações contextuais sobre o evento.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Verifique se o evento ao qual você está adicionando ou atualizando o atributo pertence à mesma organização que o usuário MISP.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **MISP** > **Eventos de MISP associados**.
   Você também pode navegar até a lista relacionada ao Evento de MISP associado em qualquer incidente de segurança.
2. Clique no evento MISP ao qual você deseja adicionar um atributo.
3. Clique **em Adicionar atributo ao evento de MISP**.
4. Na caixa de diálogo Adicionar atributo ao evento, preencha os detalhes.

Caixa de diálogo Adicionar atributo ao evento

Campo	Descrição
Valor	Valor real do atributo. Insira dados sobre o valor que se baseia no que é válido para o tipo de atributo escolhido. Por exemplo, para um atributo do tipo ip-src (endereço IP de origem), 11.11.11.11 é um valor válido. **Nota:** Você só pode selecionar atributos ou observáveis que compartilham contexto com o evento. Os observáveis ainda não podem ter um atributo em MISP.
Categoria	Categoria do atributo. A categoria descreve o aspecto do malware para este atributo. Um exemplo seriam os mecanismos de persistência do malware ou da atividade de rede.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo	Tipo que explica a categoria. Por exemplo, se um invasor usar um endereço IP para um ataque, um endereço de e-mail de origem ou um arquivo enviado por meio de um anexo poderá descrever a entrega de carga de um malware. Esses tipos de atributos têm a categoria de entrega de carga.
Distribuição	Usuários que podem exibir este atributo. A distribuição é herdada por atributos. A configuração mais restritiva vence.
Usar atributo como uma assinatura de IDS	Observável marcado como mal-intencionado em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
Comentários	Comentários que você adiciona aos atributos.

O exemplo a seguir mostra que, ao navegar na lista Eventos MISP associados, você pode exibir o registro de evento 5627 e adicionar atributos ao evento. Os atributos incluem o valor (testdomain.com), categoria como análise externa, tipo como domínio. Você também pode habilitar o IDS. A mensagem de sucesso no registro do evento mostra que o atributo foi adicionado ao evento, conforme mostrado no exemplo a seguir.

Adicionar atributo a um evento de MISP

5. Clique **em Adicionar atributo ao evento de MISP**.

Resultados

Você pode exibir o atributo adicionado na seção Atributos.

Adicionar marcadores a um evento MISP

Adicione marcadores em Now Platform MISP para classificar eventos ou atributos. Você pode usar a marcação globalmente para habilitar sua classificação ou usar marcadores

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

localmente quando não quiser que os eventos MISP sejam modificados durante a classificação.

Antes de Iniciar

- Revise MISP função e permissões do usuário para usar os MISP recursos bidirecionais.
- Verifique se o evento que você está editando pertence à mesma organização que o usuário MISP.
- Observe que os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que contém o evento ao qual você deseja adicionar marcadores.
3. Clique **em Mostrar todas as listas relacionadas** e na lista relacionada de Resultados de aprimoramento do MISP.
4. Clique no ID do evento na lista de resultados de aprimoramento.
   Você também pode navegar pelo **MISP** > **Eventos de MISP associados** módulo.
5. Revise o registro de eventos de MISP.

Exibição do formulário de eventos de MISP

Campo	Descrição
ID de Evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para o servidor MISP.
UUID	ID que identifica exclusivamente eventos e atributos.
Organização do criador	Organização que criou o evento na instância MISP.
Organização do proprietário	Organização proprietária do evento na instância MISP. Este campo está visível somente para os administradores.
Usuário do criador	Usuário que criou o evento em MISP.
Última mudança	Data em que o evento foi modificado pela última vez.
Origem do MISP	MISP origem em que o evento é criado.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez no servidor MISP.
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média e alta). Este campo pode ser deixado como indefinido. A seguir estão as opções:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Baixo: malware geral em massa ◦ Médio: ameaças persistentes avançadas (APT) ◦ Alto: APTs sofisticados e ataques de dia 0
Análise	Fase atual da análise do evento com as seguintes opções possíveis: ◦ Inicial: a análise está apenas começando ◦ Em andamento: a análise está em andamento ◦ Concluído: a análise está concluída
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Publicado	Status que indica se o evento foi publicado ou não. A publicação permite que os atributos do evento sejam usados para todas as exportações qualificadas e notifique os usuários que assinaram os alertas de evento.
Hiperlink de evento MISP	Link para o evento MISP que está armazenado no servidor MISP.
Informações	Descrição resumida do evento.
Marcadores (local)	Marcadores que estão disponíveis na instância MISP da organização host para habilitar a marcação para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa marcadores locais. Os marcadores locais são sempre removidos antes de serem sincronizados com outras MISP instâncias e comunidades de compartilhamento.
Marcadores (global)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outras MISP instâncias e comunidades de compartilhamento. Ao adicionar marcadores globais a instâncias MISP, você pode modificar eventos.
Galáxias (local)	Galáxias que estão disponíveis na instância MISP da organização host para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa galáxias locais. Essas galáxias locais são sempre eliminadas antes de serem sincronizadas com outras MISP instâncias e comunidades de compartilhamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Galáxias (global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras MISP instâncias e comunidades de compartilhamento. Ao adicionar galáxias globais, MISP, você pode modificar eventos.

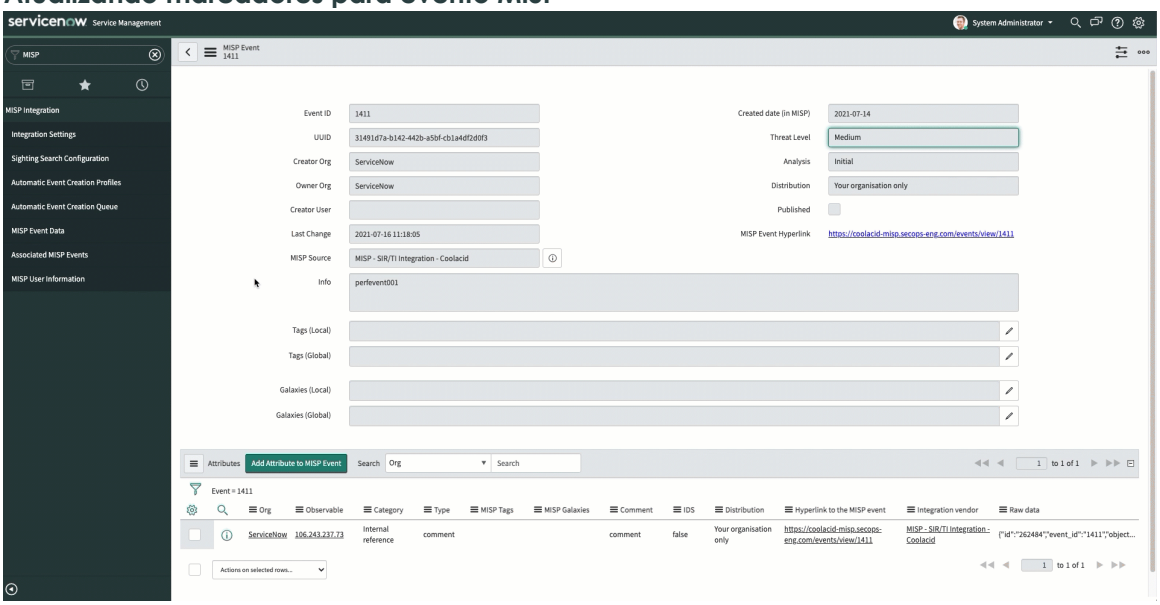
6. Para editar um marcador local ou global, clique no ícone de edição ícone de em uma das seguintes opções:

- **Marcadores (local)**
- **Marcadores (global)**

7. Na caixa de diálogo Marcadores de evento do MISP, insira o nome do marcador para pesquisar e adicionar os marcadores.
8. Clique **em Atualizar marcadores para evento MISP**.

   O exemplo a seguir mostra que, ao clicar no ícone de edição dos marcadores locais, você pode pesquisar e adicionar os marcadores C3, Adware, C2 e Botnet 3101 e atualizar o servidor MISP com os marcadores. A mensagem de confirmação mostra que todos os marcadores foram atualizados em MISP.

Atualizando marcadores para evento MISP



9. Clique em **Recarregar formulário** na mensagem de sucesso para exibir as mudanças no registro.

Resultados

Os marcadores foram atualizados com sucesso no servidor MISP.

Atualizar galáxias para um evento ou atributo MISP

Adicione ou remova galáxias em Now Platform MISP para que você possa classificar esses objetos como um cluster na instância MISP e anexá-los a eventos ou atributos MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Revise MISP função e permissões do usuário necessário para usar os MISP recursos bidirecionais.
- Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do servidor MISP correspondente.
- Os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

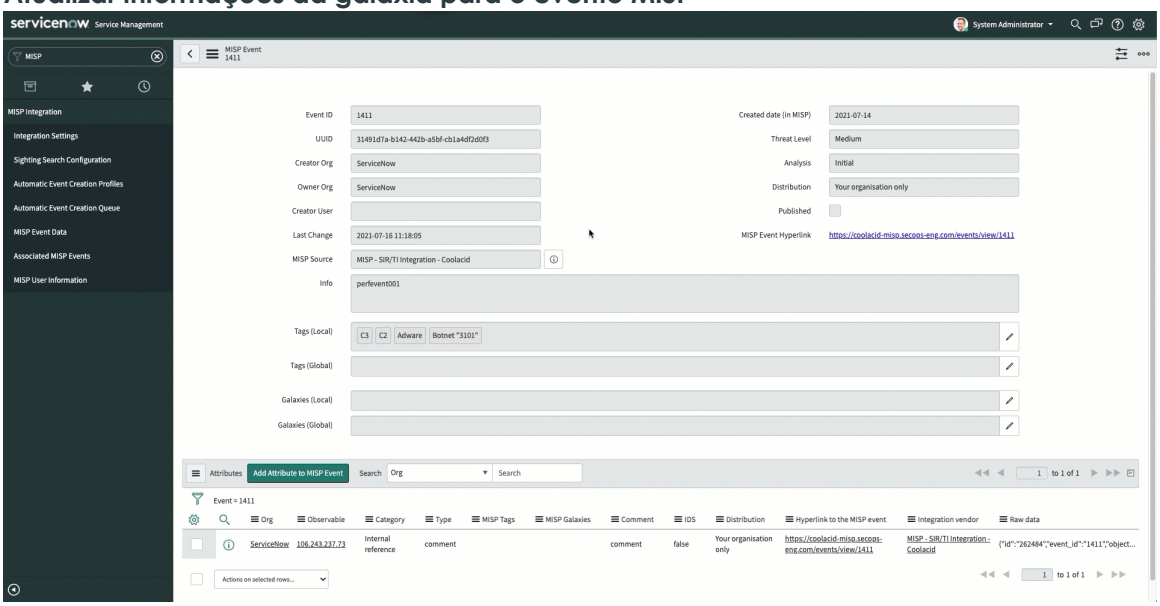
1. Clique no ícone de edição Ícone de em uma das seguintes opções.

- **Galáxias (local)**
- **Galáxias (global)**

2. Na caixa de diálogo Galáxias de eventos do MISP, digite e pesquise para adicionar os marcadores.
3. Clique **em Atualizar galáxias para evento de MISP**.

   O exemplo a seguir mostra como clicar no ícone de edição das galáxias locais, selecionar o namespace descontinuado, selecionar a galáxia Ataque empresarial - padrão de ataque e adicionar informações do cluster. Depois que as informações da galáxia forem atualizadas, você poderá exibir a mensagem de sucesso.

Atualizar informações da galáxia para o evento MISP



   As galáxias foram atualizadas com sucesso no servidor MISP.

4. Clique em **Recarregar formulário** na mensagem de sucesso para exibir as mudanças no registro.

Acumular MITRE-ATT&CK informações usando MISP resultados de enriquecimento

Acumule os resultados de aprimoramento do MISP manualmente se você não tiver habilitado o acúmulo automático de MISP informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

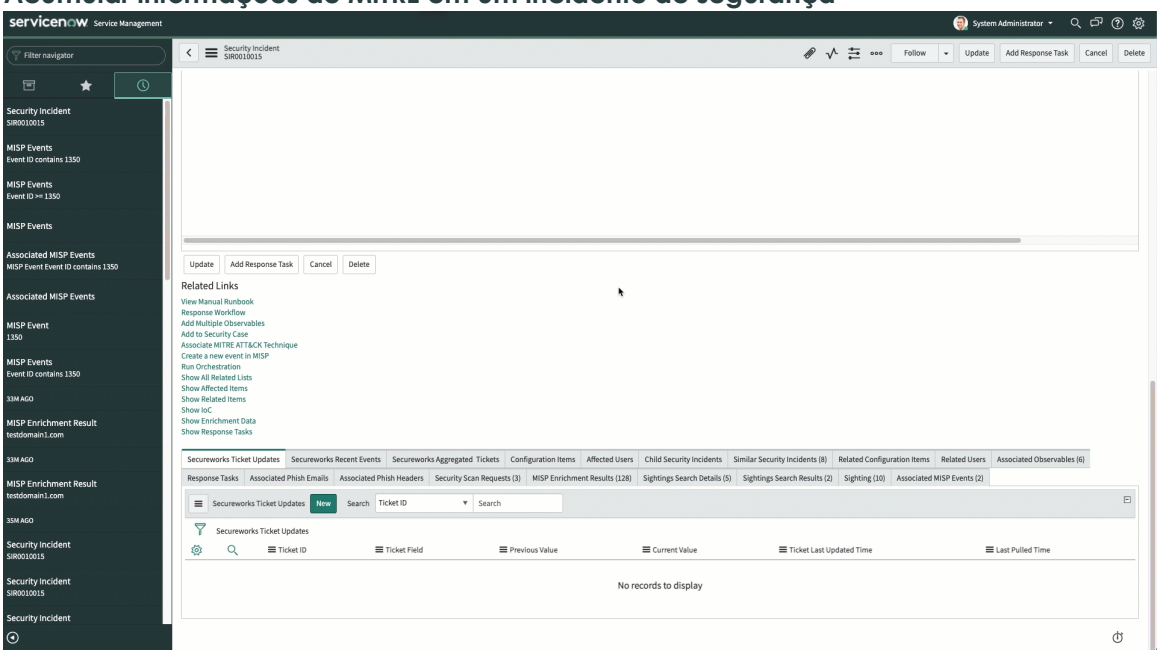
Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Use as regras de extração automática do sistema de base para importar as informações MITRE-ATT&CKMISP da integração []. O MISP integration for Security Operations apresenta duas regras de extração da técnica do sistema base MITRE-ATT&CK para galáxias MISP - MISP e marcadores MISP. Para obter mais informações sobre regras de extração automática em MITRE-ATT&CK, consulte regras de técnica de extração automática para importar informações do MITRE-ATT&CK.

Se você tiver habilitado acúmulo automático de MITRE-ATT&CK informações usando MISP resultados de aprimoramento a um incidente de segurança, as informações são acumuladas automaticamente. Se você não habilitou o acúmulo automático, poderá fazer essa tarefa manualmente.

Procedimento
1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar todos os incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Resultados de aprimoramento do MISP**.
4. Selecione o observável e, no menu Ações, clique em **Acumular informações do MITRE ATT&CK no SI**.
   Você pode selecionar vários observáveis e acumular as informações.
5. Para confirmar as mudanças, clique em **Recarregar**.
   O exemplo a seguir mostra como selecionar um observável e acumular os resultados de enriquecimento MISP para o incidente de segurança.

Acumular informações de MITRE em um incidente de segurança



Resultados
Você pode exibir o cartão MITRE-ATT&CK para confirmar que os resultados de aprimoramento do MISP foram acumulados para o incidente de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração do OPSWAT Metadefender

OPSWAT Metadefender permite que os dados de ameaças, detectados pelo scanner Metadefender de terceiros, sejam baixados para a aplicação Inteligência contra ameaças para acompanhamento, priorização e resolução.

Explorar • OPSWAT Metadefender visão geral da integração • Integrações do Inteligência contra ameaças	Configuração Ativar e configurar a integração OPSWAT Metadefender
Usar Executar pesquisas em observáveis	Desenvolver • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

OPSWAT Metadefender visão geral da integração

OPSWAT Metadefender é uma solução de segurança que fornece acesso a várias máquinas antimalware e se integra facilmente a Operações de segurança.

Antes de poder usar a integração OPSWAT Metadefender, você deve ativar o plug-in e configurar a integração. Se necessário, você também pode atualizar sua certificação SSL X509.

Pesquisa de ameaças - OPSWAT Metadefender flow

O fluxo Pesquisa de ameaças - OPSWAT Metadefender realiza uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo OPSWAT Metadefender, eles serão verificados quanto a malware e os resultados serão retornados.

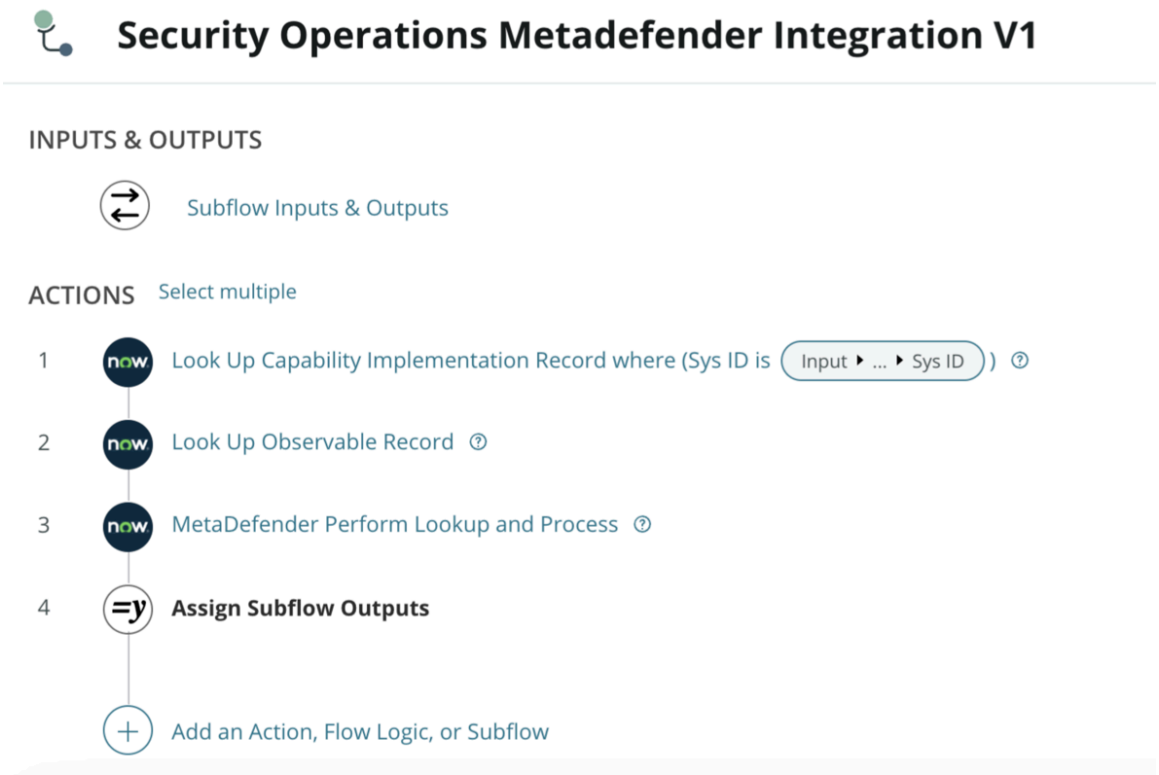
Este fluxo é acionado pelo Integração de Operações de segurança - Capacidade de pesquisa de ameaças quando você executa uma pesquisa de ameaças em um ou mais observáveis e a implementação do OPSWAT Metadefender é selecionada. Para obter mais informações, consulte Executar pesquisas em observáveis.

Função necessária: sn_si.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - OPSWAT Metadefender flow



Para obter informações sobre as atividades usadas por este fluxo, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Ativar e configurar a integração OPSWAT Metadefender

Antes de poder usar a integração OPSWAT Metadefender, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a integração estiver concluída, acesse o portal OPSWAT e obtenha a chave de API do Metadefender Cloud
3. Em sua instância, navegue até **Operações de segurança** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão do OPSWAT Metadefender, clique em **Configurar**.
5. Insira (ou cole) a **chave de API** que você adquiriu no portal do OPSWAT.
6. Clique em **Enviar**.

Resultados

Depois de configurado, o OPSWAT Metadefender pode ser selecionado para realizar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Informações relacionadas

Executar pesquisas em observáveis

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizar seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor de terceiros ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira a URL do endpoint na barra de endereço do navegador.
   Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM no sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou na área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

   Nota: Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Como substituir um certificado SAML expirando .

Integração do VirusTotal

A integração VirusTotal permite que você solicite a análise de endereços IP, arquivos, hashes de arquivo e endereços URL suspeitos para ajudar em sua investigação para determinar se eles são mal-intencionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar Integrações do Inteligência contra ameaças	Configurar • VirusTotal configuração de integração • Ativar e configurar a integração VirusTotal
Usar • Executar pesquisas em observáveis • Pesquisa de ameaças - Fluxo de trabalho VirusTotal	Desenvolver • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança • Pesquisar artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

VirusTotal configuração de integração

VirusTotal é um serviço gratuito que analisa arquivos e URLs suspeitos e facilita a detecção rápida de vírus, worms, trojans e todos os tipos de malware. Ele se integra facilmente com Operações de segurança.

Antes de poder usar a integração VirusTotal, você deve ativar o plug-in e adicionar a chave de API apropriada. Se necessário, você também pode atualizar sua certificação SSL X509.

Se a origem de pesquisa VirusTotal for usada e o malware for encontrado, um observável será criado. Para pesquisas de IP, uma lista adicional de URLs que compartilham o endereço IP é criada e os observáveis são criados para cada uma das URLs.

Nota:

- O plug-in Inteligência contra ameaças é necessário para implementar a integração VirusTotal.
- A integração VirusTotal foi atualizada para as APIs da versão 3.

Ativar e configurar a integração VirusTotal

Antes de poder usar a integração VirusTotal, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Inteligência contra ameaças deve ser instalado e ativado para que você possa usar o VirusTotal. A integração VirusTotal foi atualizada para as APIs da versão 3.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse o VirusTotal e obtenha a chave de API no seu perfil do VirusTotal.
3. Em sua instância, navegue até **Operações de segurança** > **Configuração de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão VirusTotal, clique em **Configurar**.

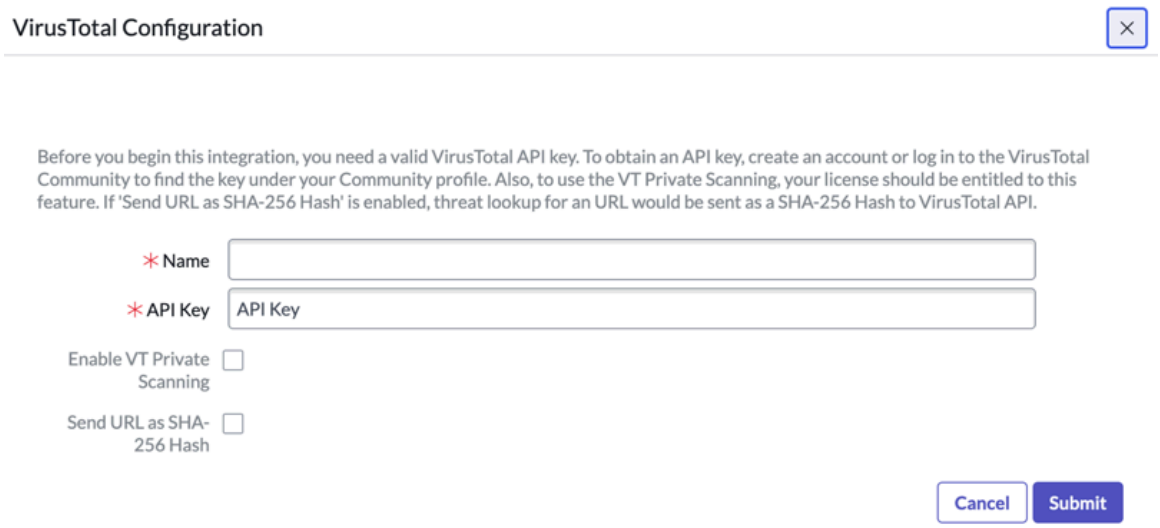
Configuração de VirusTotal

Campo	Descrição
Nome	Nome da integração. Por exemplo, VirusTotal.
Chave de API	Insira (ou cole) a **chave de API** que você adquiriu no site VirusTotal.
Habilitar verificação privada de VT	Marque esta caixa de seleção para analisar arquivos com VirusTotal preservando a privacidade. Os arquivos carregados por meio desta oferta não serão compartilhados com ninguém além da sua organização e permanecerão no VirusTotal por apenas um breve período. As análises resultantes também serão efêmeras e visíveis somente para o seu grupo VirusTotal. **Importante:** Para usar a verificação privada de VT, sua licença do VirusTotal deve estar qualificada para este recurso.
Enviar URL como hash SHA-256	Marque esta caixa de seleção para enviar os URLs como hashes para pesquisa de ameaças e proteger a privacidade dos usuários na integração. **Nota:** Se desabilitado, o URL será enviado como codificação Base64 para a API VirusTotal.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.



Resultados
Depois de configurado, o VirusTotal pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Informações relacionadas

Executar pesquisas em observáveis

Pesquisa de ameaças - Fluxo de trabalho VirusTotal

O fluxo de trabalho Pesquisa de ameaças - VirusTotal executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por VirusTotal, eles serão verificados quanto a malware e os resultados serão retornados.

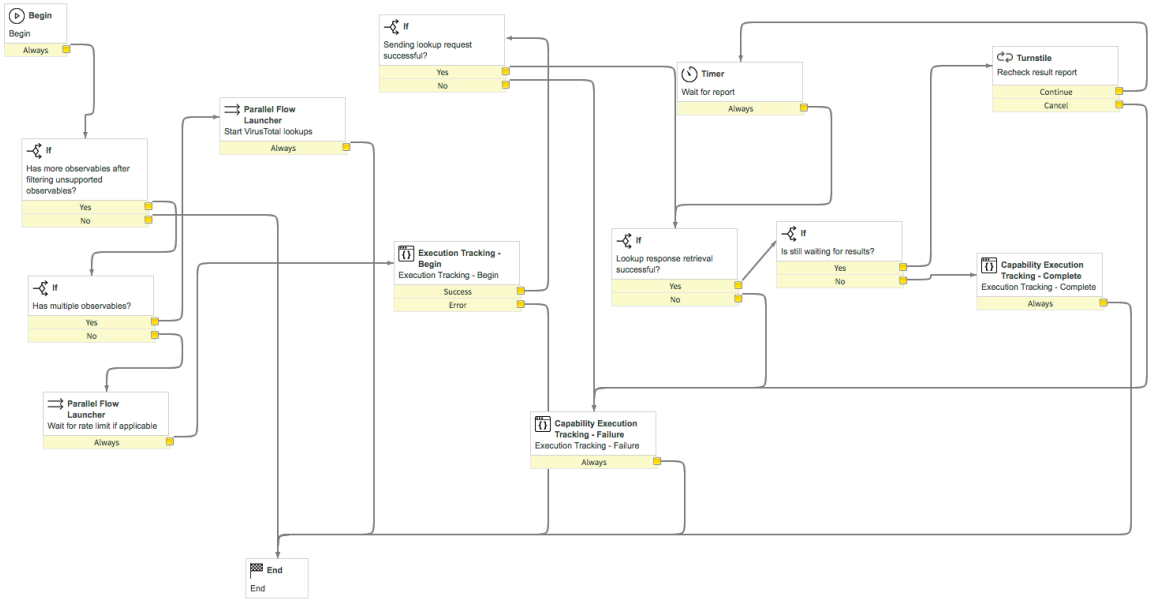
Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pelo Integração de Operações de segurança - Capacidade de pesquisa de ameaças quando você executa uma pesquisa de ameaças em um ou mais observáveis e a implementação VirusTotal é selecionada. Para obter mais informações, consulte Executar pesquisas em observáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - Fluxo de trabalho VirusTotal



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Integração da API WhoisXML

A integração da API WhoisXML permite que você envie pesquisas Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para determinar melhor as ameaças.

Explorar Integrações do Inteligência contra ameaças	Configurar • Configuração da integração da API WhoisXML • Ativar e configurar a integração Whois das Operações de segurança
Usar Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC	Desenvolver • ServiceNow Operações de segurança diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Fazer ou responder a perguntas na comunidade das Operações de segurança	

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configuração da integração da API WhoisXML

Antes de poder usar a integração Whois, você deve ativar o plug-in e adicionar as credenciais. Se necessário, você também pode atualizar sua certificação SSL X509.

Os plug-ins Inteligência contra ameaças e WhoisXML API Integration são necessários para implementar a integração da API WhoisXML.

Ativar e configurar a integração Whois das Operações de segurança

O recurso Configuração de integração permite ativar e configurar rapidamente integrações de segurança de terceiros, incluindo a integração Whois das Operações de segurança. Antes de poder usar a integração Whois das Operações de segurança, você deve baixá-la do ServiceNow Storee deve ter uma conta válida da API WhoisXML.

Antes de Iniciar

Inteligência contra ameaças O deve ser instalado e ativado para que você possa usar a integração Whois das Operações de segurança.

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão da API Whois, clique em **Configurar**.
4. Insira o nome de usuário e a senha da sua conta da API WhoisXML.
5. Clique em **Enviar**.

Atualizar seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor de terceiros ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira a URL do endpoint na barra de endereço do navegador.
      Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique em **Mais informações** e na guia **Segurança**.

d. Clique em **Exibir certificado** e na guia **Detalhe**.

e. Clique em **Exportar** para salvar o PEM no sistema de arquivos local.

f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou na área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
Os outros campos no registro são gerados automaticamente.

Nota: Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Como substituir um certificado SAML expirando .

Aprimorar fluxo de trabalho WhoIs do observável

O fluxo de trabalho **Enriquecer observável WhoIs** executa o enriquecimento em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo WhoisXML API Integration, os observáveis serão aprimorados.

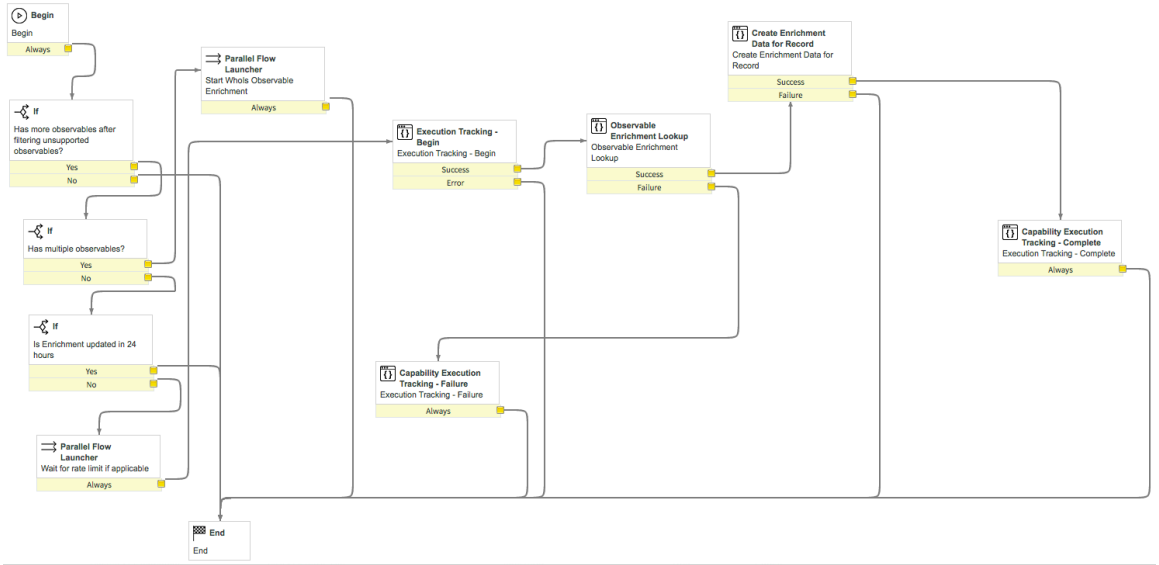
Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pelo Integração de Operações de segurança - Capacidade de aprimorar observável quando você executa o aprimoramento em um ou mais observáveis e a implementação de WhoIs está selecionada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprimorar fluxo de trabalho WhoIs do observável



As atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade de pesquisa de aprimoramento de observável

A atividade de fluxo de trabalho **Pesquisa de aprimoramento de observável** inicia o processo de aprimoramento de observável.

A atividade **Pesquisa de aprimoramento de observável** pode ser usada com qualquer fluxo de trabalho de observáveis para iniciar o aprimoramento.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	A pesquisa foi bem-sucedida.
Falha	Ocorreu um erro ao tentar executar a pesquisa. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
Id_implementação	Identificador do sistema da implementação usada para executar a pesquisa.
domain_id	O identificador do domínio no qual a pesquisa está sendo realizada.
observáveis_ids	Um ou mais observáveis para executar a ação desejada. Os IDs são usados como uma entrada de fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
capabilityExcutionId	Identificador do sistema da capacidade que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch.
task_sys_id	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta_dados	Dados brutos retornados pelo endpoint da API da implementação para o domínio fornecido.
mapping_id	O identificador do mapeamento de aprimoramento. Por exemplo, a integração WhoIs retorna dados em dois formatos diferentes, IP e URL, com um ID de mapeamento para cada um.

Orquestração de inteligência contra ameaças

Orquestração de inteligência contra ameaças As atividades permitem que os usuários determinem se uma ameaça foi vista antes em outros incidentes de segurança ou em outros sistemas usando a orquestração de fluxo de trabalho.

Para obter mais informações sobre como editar Orquestração do Security Incident Response fluxos de trabalho ou criar fluxos de trabalho personalizados, consulte Introdução a fluxos de trabalho e Editor de fluxo de trabalho Editor de fluxo de trabalho .

Configurar Orquestração de inteligência contra ameaças

Antes de usar Orquestração de inteligência contra ameaças, execute as etapas para configurar várias partes do sistema, incluindo o preenchimento do CMDB, a configuração do MID Server e a configuração de credenciais.

Antes de Iniciar

Função necessária: administrador
Para usar Orquestração de inteligência contra ameaças, você precisa de um CMDB totalmente preenchido com nomes de domínio. Para obter mais informações, consulte Descoberta .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Ativar o plug-in Inteligência contra ameaças.
2. Configurar o MID Server
3. Configurar credenciais de serviço do MID Server
   Agora você está pronto para usar Orquestração de inteligência contra ameaças atividades em um fluxo de trabalho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxos de trabalho e atividades da Orquestração de inteligência contra ameaças

O sistema base inclui fluxos de trabalho e atividades de fluxo de trabalho que você pode usar para automatizar ações em sua instância.

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC

O fluxo de trabalho **Inteligência contra ameaças - Executar pesquisa de IoC** verifica se há um observável não expirado e, em caso afirmativo, a pesquisa é definida como **Concluída** e atualizada com os dados do observável.

Antes de Iniciar

Função necessária: sn_si.basic

Nota: Este fluxo de trabalho substitui Orquestração de inteligência contra ameaças regras de negócio (**Preencher com tabelas IoC existentes**, **Enfileirar a pesquisa**e **Atualizar observável**) por atividades.

Se uma pesquisa for inserida ou atualizada e atender às condições, a regra de negócio Pesquisar acionará este fluxo de trabalho.

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Inteligência contra ameaças - Executar pesquisa de IoC** verifica se há um observável não expirado e, em caso afirmativo, a pesquisa é definida como **Concluída** e atualizada com os dados do observável. Todos os indicadores associados ao observável são reativados.

Se o observável estiver expirado, o fluxo de trabalho executará as pesquisas e incrementará a **contagem de detecções** no observável expirado existente.

Se não existir nenhum observável correlacionado, um novo observável com o indicador será criado.

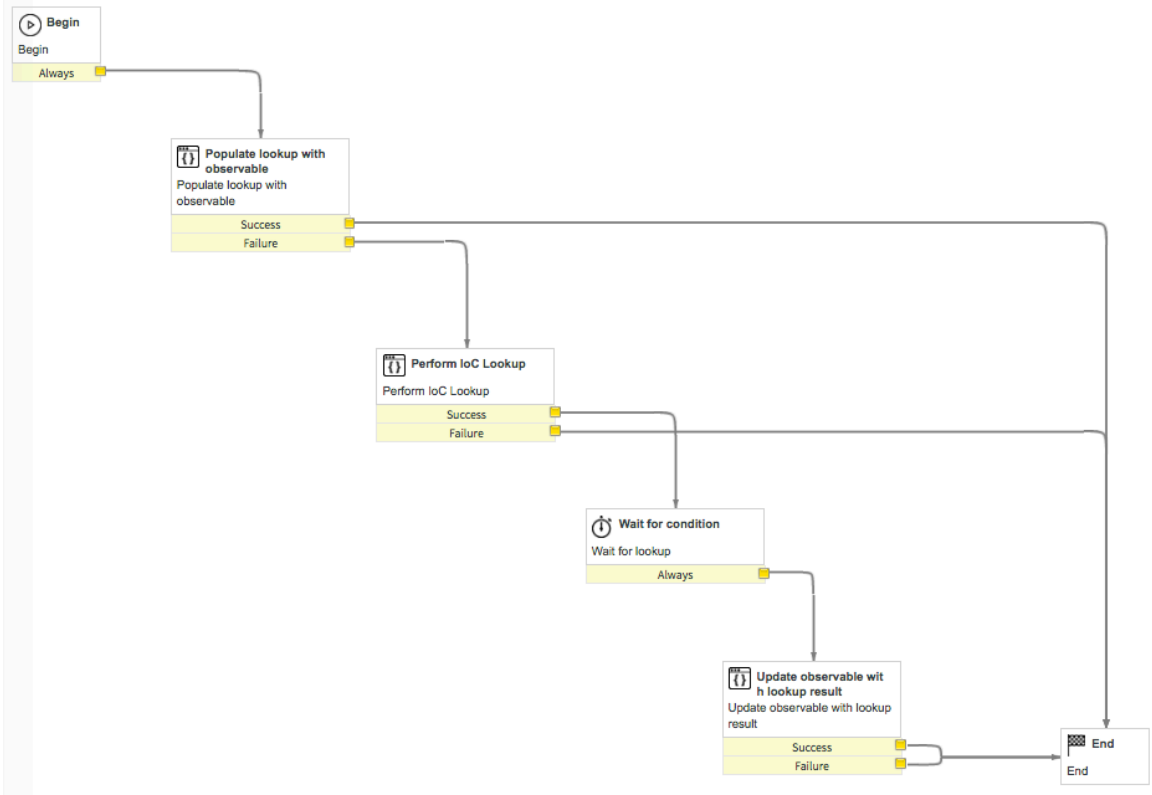
As atividades do processo de fluxo de trabalho incluem:

- Preencher pesquisa com atividade de observável
- Executar atividade de pesquisa de IoC
- Aguardar pesquisa (atividade principal)
- Atualizar observável com atividade de resultado de pesquisa

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC



Preencher pesquisa com atividade de observável

Se um observável não expirado for encontrado, a atividade de fluxo de trabalho **Orquestração de inteligência contra ameaças - Preencher pesquisa com observável** fornecerá dados de um observável existente para uma pesquisa. Esta atividade pode acelerar o processo de investigação e correção.

Quando acionado por um fluxo de trabalho, a **pesquisa Preencher com observável** tenta encontrar um observável existente para uma pesquisa que corresponda ao **valor** e ao **tipo** da pesquisa fornecida para a atividade como entrada.

Se o observável existir e não estiver expirado, esta atividade:

- Atualiza a pesquisa com as informações encontradas no observável
- Reativa um indicador se ele estiver inativo, incrementa a **contagem**de itens encontrados e atualiza a data de **visto pela última vez**
- Define **o estado** como Concluído.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável de entrada	Descrição
scanID[cadeia de caracteres]	identificador de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída	Descrição
Verdadeiro	Observável válido encontrado e pesquisa atualizada.
Falso	Não foi encontrado um observável válido. O observável está ausente ou expirou.

Executar atividade de pesquisa de IoC

A atividade de fluxo de trabalho **Orquestração de inteligência contra ameaças - Executar pesquisa de IoC** executa uma determinada pesquisa. Esta atividade pode acelerar o processo de investigação e correção.

Quando acionado por um fluxo de trabalho, **Executar pesquisa de IoC** usa um scanID, pesquisa o registro de pesquisa e adiciona a pesquisa à fila criando uma entrada de fila de pesquisa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
scanID[cadeia de caracteres]	identificador de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Verdadeiro	A pesquisa foi acionada.
Falso	Não acionou a pesquisa.

Atualizar observável com atividade de resultado de pesquisa

A atividade de fluxo de trabalho **Orquestração de inteligência contra ameaças - Atualizar observável com resultado de pesquisa** atualiza o registro do observável. Se não existir, ele criará um novo observável. Esta atividade é útil para registrar informações.

Quando acionado por um fluxo de trabalho, **Atualizar observável com resultado de pesquisa** atualiza um observável existente para incluir a nova **Contagem de detecções**, adiciona uma anotação e, se inativo, reativa todos os indicadores. A **contagem de Encontrados** e a Data da **última visita** no indicador também são atualizadas.

Se não houver nenhum observável correlacionado, o fluxo de trabalho criará um novo observável com o indicador da seguinte forma:

- Executa as pesquisas de IoC
- Cria um novo observável
- Cria um indicador para o observável

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adiciona uma **contagem de detecções** ao observável
- Adiciona uma **contagem de encontrados** e a data da **última visita** ao indicador
- Adiciona uma mensagem indicando de qual pesquisa ela foi criada

.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
scanID[cadeia de caracteres]	Identificador de pesquisa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Verdadeiro	A atualização ou criação do observável foi bem-sucedida.
Falso	Falha na atualização ou criação do observável.

Atividade Executar pesquisa de origens de IoC padrão

Quando acionado por um fluxo de trabalho, Inteligência contra ameaças - **Executar origens de pesquisa de IoC padrão** usa um ID de solicitação de pesquisa e cria várias pesquisas, dependendo dos valores de dados inseridos.

Para cada tipo de dados, a coluna de **verificação include_in_bulk** da tabela de tipo de pesquisa compatível de cada origem de pesquisa é avaliada. Se verdadeiro, uma pesquisa será adicionada à solicitação de pesquisa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
scan_request_id	Identificador do sistema de solicitação de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
Número de verificações criadas	Inteiro

Security Case Management

Gestão de casos de segurança fornece um meio para os analistas de segurança que estão envolvidos na caça de ameaças coletarem informações sobre atividades suspeitas em seu ambiente. Registros relacionados a casos, como incidentes de segurança, observáveis, ICs e usuários afetados, podem ser adicionados a casos para acomodar análises amplas e específicas.

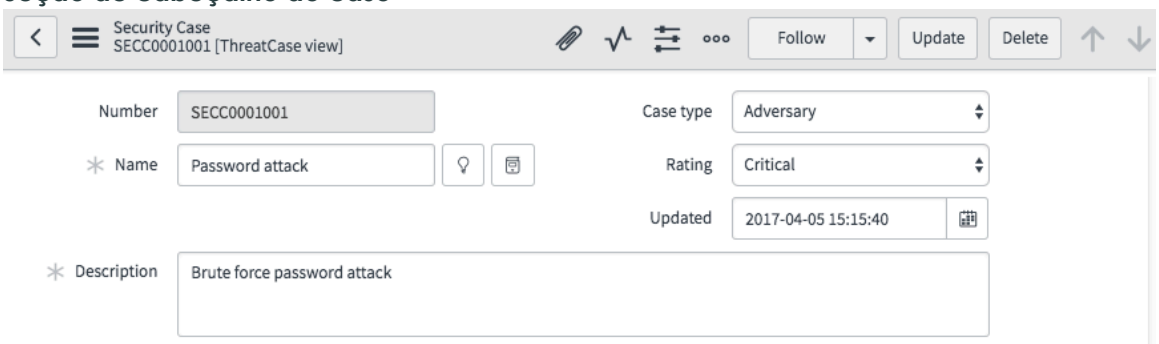
Com a capacidade de alternar facilmente os registros e as informações relacionadas, os analistas podem avaliar se estão enfrentando uma campanha direcionada, uma ameaça persistente avançada e assim por diante.

Os casos de segurança podem ser criados de várias origens em sua instância, incluindo Gestão de casos de segurança, Security Incident Responsee Inteligência contra ameaças. Você também pode criar casos a partir de itens de configuração e usuários afetados nas tabelas Itens de configuração [cmdb.ci] e Usuários [sys.user], respectivamente. Depois que os casos foram criados, cada uma dessas origens também pode ser usada para adicionar recursos de análise valiosos aos casos existentes.

Cada caso de segurança consiste em três seções principais, uma seção de cabeçalho, uma seção com detalhes adicionais do caso e uma seção de artefatos de caso que contém uma coleção de registros que ajudam a criar um argumento para identificar e lidar com ameaças específicas.

Cabeçalho do caso

Seção de cabeçalho do caso



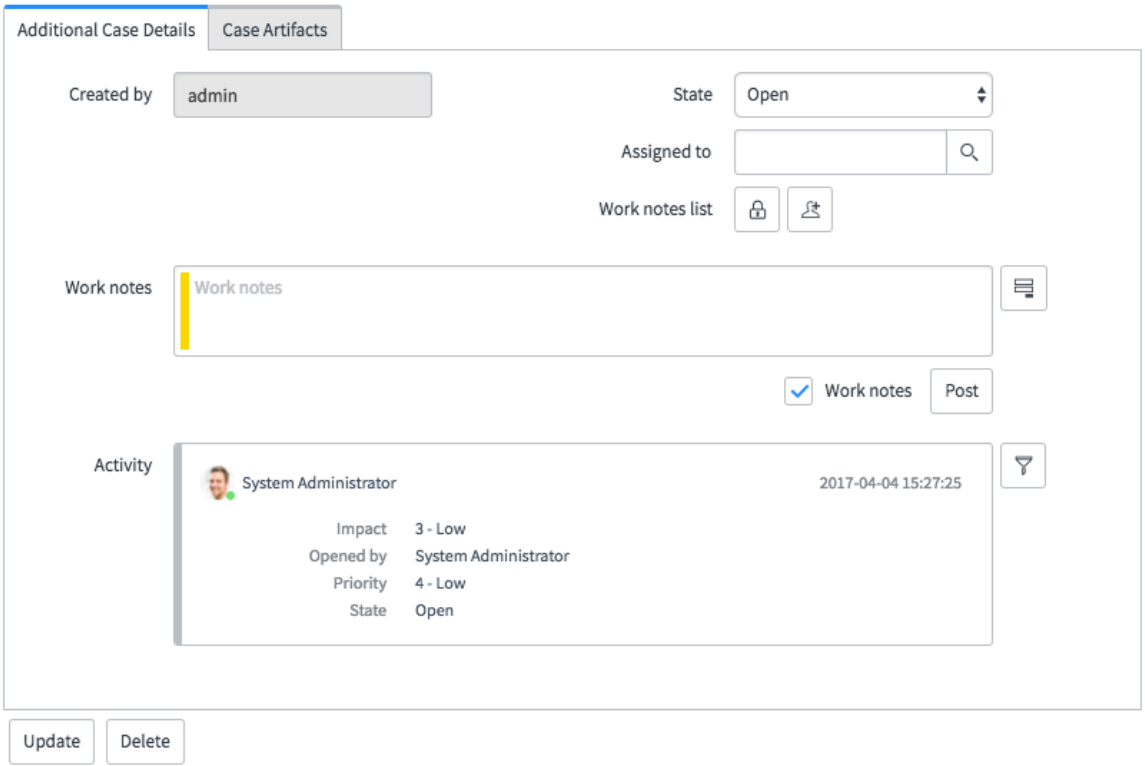
O cabeçalho do caso fornece informações básicas usadas para identificar e classificar o caso de segurança. O número do caso usa o prefixo SECC.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes adicionais do caso

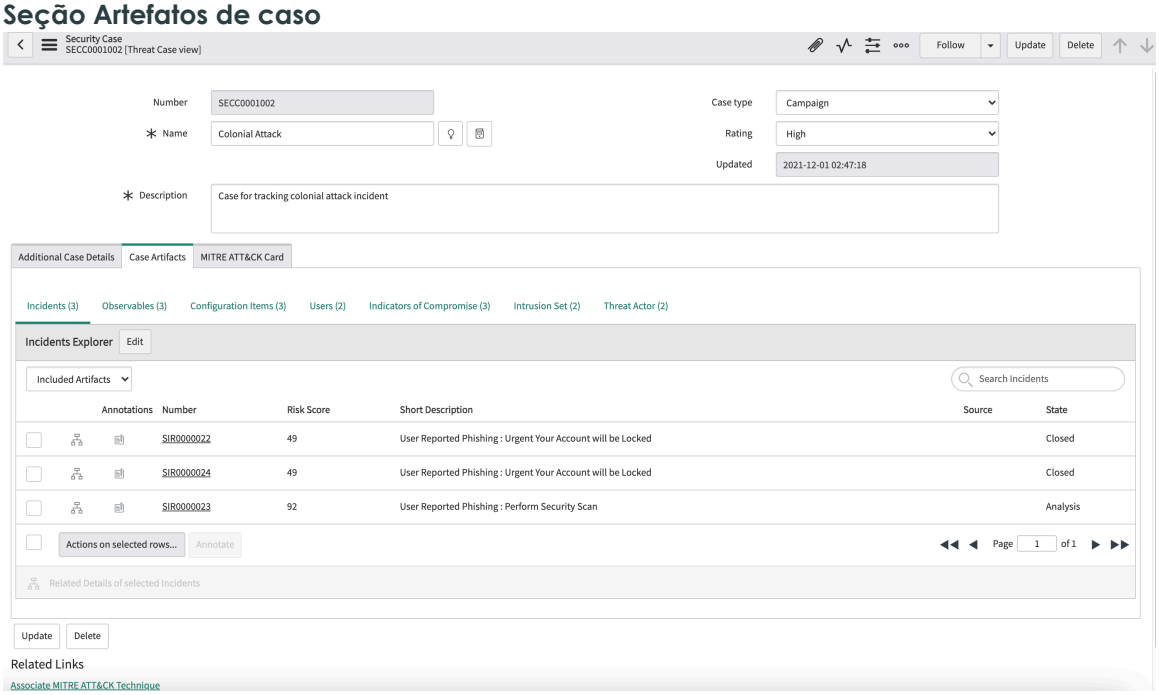
Seção Detalhes adicionais do caso



A seção **Detalhes adicionais do caso** fornece informações específicas para a análise que já foi realizada no caso, incluindo seu estado atual e anotações de trabalho e atividades registradas para o caso.

Artefatos de caso

Seção Artefatos de caso



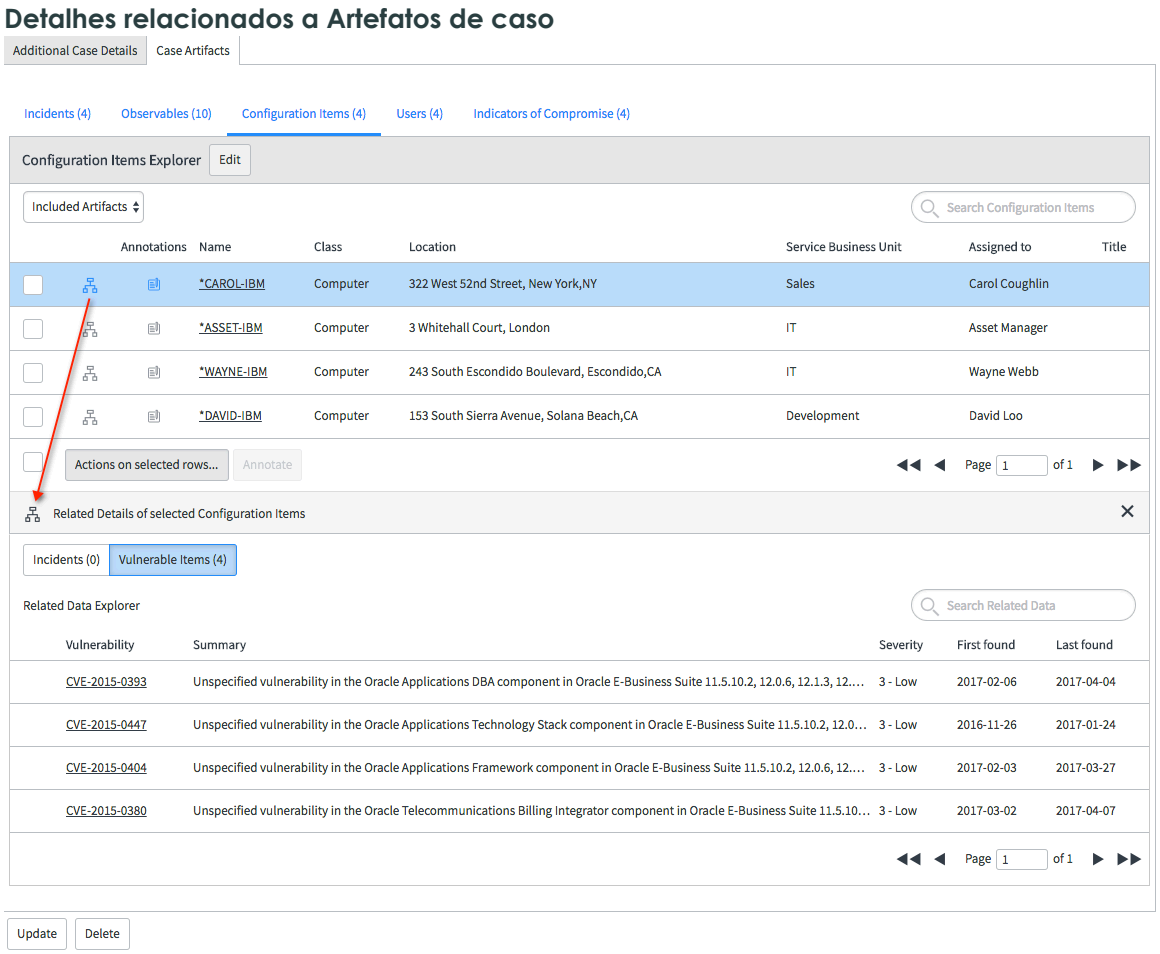
A seção **Artefatos de caso** fornece uma série de guias de informações contidas no caso de segurança.

Tradução automática

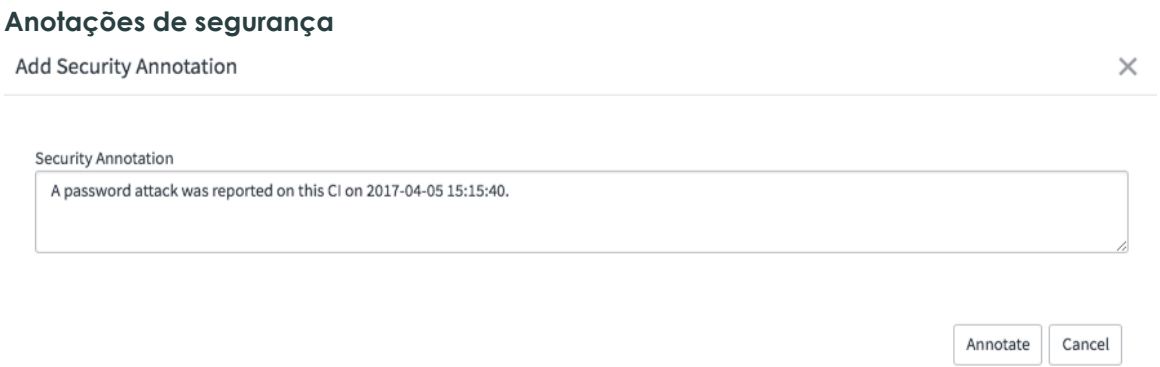
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode realizar pesquisas no conteúdo de cada guia. Você também pode excluir registros específicos que já avaliou como seguros ou que não têm valor em sua investigação. Os registros excluídos não são excluídos, mas ficam ocultos. Se necessário, você pode exibir os registros excluídos e adicioná-los novamente.

Em cada guia, você pode clicar no ícone Detalhes adicionais para mostrar informações relacionadas ao registro selecionado. Por exemplo, se você clicar na guia **Itens de configuração** para exibir o Explorador de itens de configuração e clicar em Detalhes adicionais para um IC específico, poderá exibir incidentes, itens vulneráveis e anotações associadas a esse IC.



Você também pode selecionar um registro e clicar no botão **Anotar** de um artefato relacionado ao caso para adicionar anotações ao registro. Anotações são simplesmente anotações que cada analista pode fazer em um artefato específico.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Outras ferramentas que o analista pode usar para examinar casos incluem:

- Executar uma pesquisa de detecções em observáveis em um caso
- Pesquisar artefatos de segurança

Criar casos na Gestão de casos de segurança

Os casos são usados para rastrear informações sobre uma campanha ou agente de estado que ameaça sua organização. Depois que um caso é criado, você pode adicionar artefatos que permitem revisar e analisar todas as informações relacionadas em um único registro de caso.

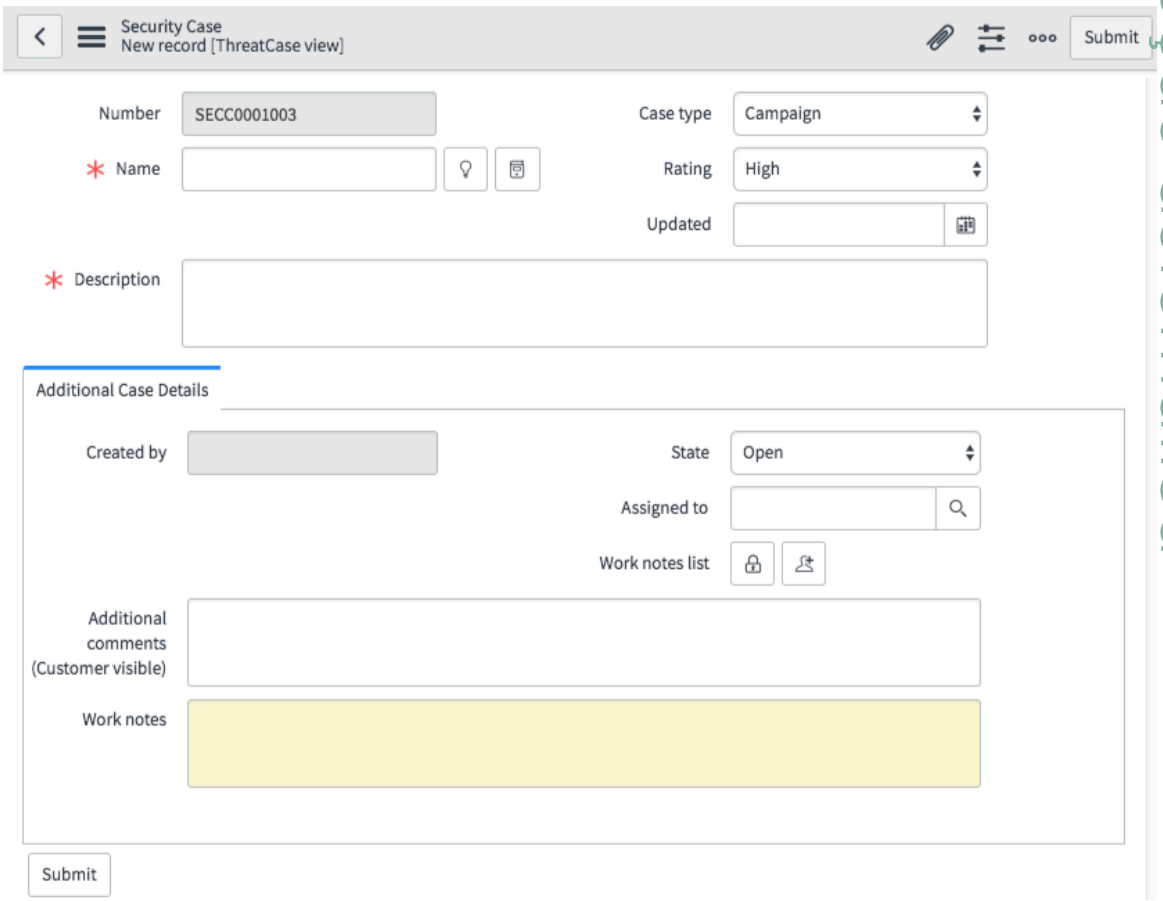
Antes de Iniciar

Função necessária: sn_ti.case_use

r

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
   A lista Casos de segurança é aberta.
2. Clique em **Nova**.
   A tela Casos de segurança é aberta.



3. Preencha os campos, se for o caso.

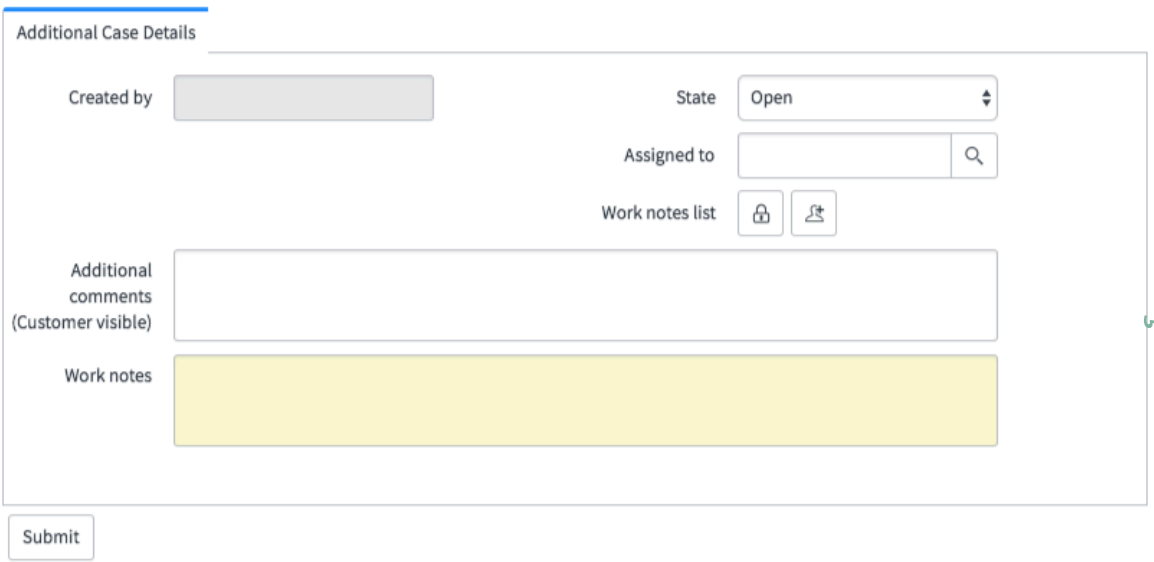
Campo	Descrição
Número do caso	[Somente leitura] O número do caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de Caso	Insira um nome descritivo para o caso.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado.
Classificação	Selecione a importância deste caso (de Crítico a Baixo).
Última atualização	[Somente leitura] A data e hora em que o caso foi atualizado pela última vez.
Descrição resumida	Uma breve descrição do caso.

4. Clique na guia **Detalhes adicionais do caso**.



5. Preencha os campos, se for o caso.

Campo	Descrição
Criado(a) por	[Somente leitura] O nome do usuário que criou este caso.
Estado	O estado atual do caso. Na criação do caso, o padrão do Estado é Rascunho.
Atribuído a	Clique no ícone de pesquisa e atribua o caso a um analista.
Lista de Anotações de trabalho	Clique no ícone de cadeado e adicione usuários internos que podem exibir anotações de trabalho.
Comentários adicionais	Conforme necessário, insira anotações no caso que ficarão visíveis para o cliente.
Anotações de trabalho	Se necessário, digite uma anotação de trabalho para o caso.

6. Clique em **Enviar**.
Depois que o registro tiver sido salvo, você poderá clicar na guia **Artefatos de caso** e adicionar artefatos ao caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar artefatos a um caso

Depois de criar um caso, você pode adicionar artefatos, como incidentes de segurança, ICs e indicadores de comprometimento, ao caso. Esses artefatos atuam como pistas na resolução do caso.

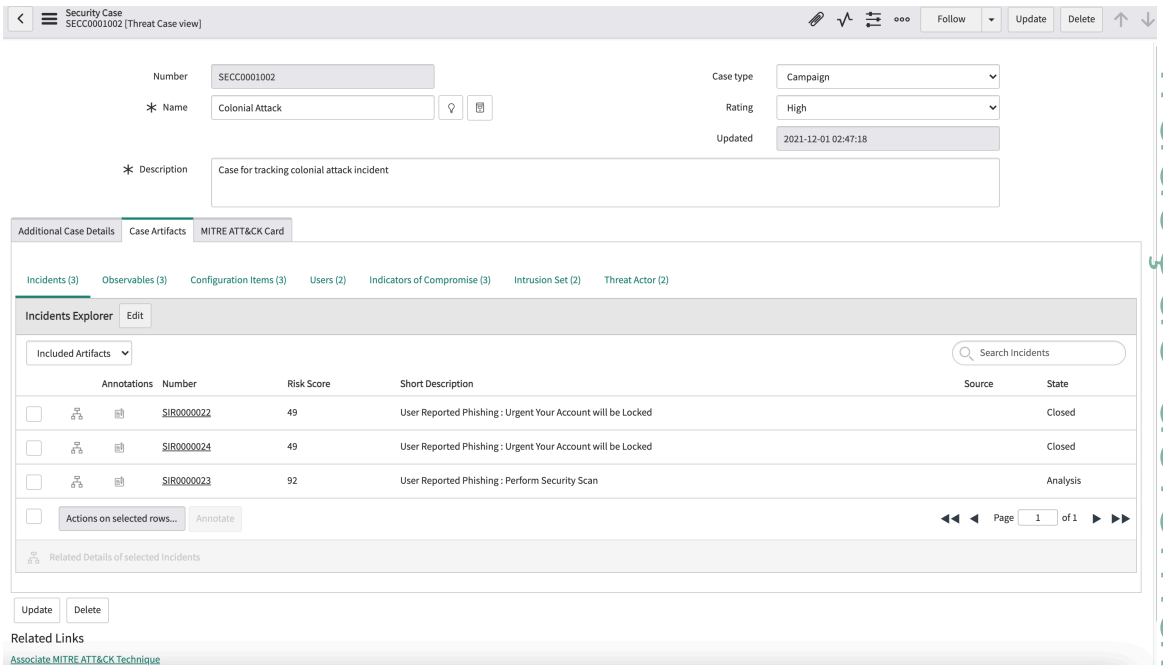
Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

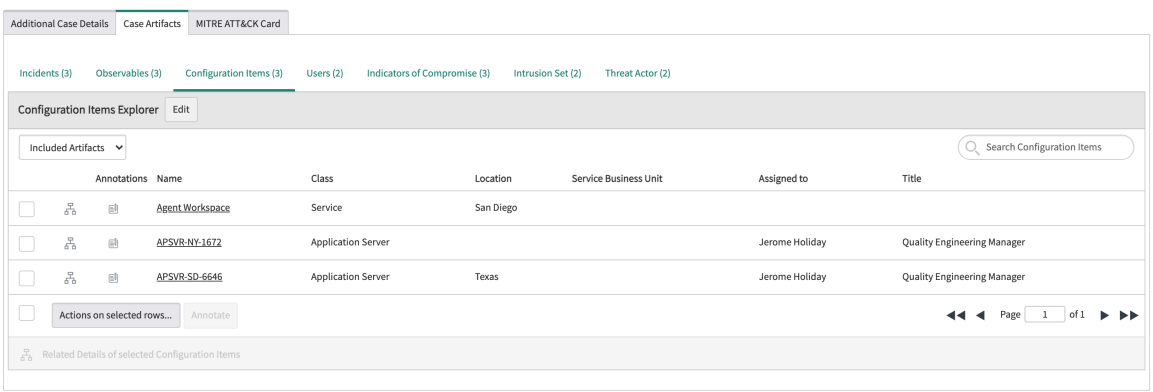
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso ao qual você deseja adicionar artefatos.
2. Clique na lista relacionada **Artefatos de caso**.



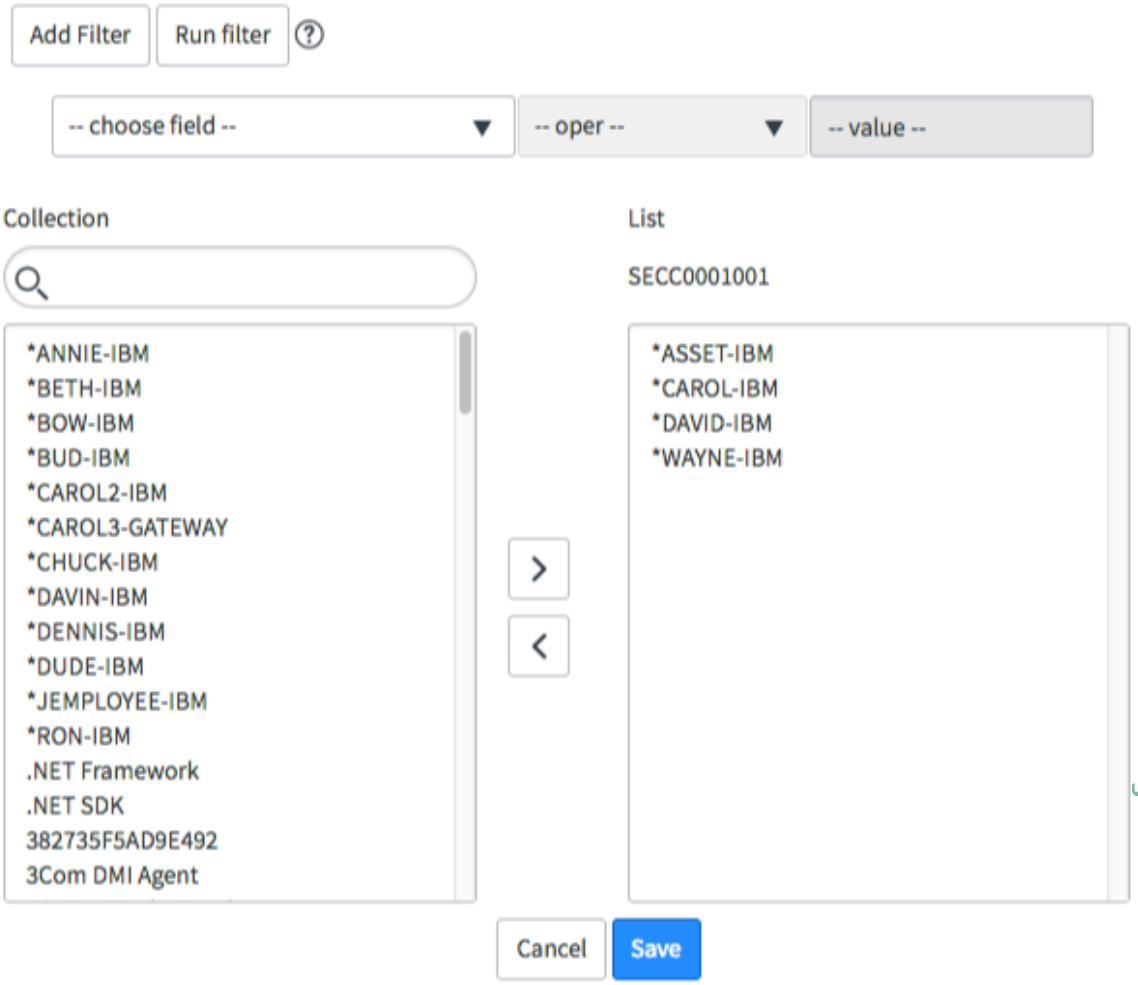
3. Clique na guia associada ao tipo de artefato que você deseja adicionar ao caso. Por exemplo, clique em **Itens de configuração** para adicionar um ou mais ICs ao caso.



4. Clique em **Editar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Usando o slushbucket e os filtros, localize os registros de artefato que deseja adicionar ao caso e mova-os do bucket Coleção para o bucket Lista e clique em **Salvar**.
   A lista aparece na guia selecionada e os artefatos selecionados são adicionados à lista.

Informações relacionadas

- Adicionar IoCs e observáveis a um caso existente
- Adicionar incidentes de segurança a um caso existente
- Adicionar ICs a casos existentes
- Adicionar usuários afetados a casos existentes

Associar MITRE-ATT&CK informações ao caso de segurança

Associe MITRE-ATT&CK táticas e técnicas a um caso de segurança para melhorar a gestão de casos de segurança e a análise de ameaças em um nível granular.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Selecione o caso de segurança que você deseja aprimorar com as informações do MITRE-ATT&CK.

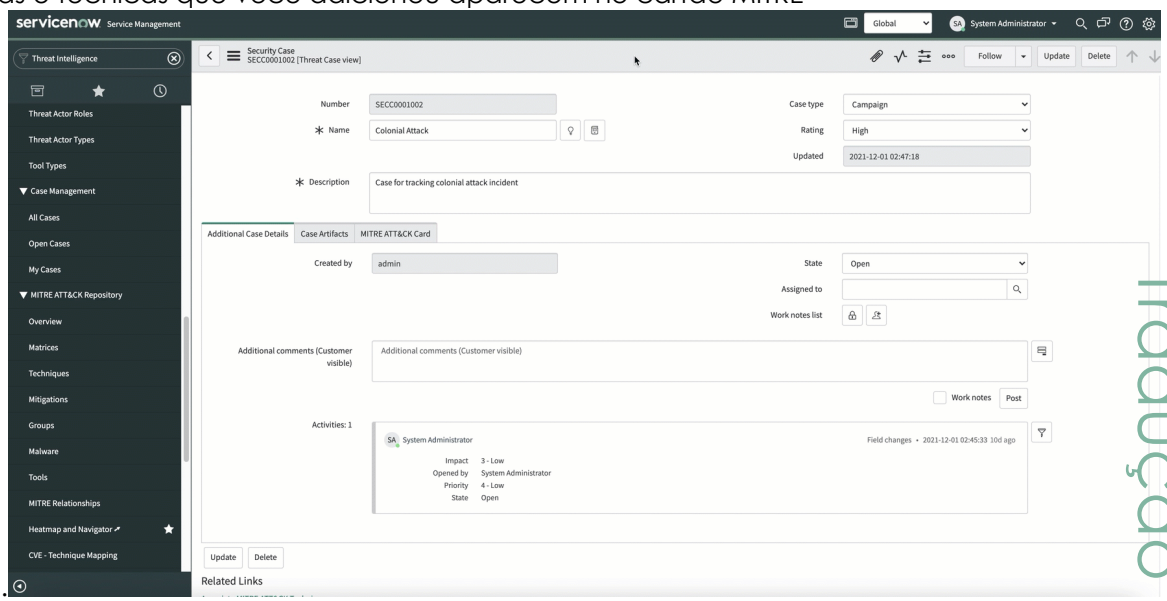
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista relacionada, clique em **Associar técnica do MITRE ATT&CK**.

   Na ilustração a seguir, você pode ver como navegar na lista relacionada até **Associar técnica do MITRE ATT&CK**, revisar a origem e adicionar uma tática e uma técnica.

4. Nas listas de origens, revise a **Origem**.
5. Revise a **Tática** e as **Técnicas**e adicione ou remova-as com base na relevância do caso.
6. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem no cartão MITRE-ATT&CK.



Criação de caso a partir de artefatos de segurança

Além de criar casos manualmente a partir de Gestão de casos de segurança, você também pode criar casos a partir de artefatos de segurança, como incidentes de segurança, indicadores de comprometimento, usuários afetados e itens de configuração.

IoCs e observáveis em casos

Em Inteligência contra ameaças, você pode criar casos a partir de IoCs e observáveis, bem como adicionar IoCs e observáveis a casos existentes. Você também pode criar observáveis diretamente de um caso.

Criar um caso a partir de IoCs ou observáveis

Em Inteligência contra ameaças, você pode criar um caso a partir de artefatos (IoCs ou observáveis). Depois que os IoCs ou observáveis tiverem sido usados para criar um caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Tradução automática

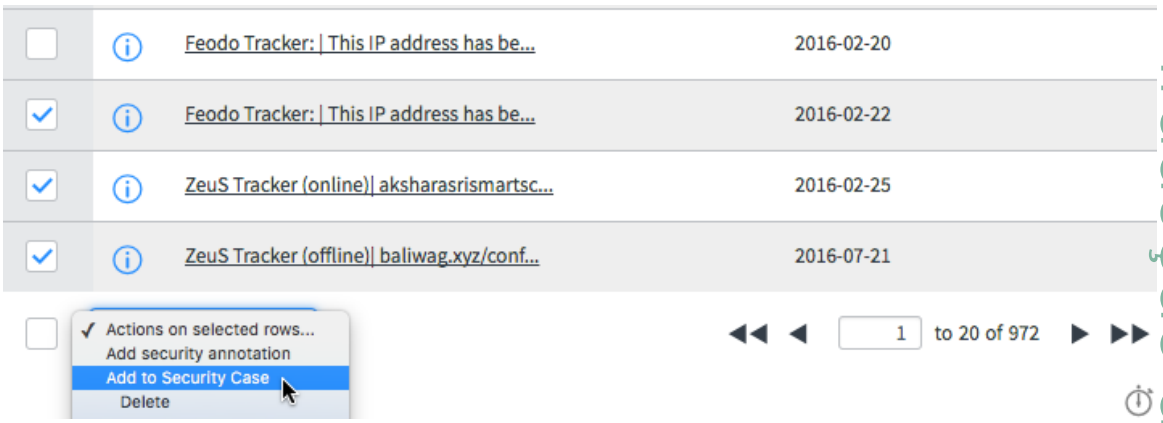
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

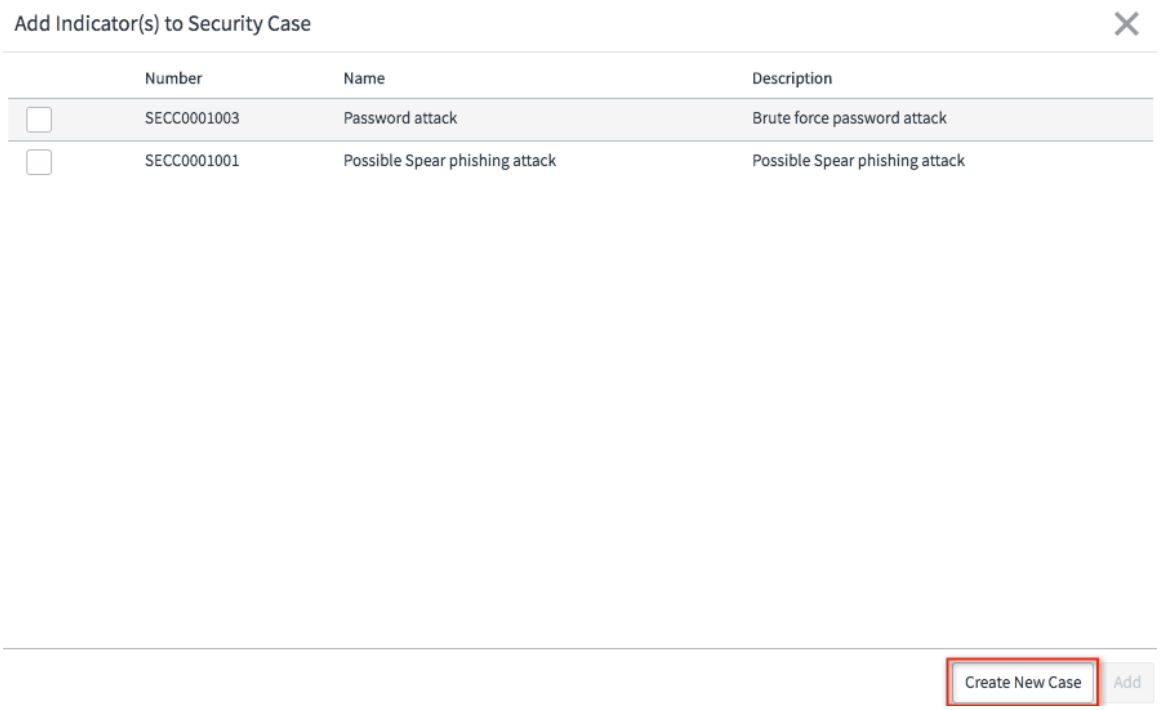
1. Navegue até os artefatos (IoCs ou observáveis) que você deseja usar para criar um caso.
   - Para criar um caso a partir de IoCs, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   - Para criar um caso a partir de observáveis, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Na lista, selecione os artefatos que você deseja adicionar a um novo caso.

   Nota: Se você selecionar vários IoCs ou observáveis, todos serão adicionados ao caso.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.



A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Adicionar IoCs e observáveis a um caso existente

Você pode adicionar IoCs e observáveis a casos existentes. Depois que os incidentes de segurança forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Procedimento

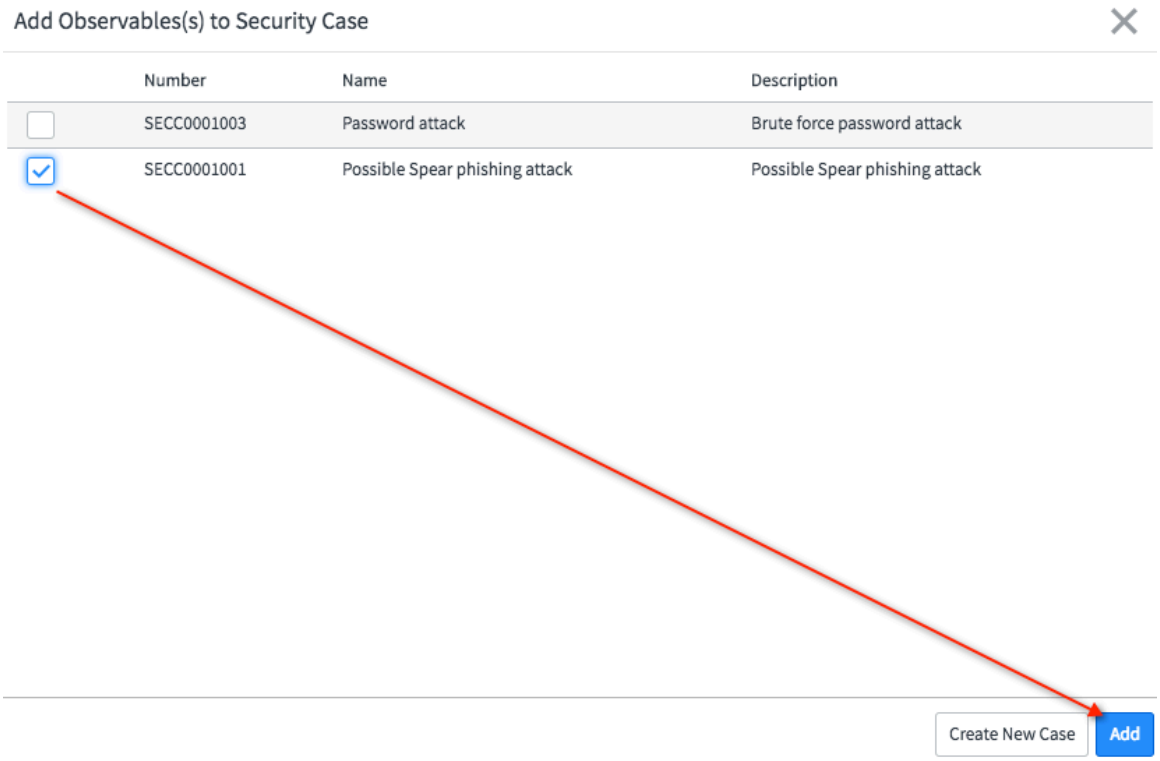
1. Navegue até os artefatos (IoCs ou observáveis) que você deseja adicionar aos casos existentes.
   - Para adicionar IoCs a um ou mais casos, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   - Para adicionar observáveis a um ou mais casos, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Na lista, selecione os registros de artefato que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários casos, os IoCs ou observáveis selecionados serão adicionados a cada um dos casos selecionados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.
4. Selecione os casos aos quais você deseja adicionar os IoCs ou observáveis selecionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Criar um observável a partir de um caso

Novos observáveis podem ser criados a partir de casos em Gestão de casos de segurança.

Antes de Iniciar

Função necessária: sn_ti.case_user

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
   A lista Casos de segurança é aberta.
2. Abra um caso existente ou clique em **Novo** para criar um novo caso.
3. Clique no link relacionado **Artefatos de caso** e clique na guia **Observáveis**.
4. Clique em **Novo** e insira as informações solicitadas.

Campo	Descrição
Valor	[Somente leitura] O número do caso.
Tipo de observável	Insira um nome descritivo para o caso.
Categoria de tipo de observável	Selecione o tipo de caso que está sendo investigado.
Contagem de incidentes	Selecione a importância deste caso (de Crítico a Baixo).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descoberta	[Somente leitura] A data e hora em que o caso foi atualizado pela última vez.
Anotações	Uma breve descrição do caso.

5. Clique na guia **Detalhes adicionais do caso**.
6. Preencha os campos, se for o caso.

Campo	Descrição
Criado(a) por	[Somente leitura] O nome do usuário que criou este caso.
Estado	O estado atual do caso. Na criação do caso, o padrão do Estado é Rascunho.
Lista de Anotações de trabalho	Clique na caixa de seleção para exibir as anotações de trabalho na seção Detalhes adicionais do caso do registro do caso.
Anotações de trabalho	Se necessário, digite uma anotação de trabalho para o caso. Se a **lista Anotações de trabalho** estiver selecionada, a anotação de trabalho aparecerá na seção Detalhes adicionais do caso do registro do caso.

7. Clique em **Enviar**.
   Conforme necessário, você pode clicar na guia **Artefatos de caso** e adicionar artefatos ao caso.

Executar uma pesquisa de detecções em observáveis em um caso

Você pode pesquisar observáveis usando o recurso Pesquisa de detecções para determinar com que frequência eles ocorrem. Cada ocorrência é considerada uma detecção. Você pode limitar a pesquisa ao número de detecções dentro de um número selecionado de dias ou dentro de um intervalo de datas.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

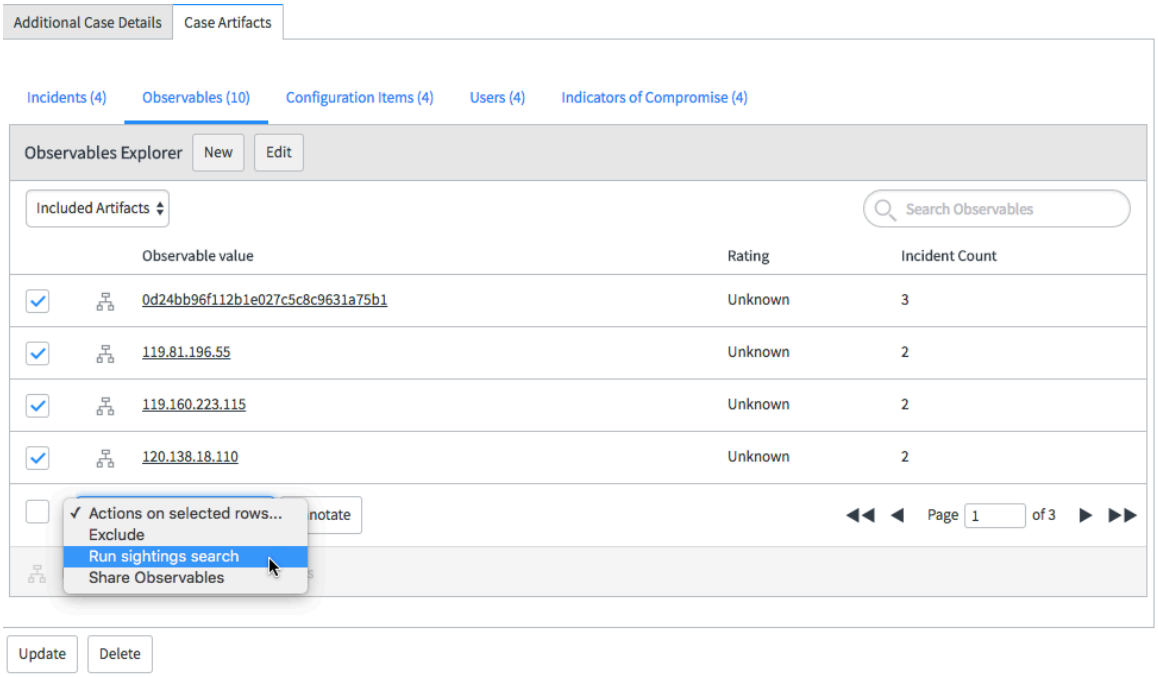
Função necessária: sn_ti.case_user_write

Procedimento

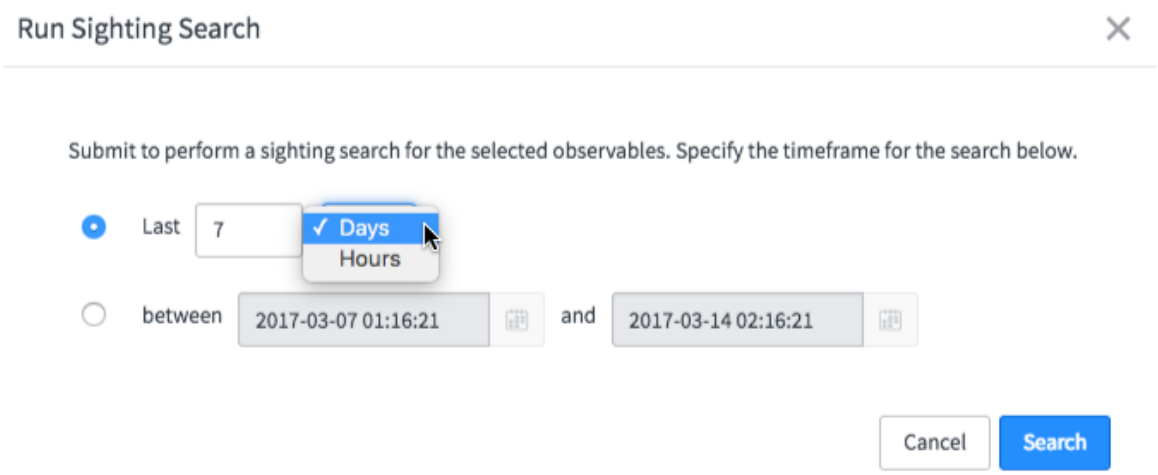
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Abra o caso que contém observáveis para os quais você deseja executar uma pesquisa de detecções.
3. Clique no link relacionado **Artefatos de caso**.
4. Clique na guia **Observáveis**.
5. Selecione um ou mais observáveis para os quais você deseja pesquisar detecções.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na lista suspensa **Ações nos itens selecionados**, selecione **Executar pesquisa de detecções**.
   A caixa de diálogo **Executar pesquisa** de detecções é exibida.



7. Insira o número de dias ou horas que você deseja pesquisar detecções dos observáveis selecionados ou selecione um intervalo de datas.
8. Clique em **Pesquisar**.

Incidentes de segurança nos casos

Em Security Incident Response, você pode criar casos a partir de incidentes de segurança, ICs e usuários afetados, bem como adicionar esses artefatos a casos existentes.

Criar um caso a partir de incidentes de segurança

Em Security Incident Response, você pode criar casos a partir de incidentes de segurança. Depois que os incidentes de segurança forem usados para criar um novo caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Tradução automática

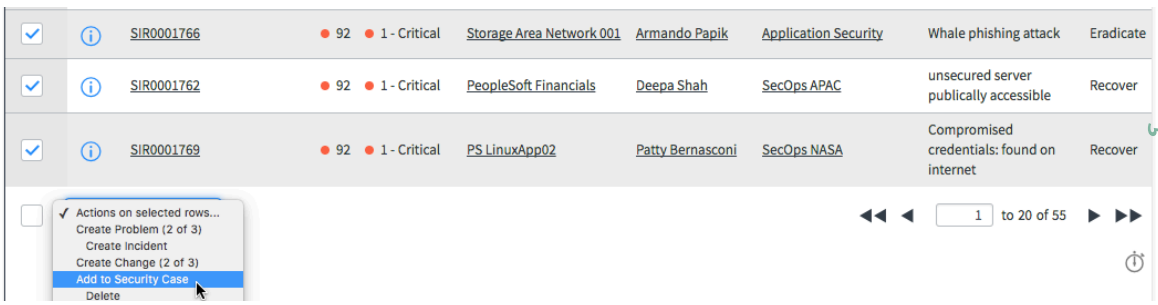
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

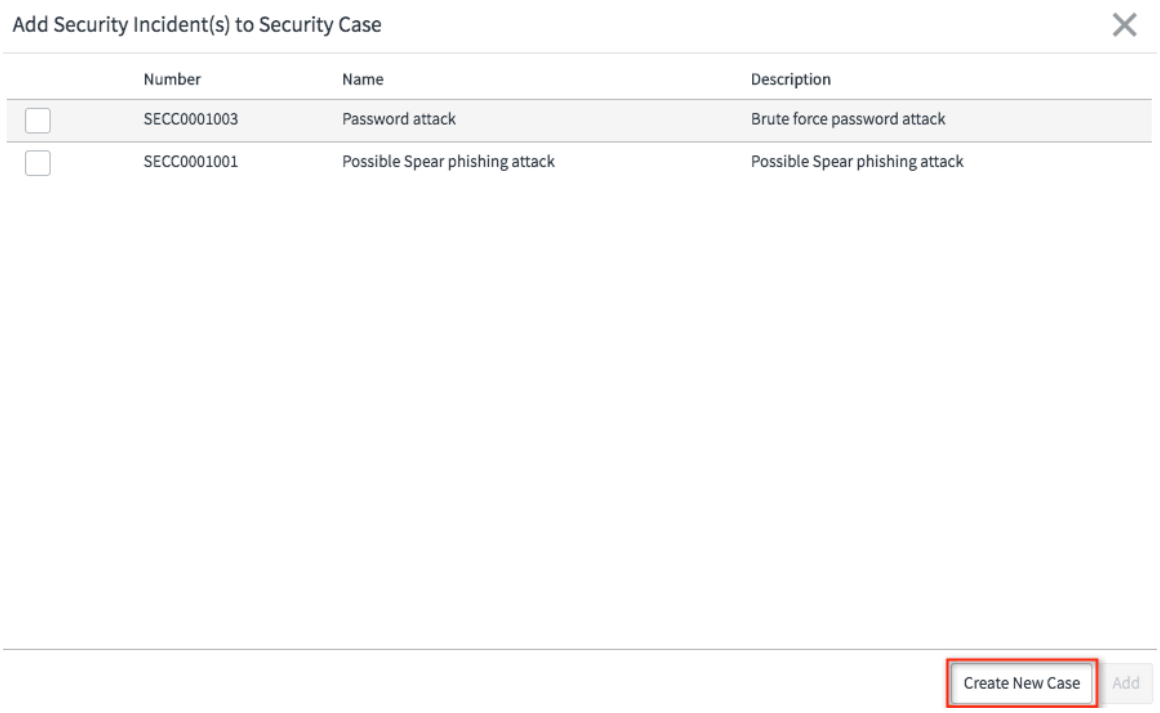
Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa
Você precisa navegar até os incidentes de segurança que deseja usar para criar casos.

Procedimento
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
   A lista Incidentes de segurança é aberta. Na lista, você pode criar um novo caso a partir de um ou mais incidentes de segurança ou pode selecionar um incidente de segurança específico e criar um novo caso a partir do formulário.
2. Para criar um caso na lista, selecione os artefatos que você deseja adicionar a um novo caso.
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.



   A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Adicionar incidentes de segurança a um caso existente

Você pode adicionar incidentes de segurança a um ou mais casos existentes. Depois que os incidentes de segurança forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os incidentes de segurança que deseja adicionar aos casos existentes.

Procedimento

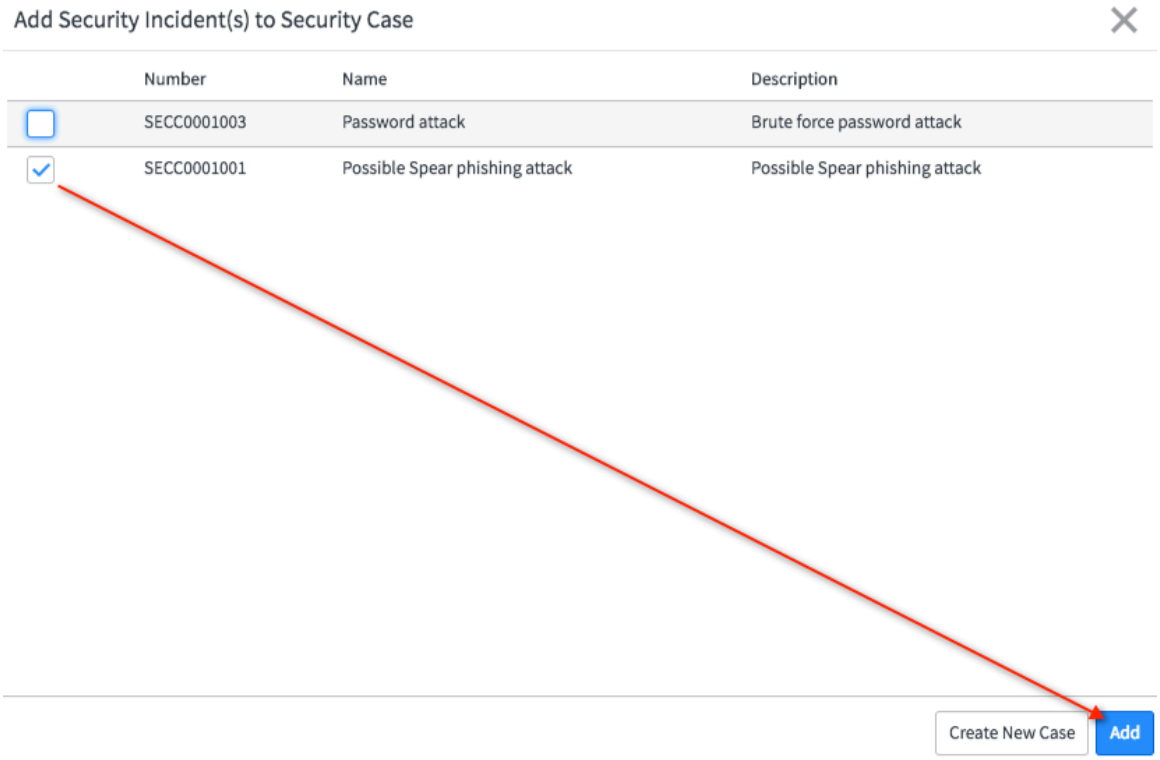
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
   A lista Incidentes de segurança é aberta.
2. Na lista, selecione um ou mais incidentes de segurança que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários incidentes de segurança, os incidentes de segurança selecionados serão adicionados a cada um dos casos selecionados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta e exibe os casos atribuídos a você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione os casos aos quais você deseja adicionar os incidentes de segurança selecionados.
5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Itens de configuração em casos

Você pode criar um novo caso a partir de um ou mais itens de configuração (IC) na tabela Item de configuração [cmdb_ci]. Você também pode adicionar ICs a casos existentes.

Criar um caso a partir de ICs

Você pode criar um caso de segurança a partir de itens de configuração na tabela Item de configuração [cmdb_ci]. Depois que os ICs tiverem sido usados para criar um novo caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os itens de configuração que deseja usar para criar um caso.

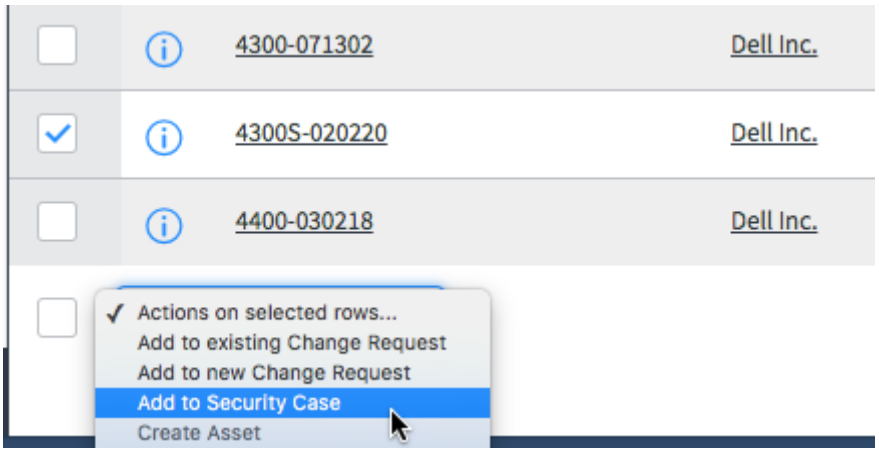
Procedimento

1. Navegar até **Todos** > **Configuração** > **Itens de Base** > **Computadores** para exibir ICs de computadores.
   A lista do tipo de IC selecionado é aberta. Na lista, você pode criar um novo caso a partir de um ou mais ICs ou pode selecionar um IC específico e criar um novo caso a partir do formulário.

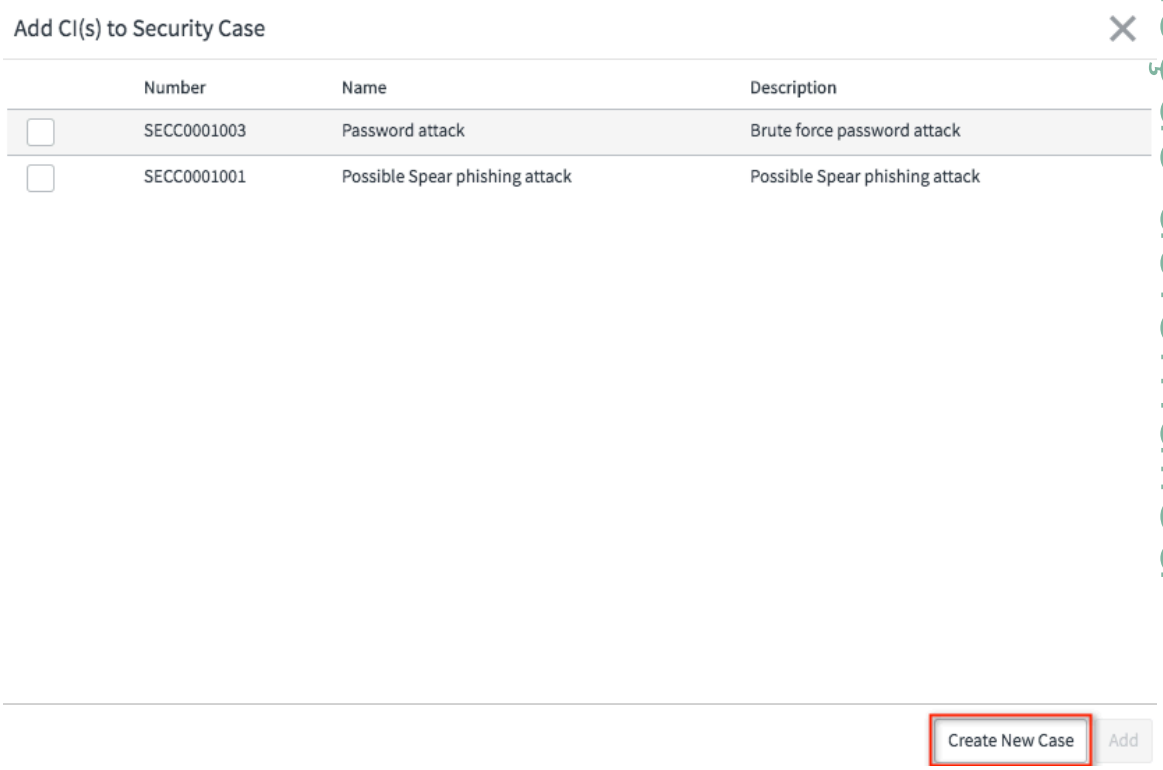
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Na lista, selecione os ICs que você deseja adicionar a um novo caso.
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.



A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.
5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Adicionar ICs a casos existentes

Você pode adicionar itens de configuração a um ou mais casos existentes. Depois que os ICs forem adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os ICs que deseja adicionar aos casos existentes.

Procedimento

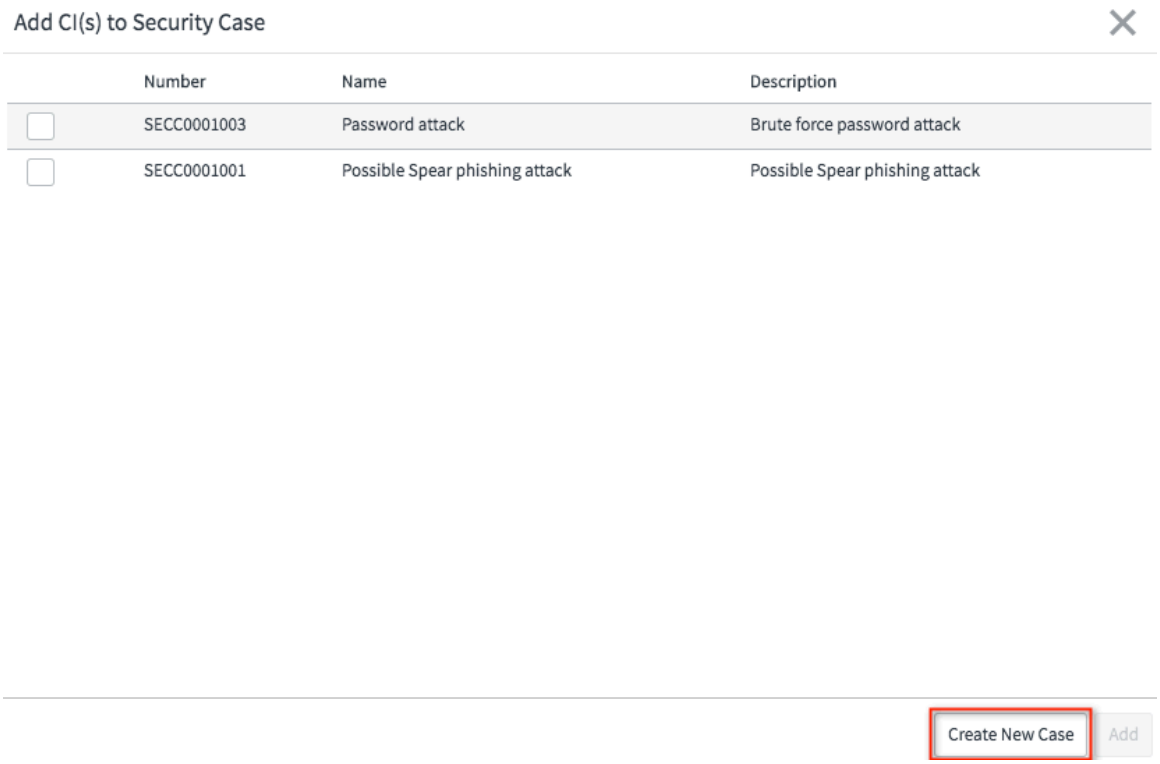
1. Navegar até **Todos** > **Configuração** > **Itens de Base** > **Computadores** para exibir ICs de computadores.
   A lista de ICs selecionados é aberta.
2. Na lista, selecione um ou mais ICs que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários ICs, os ICs selecionados serão adicionados a cada um dos casos selecionados.

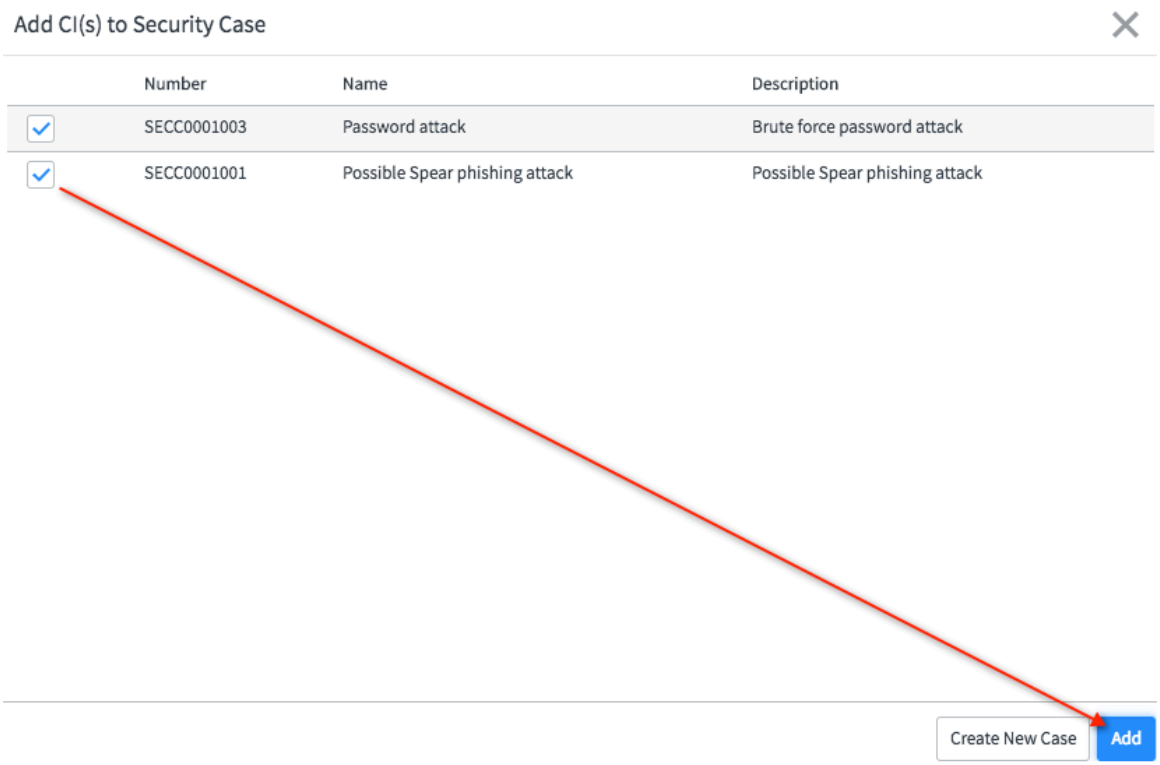
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta e exibe os casos atribuídos a você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione os casos aos quais você deseja adicionar os ICs selecionados.



5. Clique em **Adicionar**.
Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuários afetados nos casos

Você pode criar um novo caso a partir de um ou mais usuários afetados na tabela Usuário [sys_user]. Você também pode adicionar usuários a casos existentes.

Criar um caso a partir de usuários afetados

Você pode criar um caso de segurança a partir de usuários afetados na tabela Usuário [sys_user]. Depois que os usuários afetados tiverem sido usados para criar um novo caso, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os usuários que deseja usar para criar um caso.

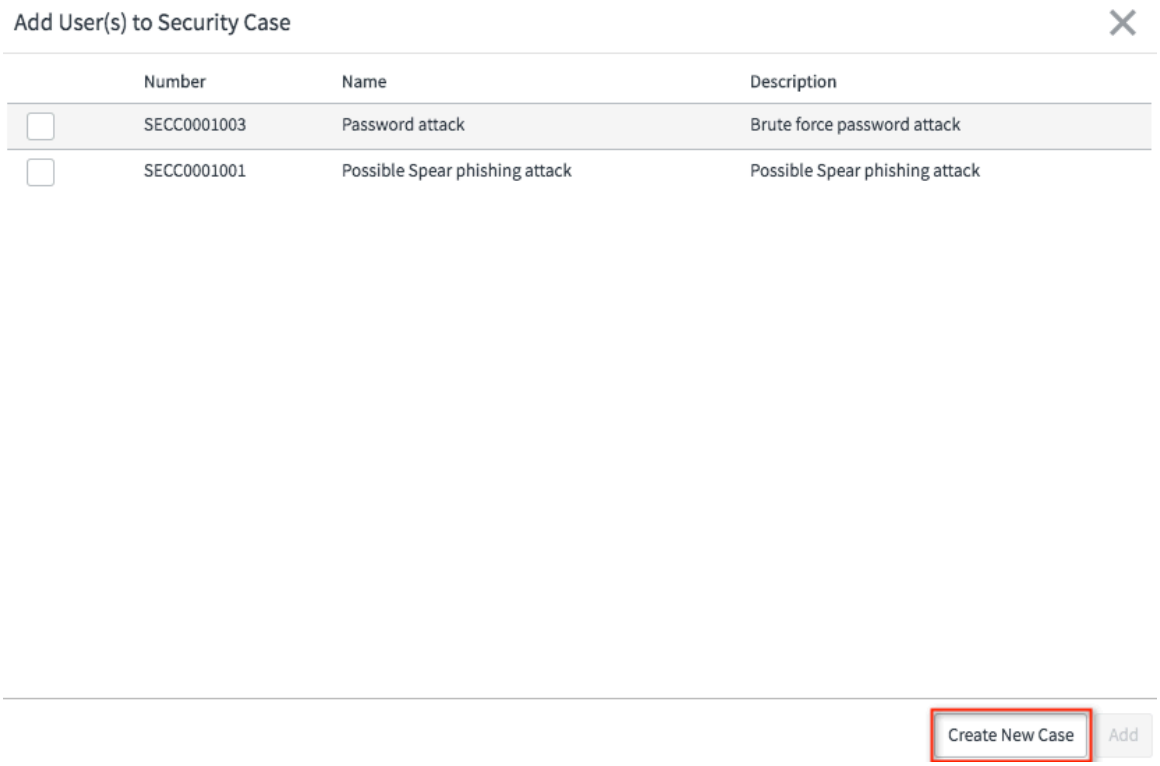
Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Usuários**.
   A lista dos usuários selecionados é aberta. Na lista, você pode criar um novo caso a partir de um ou mais registros de usuário ou pode selecionar um registro de usuário específico e criar um novo caso a partir do formulário.
2. Na lista, selecione os usuários que você deseja adicionar a um novo caso.
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.

   A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique **em Criar novo caso**.
5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja de valor para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Gestão de casos de segurança.
7. Clique no link para exibir o novo caso.

Adicionar usuários afetados a casos existentes

Você pode adicionar usuários afetados a um ou mais casos existentes. Depois que os registros de usuário tiverem sido adicionados aos casos, você poderá usar Gestão de casos de segurança para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os registros de usuário que deseja adicionar aos casos existentes.

Tradução automática

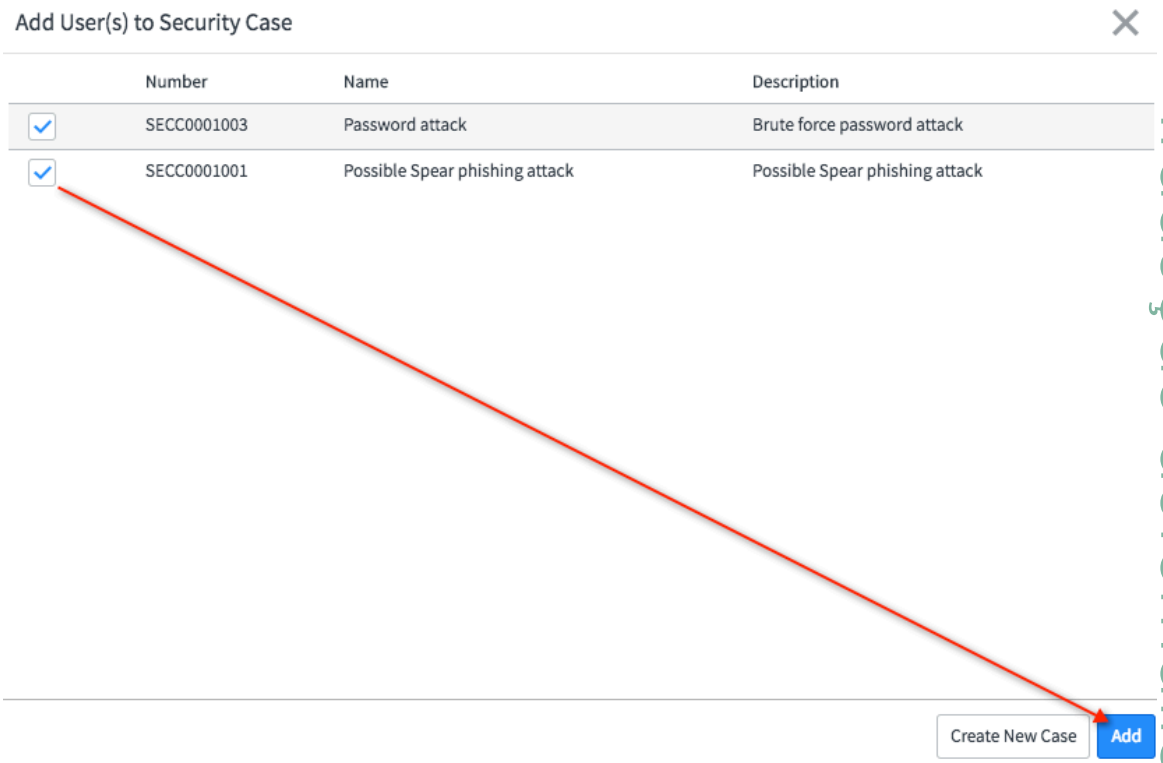
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Usuários**.
   A lista de registros de usuário é aberta.
2. Na lista, selecione um ou mais usuários que você deseja adicionar aos casos existentes.

   Nota: Se você selecionar vários usuários, os registros de usuário selecionados serão adicionados a cada um dos casos selecionados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta e exibe os casos atribuídos a você.



4. Selecione os casos aos quais você deseja adicionar os usuários selecionados.
5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Gestão de casos de segurança.

Análise de artefatos de segurança

Depois de criar casos, usando Gestão de casos de segurançaou a partir de artefatos como IoCs, observáveis, incidentes de segurança e assim por diante, você pode continuar a adicionar artefatos para ajudar na análise das ameaças identificadas.

Detalhes relacionados para artefatos de caso

Conforme você adiciona artefatos a um caso, detalhes relacionados adicionais para cada artefato também podem ser adicionados automaticamente. Por exemplo, se você adicionar um incidente de segurança, ele poderá conter ICs afetados e registros de usuário. Você pode exibir rapidamente os detalhes relacionados a um artefato selecionado sem sair da lista de artefatos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir detalhes relacionados a um artefato de incidente de segurança

Se o seu caso incluir artefatos de incidente de segurança, você poderá exibir todos os detalhes relacionados contidos em cada incidente de segurança referenciado pelo caso.

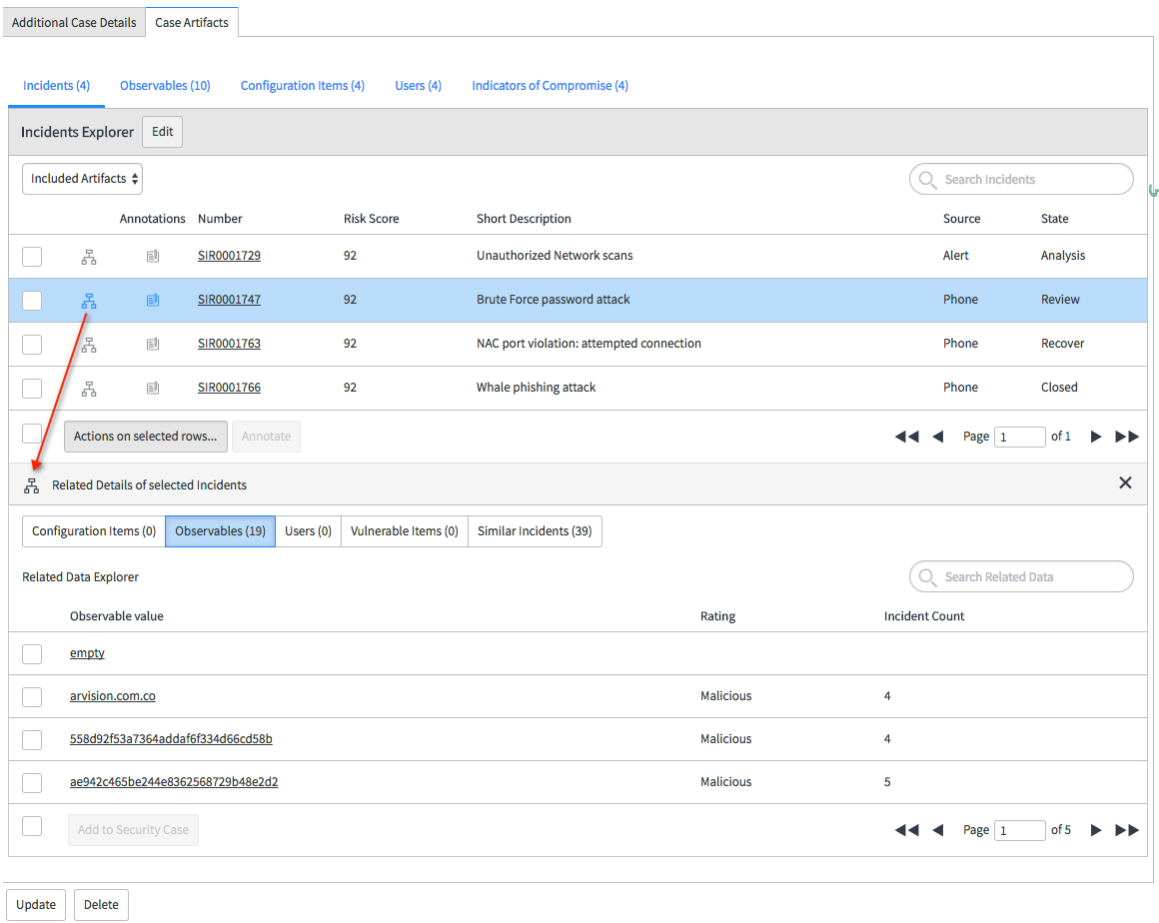
Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de incidente de segurança.
2. Clique na guia **Incidentes**.
3. Clique no ícone Detalhes adicionais do incidente de segurança para o qual você deseja exibir os detalhes relacionados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato de item de configuração

Se o seu caso incluir artefatos de item de configuração, você poderá exibir todos os detalhes relacionados contidos em cada IC referenciado pelo caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

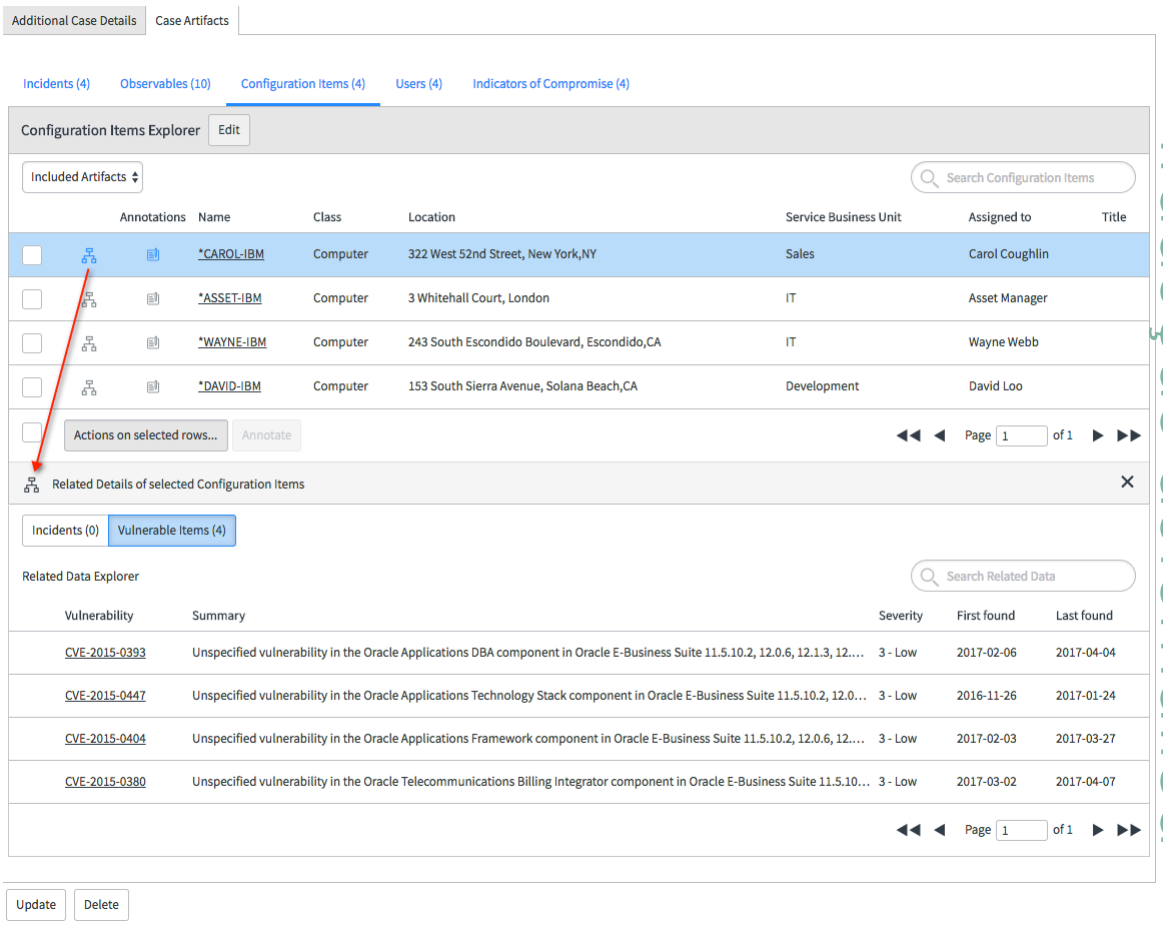
Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de IC.
2. Clique na guia **Itens de configuração**.
3. Clique em Detalhes adicionais para o artefato de IC cujos detalhes relacionados você deseja exibir.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato de IoC

Se o seu caso incluir indicadores de artefatos de comprometimento (IoC), você poderá exibir todos os detalhes relacionados contidos em cada IoC referenciado pelo caso.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

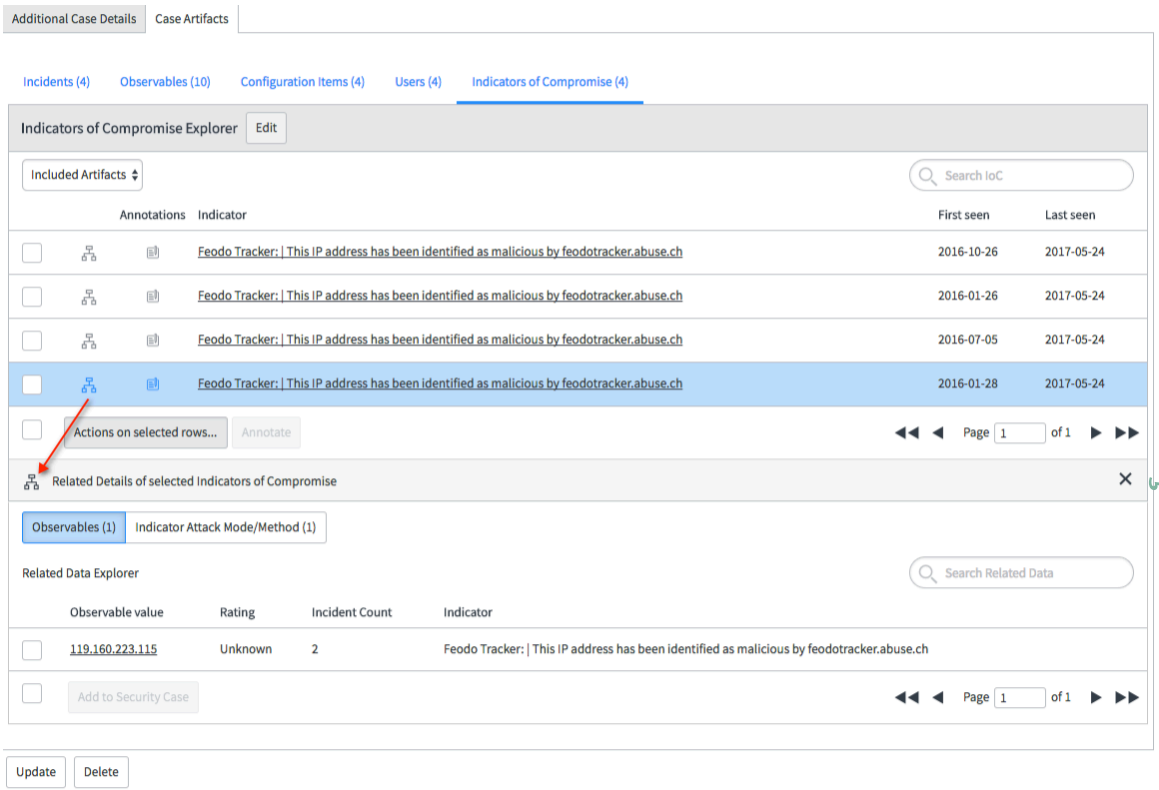
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de IoC.
2. Clique na guia **Indicadores de compromisso**.
3. Clique no ícone Detalhes adicionais do artefato de IoC para o qual você deseja exibir detalhes relacionados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato de usuário afetado

Se o seu caso incluir artefatos de usuário afetado, você poderá exibir todos os detalhes relacionados contidos em cada usuário afetado referenciado pelo caso.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

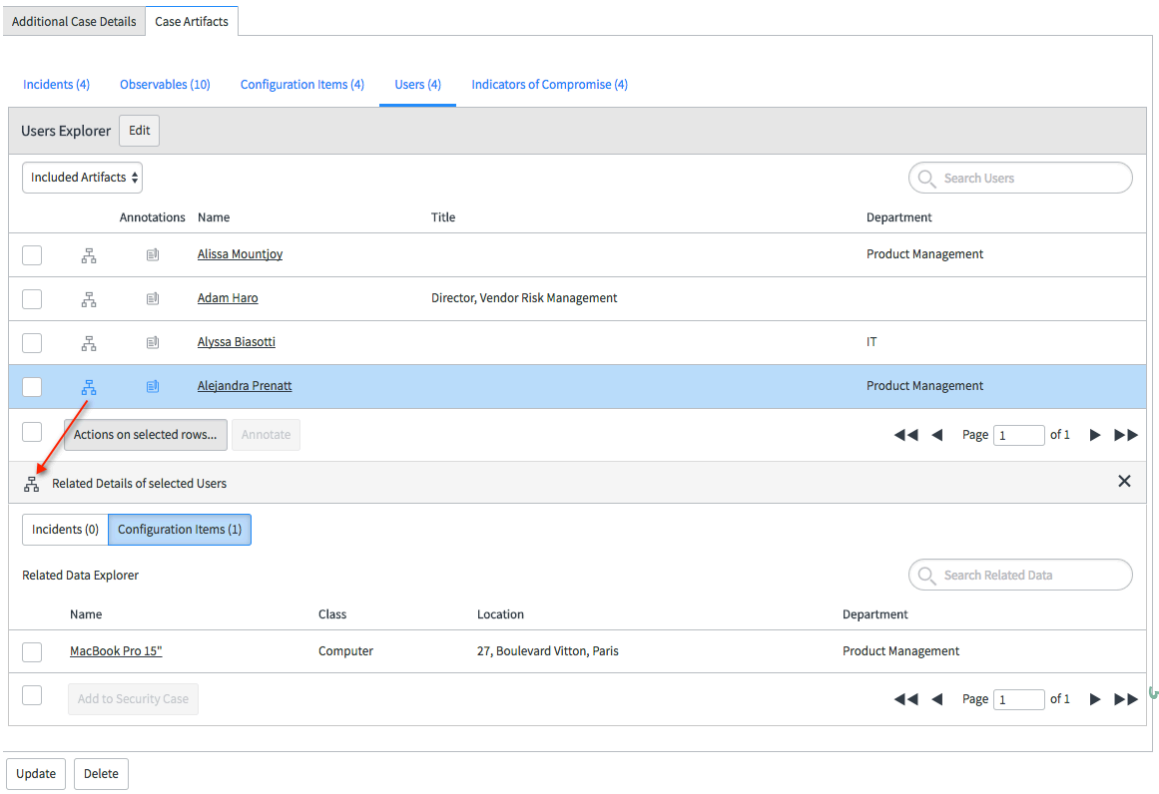
Procedimento

1. Abra um caso que contenha artefatos de usuário afetados.
2. Clique na guia **Usuários**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em Detalhes relacionados para o artefato do usuário afetado para o qual você deseja exibir detalhes relacionados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato observável

Se o seu caso incluir artefatos observáveis, você poderá exibir todos os detalhes relacionados contidos em cada observável referenciado pelo caso.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

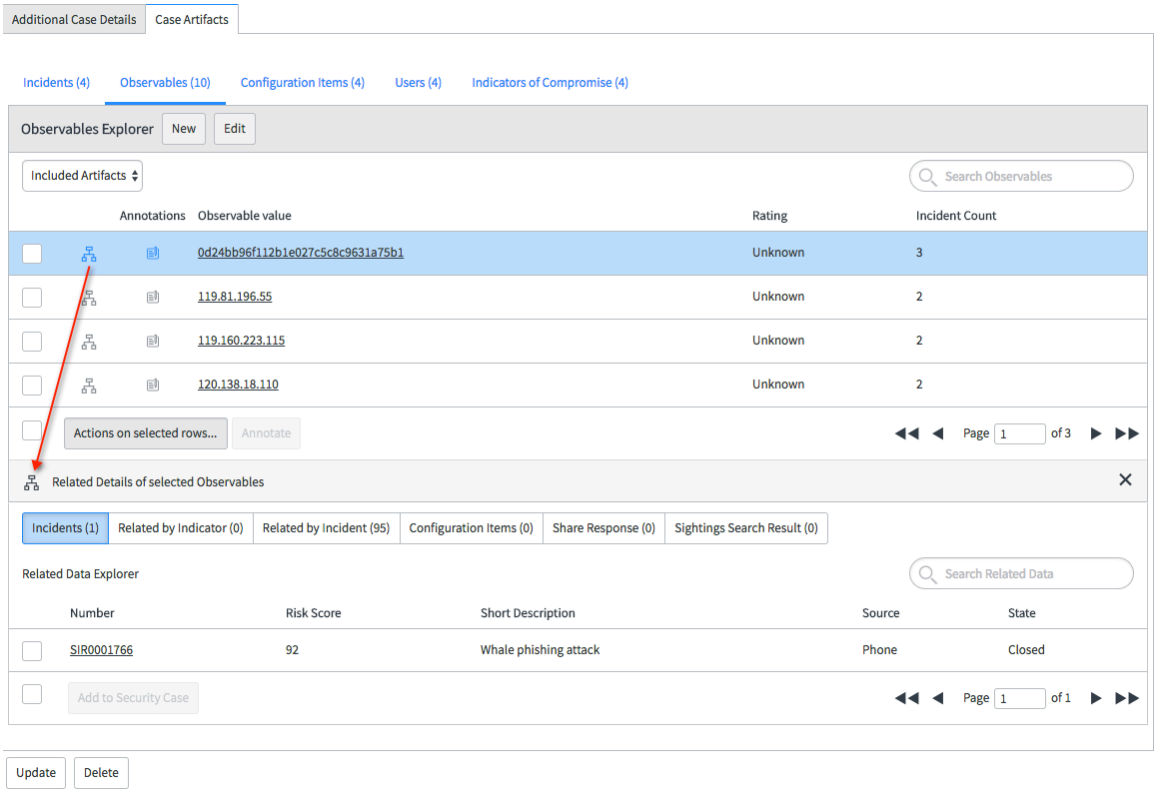
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos observáveis.
2. Clique na guia **Observáveis**.
3. Clique no ícone Detalhes adicionais do artefato observável cujos detalhes relacionados você deseja exibir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exclusão e inclusão de artefatos de segurança

As listas de artefatos de suporte atribuídos a um caso às vezes podem ser longas e pode haver instâncias em que você deseja remover artefatos específicos de uma lista. Em vez de remover permanentemente os artefatos, você pode excluí-los da lista e, conforme necessário, retorná-los à lista posteriormente.

Excluir artefatos de segurança de um caso

Você pode remover artefatos das listas de artefatos de suporte. Eles não são removidos permanentemente e podem ser devolvidos ao caso conforme necessário.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

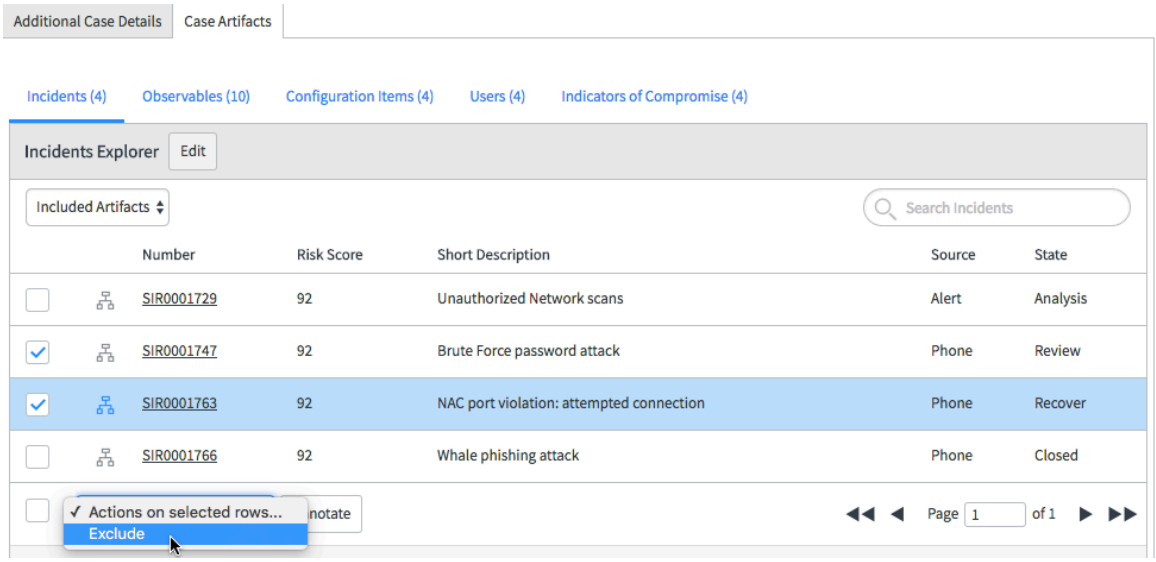
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos que você deseja excluir de uma lista.
2. Clique na lista relacionada **Artefatos de caso**.
3. Clique na guia associada aos artefatos que você deseja excluir.
   Por exemplo, clique em **Incidentes** para excluir incidentes de segurança da lista.
4. Selecione um ou mais registros de artefato que você deseja excluir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na lista suspensa **Ações em itens selecionados**, selecione **Excluir**.
6. Clique em **Excluir** na caixa de confirmação.
   Os artefatos selecionados são removidos da lista.

Retornar artefatos de segurança excluídos para um caso

Depois de excluir artefatos de uma lista em um caso, você pode devolvê-los ao caso em que pode continuar a trabalhar neles.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

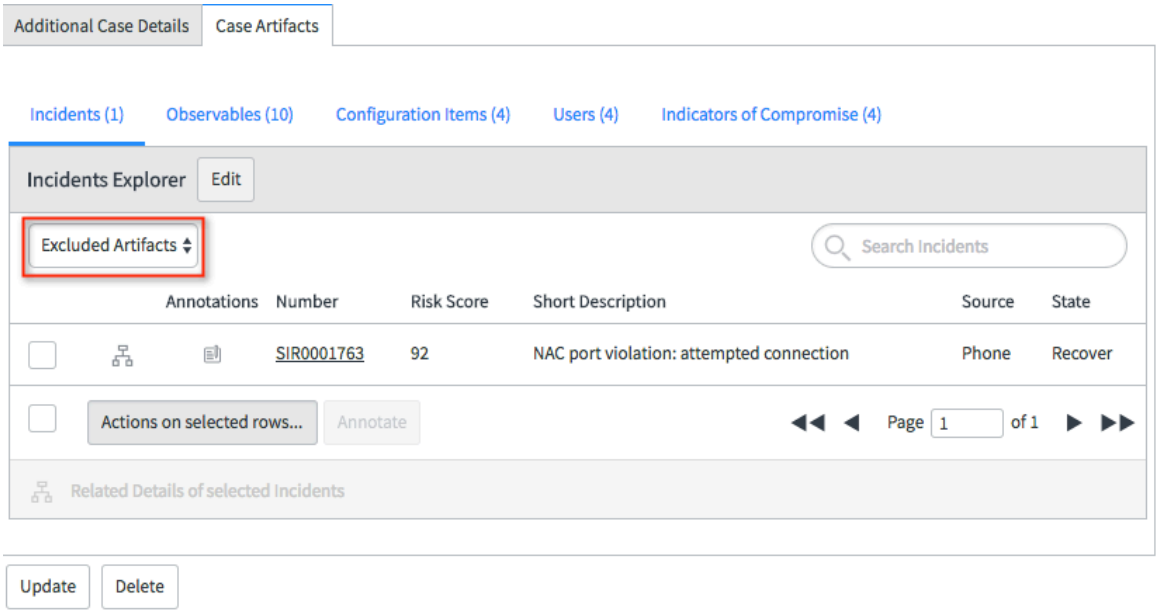
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos que você excluiu anteriormente de uma lista que deseja retornar para a lista.
2. Clique na lista relacionada **Artefatos de caso**.
3. Clique na guia associada aos artefatos que você deseja retornar à lista.
4. Clique na lista suspensa Filtro de artefato e selecione **Artefatos excluídos**.

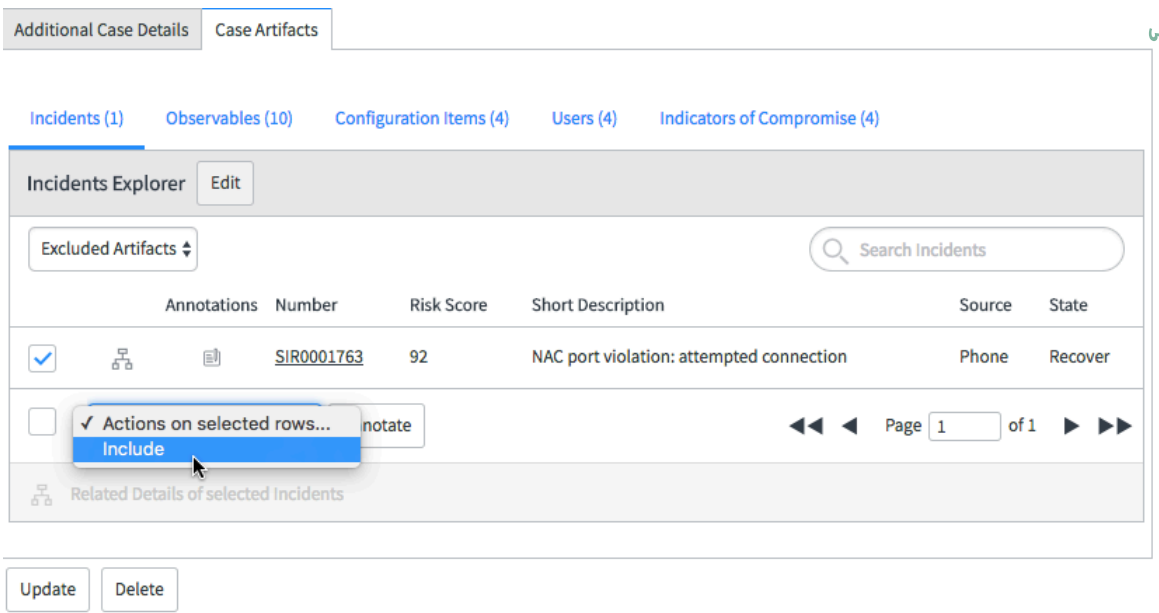
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Selecione um ou mais registros de artefato que você deseja retornar à lista Incluir.

6. Na lista suspensa **Ações em itens selecionados**, selecione **Incluir**.



7. Clique em **Incluir** na caixa de confirmação.
Os artefatos selecionados são removidos da lista de artefatos excluídos e retornados para a lista de artefatos incluídos no caso.

Anotar artefatos de segurança

Ao analisar um caso, você pode adicionar anotações a qualquer artefato.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

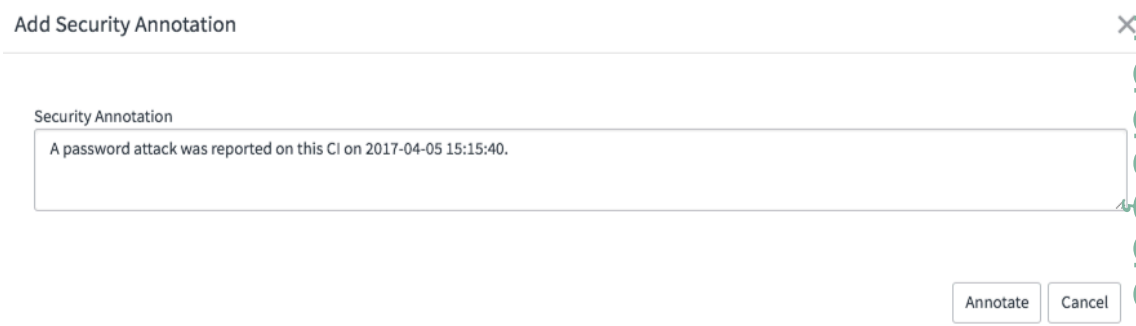
- sn_ti.case_user_write para adicionar anotações
- sn_ti.case_user_read para exibir anotações

Procedimento

1. Abra um caso que contenha artefatos que você deseja anotar.
2. Clique na lista relacionada **Artefatos de caso**.
3. Clique na guia associada aos artefatos que você deseja anotar.
   Por exemplo, clique em **Indicadores de compromisso** para adicionar anotações aos IoCs.
4. Para adicionar uma anotação a um ou mais artefatos, execute as seguintes etapas:

   a. Selecione os artefatos aos quais você deseja adicionar uma anotação.

   b. Clique **em Anotar**.

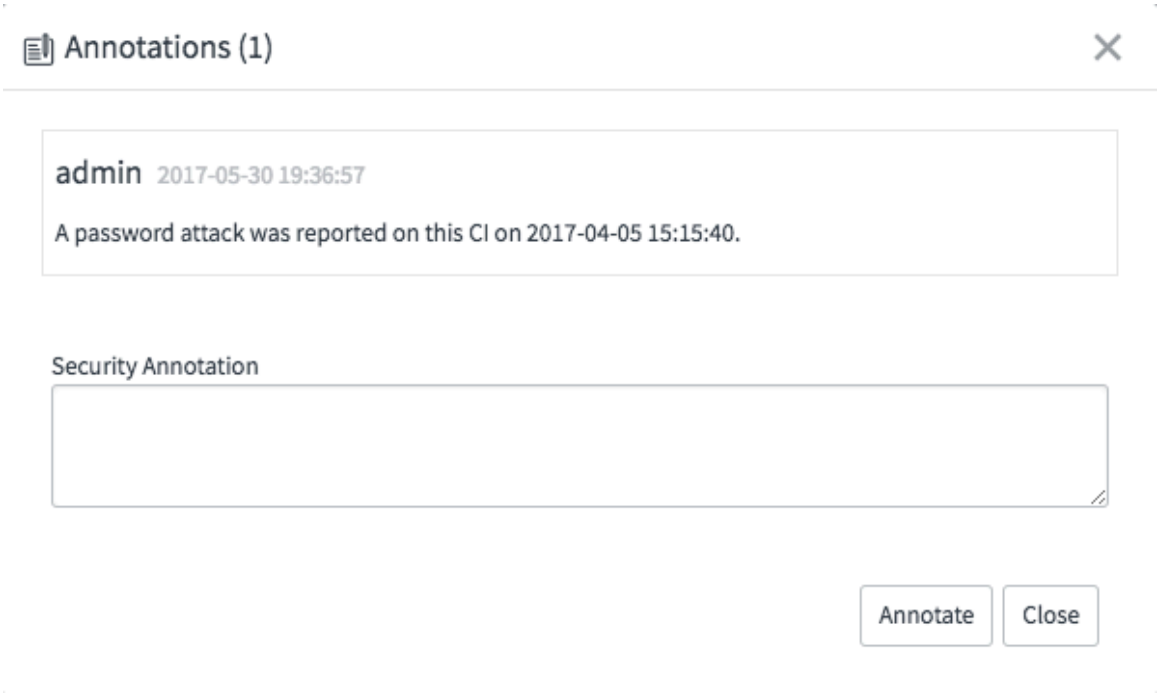


   c. Digite a anotação e clique em **Anotar**.
   A anotação é adicionada aos artefatos selecionados.

5. Para exibir anotações de um artefato, clique no ícone Exibir anotações ( ).
   As anotações existentes aparecem na caixa de diálogo Anotações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Você também pode inserir uma nova anotação para o artefato na caixa **Anotação de segurança** e clicar em **Anotar**.

Pesquisar artefatos de segurança

Você pode executar uma pesquisa de palavra-chave em qualquer lista de artefatos de segurança.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Gestão de casos de segurança.

Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de segurança.
2. Clique na guia dos artefatos de segurança nos quais você deseja executar uma pesquisa de palavra-chave.
3. Na caixa **Pesquisa de palavra** -chave, comece a digitar o nome do artefato que você deseja localizar.
   Quando artefatos que correspondem à sua entrada são encontrados, eles são exibidos.

Controle de posturas de segurança

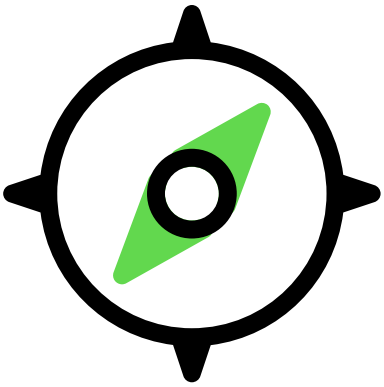
Obtenha visibilidade do inventário de ativos empresariais e da cobertura da ferramenta de segurança. Use as políticas fornecidas com o produto ou crie a sua própria para identificar ativos sem as principais ferramentas de segurança, como proteção de endpoint, gestão de configuração e verificação de vulnerabilidades. Monitore ativos para configurações de ferramentas de segurança específicas para seu ambiente e automatize o fluxo de trabalho de correção de lacunas de segurança na aplicação Conformidade de configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

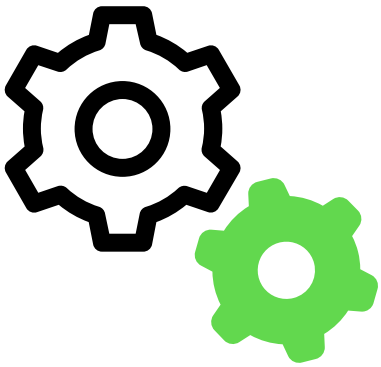
Iniciar

Explorar



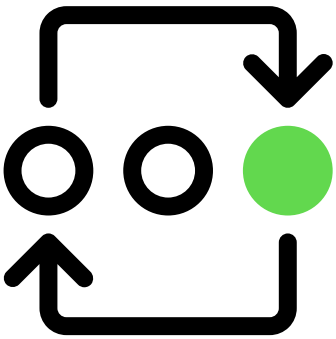
Saiba mais sobre conceitos e recursos do Controle de posturas de segurança

Instalar



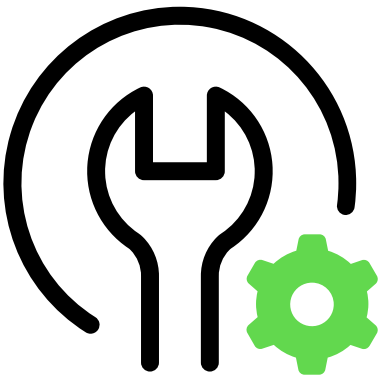
Instalar aplicações de controle de posturas de segurança

Integrar



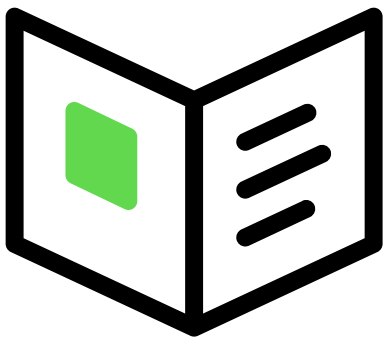
Integre os Conectores do Service Graph ao Security Posture Control

Uso



Aprenda a usar o espaço para pesquisar seus ativos e identificar lacunas de segurança

Referência



Obtenha detalhes sobre cenários que ajudam a identificar tipos específicos de lacunas de cobertura da ferramenta. Veja exemplos de políticas base, secundárias e clonadas e veja uma lista de conectores do Service Graph de hardware e software compatíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solucionar problemas e obter ajuda

- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Exploração do Controle de posturas de segurança

Controle de posturas de segurança permite que as equipes de segurança cibernética tenham visibilidade de todo o inventário de ativos empresariais e determinem sua postura geral de segurança.

Os analistas de segurança obtêm informações sobre como as ferramentas de segurança estão implantadas e cobrem seus ativos com base em seu inventário de ativos e dados importados de conectores do Service Graph e produtos da ServiceNow, como Gestão de ativos de hardware (HAM) e ITOM Descoberta.

Versão de lançamento	Notas de versão
Núcleo de controle de posturas de segurança v4.0, v3.0, v2.0, v1.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão Notas de versão Controle de posturas de segurança
Gestão de posturas de segurança para ativos v4.0. v3.0, v2.0, v1.0	

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

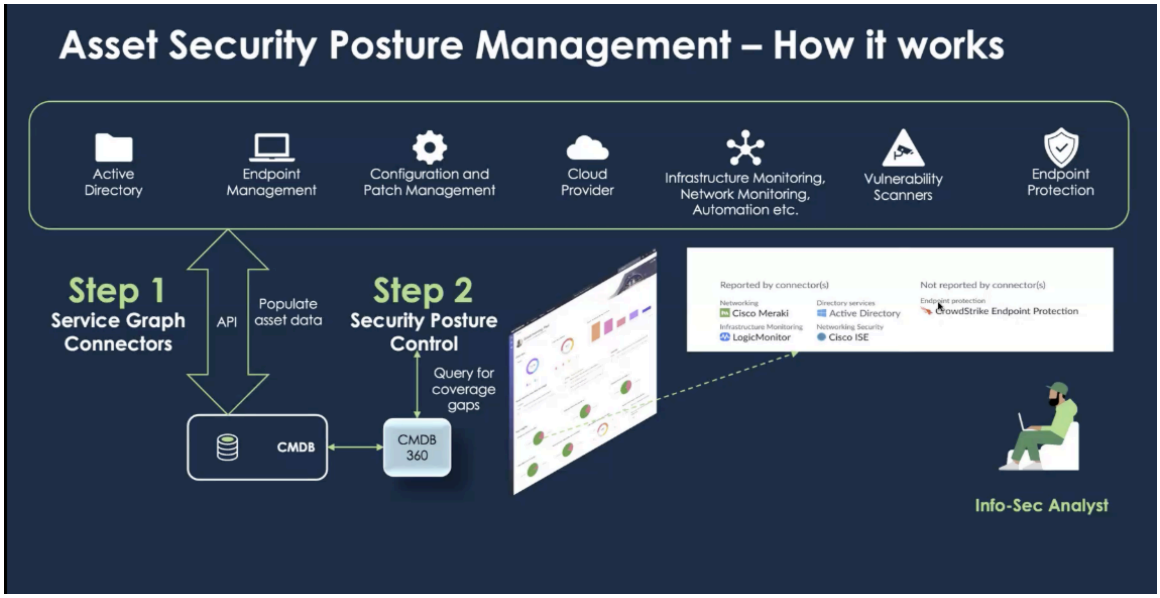
Com o produto SPC, as equipes de segurança da informação podem executar as seguintes tarefas:

- Monitore seus ativos quanto à conformidade com os padrões de configuração da ferramenta de segurança interna. Por exemplo, certifique-se de que a versão mais recente de um produto de proteção de endpoint esteja sendo usada.
- Automatize o fluxo de trabalho de correção das lacunas de postura de segurança que você encontrar com a aplicação ServiceNow Configuration Compliance.
- Crie políticas e informações personalizadas com base em metadados de ativos, dados de cobertura da ferramenta de segurança e dados de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como o Gestão de posturas de segurança para ativos funciona



A Gestão de posturas de segurança de ativos (ASPM) identifica lacunas na cobertura da ferramenta de segurança em ativos usando integrações de API com várias ferramentas de terceiros (Conectores do Service Graph) junto com os produtos da ServiceNow.

Gestão de posturas de segurança para ativos identifica lacunas de cobertura da ferramenta de segurança em ativos usando integrações de API com várias ferramentas (Conectores do Service Graph) e produtos da ServiceNow. As categorias incluem, entre outras, as seguintes:

- Experiência do Funcionário Digital
- Descoberta
- Gestão de endpoint
- IT Asset Management
- Monitoramento de infraestrutura
- Rede
- Segurança de rede
- Monitoramento de desempenho de rede
- Gestão de configurações e patches
- Proteção de endpoint
- Provedor de nuvem
- Monitoramento de desempenho da aplicação
- Serviços de diretório
- Avaliação de vulnerabilidade

Instalar as aplicações compatíveis com o Controle de posturas de segurança

As aplicações necessárias para esta integração estão disponíveis no ServiceNow Store. Algumas aplicações têm dependências que você deve baixar e instalar separadamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador para download, instalação e ativação de todas as aplicações.

Procedimento

1. Baixe as aplicações necessárias de ServiceNow Store para sua instância ServiceNow.
2. Depois de baixar as aplicações, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
3. Localize as aplicações que você baixou e selecione **Instalar** para ativá-las junto com suas dependências.
   Todas as aplicações de dependência que também são instaladas automaticamente junto com uma aplicação são exibidas na caixa de diálogo de instalação da aplicação. No entanto, se você for solicitado a instalar plug-ins de dependência durante a instalação, siga os avisos fornecidos. Verifique se você tem todas as aplicações e dependências listadas na tabela anterior instaladas e ativadas.

   Uma caixa de diálogo é exibida depois que uma aplicação é ativada com sucesso.
4. Depois de instalar e ativar as aplicações, atribua usuários aos seguintes grupos de controle de posturas de segurança:

   Esses grupos herdam todas as funções necessárias para ler e editar registros SPC.
5. Modifique a reconciliação e recalcule as fontes de dados do CMDB para definir a origem de verdade dos valores de atributo.

   O painel do CMDB 360 fornece agregações e análises de dados do CMDB 360. O CMDB 360 coleta dados sobre todas as origens de descoberta que relatam valores de atributo para ICs. Use a exibição do CMDB 360 no Espaço do Configuration Management Database (CMDB) para rastrear atividades e identificar possíveis problemas de origens de descoberta. Para obter mais informações, consulte Exibição do CMDB 360 no Espaço do CMDB .

Conectores do Service Graph para Controle de posturas de segurança

Controle de posturas de segurança O conta com integrações de API ou Conectores do Service Graph como uma fonte de chave para os dados de ativos usados para identificar lacunas de segurança.

Controle de posturas de segurança atualmente, o é compatível com Conectores do Service Graph (SGC) que podem fornecer uma ampla variedade de dados sobre seus ativos. Esses aplicativos de integração estão disponíveis no ServiceNow Store.

Escolha os conectores que deseja usar, baixe as aplicações e ative-as. A lista de conectores compatíveis na Store aumentará conforme Controle de posturas de segurança oferecer suporte a mais conectores.

Os conectores do Service Graph compatíveis com Controle de posturas de segurança incluem atualmente as seguintes categorias:

Depois de instalá-los, você pode exibir os conectores e suas categorias na tabela de conectores [sn_sec_spc_core_connector] em sua instância.

Você pode exibir os tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Conectores do Service Graph de hardware compatíveis para Controle de posturas de segurança e Conectores do Software Service Graph compatíveis para Controle de posturas de segurança para obter mais informações e exemplos dessas tabelas. Embora não sejam listas extensas, você pode ver como os conectores compatíveis fornecem uma ampla variedade de dados.

Controle de posturas de segurança é compatível com produtos da ServiceNow, como Software Asset Management (SAM) e Gestão de ativos de hardware (HAM), que você pode usar junto com conectores do Service Graph para ajudá-lo a procurar discrepâncias existentes entre o software instalado relatado por seus produtos de scanner de vulnerabilidade e o software relatado por scanners que já é contabilizado no SAM e em outros produtos da ServiceNow.

Para obter mais informações sobre como baixar, configurar e ativar aplicações compatíveis com conectores do Service Graph, consulte os seguintes tópicos:

- Conectores do Service Graph .
- .
- .

Políticas para Controle de posturas de segurança

As políticas auditam seus ativos com base nos dados importados dos conectores do Service Graph para ajudá-lo a encontrar possíveis violações.

Políticas

Controle de posturas de segurança As políticas são criadas em um modelo de dados asset-relationships-properties. Há políticas incluídas na aplicação e você pode criar suas próprias políticas para procurar critérios específicos.

Os critérios para políticas podem ser especificados na forma de condições nas propriedades desse ativo ou nas propriedades de uma entidade relacionada. No construtor de políticas no módulo Política e descobertas no espaço, você pode definir políticas para procurar um tipo de ativo (Hardware, Software) e uma Conexão (Relatado por, Não relatado por) ou uma Entidade (Origem do ativo, gráfico de serviço produto do conector ou metadados do CMDB), ou você pode corresponder a outros tipos de critérios específicos.

Para ajudá-lo a modificar ou criar políticas:

- Defina suas condições no módulo Pesquisa de ativos e pesquise ativos por produtos específicos do conector do Service Graph ou ativos que tenham dados específicos relatados por um conector. Você pode salvar suas pesquisas como políticas.
- Clone as políticas incluídas na aplicação para criar políticas mais expansivas. Você copia e refina as condições de uma política existente sem precisar inseri-las novamente.
- Crie novas políticas (políticas secundárias) usando as políticas de base selecionadas como ponto de partida para novas políticas.

Exemplo de preenchimento de dados e auditoria de política: classes de IC no CMDB

Se uma política tentar recuperar uma classe de ativo relatada ou não relatada por um Conector do Service Graph específico, o Controle de postura de segurança mapeará todas as classes de item de configuração (IC) relevantes que estão relacionadas a essa classe de ativo no CMDB que são preenchidas ou não preenchido por esse Conector do Service Graph ou Categoria de conector.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, digamos que uma política procure todos os ativos de hardware relatados pelo Jamf Pro do Conector do Service Graph. A lógica a seguir se aplica.

1. O controle de postura de segurança identifica quais classes de IC no CMDB estão mapeadas para a classe "Ativo de hardware" do Jamf Pro.

   Nota: Conectores do Service Graph diferentes preenchem classes de IC diferentes no CMDB e o mapeamento para classes de IC de "Ativo de hardware" varia de um Conector do Service Graph para outro.

2. Controle de posturas de segurança determina que as classes de IC Computador, Servidor e Impressora no CMDB são mapeadas para a classe de ativo "Ativo de hardware" do Jamf Pro do Conector do Service Graph.
3. Controle de posturas de segurança em seguida, consulta todos os registros de ativos preenchidos em qualquer uma destas três classes de IC: Servidor, Computador e Impressora pelo Conector do Service Graph para Jamf Pro no CMDB e retorna esses ativos.

   A coluna "Classes de IC compatíveis com SPC" na tabela a seguir indica quais classes de registros de IC são consideradas durante uma consulta pelo produto Controle de posturas de segurança como parte de uma avaliação de política. Esta tabela não é uma lista abrangente, mas você pode usá-la para ver como os dados ingeridos de várias categorias e origens geralmente são mapeados e consultados.

Como criar suas próprias políticas

Consulte Como criar suas próprias políticas na aplicação Controle de posturas de segurança para obter mais informações sobre como criar suas próprias políticas.

Para obter exemplos de políticas, consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança.

Consulte Criar e ativar políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

SGCs compatíveis

Para obter uma lista de alguns dos conectores do Service Graph compatíveis, consulte Conectores do Service Graph de hardware compatíveis para Controle de posturas de segurança e Conectores do Software Service Graph compatíveis para Controle de posturas de segurança.

Políticas incluídas com a aplicação Controle de posturas de segurança

Existem algumas políticas incluídas com a aplicação Controle de posturas de segurança que estão vinculadas a casos de uso importantes e são mostradas como informações importantes no painel da página principal (módulo inicial) no Espaço do SPC.

Exibição de políticas

Para exibir essas políticas, navegue até **Espaços** > **Controle de posturas de segurança** > **Políticas e descobertas** > **Todos**.

Essas políticas são desativadas por padrão. Você deve ativá-los para poder exibir os resultados retornados (Descobertas). Você não pode editar essas políticas, mas pode usá-las para ajudá-lo a criar outras políticas clonando suas condições como ponto de partida. Para obter mais informações, consulte Clonar uma política ou criar uma política secundária em Controle de posturas de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode configurar informações ou relatórios personalizados para as políticas clonadas ou, como alternativa, configurar descobertas para essas políticas clonadas para gerenciar a correção. Você também pode criar suas próprias políticas personalizadas a partir do zero para monitorar a cobertura dos controles de segurança de acordo com seus requisitos internos.

Depois de clonar e ativar todas as políticas criadas, você deve criar seu próprio registro de informações personalizadas no módulo Construtor de informações personalizadas no espaço (o último módulo no painel do navegador). Somente então você pode exibir os dados de suas políticas no painel de informações personalizadas (o segundo ícone a partir da parte superior no espaço).

Como criar suas próprias políticas

Consulte Como criar suas próprias políticas na aplicação Controle de posturas de segurança para obter mais informações sobre como criar suas próprias políticas.

Para obter exemplos de políticas, consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança.

Consulte Criar e ativar políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

Como criar suas próprias políticas na aplicação Controle de posturas de segurança

Você pode criar suas próprias políticas personalizadas para monitorar dados específicos dos ativos em seu ambiente. Você baseia essas políticas nos dados que importará dos vários Conectores do Service Graph instalados e ativados.

Como começar

Você pode clonar as políticas existentes e adicionar mais condições a elas ou criar uma política do zero. Para suas políticas personalizadas, você pode incluir critérios para propriedades comuns do CMDB preenchidas por vários Conectores do Service Graph.

Como alternativa, você pode usar uma política de base como ponto de partida e incluir condições para exceções aprovadas com políticas para a aplicação de Governança, risco e conformidade (GRC), por exemplo. Essas exceções são para ativos que você não deseja monitorar e incluir em suas contagens de ativos.

Para suas políticas personalizadas, você pode incluir condições para metadados, como SO, versão do SO e FQDN, por exemplo, para ajudá-lo a monitorar ativos com software mais antigo. Observe que essas propriedades são propriedades comuns do CMDB preenchidas por vários Conectores do Service Graph para um determinado ativo.

Consulte Políticas incluídas com a aplicação Controle de posturas de segurança para obter mais informações sobre os tipos de ativo de nível superior e seus relacionamentos no construtor de condições de política para suas políticas.

Para obter exemplos de políticas, consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança.

Consulte Criar e ativar políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

Como usar os decoradores AND, OR no construtor de condições

Você navega dos tipos de ativos de nível superior para hardware e software para suas entidades secundárias usando o construtor de condições no módulo Políticas e descobertas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

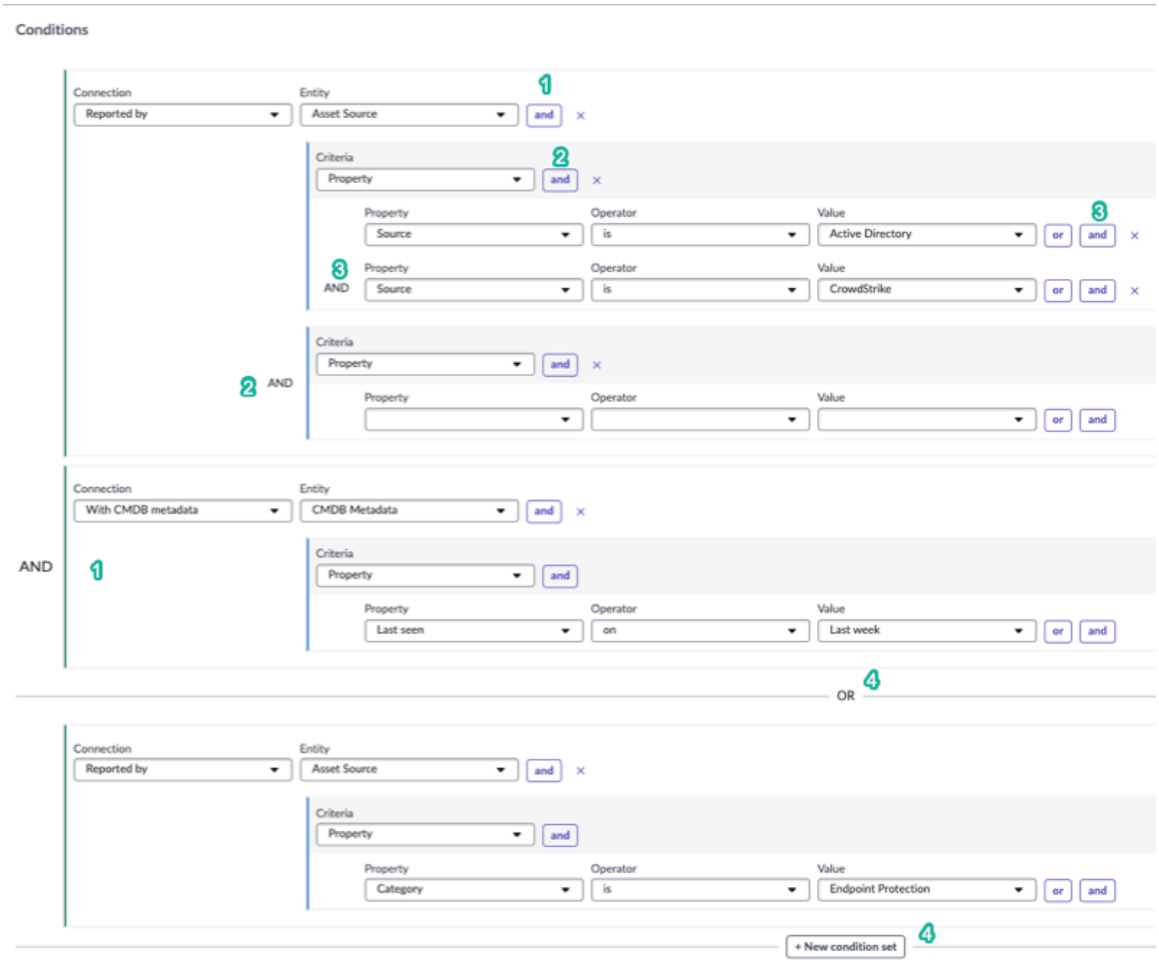
no espaço. Dependendo das suas escolhas, os campos são exibidos para você e você modifica ou adiciona critérios.

Os decoradores AND, OR no construtor de condições permitem que você configure a lógica dos dados retornados que deseja retornar para a política.

Decorador	Descrição	Número referenciado na imagem
Selecione **E** ao lado dos campos Conexão e Entidade mais altos para o novo conjunto de condições.	Adiciona um E lógico entre os critérios atuais da Entidade de conexão e novos critérios de outra Entidade de conexão.	1
Selecione **E** à direita de um campo Critérios ou Propriedade para o novo conjunto de condições de Critérios e Propriedade.	Adiciona um AND lógico entre os critérios atuais de entidade de conexão e um novo critério na mesma entidade de conexão.	2
Selecione **OU/E** à direita de um campo de propriedade para o novo conjunto de condições de propriedade.	Adiciona um OR/AND lógico entre a propriedade atual e uma nova propriedade dos mesmos critérios de entidade de conexão.	3
Selecione **+ Novo conjunto de condições** para um novo conjunto de condições.	Adiciona um OU lógico entre o Conjunto de condições de todos os critérios atuais e um novo Conjunto de condições.	4

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Uso de políticas de base, clonagem e políticas secundárias

Você pode usar várias políticas para avaliar seus ativos e criar suas próprias informações personalizadas. Você tem as seguintes opções para ajudá-lo a criar políticas personalizadas ou editar políticas existentes rapidamente:

- Clonar política - Crie uma cópia de uma política. O nome da política e suas condições são exibidos com uma "cópia" no título. As condições são exibidas e você pode editá-las. Consulte Editar uma política ativada no Controle de posturas de segurança.
- Criar política secundária - O nome da política a partir da qual você iniciou é exibido como a "Política de base" no novo registro. As condições da sua política de base são herdadas na nova política e um novo conjunto de condições vazio é exibido. Consulte Clonar uma política ou criar uma política secundária em Controle de posturas de segurança.
- Políticas de exclusão – adicione políticas às suas políticas personalizadas para que as descobertas de ativos das políticas selecionadas sejam excluídas dos resultados. Consulte Criar e ativar políticas personalizadas para Controle de posturas de segurança.

Filtragem de metadados e CMDB

Pode ser importante para suas equipes de segurança monitorar ativos com software mais antigo. Você pode especificar critérios de política começando com a Conexão "Com metadados do CMDB" após o tipo de Ativo de hardware para incluir as propriedades comuns listadas abaixo. Esta não é uma lista com tudo incluído. Para coletar esses metadados, as propriedades devem estar disponíveis na conexão de metadados do CMDB preenchida pelos conectores do Service Graph.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- RAM
- Nome do host
- Número de série
- Domínio do SO
- Versão do SO
- Espaço em disco
- Visto pela última vez
- SO
- Visto pela primeira vez
- Contagem de CPUs
- Fabricante do MAC
- NIC
- Endereço IP
- Local
- FQDN
- Máscara de rede
- Versão do IP
- Tipo de Número de Série
- Service pack do SO

A partir da v3.0 de Controle de posturas de segurança:

A conexão "Com metadados do CMDB" permite que você adicione a propriedade do nome do host e use o operador regex de correspondências para ajudá-lo a digitar expressões regulares em suas condições para o tipo de ativo de hardware. Por exemplo, se você inserir 'lp', poderá procurar todos os laptops com 'lp' como o segundo e o terceiro caracteres no nome do host.

"Visto pela primeira vez": ativos que foram descobertos pela primeira vez por qualquer origem dentro do intervalo de tempo selecionado com a propriedade de carimbo de data/hora "Visto pela primeira vez".

"Vistos pela última vez": ativos que foram "vistos pela última vez nos últimos n dias" por qualquer origem. Insira o número de dias até 30 como um Valor. Por exemplo, insira 3 como um Valor para monitorar ativos por "último logon" do Active Directory nos últimos três dias.

Tipo de ativo de software: procure fornecedores de software ou use SGCs instalados para importar os dados e metadados de software desejados se você começar com a conexão "Com detalhes do software".

Para tipos de ativos de hardware, você pode usar a conexão "Tem informações de modelo" com a conexão "Com metadados do CMDB" para dispositivos baseados em modelos e informações de modelo específicos.

Os tipos de ativos de hardware também permitem que você pesquise todos os ativos relatados por uma origem, Qualys, por exemplo, mas que não são relatados pela Descoberta do ITOM da ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Políticas para Controle de posturas de segurança para obter mais informações sobre o esquema de política Controle de posturas de segurança.

Exceções com a aplicação de Governança, risco e conformidade (GRC)

Uma exceção da Gestão integrada de riscos (IRM) é um ativo com uma exceção aprovada do produto de Governança, risco e conformidade (GRC). Você tem a opção em uma política de adicionar uma condição para uma exceção para não monitorar esses ativos e incluí-los em suas contagens.

Por exemplo, alguns ativos podem ter exceções aprovadas para determinados objetivos de controle com IRM. Para reduzir as correspondências retornadas, as equipes de segurança da informação podem excluir esses ativos do monitoramento de controles de segurança com exceções de IRM que já foram aprovadas.

Informações principais e informações configuradas para Controle de posturas de segurança

As informações principais e configuradas (personalizadas) fornecem relatórios visuais que são criados e atualizados pelos critérios de avaliação que correspondem aos seus ativos. As informações ajudam a monitorar as métricas de controles de segurança em um painel.

Informações principais

Os critérios usados para as avaliações de seus ativos são fornecidos pelas políticas incluídas na aplicação.

- As informações principais usam as políticas incluídas na aplicação.
- As informações configuradas podem ser criadas usando as políticas incluídas na aplicação, suas próprias políticas personalizadas ou uma combinação de ambas.

Na página inicial (página principal) do espaço do Controle de posturas de segurança, a seção Informações principais abaixo da Visão geral exibe relatórios visuais que são criados e atualizados pelas políticas incluídas na aplicação. Essas informações também estão incluídas na aplicação e exibem as seguintes informações:

- Agente de proteção de endpoint instalado: número total de ativos que têm ou não proteção de endpoint.
- Cobertura de dispositivo gerenciado: número de ativos gerenciados em comparação com aqueles que não são gerenciados.
- Cobertura de verificação de vulnerabilidades: número total de ativos verificados em comparação com aqueles que não são verificados quanto a vulnerabilidades conhecidas por um scanner de vulnerabilidade de terceiros.
- Ativos com vulnerabilidades críticas: número de ativos do número total de ativos que têm vulnerabilidades críticas.
- Itens vulneráveis por criticidade: número total de itens vulneráveis divididos por gravidade. Uma vulnerabilidade conhecida que corresponde a um ativo no seu CMDB resulta em um item vulnerável. Esta informação requer que você instale a aplicação Resposta a vulnerabilidades e pelo menos uma integração de scanner: Qualys, Rapid7 ou Tenable Vulnerability Integration. Todas essas aplicações estão disponíveis no ServiceNow® Store.
- 3 principais políticas por descobertas: políticas que retornam o maior número de descobertas (correspondências) em seus ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações configuradas

Você pode criar suas próprias informações se quiser mais informações não encontradas nas principais informações. Você pode criar essas informações configuradas e usar as políticas existentes ou suas próprias políticas personalizadas para avaliação. Suas informações configuradas são exibidas no módulo do painel Informações configuradas, o segundo ícone a partir da parte superior no espaço.

Os seguintes tipos de informações podem ser configurados.

- Gráfico de comparação: compare os resultados entre várias políticas com gráficos de barras.
- Widget de contagem de correspondência de política: exibe o número de dispositivos que correspondem a uma política.
- Gráfico de porcentagem de correspondência de política: exibe a porcentagem de dispositivos que correspondem a uma política em um gráfico de pizza. Você pode escolher o grupo de ativos total como todos os ativos monitorados pelo SPC ou os ativos que correspondem à política base a partir da qual a política selecionada atual é criada.
- Gráfico de tendências de política: exibe as tendências de ativos que correspondem a várias políticas.

Grupos

Você deve criar ou atribuir grupos às informações configuradas ao criar novos registros no módulo do Construtor de informações personalizadas. Os grupos permitem que você organize seus relatórios no painel Informações configuradas.

Usando o espaço Controle de posturas de segurança

O espaço Controle de posturas de segurança contém os módulos que você usa para configurar, usar e monitorar os dados importados sobre seus ativos.

Os módulos do espaço

Para acessar o espaço, navegue até **Espaços** > **Controle de posturas de segurança** A página inicial (página principal) é exibida. O espaço Controle de posturas de segurança contém os seguintes módulos.

Módulos

Módulo	Descrição
Página inicial	Exiba visualizações de dados e outras informações nas seções Visão geral, Informações principais e Cobertura de caso de uso principal para ajudá-lo a monitorar seus ativos. As informações fornecidas nesta página permitem que você relate o status de sua postura geral de segurança para TI, gerentes de TI e segurança e outras partes interessadas importantes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos

Módulo	Descrição
	Consulte Informações principais e informações configuradas para Controle de posturas de segurança e Políticas para Controle de posturas de segurança.
Informações configuradas	Veja as visualizações de dados sobre os ativos que você cria, configura e ativa. Consulte Informações principais e informações configuradas para Controle de posturas de segurança.
Pesquisa de ativos	Pesquise rapidamente ativos em seu ambiente com base nas condições definidas. Verifique se você pode localizar ativos com um conjunto de condições antes de confirmar essas condições para uma política. Você pode refinar essas pesquisas para obter uma visualização dos ativos que atendem aos seus critérios de pesquisa. Quando estiver pronto, você poderá salvar suas condições como uma política. Consulte Criar uma pesquisa de ativos no Controle de posturas de segurança.
Políticas e descobertas	Criar, clonar, editar e ativar políticas. Há políticas incluídas na aplicação e você pode criar as suas próprias. As políticas auditam seus ativos para encontrar correspondências para possíveis violações. Informações, visualizações e casos de uso dependem de políticas. Consulte Políticas para Controle de posturas de segurança. Os ativos que correspondem às condições da política são relatados como Descobertas e são mapeados para a aplicação Conformidade de configurações para correção. Consulte Exibir descobertas para Controle de posturas de segurança.
Configuração de conectores e casos de uso	Ativar e exibir o status dos conectores do Service Graph (SGC) instalados e integrações de API. Os Conectores do Service Graph e as integrações de API são origens que você usa para importar dados sobre seus ativos. Uma grande variedade de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos

Módulo	Descrição
	(SGCs) são compatíveis e estão disponíveis no ServiceNow® Store. Configure e monitore os principais casos de uso. Casos de uso são diferentes cenários que você configura para ajudá-lo a identificar tipos específicos de lacunas de cobertura da ferramenta. Cada caso de uso requer uma política ou políticas para auditar seus ativos quanto a possíveis violações. Consulte Casos de uso, exemplos de política e conectores do Service Graph compatíveis no Controle de posturas de segurança.
Construtor de informações personalizadas	Crie suas próprias visualizações de dados. As informações personalizadas fornecem relatórios visuais que são atualizados pelos resultados de auditoria de suas políticas e dados importados. Depois de ativá-los, suas informações personalizadas serão exibidas no painel do módulo Informações configuradas. Você pode determinar onde os dados de uma informação são exibidos no painel usando Grupos. Consulte Criar e ativar uma informação configurada para o Controle de posturas de segurança.

Usando os módulos do espaço para identificar lacunas na cobertura da ferramenta

A identificação de lacunas na ferramenta de segurança requer que você execute as etapas a seguir.

1. Configure e ative conexões de API com qualquer uma das ferramentas que você está usando em várias categorias. Você pode usar Conectores do Service Graph para produtos que estão disponíveis na ServiceNow Store para as conexões de API necessárias. Para obter mais informações sobre os conectores do Service Graph compatíveis, consulte Conectores do Service Graph para Controle de posturas de segurança e Conectores do Service Graph . Os conectores do Service Graph compatíveis estão disponíveis no ServiceNow® Store com assinaturas separadas.
2. Execute uma ou mais pesquisas de ativos com base em critérios específicos para obter um inventário.
3. Ative as políticas enviadas com a aplicação Controle de posturas de segurança. Você também pode criar suas próprias políticas e ativá-las com base nos resultados de suas pesquisas de ativos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Crie e ative suas próprias informações configuradas para ajudá-lo a monitorar seus ativos.
5. Configure regras para automatizar o fluxo de trabalho de correção na aplicação Conformidade de configuração.

A identificação de lacunas na ferramenta de segurança envolve as seguintes etapas:

1. Ative as políticas enviadas com a aplicação Controle de posturas de segurança.
   O produto Controle de posturas de segurança encontra lacunas na ferramenta de segurança executando as seguintes tarefas:
   a. Identifica a lista de todos os ativos exclusivos preenchidos por vários Conectores do Service Graph no CMDB.
   b. Identifica ativos que não são relatados por categorias específicas deste grupo de ativos, por exemplo, Proteção de endpoint. Os ativos são identificados com base na política ativa que está sendo avaliada.
   c. Ativos identificados como não relatados por categorias específicas são relatados como "Descobertas" ou "Resultados de testes" na aplicação Conformidade de configurações.
2. Atribua automaticamente "Descobertas" a diferentes equipes para correção com a aplicação Conformidade de configuração.

Como criar suas próprias políticas

Consulte Como criar suas próprias políticas na aplicação Controle de posturas de segurança para obter mais informações sobre como criar suas próprias políticas.

Consulte Criar e ativar políticas personalizadas para Controle de posturas de segurança para obter mais informações sobre as etapas necessárias para criar uma política.

Para obter exemplos de políticas, consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança.

Ativar uma política incluída com a aplicação Controle de posturas de segurança

As políticas incluídas com a aplicação devem ser ativadas antes que Controle de posturas de segurança possa monitorar os ativos que correspondem a essa política. Por padrão, nenhuma das políticas incluídas com a aplicação está ativada.

Antes de Iniciar

Você deve verificar se todos os pré-requisitos necessários foram atendidos antes de ativar as políticas incluídas na aplicação.

- Verifique se os Conectores do Service Graph necessários estão ativados.
- Verifique se todas as aplicações necessárias, como a Resposta a vulnerabilidades, estão instaladas e ativadas, se aplicável.

Nota:

Você não pode editar as políticas incluídas na aplicação, mas pode criar novas políticas com base em seus critérios com os recursos **Clonar política** e **Criar política** secundária. Esses recursos estão disponíveis no menu Mais opções (três pontos verticais).

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Políticas e descobertas** > **Todos**.

   Para determinar se uma política está ativada, confirme seu status (`verdadeiro` ou `falso`) na coluna Ativa.

2. Selecione um registro de política para abri-lo.
3. Você tem as seguintes opções em registros de política que estão incluídos com a aplicação:

Opção	Descrição
Ativar política	Ative uma política se quiser monitorar todos os ativos que correspondem às condições da política e gerar descobertas. Se disponível, selecione Desativar política para interromper as avaliações de ativos e a geração de descobertas para esta política.
Configurar descobertas	Selecione **Sim** no modal para gerar descobertas para a política. Selecione o link **Configurar regras de atribuição** para configurar regras de atribuição na aplicação Conformidade de configuração para atribuir quaisquer descobertas da sua política para resolução. **Nota:** Para políticas criadas com "Software" como o tipo de ativo, você pode salvar a política e criar informações personalizadas, mas não pode configurar as descobertas do registro de política.
Clonar política	Crie uma nova política com todas as condições da política exibida como ponto de partida. Para obter mais informações, consulte Criar e ativar políticas personalizadas para Controle de posturas de segurança.
Criar uma política secundária	Crie uma política secundária que herde as condições da política atual. As condições da política atual são exibidas no campo "Política de base" no novo registro e você adiciona mais condições.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Desativar política (exibido somente em políticas ativadas)	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em relação a essa política. Esta opção de edição só está visível em registros de apólice ativados.
Exibir descobertas	Abra uma nova guia e exiba os ativos correspondentes, se disponíveis. As descobertas também são chamadas de CTRs ou registros de resultados de testes para a política.

Criar e ativar políticas personalizadas para Controle de posturas de segurança

Crie suas próprias políticas personalizadas para monitorar ativos quanto à cobertura da ferramenta e outras combinações de alto risco.

Antes de Iniciar

Para ajudá-lo a entender as etapas necessárias para criar uma política com mais detalhes, consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança. Os exemplos orientam você nas etapas necessárias para criar uma política de base, usar a política de base para criar uma política secundária e clonar uma política.

Para obter exemplos de políticas, consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Todos**.
2. Selecione **Nova política**.
3. Selecione o ícone de lápis ao lado do nome na parte superior para modificar os metadados.

   Preencha os campos.

Campo	Descrição
Nome	Um nome exclusivo para sua política.
Criticidade	Selecione um na lista.
Descrição resumida	Uma descrição exclusiva para sua apólice.

4. Selecione **Salvar metadados**.
5. Para Tipo de ativo, selecione na lista.

Opção de entidade	Descrição da entidade
Hardware	Localize dispositivos IP que incluem dispositivos de computação pessoal, máquinas virtuais em nuvem, servidores, dispositivos de rede e outro hardware.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção de entidade	Descrição da entidade
Software	Localize o software instalado em dispositivos relatados por de SGCs e seus scanners de vulnerabilidade.

6. Opcional: Escolha nenhum, um ou ambos.

Opção	Descrição
Política de base	As condições da sua opção de política de base são herdadas na nova política.
Políticas de exclusão	Selecione as políticas que você deseja excluir das descobertas de ativos para esta política. Todas as descobertas dessas políticas são ignoradas.

(Optional) Os campos Conexão e Entidade são exibidos.

7. Selecione um na lista para o campo Conexão.
O campo Entidade de destino é preenchido automaticamente com base em sua escolha. Um novo campo Critérios é exibido junto com os campos Propriedade, Operador e Valor. Para obter mais informações sobre os tipos de ativos e o esquema para relacionamentos, consulte Políticas para Controle de posturas de segurança.
8. Selecione um na lista para Propriedade.
9. Selecione **Categoria** ou **Origem**.
10. Selecione um operador e insira uma categoria de conector, por exemplo, Gestão de endpoint, ou um nome de produto de categoria (origem).
11. Opcional: Use o construtor de condições e adicione mais condições ou conjuntos de condições.

    (Optional) Você navega dos tipos de ativos de nível superior para hardware e software para suas entidades secundárias usando o Construtor de condições. Dependendo das suas escolhas, os campos são exibidos para você e você modifica ou adiciona critérios.

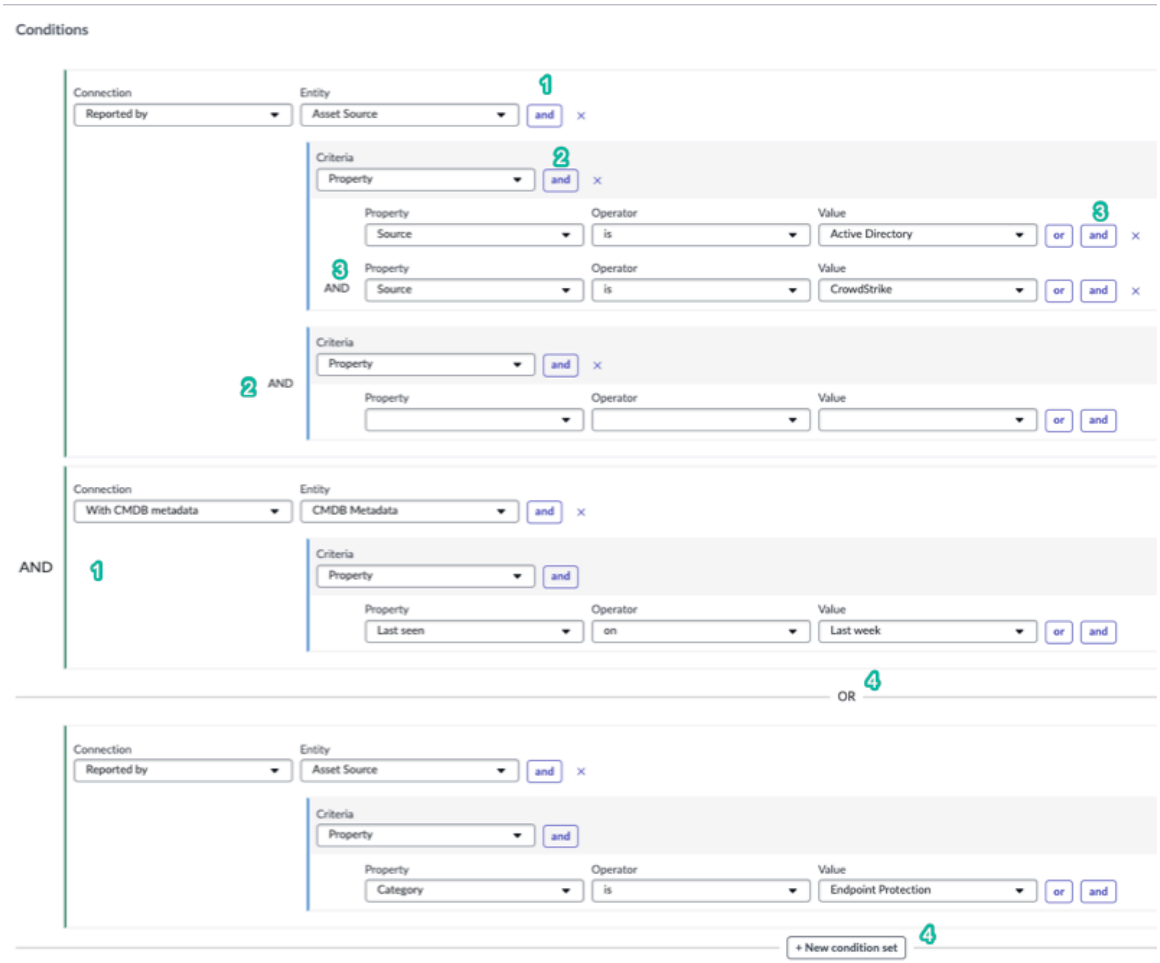
    Os decoradores AND, OR no construtor de condições permitem que você configure a lógica dos dados retornados que deseja retornar para a política. Consulte a tabela e a imagem a seguir para obter mais informações.

Decorador	Descrição	Número referenciado na imagem
Selecione **E** ao lado dos campos Conexão e Entidade mais altos para o novo conjunto de condições.	Adiciona um E lógico entre os critérios atuais da Entidade de conexão e novos critérios de outra Entidade de conexão.	1
Selecione **E** à direita de um campo Critérios ou Propriedade para o novo conjunto de condições de Critérios e Propriedade.	Adiciona um AND lógico entre os critérios atuais de entidade de conexão e um novo critério na mesma entidade de conexão.	2

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Decorador	Descrição	Número referenciado na imagem
Selecione **OU/E** à direita de um campo de propriedade para o novo conjunto de condições de propriedade.	Adiciona um OR/AND lógico entre a propriedade atual e uma nova propriedade dos mesmos critérios de entidade de conexão.	3
Selecione **+ Novo conjunto de condições** para um novo conjunto de condições.	Adiciona um OU lógico entre o Conjunto de condições de todos os critérios atuais e um novo Conjunto de condições.	4



12. Selecione **Salvar política** quando terminar de editar.
    Sua política foi salva. Você pode optar por ativá-lo agora ou retornar mais tarde para ativá-lo.
13. No menu mais opções ao lado de **Salvar política**, selecione Configurar descobertas.
14. Preencha os campos.

Opção	Descrição
Gerar descobertas para esta política?	Escolha **Sim** para gerar descobertas para ativos correspondentes. Depois que os

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	dados forem importados, selecione Exibir descobertas é exibido no registro de política. Escolha **Não** se você não quiser gerar descobertas.
Configurar regras de atribuição	Selecione o link para configurar regras de atribuição para atribuir descobertas para correção na aplicação Conformidade de configurações. Há uma regra de atribuição padrão na tabela [sn_vulc_assignment_rule_list] que você pode usar no Configuration Compliance.

15. Selecione **Salvar configuração**.

    Depois de salvar e ativar uma política, ela avalia os dados importados do conector do Service Graph programado na próxima execução. Se você quiser exibir os dados no painel Informações configuradas no espaço, deverá criar uma Nova informação no módulo do Construtor de informações personalizadas. Depois de ativar a informação configurada, seus dados são exibidos no painel Informações configuradas no espaço.

Editar uma política ativada no Controle de posturas de segurança

Você pode editar as políticas ativadas para ajudá-lo a personalizar suas condições para melhor corresponder aos seus ativos.

Antes de Iniciar

Você não pode editar as políticas incluídas na aplicação, mas pode clonar e criar políticas secundárias a partir delas. Consulte Clonar uma política ou criar uma política secundária em Controle de posturas de segurança.

Se você editar políticas e publicar suas mudanças, as versões serão rastreadas e os números de versão serão exibidos no registro da política e nos resultados de testes relacionados.

Antes de editar uma política ativada, talvez você prefira desativá-la para que a política não continue a avaliar seus ativos enquanto você edita.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Todos**.
2. Selecione um registro de política para abri-lo.
3. Selecione **Editar política**.
   Se você estiver editando pela primeira vez, dois botões desativados serão exibidos ao lado do botão ativo **Sair do modo de edição** : **Salvar mudanças** e **Publicar mudanças**.
   Se você já editou esta política e a salvou como rascunho, a notificação `Você tem uma edição não publicada` também será exibida.
4. Faça suas edições e escolha uma para continuar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Salvar mudanças	Salve suas mudanças como rascunho e retorne ao modo de edição. Suas mudanças não estão publicadas neste ponto e você pode retornar à política e continuar editando mais tarde.
Publicar mudanças	Publique suas mudanças como uma nova versão da política e saia automaticamente do modo de edição. Pode levar algum tempo para que as descobertas sejam exibidas em sua nova versão da política no botão Exibir descobertas na política. Se você publicar uma nova versão de uma política, terá a opção de fechar todas as descobertas existentes da política que alterou. Você pode preferir fechar todas as descobertas existentes da política original se quiser apenas exibir as descobertas da política alterada. Se você cancelar neste ponto ou sair do modo de edição, será exibida uma mensagem informando que você tem uma edição não publicada para esta política. Se você optar por fechar os resultados de testes relacionados existentes (descobertas), os estados do resultado de testes e da tarefa de correção farão a transição de acordo com os processos de transição de estado da aplicação Conformidade de configurações. Para obter mais informações, consulte Resultados de testes e transições de estado da tarefa de correção na aplicação Controle de posturas de segurança.
Exibir histórico de versões	Para mudanças publicadas, as versões são rastreadas e os números de versão são exibidos no registro da política e nos resultados de testes relacionados.
Sair do modo de edição	Saia sem salvar suas mudanças ou salve suas mudanças e saia sem publicar. Se você salvar suas mudanças e não publicá-las, deverá publicar sua nova versão antes que ela possa criar descobertas.
Desativar política (exibido somente em políticas ativadas)	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em relação a essa política.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Esta opção de edição só está visível em registros de apólice ativa.
Exibir descobertas	Abra uma nova guia e exiba os ativos correspondentes, se disponíveis. As descobertas também são chamadas de CTRs ou registros de resultados de testes da política.

5. Depois de salvar a política como rascunho e sair do modo de edição, selecione uma das seguintes opções:

Opção	Descrição
Editar política	Retorne ao modo de edição.
Desativar política (exibido somente em políticas ativadas)	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em relação a essa política. Esta opção só está visível em registros de apólice ativa.
Menu de mais opções	
Configurar descobertas	Selecione **Sim** no modal para gerar descobertas para a política. Consulte Exibir descobertas para Controle de posturas de segurança.
Clonar política	Crie uma cópia do registro de política. Consulte Clonar uma política ou criar uma política secundária em Controle de posturas de segurança.
Criar política secundária	Crie uma nova política usando esta política como base. Consulte Clonar uma política ou criar uma política secundária em Controle de posturas de segurança.
Excluir política	Remova o registro de política da lista de políticas.
Exibir descobertas	Abra uma nova guia e exiba os ativos correspondentes, se disponíveis. As descobertas também são referenciadas para registros de resultados de testes (CTRs) da política.
Exibir registros vinculados	Para políticas publicadas, exiba as informações personalizadas, se disponíveis. Veja Criar e ativar uma informação configurada para o Controle de posturas de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clonar uma política ou criar uma política secundária em Controle de posturas de segurança

Clone uma política existente e adicione condições a ela para criar sua própria política personalizada. Você também pode criar políticas secundárias a partir de políticas existentes.

Antes de Iniciar

Você pode clonar políticas para criar suas próprias políticas personalizadas. Você pode clonar uma política ou criar uma política secundária usando qualquer política como base para ajudá-lo a estender as políticas existentes sem precisar inserir as condições novamente. Todas as condições na política base também são herdadas na política secundária. Para obter mais informações, consulte Clonar uma política para Controle de posturas de segurança (exemplo).

Você pode clonar todas as políticas incluídas na aplicação, mas as correspondências de política não são refletidas como informações importantes no painel na página inicial inicial. Somente as informações principais das políticas incluídas na aplicação são exibidas na página inicial do.

Depois de clonar e ativar todas as políticas criadas, você deve criar seu próprio registro de informações configuradas no módulo Construtor de informações personalizadas no espaço (o último módulo no painel do navegador). Somente então você pode exibir os dados de suas políticas no painel Informações configuradas (o segundo ícone a partir da parte superior no espaço).

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Todos**.
2. Selecione o registro de política que você deseja clonar.
3. Selecione uma no menu de mais opções ao lado de **Ativar política**.

Opção	Descrição
Clonar política	Selecione esta opção se quiser usar as condições de uma política existente como ponto de partida para sua nova política. Uma nova guia com o registro de política clonado é exibida com "cópia" no nome. (Opcional) Selecione a Política de base e adicione uma da lista para sua nova política.
Criar política secundária	Selecione esta opção se quiser criar uma nova política usando a política atual como ponto de partida. Uma nova guia com um registro de política em branco com uma política base escolhida é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Opcional: Selecione **Política de base** e selecione uma política como base para sua nova política.

   (Optional) Você pode escolher esta opção se quiser herdar as condições de uma política existente como ponto de partida para sua nova política.

5. Opcional: Selecione **Políticas de exclusão** e selecione as políticas que você deseja excluir das descobertas desta política.
   Quaisquer descobertas em sua nova política que correspondam a quaisquer políticas excluídas não serão incluídas em suas descobertas.
6. Para uma política clonada, edite as condições.
   Para obter mais informações sobre os relacionamentos ativo-conexão-entidade no Construtor de condições, consulte Políticas para Controle de posturas de segurança. Para obter mais informações sobre os decoradores no Construtor de condições, consulte Como criar suas próprias políticas na aplicação Controle de posturas de segurança.
7. Edite e salve sua apólice com **Salvar mudanças**.
   Sua política é exibida na lista Todos no módulo Lista no espaço.
8. Para ativar uma política, siga as etapas descritas em Criar e ativar políticas personalizadas para Controle de posturas de segurança.
9. Opcional: Selecione Excluir política para excluir uma política.
   A opção de exclusão não é compatível com políticas que vêm com a aplicação ou com políticas que geraram descobertas. Você só pode desativar políticas com descobertas.

Criar e ativar uma informação configurada para o Controle de posturas de segurança

Você pode criar suas próprias informações. Informações configuradas são informações que você pode criar usando políticas existentes ou suas próprias políticas personalizadas.

Antes de Iniciar

Você deve criar um registro de informações e ativá-lo antes de exibir seus dados no painel Informações configuradas. Você pode ter até seis informações e 21 gráficos no módulo Painel de informações configuradas no espaço.

Todas as políticas usadas para uma informação personalizada devem ser ativadas.

Para políticas criadas com "Software" como o tipo de ativo, você pode salvar a política e criar informações personalizadas, mas não pode configurar as descobertas do registro de política.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Construtor de informações personalizadas** (último ícone no espaço).

   Nesta página principal, há três guias:

   Ativo

   Suas informações personalizadas ativadas. As informações personalizadas ativadas são exibidas na página principal de Informações configuradas (segundo ícone a partir da parte superior no espaço).

   Inativo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Suas informações personalizadas inativas. As informações desativadas não são exibidas na página principal de Informações configuradas até que as informações e suas políticas de suporte sejam ativadas.

Todos

Todas as suas informações configuradas ativas e inativas.

2. Selecione **Nova informação** à direita da página para criar um novo registro.
3. No campo Tipo, selecione uma informação na lista de seleção.

Opção	Descrição
Gráfico de comparação	Comparar contagens de ativos correspondentes para até cinco apólices.
Widget de contagem de correspondência de política	O número total de ativos que correspondem a uma política ou políticas.
Gráfico de porcentagem de correspondência de política	A porcentagem do total de ativos que correspondem ou não a uma apólice.
Gráfico de tendências de correspondência de política	Tendência histórica de ativos que correspondem a uma política ou políticas.

4. Selecione um.
   - Ativo de hardware
   - Software
5. Selecione grupos para suas informações.
   Uma informação deve pertencer a pelo menos um grupo. Você deve criar ou atribuir grupos às informações configuradas ao criar novos registros no módulo do Construtor de informações personalizadas. Os grupos permitem que você organize seus relatórios no painel Informações configuradas.
6. Selecione as políticas e os rótulos de informações desejados para os dados de informações.
7. Selecione **Salvar**.
   Sua informação é salva na guia Informações inativas.
8. Para ativar sua nova informação, abra o registro na lista Inativa e selecione **Ativar**.
   Os dados são coletados da próxima importação agendada para os Conectores do Service Graph associados às políticas de informações e os dados são exibidos no módulo Painel de informações personalizadas no espaço.

Exibir descobertas para Controle de posturas de segurança

Você pode exibir as descobertas geradas pela avaliação de políticas em Controle de posturas de segurança no espaço Controle de posturas de segurança.

Onde exibir descobertas

Você tem essas opções para exibir as descobertas geradas pela avaliação de políticas.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Navegar até **Espaço de controle de posturas de segurança** > **Políticas e descobertas** > **Descobertas** > **Todos.**
- Em um registro de política, selecione **Exibir descobertas**. A lista exibe grupos de descobertas que as organizam em categorias gerais, como "Combinação de alto risco", "Exposição na Internet" e assim por diante, mas esses grupos não são agrupamentos formais que podem ser usados para correção. Você precisa configurar regras de correção e atribuição em Conformidade de configuração para descobertas.
- Na aplicação Conformidade de configuração, selecione **Resultados de testes** e filtre os registros por **Origem é ServiceNow SPC**.

O painel

No Espaço de controle de posturas de segurança, a página inicial (página principal) exibe estas visualizações:

Visão geral

- Ativos: número de ativos monitorados no local e na nuvem.
- Descobertas por criticidade: número de descobertas críticas do total de ativos.
- Ativos monitorados pelas 5 principais origens: os cinco principais Conectores do Service Graph que emitiam relatórios sobre ativos.
- Contas em nuvem: número de contas em nuvem monitoradas pela AWS e pelo Azure.
- Descobertas abertas versus encerradas: comparação de registros ainda em processo ou aguardando resolução e aqueles que foram resolvidos.

Informações principais

- Agente de proteção de endpoint instalado: número total de ativos que têm ou não proteção de endpoint.
- Cobertura de dispositivo gerenciado: número de ativos gerenciados em comparação com aqueles que não são gerenciados.
- Cobertura de verificação de vulnerabilidades: número total de ativos verificados em comparação com o número que não foi verificado quanto a vulnerabilidades conhecidas por um scanner de vulnerabilidade de terceiros.
- Ativos com vulnerabilidades críticas: número de ativos do número total de ativos que têm vulnerabilidades críticas.
- Itens vulneráveis por criticidade: número total de itens vulneráveis divididos por gravidade. Uma vulnerabilidade conhecida que corresponde a um ativo no seu CMDB resulta em um item vulnerável.
- 3 principais políticas por descobertas: políticas que retornam o maior número de descobertas (correspondências) em seus ativos.

Cobertura de caso de uso principal

Selecione um caso de uso e selecione **Ajudar a ativar** ou **Ajudar a melhorar** para exibir quais conectores e políticas do Service Graph devem ser ativados para os principais casos de uso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados de testes e transições de estado da tarefa de correção na aplicação Controle de posturas de segurança

Os estados nas descobertas (registros de teste de configuração) e suas tarefas de correção associadas serão afetados se você modificar suas políticas na aplicação Controle de posturas de segurança.

Cenários de transição de estado entre resultados de testes e tarefas de correção

Com algumas exceções, os estados geralmente fazem a transição entre suas descobertas (resultados de testes) e as tarefas de correção associadas no Controle de posturas de segurança da mesma forma que fazem a transição entre os resultados de testes e as tarefas de correção na aplicação Conformidade de configurações. No entanto, se você modificar suas políticas no Controle de posturas de segurança, suas mudanças afetarão a forma como os estados fazem a transição em suas descobertas e nas tarefas de correção associadas.

As tabelas a seguir ilustram como os estados fazem a transição em suas descobertas se você editar e publicar uma nova versão (editar), desativar ou excluir suas políticas.

Para obter mais informações sobre mudanças de estado em Conformidade de configurações, consulte Resultados de testes e transições de estado da tarefa de correção na aplicação Conformidade de configurações.

Nota: A partir da v14.9 de Conformidade de configurações, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de grupo	Regras de tarefa de correção
Política	Grupo de teste

As melhorias nas auditorias de política garantem que os ativos desativados não sejam avaliados por políticas ativadas. Se o estado de um ativo mudar de **Descontinuado** para **Ativo**, ele será incluído na próxima avaliação de política.

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Desativado	Resultado	Manter valores originais
	Estado	Encerrado
	Resolução	Obsoleto

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Editado com a opção de fechar quaisquer	Resultado	Manter valores originais

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
descobertas existentes selecionada		
	Estado	Encerrado
	Resolução	Resultado Inválido

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Editado com a opção de manter as descobertas existentes selecionadas	Resultado	Os casos de teste válidos (Aprovados) retêm os valores originais e os casos de teste inválidos (Reprovados) são encerrados.
	Estado	Encerrado
	Resolução	Resultado Inválido

Se uma política for...	Valores de campo em registros de descoberta existentes para...	Transição para...
Excluídos	Resultados	Manter valores originais
	Estado	Encerrado
	Resolução	Resultado Inválido

Criar uma pesquisa de ativos no Controle de posturas de segurança

Defina suas condições e pesquise ativos por produtos específicos do conector do Service Graph ou ativos que tenham dados específicos relatados por um conector.

Antes de Iniciar

Como uma pesquisa de exemplo, digamos que você queira identificar seus ativos que têm servidores Windows e uma versão específica encontrada em CrowdStrike detalhes de metadados.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Pesquisa de ativos**.
2. Escolha um.

Opção	Descrição
Ativo de Hardware	Pesquise qualquer dispositivo que inclua dispositivos de computação pessoal, servidores, dispositivos de rede, máquinas virtuais em nuvem e outro hardware.
Software	Pesquise o software instalado em seus ativos relatados por conectores do Service Graph, seus produtos de scanner de vulne-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	rabilidade e o software relatado por scanners que já estão contabilizados no Software Asset Management (SAM) e em outros produtos da ServiceNow.

Para este exemplo, selecione **Ativo de hardware** para o tipo de ativo.

3. Opcional: Selecione **Política de base e Políticas** de **exclusão** se quiser usar as condições de uma política existente como início e excluir ativos que correspondam às políticas existentes, respectivamente.
   As políticas selecionadas são exibidas.
4. Selecione **Com dados de conector** para o campo Conexão.
5. Selecione Detalhes do **dispositivo CrowdStrike** para a entidade.
6. Para Propriedade, Operador e Valor, selecione **[Versão do agente][é]** e insira a versão, por exemplo, **6.26.14003.0**.
7. Selecione o operador e à direita do campo Entidade com CrowdStrike Detalhes do dispositivo como o valor para outra condição.
8. Selecione **Com metadados do CMDB** para o campo Conexão.
   O campo Entidade é preenchido com metadados do CMDB.
9. Selecione **Propriedade** para o campo Critérios.
10. Para Propriedade, Operador e Valor, selecione **[SO][contém]** e insira **Servidor Windows**.
11. Selecione **Exibir ativos**.
    Depois de alguns momentos, os resultados são exibidos na guia Ativos correspondentes. Se não houver correspondências, você poderá refinar a pesquisa. Depois que estiver satisfeito com a definição das condições corretamente, você poderá salvar a pesquisa como uma política e ativá-la. Como outras políticas, ela pesquisa seus ativos com um trabalho em segundo plano continuamente depois que você a ativa.

Casos de uso, exemplos de política e conectores do Service Graph compatíveis no Controle de posturas de segurança

Casos de uso são diferentes cenários que você configura para ajudá-lo a identificar tipos específicos de lacunas de cobertura da ferramenta. Cada caso de uso requer uma política ou políticas para auditar seus ativos quanto a possíveis violações. Você também pode definir suas próprias políticas para ajudá-lo a atender aos requisitos de seus padrões de segurança interna específicos.

Casos de uso

A aplicação Controle de posturas de segurança é compatível com vários casos de uso incluídos com a aplicação. Os casos de uso ajudam a identificar tipos específicos de lacunas de cobertura da ferramenta em seus ativos, exposição na Internet de ativos em nuvem e combinações com vulnerabilidades. As políticas necessárias para os casos de uso compatíveis também estão incluídas no produto.

Você pode exibir o status de cobertura de alguns dos principais casos de uso na página inicial (principal) do espaço de controle de posturas de segurança em **Espaços** > **Controle de posturas de segurança** > **Página inicial** no módulo Página inicial (página principal).

Como alternativa, você pode exibir os conectores do Service Graph compatíveis e o status de cobertura de alguns dos principais casos de uso nas guias "Conectores do Service Graph compatíveis" e "Configuração de caso de uso principal" em **Todos** > **Espaços** >

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Controle de posturas de segurança > **Configuração de conectores e casos de uso** (ícone de engrenagem).

Nota:

A guia Casos de uso principais nas Páginas iniciais iniciais não lista todos os casos de uso possíveis. Ele apresenta alguns casos de uso importantes que você ativa para ajudá-lo a começar a implantar o produto Controle de posturas de segurança.

Antes de ativar as políticas para os casos de uso compatíveis fornecidos com a aplicação, verifique se você concluiu as tarefas a seguir.

- Você instalou e configurou todas as aplicações necessárias descritas em Instalar as aplicações compatíveis com o Controle de posturas de segurança.
- Você atendeu a um ou mais dos seguintes pré-requisitos para cada caso de uso.

1. No momento, você está usando ou instala e ativa conectores do Service Graph para várias categorias.

   As categorias para os casos de uso incluem conectores do Service Graph que você deve ativar para obter informações iniciais e conectores do Service Graph que você tem a opção de ativar para melhorar a cobertura dos ativos que o Controle de posturas de segurança está monitorando.

2. No momento, você está usando ou instala e ativa a aplicação Resposta a vulnerabilidades.
3. No momento, você está usando ou configura a Verificação de conta em nuvem para suas contas da AWS e do Azure em "Gestão de posturas de segurança para nuvem".

Os requisitos específicos para cada caso de uso compatível são descritos nas seções a seguir. Além disso, você deve ativar uma ou mais das políticas enviadas com o Controle de posturas de segurança para um caso de uso. Esse conceito também é abordado nas seções a seguir.

Exemplos de políticas base, secundárias e clonadas

Consulte Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança e como você pode reutilizar as condições de uma política de base ao criar outras políticas. Crie políticas básicas, secundárias e clone políticas existentes nesses exemplos. Esses exemplos também ajudam a ver como o construtor de políticas funciona no módulo Políticas e descobertas.

Conectores do Service Graph compatíveis

Consulte as tabelas de conectores do Service Graph compatíveis, suas categorias de ferramentas e os tipos de dados que eles importam em Conectores do Service Graph de hardware compatíveis para Controle de posturas de segurança e Conectores do Software Service Graph compatíveis para Controle de posturas de segurança.

Controle de posturas de segurança caso de uso: detecção de ativos sem proteção de endpoint

Para detectar ativos sem um agente de proteção de endpoint, os pré-requisitos a seguir são necessários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph da categoria Endpoint Protection.
2. Ative pelo menos um Conector do Service Graph para UMA das seguintes categorias.
   a. Serviços de Diretório (Microsoft Active Directory).
   b. Gestão de endpoints: Microsoft Intune ou Jamf Device and Endpoint Management.
   c. Gestão de configurações e patches: Microsoft SCCM ou IBM Bigfix.
   d. Provedor de nuvem: Amazon AWS Cloud, Microsoft Azure, GCP.

   Nota: Se a Descoberta na nuvem estiver ativada, esses produtos do conector do Service Graph não serão necessários.

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das seguintes categorias para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Controle de posturas de segurança.
   a. Segurança de rede
   b. Monitoramento de infraestrutura
   c. Rede
   d. Gestão de endpoints .
   e. Monitoramento de desempenho de aplicações .

Depois de verificar se atende a esses pré-requisitos, você deve ativar a seguinte política, Ativos sem proteção de endpoint. Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

Controle de posturas de segurança caso de uso: detecção de ativos perdidos por ferramentas de avaliação de vulnerabilidade

Para detectar ativos perdidos por ferramentas de avaliação de vulnerabilidade, os seguintes pré-requisitos são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou na nuvem. Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph da categoria Avaliação de vulnerabilidade.
2. Ative pelo menos um Conector do Service Graph para UMA das seguintes categorias.
   a. Serviços de Diretório (Microsoft Active Directory).
   b. Gestão de endpoints: Microsoft Intune ou Jamf Device and Endpoint Management.
   c. Gestão de configurações e patches: Microsoft SCCM ou IBM Bigfix.
   d. Provedor de nuvem: Amazon AWS Cloud, Microsoft Azure, GCP.

   Nota: Se a Descoberta na nuvem estiver ativada, esses produtos do conector do Service Graph não serão necessários.

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das seguintes categorias para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Controle de posturas de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Segurança de rede .

b. Rede.

c. Monitoramento de infraestrutura.

d. Monitoramento de desempenho de aplicações .

Depois de verificar se atende a esses pré-requisitos, você deve ativar a seguinte política, Ativos não verificados quanto a vulnerabilidades. Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

Controle de posturas de segurança caso de uso: detecção de ativos não gerenciados

Este caso de uso inclui duas partes, a detecção de ativos com agentes de configuração e gestão de patches ausentes.

Para detectar ativos sem ferramentas de configuração e gestão de patches, os seguintes pré-requisitos são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem.

Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph nas categorias Configuração e Gestão de patches.
2. Pelo menos um Conector do Service Graph deve ser habilitado para UMA das categorias a seguir.
   a. Serviços de Diretório (Microsoft Active Directory).
   b. Proteção de endpoint: CrowdStrike ou SentinelOne.
   c. Avaliação de vulnerabilidade: Qualys, Rapid7ou Tenable.
   d. Gestão de configurações e patches: Microsoft SCCM ou IBM Bigfix.
3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das seguintes categorias para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Controle de posturas de segurança.
   a. Rede.
   b. Monitoramento de infraestrutura
   c. Segurança de rede
   d. Monitoramento de desempenho de aplicações .

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas a seguir. Para qualquer política que comece com "Ativos de nuvem", os Conectores do Service Graph na categoria "Provedor de nuvem" devem ser habilitados. Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

- Ativos sem configuração e gestão de patches.
- Ativos em nuvem sem configuração e gestão de patches.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Controle de posturas de segurança caso de uso: detecção de ativos sem uma solução de gestão de endpoint

Para detectar ativos sem uma solução de gerenciamento de endpoint, os seguintes pré-requisitos são necessários.

Dependendo do seu caso de uso, você pode optar por ativar somente os conectores necessários.

1. Ative pelo menos um Conector do Service Graph da categoria Gestão de endpoints.
2. Pelo menos um Conector do Service Graph deve estar habilitado para UMA das categorias a seguir.
   a. Serviços de Diretório (Microsoft Active Directory).
   b. Proteção de endpoint: CrowdStrike ou SentinelOne.
   c. Avaliação de vulnerabilidade: Qualys, Rapid7ou Tenable.
   d. Gestão de configurações e patches: Microsoft SCCM ou IBM Bigfix.

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar a política a seguir, Ativos sem solução de gerenciamento de endpoint. Para obter mais informações sobre políticas, consulte Políticas para Controle de posturas de segurança.

Controle de posturas de segurança caso de uso: detecção de ativos com vulnerabilidades e lacunas de cobertura da ferramenta de segurança

Você pode identificar ativos com vulnerabilidades críticas e ferramentas de segurança críticas ausentes, como proteção de endpoint, para priorizar esses ativos para correção. O controle de posturas de segurança envia algumas políticas incluídas com o produto para oferecer suporte a este caso de uso.

Este caso de uso requer que você instale a aplicação Resposta a vulnerabilidades e uma integração com pelo menos um produto de avaliação de vulnerabilidade, como Qualys, Rapid7ou Tenable.

As políticas a seguir estão incluídas com o produto Controle de posturas de segurança para oferecer suporte a este caso de uso de ativos com vulnerabilidades críticas que também não têm cobertura da ferramenta de segurança.

1. Ativos com vulnerabilidades críticas e proteção de endpoint ausente.
2. Ativos com vulnerabilidades críticas e gestão de patches e configuração ausente.
3. Ativos com vulnerabilidades críticas e gerenciamento de endpoint ausente.

Controle de posturas de segurança caso de uso: detecção de exposição na Internet de ativos em nuvem e combinações de alto risco

É essencial monitorar a possível exposição na Internet de ativos em nuvem (máquinas virtuais) em várias portas para garantir que as vulnerabilidades nesses ativos não sejam exploradas remotamente. Este caso de uso ajuda a identificar esses ativos.

O controle de postura de segurança permite que você avalie a configuração de ativos de nuvem para ajudá-lo a identificar os ativos voltados para a internet, ou seja, quais ativos podem ser acessados de qualquer lugar na internet e de quais portas eles estão expostos.

O controle de posturas de segurança combina essas informações com lacunas de cobertura da ferramenta de segurança e dados de vulnerabilidade de scanners de terceiros, como Qualys, Rapid7ou Tenable para identificar combinações de alto risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualmente, este caso de uso é compatível com a AWS e requer os seguintes pré-requisitos.

1. O Conector do Service Graph para AWS é ativado para as mesmas contas da AWS que você configurou.
2. Você ativou uma ou mais das políticas incluídas com o produto no Controle de posturas de segurança.
   - Ativos em nuvem com a porta SSH 22 aberta para a internet.
   - Ativos em nuvem com porta SSH 22 aberta para a internet e proteção de endpoint ausente.
   - Ativos em nuvem com porta HTTP 80 aberta para a internet e proteção de endpoint ausente.
   - Ativos em nuvem com vulnerabilidades críticas e porta SSH 22 aberta para a internet (requer a Resposta a vulnerabilidades).
   - Ativos em nuvem com vulnerabilidades críticas, proteção de endpoint ausente e porta SSH 22 aberta para a Internet (requer Resposta a vulnerabilidades).
   - Ativos em nuvem com portas HTTP abertas para a Internet, vulnerabilidades críticas e proteção de endpoint ausente (requer Resposta a vulnerabilidades).

Conectores do Service Graph de hardware compatíveis para Controle de posturas de segurança

Conectores do Service Graph de hardware compatíveis com categorias de classe de IC, origem (produto) e ferramenta. Esta lista não está completa e está sujeita a mudanças com a adição de mais produtos.

Para a origem de descoberta de um conector listado, 'SG', 'SGO' ou 'SGC' precede o nome do produto para produtos de terceiros, por exemplo, SG-AWS, SGO-Datadog ou SGC-AD (Active Directory). Para produtos da ServiceNow, "SN" ou "ServiceNow" precede o nome do produto, por exemplo, SNAssetManagement para ServiceNow Hardware Asset Management.

Depois de instalá-los, você pode exibir os conectores e suas categorias na tabela de conectores [sn_sec_spc_core_connector] em sua instância.

Você pode exibir os tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

Conectores do Hardware Service Graph

Tipo de ativo	Classe do IC	Origem do ativo	Categoria do conector
Ativo de Hardware	cmdb_ci_computer	Active Directory	Serviços de diretório
Ativo de Hardware	cmdb_ci_server	AppDynamics	Monitoramento de desempenho da aplicação
Ativo de Hardware	cmdb_ci_server	Automox	Configuração e gestão de patches
Ativo de Hardware	cmdb_ci_computer	Automox	Configuração e gestão de patches
Ativo de Hardware	cmdb_ci_computer	BigFix	Configuração e gestão de patches

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Hardware Service Graph

Tipo de ativo	Classe do IC	Origem do ativo	Categoria do conector
Ativo de Hardware	cmdb_ci_server	BigFix	Configuração e gestão de patches
Ativo de Hardware	cmdb_ci_printer	Cisco Merak	Rede
Ativo de Hardware	cmdb_ci_server	Cisco Merak	Rede
Ativo de Hardware	cmdb_ci_iot	Cisco Merak	Rede
Ativo de Hardware	cmdb_ci_hc_dispositivo	Cisco Merak	Rede
Ativo de Hardware	cmdb_ci_netgear	Cisco Merak	Rede
Ativo de Hardware	cmdb_ci_computer	Cisco Merak	Rede
Ativo de Hardware	cmdb_ci_server	CrowdStrike	Proteção de endpoint
Ativo de Hardware	cmdb_ci_server	Datadog	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_server	Dynatrace	Monitoramento de desempenho da aplicação
Ativo de Hardware	cmdb_ci_computer	Dynatrace	Monitoramento de desempenho da aplicação
Ativo de Hardware	cmdb_ci_computer	ExtraHop Reveal(x)	Segurança de rede
Ativo de Hardware	cmdb_ci_hc_dispositivo	ExtraHop Reveal(x)	Segurança de rede
Ativo de Hardware	cmdb_ci_server	ExtraHop Reveal(x)	Segurança de rede
Ativo de Hardware	cmdb_ci_iot	ExtraHop Reveal(x)	Segurança de rede
Ativo de Hardware	cmdb_ci_printer	ExtraHop Reveal(x)	Segurança de rede
Ativo de Hardware	cmdb_ci_iot	Prospecção	Segurança de rede
Ativo de Hardware	cmdb_ci_hc_dispositivo	Prospecção	Segurança de rede
Ativo de Hardware	cmdb_ci_computer	Prospecção	Segurança de rede
Ativo de Hardware	cmdb_ci_server	Prospecção	Segurança de rede
Ativo de Hardware	cmdb_ci_printer	Prospecção	Segurança de rede
Ativo de Hardware	cmdb_ci_server	Intune	Gestão de endpoint
Ativo de Hardware	cmdb_ci_computer	Intune	Gestão de endpoint
Ativo de Hardware	cmdb_ci_printer	Jamf Pro	Gestão de endpoint
Ativo de Hardware	cmdb_ci_server	Jamf Pro	Gestão de endpoint
Ativo de Hardware	cmdb_ci_computer	Jamf Pro	Gestão de endpoint
Ativo de Hardware	cmdb_ci_server	Varredor de tela	IT Asset Management
Ativo de Hardware	cmdb_ci_computer	Varredor de tela	IT Asset Management
Ativo de Hardware	cmdb_ci_printer	Varredor de tela	IT Asset Management

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Hardware Service Graph

Tipo de ativo	Classe do IC	Origem do ativo	Categoria do conector
Ativo de Hardware	cmdb_ci_hc_dispositivo	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_printer	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_server	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_vm_instance	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_iot	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_computer	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_netgear	Monitoramento lógico	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_server	Microsoft Defender	Proteção de endpoint
Ativo de Hardware	cmdb_ci_server	New Relic	Monitoramento de desempenho da aplicação
Ativo de Hardware	cmdb_ci_computer	NextThink	Experiência do Funcionário Digital
Ativo de Hardware	cmdb_ci_server	Abrir telemetria	Monitoramento de desempenho da aplicação
Ativo de Hardware	cmdb_ci_computer	Puppet	Configuração e gestão de patches
Ativo de Hardware	cmdb_ci_server	Puppet	Configuração e gestão de patches
Ativo de Hardware	cmdb_ci_computer	Qualys	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_server	Qualys	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_vm_instance	Qualys-ServiceNow	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_server	Qualys-ServiceNow	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_hardware	Rapid7	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_computer	SCCM	Configuração e gestão de patches
Ativo de Hardware	cmdb_ci_server	SCCM	Configuração e gestão de patches

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Hardware Service Graph

Tipo de ativo	Classe do IC	Origem do ativo	Categoria do conector
Ativo de Hardware	cmdb_ci_printer	Lógica de ciências	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_iot	Lógica de ciências	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_server	Lógica de ciências	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_computer	Lógica de ciências	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_hc_dispositivo	Lógica de ciências	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_vm_instance	Lógica de ciências	Monitoramento de infraestrutura
Ativo de Hardware	cmdb_ci_hardware	HAM da ServiceNow	Gestão de ativos de hardware - HAM
Ativo de Hardware	cmdb_ci_hardware	Descoberta do ITOM da ServiceNow	Descoberta
Ativo de Hardware	cmdb_ci_server	Ativo Tanium	Gestão de endpoint
Ativo de Hardware	cmdb_ci_computer	Ativo Tanium	Gestão de endpoint
Ativo de Hardware	cmdb_ci_ups	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_industrial_sensor	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_cnc	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_hardware	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_netgear	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_industrial_controller	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ip_switch	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_hub_network	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_security	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_server	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_rtu	Tenable	Avaliação de vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Hardware Service Graph

Tipo de ativo	Classe do IC	Origem do ativo	Categoria do conector
Ativo de Hardware	cmdb_ci_ot_ews	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_plc	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_control	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_dcs	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_storage_server	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_hmi	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_control_module	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_industrial_robot	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_historian	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_industrial_device	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_iot	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ip_firewall	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_computer	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_unclassed_hardware	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ids_network	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_ot_ie	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_printer	Tenable	Avaliação de vulnerabilidade
Ativo de Hardware	cmdb_ci_computer	Espaço do VMWare ONE UEM	Gestão de endpoint
Ativo de Hardware	cmdb_ci_server	Espaço do VMWare ONE UEM	Gestão de endpoint
Ativo de Hardware	cmdb_ci_printer	Espaço do VMWare ONE UEM	Gestão de endpoint

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectores do Software Service Graph compatíveis para Controle de posturas de segurança

Conectores do Graph de serviço de software compatíveis com categorias de classe de IC, origem (produto) e ferramenta. Esta lista não está completa e está sujeita a mudanças com a adição de mais produtos.

Depois de instalá-los, você pode exibir os conectores e suas categorias na tabela de conectores [sn_sec_spc_core_connector] em sua instância.

Você pode exibir os tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

Conectores do Software Service Graph

Tipo de ativo	Classe do IC	Origem do ativo	Categoria do conector
Software	cmdb_ci_spkg	BigFix	Configuração e gestão de patches
Software	cmdb_ci_spkg	Dynatrace	Monitoramento de desempenho da aplicação
Software	cmdb_ci_spkg	Prospecção	Segurança de rede
Software	cmdb_ci_spkg	Intune	Gestão de endpoint
Software	cmdb_ci_spkg	Jamf Pro	Gestão de endpoint
Software	cmdb_ci_spkg	New Relic	Monitoramento de desempenho da aplicação
Software	cmdb_ci_spkg	NextThink	Experiência do Funcionário Digital
Software	cmdb_ci_spkg	Qualys-ServiceNow	Avaliação de vulnerabilidade
Software	cmdb_ci_spkg	SCCM	Configuração e gestão de patches
Software	cmdb_ci_spkg	Descoberta do ITOM da ServiceNow	Descoberta
Software	cmdb_ci_spkg	Ativo Tanium	Gestão de endpoint
Software	cmdb_ci_spkg	Espaço do VMWare ONE UEM	Gestão de endpoint

Exemplos de políticas base, secundárias e clonadas para Controle de posturas de segurança

Você pode criar suas próprias políticas de base com amplos conjuntos de condições que podem ser usados como pontos de partida para políticas mais complexas.

Exemplos

Os exemplos a seguir ajudarão você a ver como é possível reutilizar as condições de uma política de base ao criar outras políticas, criando políticas secundárias ou clonando políticas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

existentes. Esses exemplos também ajudam a ver como o construtor de políticas funciona no módulo Políticas e descobertas.

Comece com o primeiro exemplo, a política Base. Os outros exemplos usam a política de base como ponto de partida.

Nota: O conector do gráfico de serviço do CrowdStrike é usado como o conector do gráfico de serviço nesses exemplos, mas você pode usar qualquer conector que tenha instalado. Nesses exemplos, você cria e ativa as políticas para procurar correspondências de ativo. Você pode remover essas políticas a qualquer momento do módulo Políticas e descobertas depois de ativá-las.

Criar uma política de base para Controle de posturas de segurança (exemplo)

Um exemplo de como criar uma política de base que você pode usar para criar outras políticas.

Antes de Iniciar

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Todos** > **Espaço de controle de posturas de segurança** > **Políticas e descobertas**.
2. Selecione **Nova política**.
3. Selecione o ícone de caneta no canto superior esquerdo e, no modal Editar metadados, preencha os campos.

Campo	Descrição
Nome	Digite, Política de base - Dispositivos Windows 10.
Criticidade	Selecione **Baixo**.
Descrição resumida	Digite, **localize dispositivos com o Windows 10 instalado**.

4. Selecione **Salvar metadados**.
5. No Construtor de condições, selecione **Ativo de hardware** para o tipo de ativo.

   Para esta política, deixe as opções Política de base e Políticas de exclusão em suas configurações padrão (desativadas).

6. Para Conexão, selecione **Com dados agregados**.

   Para esta política, os dados agregados ajudam a localizar ativos no seu CMDB que tenham o Windows 10 instalado. Por exemplo, alguns registros podem ter pequenas variações em como diferentes scanners relatam "Windows 10". Os dados agregados garantem que todas essas pequenas variações no "Windows 10" correspondam a esta política.

   Os campos Entidade e Critérios são preenchidos automaticamente com base na sua seleção no campo Conexão.

7. Em Propriedade, selecione **SO**.
8. Para tipo de valor no `Windows 10`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Selecione **Salvar mudanças**.
   Sua política base é exibida na lista Todos do módulo Políticas e descobertas, mas não está ativada.
10. Selecione **Ativar política** para que sua política de base monitore todos os ativos que correspondam às condições da política e gere descobertas.

Criar uma política secundária a partir de uma política de base para Controle de posturas de segurança (exemplo)

Um exemplo de como criar uma política secundária usando as condições de uma política de base.

Antes de Iniciar

Esta política secundária herda as condições de uma política de base e você adicionará mais condições à sua política secundária para ajudá-lo a se concentrar em detalhes de ativos mais específicos. Você deseja uma nova política para monitorar todos os dispositivos com o Windows 10 instalado que são relatados pelo conector do Service Graph CrowdStrike e deseja excluir todos os dispositivos que correspondam a outra política. Para este exemplo, você excluirá de suas descobertas os ativos que foram aprovados para exceções da Gestão integrada de riscos (IRM).

Nota: Se você não tiver o conector do Service Graph CrowdStrike instalado, poderá usar um que tenha instalado.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Todos** > **Espaço de controle de posturas de segurança** > **Políticas e descobertas**.
2. Na lista Ativa, localize a Política de base - Dispositivos Windows 10 que você criou no primeiro exemplo e selecione-a para abrir o registro.
3. Selecione o menu de mais opções (três pontos verticais) e escolha **Criar política secundária**.
   Uma nova guia é aberta com um novo registro e a Política de base - Dispositivos Windows 10 é exibida no campo Política de base.
4. Selecione o ícone de caneta no canto superior esquerdo e, em Editar modal de metadados, preencha os campos.

Campo	Descrição
Nome	Digite, `política secundária - Dispositivos Windows com CrowdStrike`.
Criticidade	Selecione **Médio**.
Descrição resumida	Digite, `localize todos os dispositivos com Windows 10 relatados pelo CrowdStrike.`

5. Selecione **Salvar metadados**.
6. No Construtor de condições, selecione **Ativo de hardware** para o tipo de ativo.
7. Selecione a alternância Política de base.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione na lista a política que você criou para o Exemplo 1, **Política de base - Dispositivos Windows 10**.

   Esta política secundária herda automaticamente as condições da política de base.

9. Selecione a alternância Políticas de exclusão.
10. Selecione Ativos com exceção de IRM aprovada na lista.

    Nota: Se você não tiver esta política, poderá selecionar outra política na lista que deseja excluir desta política.

    Os ativos que correspondem a esta apólice serão excluídos da sua apólice secundária. Observe que você pode adicionar mais políticas.

11. Selecione **Relatado por**.
12. Selecione **CrowdStrike** na lista.
13. Selecione **Salvar mudanças**.
    Sua nova política é exibida na lista Todos do módulo Políticas e descobertas, mas não está ativada.
14. Selecione **Ativar política** para que sua política de base monitore todos os ativos que correspondam às condições da política e gere descobertas.

Clonar uma política para Controle de posturas de segurança (exemplo)

Um exemplo de como criar uma política que copia as condições de outra política.

Antes de Iniciar

Crie uma política que copie as condições da política que você criou no Exemplo 2 para que você não precise inseri-las novamente. Você clonará essas condições e adicionará mais condições à cópia da política secundária que criou. Para este exemplo, você deseja que esta política localize dispositivos com Windows 10 com CrowdStrike, exclua ativos com exceções de IRM que não foram vistos nos últimos 7 dias.

Funções necessárias: grupo de administradores de SPC ou grupo de analistas de SPC

Procedimento

1. Navegar até **Todos** > **Espaço de controle de posturas de segurança** > **Políticas e descobertas**.
2. Na lista Ativa, localize a política secundária - Windows dispositivos com CrowdStrike que você criou para o segundo exemplo e selecione-a para abrir o registro.
3. Selecione o menu de mais opções (três pontos verticais) e escolha **Clonar política**.
   Uma nova guia é aberta e o nome da política é exibido em um novo registro com "cópia" no título: Dispositivos Windows com cópia do CrowdStrike.
4. Selecione o ícone de caneta no canto superior esquerdo e, em Editar modal de metadados, preencha os campos.

Campo	Descrição
Nome	Digite, `política clonada — Exceções de IRM do CrowdStrike para Windows 10 não vistas há 7 dias.`
Criticidade	Selecione **Crítico**.

Tradução automática

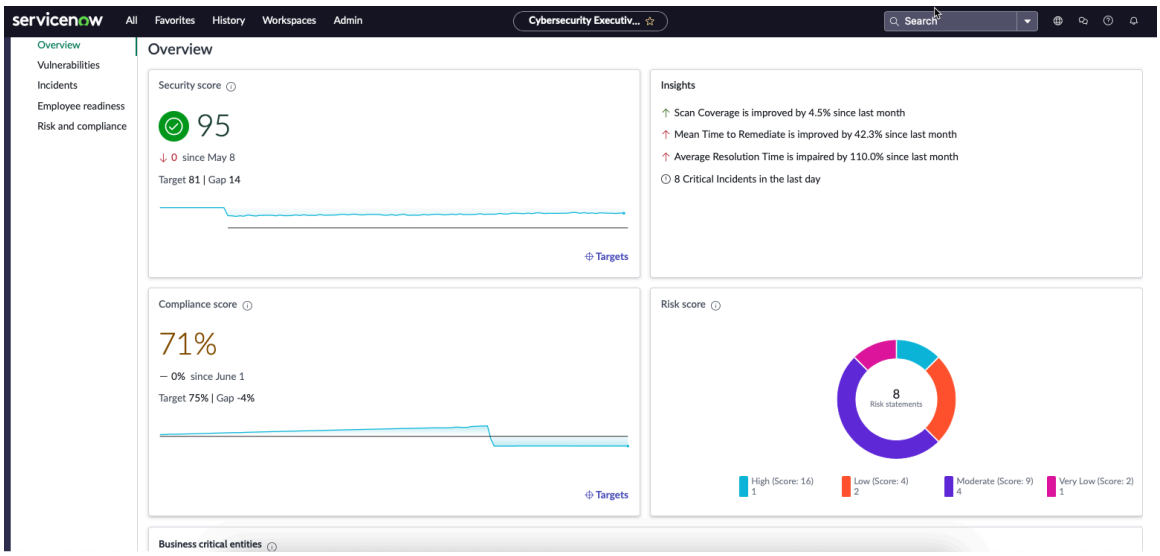
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Digite, `localize dispositivos com Windows 10 com exceções de IRM do CrowdStrike não vistas nos últimos 7 dias.`.

5. Selecione **Salvar metadados**.
6. À direita dos primeiros campos Conexão e Entidade, selecione o operador **AND** para novos campos.
   Isso adiciona um E lógico entre os critérios atuais da Entidade de conexão e novos critérios de outra Entidade de conexão. Nesse caso, você deseja especificar os dados do conector para ativos não vistos pelo CrowdStrike nos últimos 7 dias.
7. Para Conexão, selecione **Com dados do conector**.
8. Em Entidade, selecione **CrowdStrike: Detalhes do dispositivo CrowdStrike**.
   Os critérios arquivados são preenchidos automaticamente com base na sua seleção.
9. Em Propriedade, selecione **Hora da última visita**.
10. Em Valor, selecione **Esta semana**.
11. Selecione **Salvar mudanças**.
12. Selecione **Ativar política**.
    Você pode remover essas políticas a qualquer momento no módulo Políticas e descobertas.

Painel executivo de cibersegurança

O painel executivo de segurança cibernética é uma solução abrangente que capacita os diretores de segurança da informação (CISOs) e executivos de segurança cibernética com visibilidade sobre a postura e as iniciativas de segurança da organização. O painel consolida dados de vários produtos do pacote ServiceNow de Operações de segurança e Governança, risco e conformidade (GRC).



O painel fornece os seguintes recursos:

- Pontuação da postura de segurança em toda a organização
- Pontuações de segurança, risco e conformidade por unidade de negócios

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Monitoramento personalizável
- Exibição unificada do cenário de segurança de uma organização
- Parâmetro de comparação
- Interface amigável
- Visibilidade nas métricas de simulação de phishing do KnowBe4 e do Microsoft Defender para Office 365

Esses recursos permitem a tomada de decisão proativa, fornecendo acesso rápido a métricas de segurança críticas. Assim, tornando-o uma ferramenta essencial para aprimorar a resiliência e a prontidão geral da segurança.

Funções necessárias de Now Platform

- CISO (sn_bod.ciso) para exibir e compartilhar o painel.
- sn_bod.ciso_admin para exibir, compartilhar o painel e configurar pesos para classificação de postura de segurança.
- Usuário GRC CISO (sn_grc_dashboards.grc_ciso_user) para exibir relatórios de risco e conformidade.

Acessar o Painel executivo de segurança cibernética

Para abrir o painel, navegue até **Todos** > **Painel executivo de cibersegurança** > **Painel executivo de cibersegurança**.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
Diretores de segurança da informação (CISOs)	Os CISOs obtêm informações sobre gestão de vulnerabilidades, gestão de incidentes, postura de segurança da organização, métricas de simulação de phishing e assim por diante para suas organizações.

Visualização de dados

Nota: Para saber mais sobre um widget, selecione o ícone de informações ícone ⓘ.

Destinos

Métricas	Tipo	Descrição
Destinos	Percentual	Mostra o destino definido a ser coberto por uma métrica. O status dos destinos é indicado por meio de codificação de cores. Ele mostra todas as metas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Destinos

Métricas	Tipo	Descrição
		cuja data de revisão está nos últimos 30 dias ou nos próximos dias. Você pode definir o número de dias para exibir metas usando a propriedade do sistema *sn_bod.show_targets_from*. Além disso, esses destinos podem ser editados. Para obter mais informações, consulte Definir metas.

Visão geral

Métricas	Tipo	Descrição
Pontuação de segurança	Pontuação única	Pontuação geral da postura de segurança da organização, considerando itens vulneráveis, incidentes de segurança, incidentes de segurança graves e erros de configuração.
Informações	Realces	Destaques de todo o painel.
Pontuação de conformidade	Pontuação única	Fornece a postura de conformidade da organização com a ajuda da pontuação de conformidade calculada com base na porcentagem de controles compatíveis em relação ao número total de controles.
Pontuação de risco	Pontuação única	Fornece a contagem de declarações de risco com base nas classificações de risco. Ele ajuda as organizações a entender o possível impacto e a probabilidade de vários riscos, permitindo que priorizem e gerenciem esses riscos.
Entidades essenciais para os negócios		
Unidades de negócios	Pontuação única	Pontuação de segurança geral das unidades de negócios, considerando o risco associado a

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Métricas	Tipo	Descrição
		vulnerabilidades, erros de configuração, vulnerabilidades de tecnologia operacional (OT), incidentes de segurança e incidentes de segurança graves. O rótulo de integridade das unidades de negócios se baseia somente na pontuação de segurança. Para ver como esses rótulos são atribuídos, navegue até a tabela Ponderações de pontuação de risco [sn_sec_cmn_risk_score_weight_list.do] e pesquise a entidade de negócios. Rótulos como "Integridade" são atribuídos com base em intervalos de valores predefinidos. Por exemplo, uma pontuação de segurança que varia de 0 a 39 é rotulada como Íntegra. A codificação de cores para esses rótulos é especificada na inclusão de script `UnifiedCISOutils`. Você pode configurar o intervalo de valores e as cores dos rótulos. Para ver como os nomes da unidade de negócios e do chefe da unidade de negócios são atribuídos, vá para **Todos** > **Organização** > **Unidade de negócios**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Métricas	Tipo	Descrição
		Nota: Dependendo dos plug-ins habilitados, você pode acessar a Pontuação de conformidade, a Pontuação de risco e a Pontuação de segurança. Para exibir a pontuação de Conformidade e risco, você deve ativar os plug-ins do GRC. Para exibir a pontuação de segurança, você deve ativar os plug-ins relacionados às Operações de segurança. Consulte a seção Aplicações para ativo para obter mais informações.
Serviços de negócio	Pontuação única	Pontuação de segurança geral dos serviços de negócio, considerando o risco associado a vulnerabilidades, erros de configuração, vulnerabilidades de tecnologia operacional (OT), incidentes de segurança e incidentes de segurança graves. Para ver como esses rótulos são atribuídos, navegue até a tabela Ponderações de pontuação de risco [sn_sec_cmn_risk_score_weight_list.do] e pesquise a entidade de negócios. Rótulos como "Integridade", "Moderado" e "Crítico" são atribuídos com base em intervalos de valores predefinidos. Por exemplo, uma pontuação de segurança que varia de 0 a 39 é rotulada como Íntegra. A codificação de cores para esses rótulos é especificada na inclusão de script `UnifiedCISOutils`.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Métricas	Tipo	Descrição
		Você pode configurar o intervalo de valores e as cores dos rótulos. Para ver como a unidade de negócios e o nome do chefe da unidade de negócios são atribuídos, vá para **Todos** > **Organização** > **Unidade de negócios**. **Nota:** Dependendo dos plug-ins habilitados, você pode acessar a Pontuação de conformidade, a Pontuação de risco e a Pontuação de segurança. Para exibir a pontuação de Conformidade e risco, você deve ativar os plug-ins do GRC. Para exibir a pontuação de segurança, você deve ativar os plug-ins relacionados às Operações de segurança. Consulte a seção Aplicações para ativo para obter mais informações.

Vulnerabilidades

Métricas	Tipo	Descrição
Tempo médio para correção (mensal)	Linhas	Tempo médio necessário para fechar vulnerabilidades e resultados de testes com falha em todos os ativos (hosts, contêineres e aplicações) em um mês. Ele também fornece as seguintes métricas: • Meta: meta definida em dias para corrigir as vulnerabilidades. • Lacuna: diferença em dias entre o tempo de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

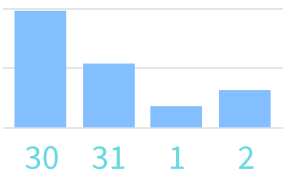
Vulnerabilidades

Métricas	Tipo	Descrição
		meta e o tempo real necessário para corrigir as vulnerabilidades. • Parâmetro de comparação do setor: média de métricas de colegas do mesmo setor. • Benchmark global: média de métricas de pares no mercado global Consulte Aceitar pontuações de parâmetro de comparação sobre como exibir as pontuações do parâmetro de comparação.
Idade média das vulnerabilidades ativas (mensal)	Pontuação única	Idade média mensal dos três tipos de itens vulneráveis. Ele também fornece uma comparação da idade do mês atual com o mês anterior. Ele também fornece as seguintes métricas: • Parâmetro de comparação do setor: média de métricas de colegas do mesmo setor. • Benchmark global: média de métricas de pares no mercado global • Meta: meta definida em dias para corrigir as vulnerabilidades.
Eficiência de correção (mensal)	Pontuação única	Percentual de itens vulneráveis encerrados mensalmente em relação aos itens vulneráveis ativos mensais. Ele também fornece as seguintes métricas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

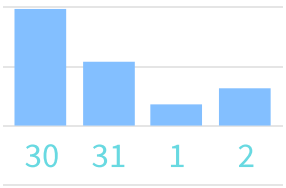
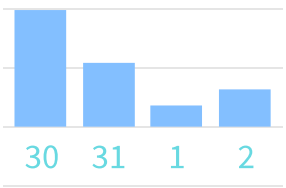
Vulnerabilidades

Métricas	Tipo	Descrição
		• Percentual de mudança em relação ao mês anterior. • Meta: meta definida em porcentagem para corrigir as vulnerabilidades. • Lacuna: a lacuna entre a pontuação desejada e a atual. • Parâmetro de comparação do setor: média de métricas de colegas do mesmo setor. • Benchmark global: média de métricas de pares no mercado global
Idade média das vulnerabilidades ativas por grupo de atribuição	Várias linhas	Idade média das vulnerabilidades ativas para cada grupo de atribuição.
Vulnerabilidades por classificação de risco e idade	Mapa térmico	Detalhamento de vulnerabilidades ativas em hosts, contêineres e aplicações por classificação de risco e idade.
Cumprimento da meta de correção por grupo de atribuição	Barra de  vertical	A proporção do número de vulnerabilidades e erros de configuração encerrados na meta de correção para o número total de vulnerabilidades e erros de configuração encerrados.
Cobertura de verificação	Percentual	Percentual de ativos verificados nos últimos 90 dias de todos os ativos no CMDB.
Ativos verificados vs. não verificado	Barra horizontal	Detalhamento de ativos verificados nos últimos 90 dias e total de ativos em CMDB por classe de IC
Ativos verificados	Barra horizontal	Ativos verificados nos últimos 90 dias quanto a vulnerabilidades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades

Métricas	Tipo	Descrição
		versus conformidade de configuração.
Tendência de descobertas críticas e altas ativas	de várias linhas	Tendência diária de vulnerabilidades e configurações incorretas com classificação de risco crítico e alto.
Vulnerabilidades por categoria de ativo e classificação de risco	Barra de  vertical	Detalhamento de vulnerabilidades ativas e configurações incorretas por categoria de ativo e classificação de risco (crítica, alta e média).
Descobertas adiadas por motivo e grupo de atribuição	Barra de  vertical	Detalhamento de vulnerabilidades ativas e configurações incorretas adiadas por motivo de adiamento e grupo de atribuição.
Tecnologia operacional (OT)		
Tendência de vulnerabilidade crítica e alta ativa	linha de mapa térmico	Tendência diária de vulnerabilidades de OT que estão ativas com classificação de risco crítico e alto.
Tempo médio para correção (mensal)	Pontuação única	Tempo médio necessário para fechar vulnerabilidades de OT. A proporção da idade total de vulnerabilidades de OT encerradas para o número total de vulnerabilidades de OT. Ele também fornece as seguintes métricas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades

Métricas	Tipo	Descrição
		• Percentual de mudança em relação ao mês anterior. • Meta: meta definida em dias para corrigir as vulnerabilidades. • Parâmetro de comparação do setor: média de métricas de colegas do mesmo setor. • Benchmark global: média de métricas de pares no mercado global Consulte Aceitar pontuações de parâmetro de comparação sobre como exibir as pontuações do parâmetro de comparação.
Vulnerabilidades por classificação de risco e idade	Mapa térmico	Detalhamento de vulnerabilidades de OT ativas por classificação de risco e idade.
Idade média das vulnerabilidades ativas (mensal)	Gráfico de linhas	Idade média mensal dos itens vulneráveis de OT. Ele também fornece uma comparação da idade do mês atual com o mês anterior.
Vulnerabilidades por estado e idade	Mapa térmico	Detalhamento de vulnerabilidades de OT ativas por estado e idade.

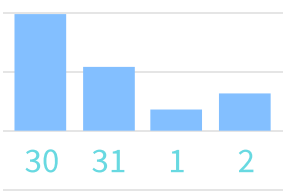
Incidentes

Métricas	Tipo	Descrição
Incidentes de segurança graves	Pontuação única	Número de incidentes de segurança graves que estão ativos no momento.
Média de tempo de resolução de incidentes de segurança (mensal)	Pontuação única	Tempo médio de resolução mensal em dias de incidentes de segurança encerrados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

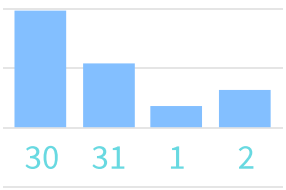
Incidentes

Métricas	Tipo	Descrição
		Ele também fornece as seguintes métricas: • Percentual de mudança em relação ao mês anterior. • Meta: meta definida em dias para corrigir os incidentes de segurança. • Lacuna: a lacuna entre os dias reais necessários para resolver e o destino definido para corrigir. • Parâmetro de comparação do setor: média de métricas de colegas do mesmo setor. • Benchmark global: média de métricas de pares no mercado global
Tempo médio para eliminar (mensal)	Gráfico de linhas	Resolução média mensal em dias para erradicar incidentes de segurança.
Tempo médio para identificar (mensal)	Pontuação única	Resolução média mensal em dias para identificar os incidentes de segurança.
Tempo médio de contenção (mensal)	Pontuação única	Resolução média mensal em dias para conter incidentes de segurança.
Incidentes ativos por prioridade e categoria	Mapa térmico	Contagem de incidentes de segurança ativos, que são categorizados por prioridade e categoria.
Tendência de incidentes encerrados e em aberto	Barra de  vertical	Detalhamento de incidentes encerrados e abertos.

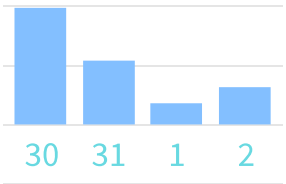
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidentes

Métricas	Tipo	Descrição
Incidentes ativos por estados	Barra de  vertical	Detalhamento de incidentes ativos com base em seus estados.

Prontidão do funcionário

Métricas	Tipo	Descrição
Visão geral da simulação de phishing mensal	Barra de  vertical	Soma de usuários que realizaram ações como abrir, clicar e relatar na simulação de phishing junto com a soma do total de usuários de cada simulação nos últimos seis meses.

Risco e conformidade

Para exibir os widgets de risco e conformidade, você deve ativar os plug-ins do GRC. Para obter informações sobre plug-ins do GRC, consulte a seção Aplicações para ativar. Para obter informações sobre widgets do GRC, consulte Painel de risco e conformidade para GRC: Metrics.

Indicadores

ANS de host – Encerrado

Este indicador é calculado diariamente. Ele considera a idade total de todas as vulnerabilidades de host que foram encerradas no dia anterior no momento do cálculo.

ANS de contêiner – Encerrado

Este indicador é calculado diariamente. Ele considera todas as vulnerabilidades de contêiner que foram encerradas no dia anterior no momento do cálculo.

ANS de aplicação – Encerrado

Este indicador é calculado diariamente. Ele considera a idade total de todas as vulnerabilidades da aplicação que foram encerradas no dia anterior no momento do cálculo.

ANS de resultado de testes – Aprovado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Ele considera todas as vulnerabilidades de resultado de testes que foram aprovadas no dia anterior no momento do cálculo.

ANS de host – Contagem encerrada

Este indicador é calculado diariamente. Ele considera a contagem de todas as vulnerabilidades de host que foram encerradas no dia anterior no momento do cálculo.

ANS de contêiner – Contagem de encerrados

Este indicador é calculado diariamente. Ele considera a contagem de todas as vulnerabilidades de contêiner que foram encerradas no dia anterior no momento do cálculo.

ANS de aplicação – Contagem de encerrados

Este indicador é calculado diariamente. Ele considera a contagem de todas as vulnerabilidades da aplicação que foram encerradas no dia anterior no momento do cálculo.

ANS de resultado de testes – Contagem aprovada

Este indicador é medido diariamente. Ele considera a contagem de todas as vulnerabilidades de resultado de testes que foram aprovadas pela última vez no dia anterior no momento do cálculo.

Ativos verificados

Este indicador é calculado diariamente. Ele considera a soma de ICs verificados da tabela sn_vul_analytics_scan_coverage_config, que inclui aqueles verificados pela última vez nos últimos 90 dias, em todas as classes de IC do CMDB.

Ativos verificáveis

Este indicador é calculado diariamente. Ele considera a soma do total de ICs da tabela sn_vul_analytics_scan_coverage_config para todas as classes de IC do CMDB presentes.

Itens vulneráveis

Este indicador é calculado diariamente. Ele considera a contagem de itens vulneráveis ativos no momento do cálculo.

Item vulnerável da aplicação

Este indicador é calculado diariamente. Ele considera a contagem de itens vulneráveis de aplicação ativos no momento do cálculo.

Item vulnerável de contêiner

Este indicador é calculado diariamente. Ele considera a contagem de itens vulneráveis de contêiner ativos no momento do cálculo.

Soma da idade dos itens vulneráveis

Este indicador é calculado diariamente. Ele considera a soma da idade dos itens vulneráveis ativos no momento do cálculo.

Soma da idade dos itens vulneráveis da aplicação

Este indicador é calculado diariamente. Ele considera a soma da idade dos itens vulneráveis da aplicação ativos no momento do cálculo.

Itens vulneráveis aberto

Este indicador é calculado diariamente. Ele considera os itens vulneráveis em aberto no momento do cálculo.

Itens vulneráveis de contêiner em aberto

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Ele considera os itens vulneráveis de contêiner em aberto no momento do cálculo.

Itens vulneráveis de aplicação em aberto

Este indicador é calculado diariamente. Ele considera os itens vulneráveis da aplicação abertos no momento do cálculo.

VITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como item vulnerável de host.

AVITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como um item vulnerável da aplicação.

CVITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como um item vulnerável de contêiner.

Resultados de testes adiados

Este indicador é calculado diariamente. Ele considera os resultados de testes que estavam em um estado adiado.

Aguardando implementação dos IVs ativos

Este indicador é calculado diariamente. Ele considera os itens vulneráveis que têm um estado como aguardando implementação no momento do cálculo.

Problemas de configuração em aberto – Resultados de testes

Este indicador é calculado diariamente. Ele tem uma origem de indicador como resultado de testes para o Painel unificado da Resposta a vulnerabilidades.

Incidente de segurança: tempo médio de identificação

Este indicador é calculado diariamente. Ele considera o incidente de segurança em que a definição é tempo de identificação no momento do cálculo.

Incidente de segurança: tempo médio de duração

Este indicador é calculado diariamente. Ele considera o incidente de segurança em que a definição é a duração do estado do incidente no momento do cálculo.

Número de incidentes de segurança importantes em aberto

Este indicador é calculado diariamente. Ele considera os incidentes de segurança graves em aberto no momento do cálculo.

Número de incidentes de segurança encerrados

Este indicador é calculado diariamente. Ele considera os incidentes de segurança encerrados no momento do cálculo.

Itens vulneráveis da aplicação encerrados

Este indicador é calculado diariamente. Ele considera os itens vulneráveis da aplicação encerrados no momento do cálculo.

Itens vulneráveis do contêiner encerrados

Este indicador é calculado diariamente. Ele considera itens vulneráveis de contêiner encerrados no momento do cálculo.

Itens vulneráveis encerrados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Ele considera itens vulneráveis encerrados no momento do cálculo.

Obter pontuação de risco máximo para itens vulneráveis

Este indicador é calculado diariamente. Ele considera a pontuação de risco máximo para itens vulneráveis no momento do cálculo.

Obter pontuação de risco máximo para item vulnerável de contêiner

Este indicador é calculado diariamente. Ele considera a pontuação de risco máximo para itens vulneráveis de contêiner no momento do cálculo.

Obter pontuação de risco máximo para itens vulneráveis de aplicação

Este indicador é calculado diariamente. Ele considera a pontuação de risco máximo para itens vulneráveis da aplicação no momento do cálculo.

Soma da pontuação de risco de VITs

Este indicador é calculado diariamente. Ele considera a soma das pontuações de risco dos itens vulneráveis no momento do cálculo.

Soma da pontuação de risco de AVIs

Este indicador é calculado diariamente. Ele considera a soma das pontuações de risco dos itens vulneráveis da aplicação no momento do cálculo.

Soma da pontuação de risco de CVIs

Este indicador é calculado diariamente. Ele considera a soma das pontuações de risco dos itens vulneráveis do contêiner no momento do cálculo.

Obter pontuação de risco máximo para incidentes de SI

Este indicador é calculado diariamente. Ele considera as pontuações de risco máximo dos incidentes de segurança no momento do cálculo.

Obter pontuação máxima de risco para resultados de testes de configuração incorreta

Este indicador é calculado diariamente. Ele considera as pontuações de risco máximo para configuração incorreta de resultados de testes no momento do cálculo.

Obter pontuação média de risco para resultados de testes de configuração incorreta

Este indicador é calculado diariamente. Ele considera as pontuações de risco médio para configuração incorreta de resultados de testes no momento do cálculo.

Número de incidentes de segurança em aberto

Este indicador é calculado diariamente. Ele considera os incidentes de segurança em aberto no momento do cálculo.

Visão geral do phishing

Este indicador é calculado diariamente. Ele considera a contagem de métricas de simulação de segurança no momento do cálculo.

MTTR agregado

Calcula o tempo médio necessário para fechar vulnerabilidades (hosts, contêineres e aplicações) e o tempo necessário para fechar os resultados de testes em dias. [[ANS de host - Encerrado]] + [[ANS de aplicação - Encerrado]] + [[ANS de contêiner - Encerrado]] + [[ANS de resultado de teste - Aprovado]]) / ([[ANS de host - Contagem de encerrados]] + [[ANS de aplicação – Contagem de encerrados]] + [[ANS de resultado de testes – Contagem de aprovados]] + [[ANS de contêiner – Contagem de encerrados]])

Cobertura de verificação atual

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calcula a porcentagem usando a proporção entre o número de itens verificados e o número total de itens qualificados para verificação durante o mesmo período. var scanItems =[[Scanned Assets]];var scannableItems = [[Scannable Assets]];var res;if (scannedItems == 0)res = 0;elseres = snapshotItems / scannableItems * 100;if (res > 100)res = 100;res;

Idade média dos itens vulneráveis ativos

Calcula a idade média de todos os itens vulneráveis ativos (hosts, contêineres e aplicações) em dias. ([[Soma da idade dos itens vulneráveis]] + [[Soma da idade dos itens vulneráveis de aplicação]] + [[Soma da idade dos itens vulneráveis de contêiner]]) / ([[Itens vulneráveis]] + [[Itens vulneráveis da aplicação]] + [[Itens vulneráveis do contêiner]])

VITs ativos por idade e classificação de risco

Calcula a contagem total de todos os itens vulneráveis ativos (hosts, contêineres e aplicações) categorizados por idade e nível de avaliação de risco. [[Itens vulneráveis abertos]] + [[Itens vulneráveis de contêiner abertos]] + [[Itens vulneráveis de aplicação abertos]]

Problemas adiados

Calcula a contagem total de todos os itens vulneráveis (hosts, contêineres, aplicações e resultados de testes) com o estado "Adiado". [[VITs adiados]] + [[AVITs adiados]] + [[Resultados de testes adiados]] + [[CVITs adiados]]

Média de tempo de resolução de incidentes de segurança em aberto

Calcula o tempo médio necessário para encerrar os incidentes de segurança em dias. ([[Soma da duração de incidentes de segurança encerrados]] / [[Número de incidentes de segurança encerrados]]) /24

Pontuação de segurança

Calcula as classificações gerais de segurança diariamente. É calculado com base na pontuação de risco acumulada. var secPostureRating = 100 - [[Pontuação de segurança]]; secPostureRating;

Pontuação de segurança (unidades de negócios)

Calcula a pontuação de risco acumulada final em que a pontuação de risco de acúmulo de itens vulneráveis, erros de configuração, incidentes de segurança e incidentes de segurança graves é multiplicada com os respectivos pesos que são obtidos da tabela de acúmulo de postura de segurança. var numMajorIncidents = [[Número de incidentes de segurança graves em aberto]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[Pontuação de risco acumulada de vulnerabilidade e configuração incorreta]] * 20 + [[Pontuação de risco acumulada de vulnerabilidade de OT]] * 20 + [[Obter pontuação de risco máximo para incidentes de SI]] * 20 + majorSIRiskScore * 40)/100 ; rollUpRiskScore;

Pontuação de segurança (serviços de negócio)

Calcula a pontuação de risco acumulada final em que a pontuação de risco de acúmulo de itens vulneráveis, erros de configuração, incidentes de segurança e incidentes de segurança graves é multiplicada com os respectivos pesos que são obtidos da tabela de acúmulo de postura de segurança. var numMajorIncidents = [[Número de incidentes de segurança graves em aberto - Serviços]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[Pontuação de risco acumulado de vulnerabilidade e configuração incorreta - Serviços]] * 20 + [[Pontuação de risco acumulado de vulnerabilidade de OT - Serviços]] * 20

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

+ [[Obter pontuação de risco máximo para incidentes de SI - Serviços]] * 20 + pontuaçãoSIRiskScore * 40)/100; rollUpRiskScore;

Pontuação de risco acumulado de vulnerabilidade

Calcula a pontuação de risco acumulada de vulnerabilidade em que a pontuação de risco máximo, a pontuação de risco média de itens vulneráveis e a contagem de itens vulneráveis são multiplicadas com seus respectivos pesos. var maxRiskScore = 100; var count = [[VITs ativos por idade e classificação de risco]]; var countRiskScore; se (0 == contagem) countRiskScore = 0; else if (contagem > 10000) countRiskScore = maxRiskScore; else if (contagem > 1000) countRiskScore = (maxRiskScore * 0,80); else if (contagem > 100) countRiskScore = (maxRiskScore * 0,60); else if (contagem > 10) countRiskScore = (maxRiskScore * 0,40); else countRiskScore = (maxRiskScore * 0,20); var vulRiskScore = ([[Obter pontuação máxima de todos os itens vulneráveis]] * 0 + [[Pontuação média de risco de todos os itens vulneráveis]] * 100 + countRiskScore * 0)/100; vulRiskScore;

Obter pontuação máxima de todos os itens vulneráveis

Calcula a pontuação de risco acumulada de vulnerabilidade em que a pontuação de risco máximo, a pontuação de risco média de itens vulneráveis e a contagem de itens vulneráveis são multiplicadas com seus respectivos pesos. var maxScoreForVI = [[Obter pontuação de risco máximo para itens vulneráveis]], maxScoreForCVI = [[Obter pontuação de risco máximo para item vulnerável de contêiner]], maxScoreForAVI = [[Obter pontuação de risco máximo para itens vulneráveis da aplicação]], maxScore; se (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI; caso contrário, se (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI; else maxScore = maxScoreForAVI; pontuação máxima;

Pontuação de risco médio de todos os itens vulneráveis

Calcula a pontuação de risco médio de todos os itens vulneráveis (hosts, contêineres e aplicações). var summedRiskScore = [[Soma da pontuação de risco de VITs]] + [[Soma da pontuação de risco de IVAs]] + [[Soma da pontuação de risco de CVIs]], avgRiskScore; var totalVulCount = [[Itens vulneráveis abertos]] + [[Itens vulneráveis de aplicação abertos]] + [[Itens vulneráveis de contêiner abertos]]; if(summedRiskScore == 0) avgRiskScore = 0; else if(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount; PontuaçãoDeRisco média;

Pontuação de risco acumulada de configuração incorreta

Calcula a pontuação de risco acumulada de configuração incorreta usando os resultados de testes categorizados como Falha, Erro ou Desconhecido. var maxRiskScore = 100; var count = [[Problemas de configuração em aberto - Resultados de testes]]; var countRiskScore; se (0 == contagem) countRiskScore = 0; else if (contagem > 10000) countRiskScore = maxRiskScore; else if (contagem > 1000) countRiskScore = (maxRiskScore * 0,80); else if (contagem > 100) countRiskScore = (maxRiskScore * 0,60); else if (contagem > 10) countRiskScore = (maxRiskScore * 0,40); else countRiskScore = (maxRiskScore * 0,20); var miRiskScore = ([[Obter pontuação de risco máximo para resultados de testes de configuração incorreta]] * 0 + [[Obter pontuação de risco médio para resultados de testes de configuração incorreta]] * 100 + countRiskScore * 0)/100; PontuaçãoDeRisco incorreta;

Tempo médio para eliminar

Calcula o tempo médio necessário para erradicar incidentes de segurança em dias [[Incidente de segurança - Tempo médio de duração > Estado do incidente de segurança = Erradicar]] / 1440

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo médio para identificar

Calcula o tempo médio necessário para identificar incidentes de segurança em dias. [[Incidente de segurança - Tempo médio de identificação]] / 1440

Tempo médio de contenção

Calcula o tempo médio necessário para conter incidentes de segurança em dias. [[Incidente de segurança - Tempo médio de duração > Estado do incidente de segurança = Conter]] / 1440

Cumprimento da meta de correção

Calcula a porcentagem mensal de adesão à meta de correção a partir de resultados de testes, itens vulneráveis, itens vulneráveis de contêiner e itens vulneráveis de aplicação. A adesão à meta é determinada pelo número de itens que atenderam à meta definida. ([[ANS de resultado de testes - Contagem aprovada > Status da correção (unificada) = Meta atingida]] + [[ANS do contêiner - Contagem encerrada > Status da correção (unificada) = Meta atendida]] + [[ANS da aplicação - Contagem encerrada > Status da correção (unificado) = Meta atingida]] + [[ANS de host - Contagem encerrada > Status da correção (unificado) = Meta atingida]]) / ([[ANS de resultado de testes - Contagem de aprovados]] + [[ANS de contêiner - Contagem encerrada]] + [[ANS de aplicação - Contagem de encerrados]] + [[ANS de host - Contagem de encerrados]]) * 100

Eficiência de correção mensal (todos os itens vulneráveis)

Calcula a porcentagem mensal de itens vulneráveis encerrados, itens vulneráveis de contêineres e itens vulneráveis de aplicação em comparação com os recém-identificados. var closedItems = [[ANS de host - Contagem de encerrados]] + [[ANS de contêiner - Contagem de encerrados]] + [[ANS de aplicação - Contagem de encerrados]] + [[ANS de resultado de teste - Contagem aprovada]];

var newItems = [[VITs de host abertos/reabertos ontem]] + [[VITs de contêiner abertos/reabertos ontem]] + [[VITs de aplicação abertos/reabertos ontem]] + [[Resultados de testes abertos/reabertos ontem]];

var res = 0;if (closedItems == 0) res = 0;else if (newItems .=0)res = closedItems / newItems * 100;if (res > 1000) res = 1000; res;

VITs do host abertos/reabertos ontem

Este indicador é calculado diariamente. Ele considera os itens vulneráveis de host que foram abertos pela última vez no dia anterior no momento do cálculo.

VITs da aplicação abertos/reabertos ontem

Este indicador é calculado diariamente. Ele considera os itens vulneráveis da aplicação que foram abertos pela última vez no dia anterior no momento do cálculo.

VITs do contêiner abertos/reabertos ontem

Este indicador é calculado diariamente. Ele considera os itens vulneráveis de contêiner que foram abertos pela última vez no dia anterior no momento do cálculo.

Resultados de testes abertos/reabertos ontem

Este indicador é calculado diariamente. Ele considera os resultados de testes que foram vistos pela última vez no dia anterior no momento do cálculo.

Itens vulneráveis de OT

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Ele considera os itens vulneráveis de OT ativos presentes no momento do cálculo.

Soma da duração de OT de vulnerabilidades encerradas

Este indicador é calculado diariamente. Ele considera a idade total de todas as vulnerabilidades de OT que estão fechadas no dia do cálculo.

Itens vulneráveis fechados de OT

Este indicador é calculado diariamente. Ele considera os itens vulneráveis de OT que estão encerrados no dia do cálculo.

Idade média dos itens vulneráveis ativos de OT

Calcula a idade média dos itens vulneráveis de OT ([[Soma da idade dos itens vulneráveis de OT]] / [[Itens vulneráveis de OT]])

Detalhamentos

- Unidade de negócios
- Serviços de negócio
- Pontuação de risco
- Faixa etária
- Grupo de atribuição (unificado)
- Status da meta de correção (Encerrado)
- Classe de ativo
- Categoria de ativo
- Classificação de risco (unificada)
- Motivo adiado (unificado)
- Estado do Incidente de segurança
- Prioridade de Incidente de segurança
- Categoria de Incidente de segurança
- Evento de phishing
- Motivo adiado de não encerramento (unificado)

Aplicações a serem ativadas

Você deve ativar as seguintes aplicações para preencher a pontuação nos widgets. Com base na aplicação que você está usando, você deve ativar as aplicações dependentes.

Se você estiver usando	Ativar
Resposta a vulnerabilidades	• Performance Analytics para Resposta a vulnerabilidades • Base para resposta a vulnerabilidades • Resposta a vulnerabilidades

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você estiver usando	Ativar
	• Vulnerability Response e Configuration Compliance para contêineres • Conformidade de configurações
Operational Technology	Resposta a vulnerabilidades para tecnologia operacional
Integrações de phishing	• Simulação de segurança e integração de treinamento para SecOps • Integração KnowBe4 para SecOps • Integração do Microsoft Defender for Office365 para SecOps
Resposta a incidentes de segurança	• Performance Analytics para Security Incident Response • Resposta a incidentes de segurança • Gestão de incidentes graves de segurança
Governança, risco e conformidade	• GRC: Elementos Comuns do Painel • GRC: Espaço de gestão de riscos • Risco avançado para GRC • GRC: Espaço de gestão de conformidade

Trabalhos agendados para coleta de dados

Os seguintes trabalhos agendados são executados para coletar pontuações em novos dados automaticamente.

Trabalho agendado	Frequência	Descrição
Carregar as pontuações do parâmetro de comparação	Sob demanda	Coleta pontuações da instância e publica na instância central. Os algoritmos de parâmetro de comparação calculam as melhores pontuações do setor.
Baixar as pontuações do parâmetro de comparação	Sob demanda	Baixa as pontuações do parâmetro de comparação. Está disponível na tabela Pontuações de parâmetro de comparação [sn_bm_client_score_list].

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aceitar pontuações de parâmetro de comparação

Obtenha pontuações de parâmetro de comparação registrando sua instância na instância central ServiceNow. Este último mantém informações de vários setores para fornecer a pontuação do parâmetro de comparação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Para registrar sua instância na instância central, siga estas etapas:
   a. Navegar até **Todos** > **Propriedades do sistema** > **Todas as Propriedades**.
   b. Selecione *sn_bm_client.central_instance_url* propriedade do sistema.
   c. No campo **Valor**, insira o URL da instância central do parâmetro de comparação.

      Nota: Se a instância for provisionada, seus detalhes serão enviados por push para a instância central automaticamente.

   d. Selecione **Aceitar no** widget para validar e estabelecer uma conexão com a instância central.
2. Para carregar sua pontuação na instância central, siga estas etapas:
   a. Navegar até **Todos** > **Scheduler do Sistema** > **Trabalhos agendados**
   b. Selecione o trabalho agendado *Upload the benchmark scores*.
   c. Selecione **Atualizar**.
      As pontuações são carregadas na instância central. No entanto, os trabalhos agendados pela instância central são executados uma vez por mês para atualizar as pontuações nos widgets do painel.
3. Para baixar a pontuação da instância central, siga estas etapas:
   a. Navegar até **Todos** > **Scheduler do Sistema** > **Trabalhos agendados**
   b. Selecione o trabalho agendado *Download the benchmark scores*.
   c. Selecione **Executar agora**.
      As pontuações estão disponíveis na tabela Pontuações de parâmetro de comparação [sn_bm_client_score_list], que é refletida nos widgets do painel.

Definir metas

Defina metas em dias para corrigir vulnerabilidades, incidentes de segurança e erros de configuração.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Selecione **Destinos** no widget ou selecione o ícone de **Destinos** na página Detalhes de KPI.
2. Selecione o botão **Para todos**.
3. No campo **Novo valor**, insira o número de dias em que você deseja atingir a meta.
4. Selecione a data de início da meta.
5. Selecione a data de revisão desejada.
6. Selecione **Atualizar**.

Simulação de segurança e integração de treinamento para Operações de segurança

Fortaleça a defesa da sua organização contra ameaças importantes à segurança cibernética, incorporando integrações de phishing ao Painel executivo de segurança cibernética. As integrações de phishing aprimoram o Painel executivo de segurança cibernética incorporando dados de ferramentas de simulação de phishing de terceiros, como KnowBe4 e Microsoft Defender para Office 365.

As seguintes integrações elevam os recursos do Painel executivo de segurança cibernética, fornecendo uma perspectiva unificada sobre a postura de segurança da sua organização, a prontidão dos funcionários e a suscetibilidade a ataques de phishing:

- Integração KnowBe4
- Integração do Microsoft Defender para Office 365

Configurar integração do Knowbe4

Obtenha informações imediatas sobre a vulnerabilidade de sua equipe a ataques de phishing, integrando ao KnowBe4, uma plataforma líder de treinamento em conscientização de segurança cibernética. Por meio da integração do KnowBe4, identifique tendências e áreas de melhoria em seus programas de treinamento de segurança cibernética, monitore a resiliência geral ao phishing e fortaleça proativamente as medidas de segurança da sua organização.

Antes de Iniciar
Função necessária: sn_sec_phish.admin e sn_sec_phish_kb4.kb4_admin

Procedimento

1. Navegar até **Todos** > **Integração KnowBe4** > **Configurações do KnowBe4**.
2. Selecione **Novo**.
3. No formulário, preencha os detalhes:

Formulário de configuração do KnowBe4

Campo	Descrição
Instância de Integração	Nome da instância de integração. Selecione a instância de integração usando o ícone de pesquisa.
URL base	URL para integração com KnowBe4.
Chave de API	Chave de API adquirida da conta KnowBe4.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Página	Número da página de onde as simulações devem ser buscadas.
Tamanho da Página	Número de simulações que devem ser incluídas.

a. Selecione **Novo** se nenhuma instância de integração estiver disponível.

b. No formulário, preencha os detalhes:

Formulário de instância de integração

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Nome da aplicação (KnowBe4 Integration for SecOps).
Integração	KnowBe4 é o padrão.
Ativo	O padrão é ativado (selecionado). Se desmarcada, a instância não está ativa.
Descrição	Descrição resumida da instância de integração.

4. Selecione **Enviar**.
5. Navegar até **Todos** > **Simulação e treinamento de segurança** > **Integrações**.
6. Selecione a integração do Knowbe4.
7. Selecione **Executar agora** para executar e coletar dados do KnowBe4.

Configurar integração do Microsoft Defender para Office 365

Obtenha informações valiosas sobre métricas de simulação de phishing diretamente no Painel executivo de segurança cibernética por meio da integração perfeita com o Microsoft Defender para Office 365.

Antes de Iniciar

Função necessária: sn_sec_phish_msatk.ms_admin

Procedimento

1. Navegar até **Todos** > **Integração de ataque da Microsoft** > **Configurações de ataque da Microsoft**.
2. Selecione **Novo**.
3. No formulário, preencha os detalhes:

Formulário de configuração de ataque da Microsoft

Campo	Descrição
Instância de Integração	Nome da instância de integração. Selecione a instância de integração usando o ícone de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID de locatário	ID do locatário da aplicação criada no portal do Microsoft Azure.
ID de cliente	ID de cliente da aplicação criada no portal do Microsoft Azure.
Segredo do cliente	Segredo do cliente da aplicação criada no portal do Microsoft Azure.
Marcador	Data a partir da qual as simulações devem ser obtidas.
URL de token	URL base de onde o token é criado para acessar a API de simulações da Microsoft.
URL de todas as simulações	URL base da API de simulações da Microsoft.

a. Selecione **Novo** se nenhuma instância de integração estiver disponível.

b. No formulário, preencha os detalhes:

Formulário de instância de integração

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Nome da aplicação (Microsoft Defender para Office 365).
Integração	Referência de integração de terceiros (integração de ataque da Microsoft).
Ativo	O padrão é ativado (selecionado). Se desmarcada, a instância não está ativa.
Descrição	Descrição resumida da instância de integração.

4. Selecione **Enviar**.

5. Navegar até **Todos** > **Simulação e treinamento de segurança** > **Integrações**.

6. Selecione a integração do Microsoft Ataque.

7. Selecione **Executar agora** para executar e coletar dados da Microsoft.

Painel de risco e conformidade para GRC: Metrics

O painel Risco e conformidade fornece aos usuários de conformidade e risco uma visão geral abrangente das informações de risco e conformidade em um único painel que ajuda em suas principais decisões.

Você pode navegar até o painel Risco e conformidade a partir do único Painel executivo de cibersegurança unificado para exibir as métricas de risco e conformidade das aplicações Governança, risco e conformidade.

O painel fornece recursos como:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Visão geral da conformidade
- Visão geral de risco
- Visão geral de privacidade
- Visão geral da continuidade de negócios
- Risco de terceiros
- Visão geral da auditoria

Pré-requisitos para acessar o painel Risco e conformidade

Importante: Você deve ter acesso primário ao Painel executivo de cibersegurança para ativar o plug-in funcional de segurança cibernética e risco com o qual você pode acessar o painel de risco e conformidade.

Um novo domínio funcional foi introduzido para separar dados relacionados à segurança cibernética e a riscos. Você pode ativar o plug-in de segurança cibernética e risco selecionando o botão **Ativar** ação de IU. Por padrão, este domínio funcional está inativo.

Funções necessárias de Now Platform

A função do usuário GRC principal é sn_grc_dashboards.grc_ciso_user, que pode exibir os relatórios no painel Risco e conformidade. Esta função contém:

- sn_compliance.reader
- sn_risk.reader

Nota: No entanto, você deve ter a função sn_bod.ciso para fazer login, exibir e compartilhar o Painel executivo de segurança cibernética a partir do qual é possível navegar até o Painel de risco e conformidade.

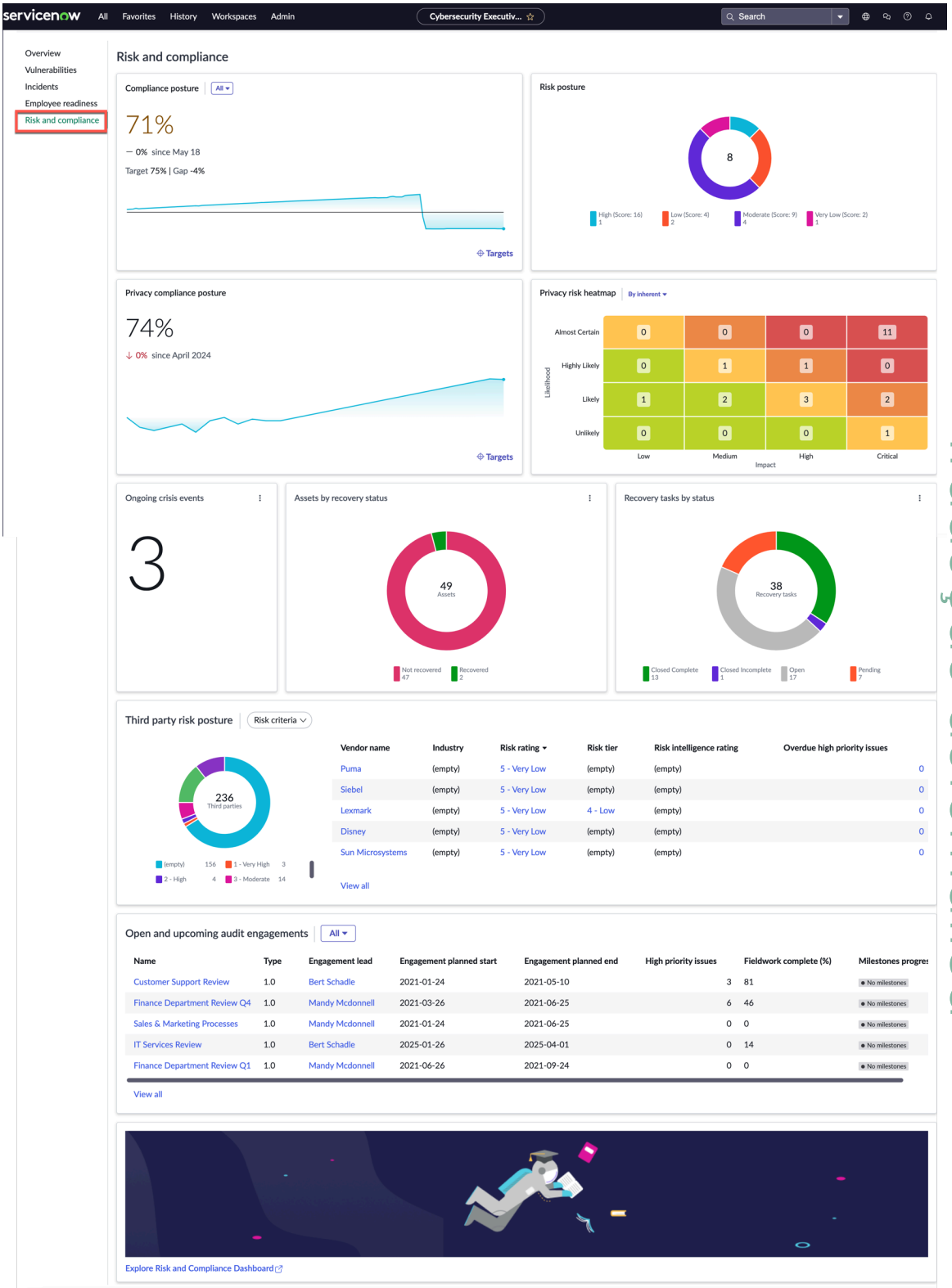
Acessar o painel de risco e conformidade

1. Para acessar o painel Risco e conformidade, navegue até **Todos** > **Painel executivo de cibersegurança** > **Painel executivo de cibersegurança**.
2. Selecione o rótulo **Risco e conformidade** na lista à esquerda do painel.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel executivo unificado de segurança cibernética para métricas de risco e conformidade



Tradução automática

3. Para visualizar seus dados e os relatórios e soluções disponíveis no painel projetado para o usuário, selecione o rótulo Explorar painel de risco e conformidade.

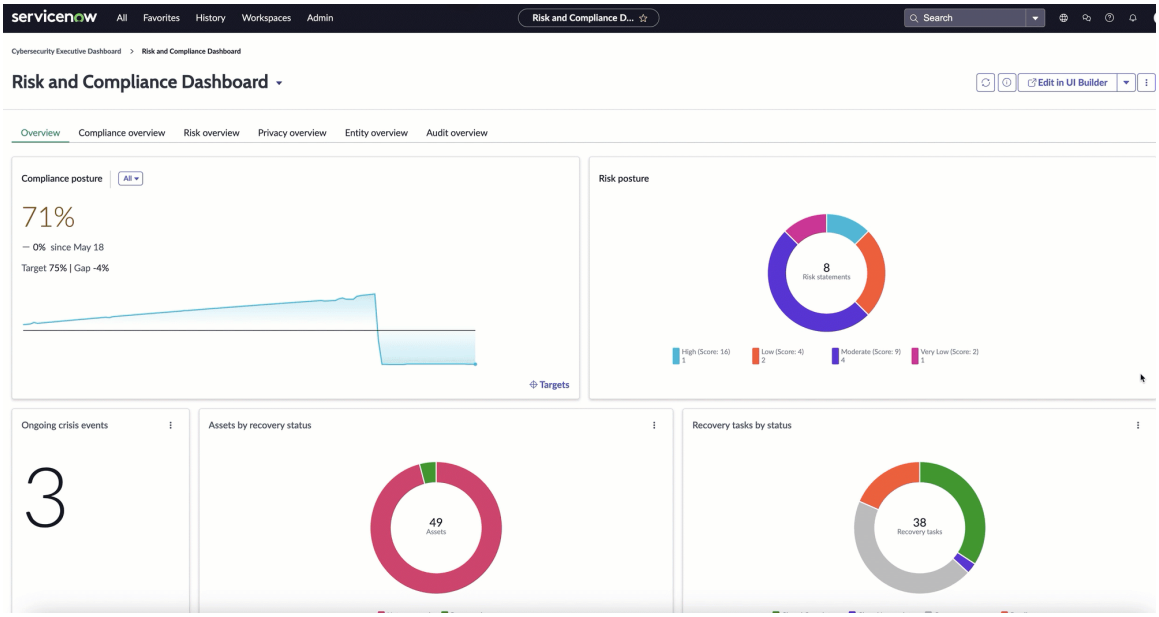
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios e soluções do Painel derisco e conformidade

O painel Risco e conformidade é um painel unificado que fornece dados analíticos abrangentes de relatórios disponíveis nas principais aplicações GRC para que o diretor de segurança da informação entenda a postura de conformidade e risco da organização. O painel consolida dados de vários produtos no pacote de aplicações ServiceNow GRC.

Nota: Todos os relatórios estão disponíveis somente quando os espaços correspondentes estão instalados.

Painel de risco e conformidade



Funções necessárias de Now Platform

Para relatórios relacionados à Conformidade

O usuário deve ter as funções sn_grc_dashboards.grc_ciso_user e sn_bod.ciso.

Para relatórios relacionados a riscos

O usuário deve ter as funções sn_grc_dashboards.grc_ciso_user e sn_bod.ciso.

Para relatórios relacionados à Gestão de continuidade de negócio

O usuário deve ter as funções sn_bcm.viewer e sn_bod.ciso.

Para relatórios relacionados a riscos de terceiros

O usuário deve ter as funções sn_vdr_risk_asmt.vendor_assessment_reviewer e sn_bod.ciso.

Para relatórios relacionados à privacidade

O usuário deve ter as funções sn_privacy.analyst e sn_bod.ciso.

Para relatórios relacionados à auditoria

O usuário deve ter as funções sn_audit_ws.auditor e sn_bod.ciso.

Acessar o Painel de risco e conformidade

Para abrir o painel, navegue até **Todos** > **Painel executivo de cibersegurança** > **Painel executivo de cibersegurança**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Postura de conformidade

- Percentual de conformidade: indicador de fórmula que descreve a postura de conformidade.
- Todos os controles: indicador automatizado que oferece suporte ao indicador de fórmula.
- Controles de conformidade: indicador automatizado que oferece suporte ao indicador de fórmula.

Postura de conformidade com a privacidade

Indicador do PA: percentual de pontuação de conformidade da atividade de processamento.

Detalhamentos

Domínio funcional.

Relatórios

Nota: Todos os relatórios estão disponíveis somente quando os espaços correspondentes estão instalados.

Guia Visão Geral

Título	Tipo	Tabela de origem	Descrição
Postura de conformidade	Gráfico	Controle [sn_compliance_control]	Fornece segurança cibernética e risco e postura de risco e conformidade de TI com base na análise de dados para os gerentes de conformidade.
Postura de risco	Gráfico	As tabelas de origem são as seguintes: • Risco [sn_risk_risk] • Risco agregado detalhado [sn_risk_advanced_risk_assessment_result] (quando a aplicação Risco avançado está instalada e a Avaliação de risco avançada está habilitada	Fornece a contagem de risco com base nas classificações de risco.
Eventos de crise em andamento	Pontuação	Evento de recuperação [sn_recovery_event]	Exibe o número total de eventos de crise em andamento

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão Geral

Título	Tipo	Tabela de origem	Descrição
		em que o tipo de evento é real	que não foram aprovados nem encerrados.
Ativos por status de recuperação	Gráfico	Ativos [sn_recovery_event_asset]	Fornece o número total de ativos para eventos de crise em andamento agrupados por status de recuperação, incluindo ativos que foram recuperados e aqueles que não foram.
Tarefas de recuperação por status	Gráfico	Tarefas de recuperação [sn_recovery_event_task]	Fornece o status das tarefas de recuperação em vários estados para eventos de crise em andamento.

Guia Visão geral de conformidade

Título	Tipo	Tabela de origem	Descrição
Documentos de autoridade	Gráfico	Documento de autoridade [sn_compliance_authority_document]	Fornece dados de documentos de autoridade em conformidade e fora de conformidade no gráfico. A lista fornece detalhes dos documentos de autoridade, sua pontuação de conformidade individual em porcentagem, contagem de problemas de alta prioridade e exceções de alto risco nos documentos de autoridade e a contagem de casos em conformidade.
Políticas	Gráfico	Política [sn_compliance_policy]	Fornece a contagem de políticas em conformidade e fora de conformidade no gráfico. A lista

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de conformidade

Título	Tipo	Tabela de origem	Descrição
			fornece detalhes das políticas, sua pontuação de conformidade individual em porcentagem, contagem de problemas de alta prioridade e exceções de risco geradas em cada política e a contagem de casos em conformidade.

Guia Visão geral de risco

Título	Tipo	Tabela de origem	Descrição
Postura de risco	Gráfico	As tabelas de origem são as seguintes: • Risco [sn_risk_risk] • Risco agregado detalhado [sn_risk_advanced_risk_assessment_result] (Quando a aplicação Risco avançado está instalada e a Avaliação de risco avançada está habilitada)	Fornece a contagem de risco com base nas classificações de risco.
Postura de risco	Lista	Status do conteúdo do GRC [sn_grc_content_reports]	Fornece a classificação de risco para cada risco organizacional para entender os resultados gerais da avaliação de risco. Essas classificações ajudam as organizações a entender o possível impacto e a probabilidade de vários riscos, permitindo que priorizem e gerenciem esses riscos. O cartão

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de risco

Título	Tipo	Tabela de origem	Descrição
			de postura de risco também destaca as seguintes informações para cada risco: • **Apetite**de risco : valor de apetite de risco definido. • **Problemas de alta prioridade**: o número de problemas com prioridade é definido como Alto. • **Tarefas**de resposta a riscos atrasadas : número de tarefas de resposta a riscos atrasadas. • Percentual de violação de**KRI**: percentual de KRIs (Key Risk Indicators, principais indicadores de risco) que excederam os limites predefinidos.
Postura de risco de terceiros	Gráfico	Riscos de terceiros [sn_grc_dashboards_third_party_risk]	Fornece a classificação de risco de cada terceiro. A classificação de risco é a classificação de avaliação geral que considera as pontuações e classificações de todas as avaliações realizadas para um terceiro ou fornecedor. O cartão de postura de risco de terceiros também destaca as seguintes informações de cada terceiro ou fornecedor:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de risco

Título	Tipo	Tabela de origem	Descrição
			• **Critérios de risco**: grupo de domínios de risco (às vezes chamados de áreas de risco em outros recursos da plataforma) que se aplica a um tipo específico de terceiro. • **Nível de risco**: valor determinado com base nas respostas coletadas após a conclusão de uma avaliação de risco inerente (IRQ). • **Classificação de inteligência de risco**: agregado de todas as pontuações coletadas de provedores de inteligência de risco. • **Tarefas**de resposta a riscos atrasadas : número de tarefas de resposta a riscos atrasadas.

Guia Visão geral de privacidade

Título	Tipo	Tabela de origem	Descrição
Postura de conformidade com a privacidade	Linha de linha	Indicador de PA: porcentagem de pontuação de conformidade da atividade de processamento [pa_indicators]	Fornece a postura de conformidade por mês e é representada graficamente com referência à pontuação de conformidade geral em todas as atividades de processamento.
Problemas de alta prioridade atrasados	Pontuação	Problemas [sn_grc_issue]	Fornece uma visão geral focada

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral de privacidade

Título	Tipo	Tabela de origem	Descrição
			de todos os problemas atrasados relacionados à privacidade de alta prioridade, permitindo a identificação e resolução rápidas de tarefas críticas para garantir a conformidade e a proteção de dados.
Mapa térmico de risco de privacidade	Mapa térmico	Metodologia de avaliação de risco [sn_risk_advanced_risk_assessment_methodology]	Fornece os dados de avaliação de risco de privacidade na forma de um mapa térmico. As avaliações de risco de privacidade são avaliações detalhadas que são realizadas se a pontuação de criticalidade for alta. Avalie cada risco associado à atividade de processamento e saiba a pontuação de risco agregada na atividade de processamento. Depois de avaliar os riscos de privacidade, você pode exibir a postura de risco de privacidade no mapa térmico de risco.

Guia Visão geral da entidade

Título	Tipo	Tabela de origem	Descrição
Entidades	Lista	Status de conformidade da entidade [sn_compliance_entities_respond]	Fornece o resumo dos riscos diretamente associados à entidade que contribuem para a classificação de risco

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da entidade

Título	Tipo	Tabela de origem	Descrição
			geral da entidade. A lista também exibe a pontuação de conformidade das entidades e problemas de alta prioridade e exceções de risco que são gerados como resultado dos controles fora de conformidade associados à entidade.

Guia Visão geral da auditoria

Título	Tipo	Tabela de origem	Descrição
Compromissos de auditoria em aberto e futuros	Lista	Compromisso [sn_audit_engagement]	Fornece uma lista de compromissos de auditoria abertos e futuros. A lista também fornece detalhes do líder do compromisso para cada documento de autoridade, as datas de início e término planejadas de cada compromisso, problemas de alta prioridade, percentual de trabalho de campo concluído e os marcos em andamento.

Filtros

Nome	Tipo	Descrição
Critérios de risco	Relatório	Dependendo dos critérios de risco selecionados, o gráfico de donut e a lista mostram os terceiros ou fornecedores que estão nessas áreas de risco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

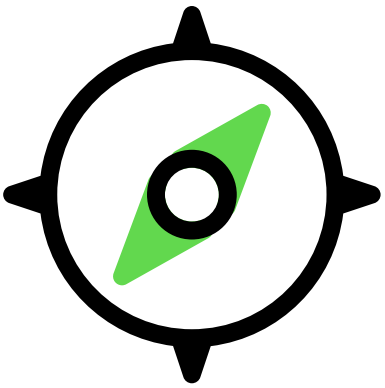
Central de segurança de inteligência contra ameaças

A plataforma Central de segurança de inteligência contra ameaças (TISC) fornece solução de tecnologia para agregação, gestão e operacionalização de inteligência contra ameaças.

Iniciar

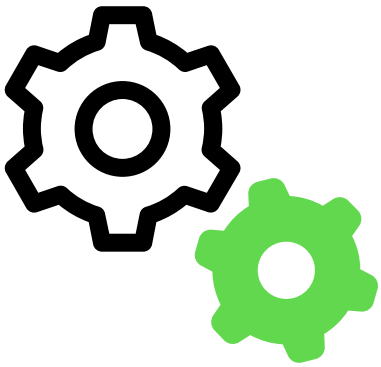
Clique em um bloco para começar.

Explorar



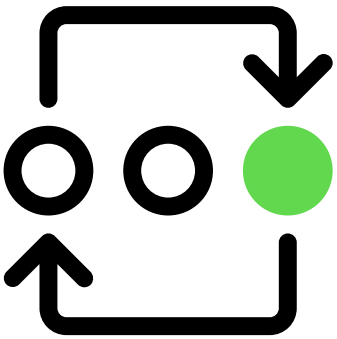
Saiba como a Central de segurança de inteligência contra ameaças pode ajudá-lo com seus principais recursos e benefícios.

Configurar



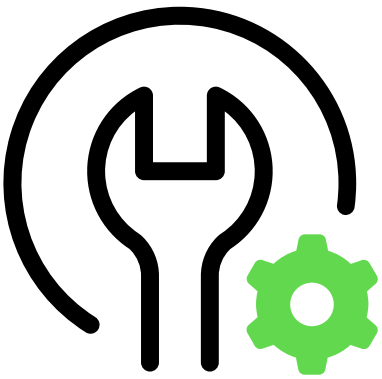
Defina e configure a Central de segurança de inteligência contra ameaças para atender às suas necessidades específicas.

Integrar



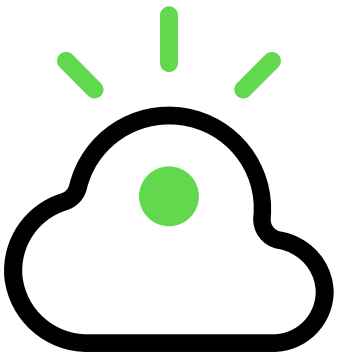
Integrar com a Central de segurança de inteligência contra ameaças

Administrar



Gerencie e personalize sua Central de segurança de inteligência contra ameaças.

Uso



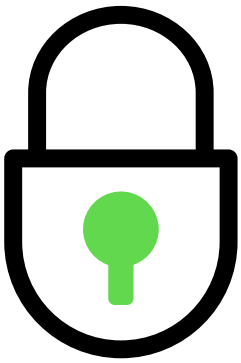
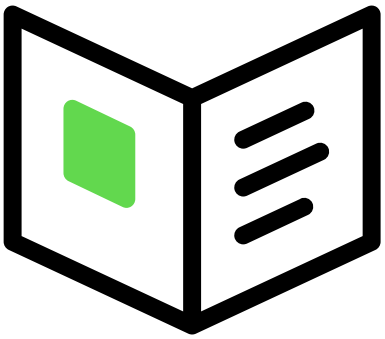
Gerencie sua biblioteca e objetos da Central de segurança de inteligência contra ameaças.

Modelos de relatório

Gerencie e personalize seus relatórios de gestão de casos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Repositório do MITRE ATT&CK	Arquivamento	Referência
		
Gerenciar dados do repositório do MITRE ATT&CK.	Gerenciar regras de arquivamento e destruição de dados.	Obtenha informações adicionais sobre a Central de segurança de inteligência contra ameaças.

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

A instalação de Central de segurança de inteligência contra ameaças (sn_sec_tisc) instalará automaticamente todas as aplicações dependentes de ServiceNow Store.

Mais recursos

Visite o Security Incident Response fórum no ServiceNow Community.

Solucionar problemas e obter ajuda

- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorar Central de segurança de inteligência contra ameaças

A Central de segurança de inteligência contra ameaças (TISC) permite que você colabore com as equipes de inteligência contra ameaças e tem vários recursos para coletar e processar vários feeds de inteligência contra ameaças e um espaço para analisar, colaborar, agir e compartilhar as informações necessárias.

A Central de segurança de inteligência contra ameaças foi aprimorada com recursos para gerenciar a coleta de dados, o processamento de dados, como desduplicação, normalização e agregação, análise de inteligência contra ameaças, disseminação de inteligência contra ameaças e também o espaço que fornece as tarefas de administração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

A seguir estão os principais recursos da Central de segurança de inteligência contra ameaças (TISC) que são explicados em detalhes nas próximas seções:

- Coleta de dados de diferentes fontes e em vários formatos.
- Agregação de dados de diversos feeds, incluindo STIX, XML, JSON e OpenIOC.
- Capacidades de aprimoramento, que envolvem a remoção de falsos positivos, confiança/pontuação de indicadores, validação de indicadores e adição de informações contextuais.
- Uma calculadora de pontuação de ameaça personalizada para avaliação de ameaças diferenciada.
- Integração de inteligência interna que abrange VR, SIR, ativos, serviços e CMDB.
- Caça a ameaças com gestão de casos e funcionalidades de tarefa.
- Painéis específicos do usuário adaptados para a persona de informações sobre ameaças.
- Ferramentas de visualização gráfica para compreender os dados de informações sobre ameaças.
- Um espaço dedicado para analistas de inteligência contra ameaças para operações simplificadas.
- Regras de correlação para estabelecer automaticamente relacionamentos entre observáveis.
- O sistema tem a capacidade de identificar e extrair automaticamente todos os observáveis dos arquivos carregados.
- Integração de feeds premium para aprimorar a inteligência contra ameaças.
- Capacitar os usuários a associar informações do MITRE ATT&CK a registros na biblioteca de Inteligência contra ameaças e gestão de casos.
- Integração com SIR e capacidades de migração de dados da Inteligência contra ameaças para a Central de segurança de Inteligência contra ameaças.

Terminologia de chave de TISC

Os termos definidos abaixo são usados em toda a Central de segurança de inteligência contra ameaças (TISC).

Definições de terminologia

Terminologia	Definição
Processamento de dados	Uma plataforma de inteligência contra ameaças (TIP) é uma solução de tecnologia que coleta, agrega e organiza dados de inteligência contra ameaças de várias origens e padrões. Inteligência contra ameaças são os dados coletados, processados e analisados para entender os alvos dos agentes de ameaça e os comportamentos de ataque.
Observáveis	Os observáveis representam propriedades com monitoramento de estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de terminologia

Terminologia	Definição
	ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes . Para obter mais informações, consulte Observáveis.
Indicadores	Os indicadores contêm um padrão que pode ser usado para detectar atividades cibernéticas suspeitas ou mal-intencionadas. Por exemplo, um indicador pode ser usado para representar um conjunto de domínios mal-intencionados e usar a linguagem de padronização STIX para especificar esses domínios. O SDO do indicador contém uma descrição textual simples, as fases da cadeia de eliminação nas quais ele detecta o comportamento, uma janela de tempo para quando o indicador é válido ou útil e uma propriedade de **padrão** necessária para capturar um padrão de detecção estruturado. Para obter mais informações, consulte Indicadores.
Objetos	Define o conjunto de objetos de domínio STIX (SDOs), cada um dos quais corresponde a um conceito exclusivo comumente representado na Inteligência contra ameaças cibernéticas (CTI). Usando SDOs e Objetos de Relacionamento STIX (SROs) como blocos de construção, os indivíduos podem criar e compartilhar informações amplas e abrangentes sobre ameaças cibernéticas. Para obter mais informações, consulte Repositório de biblioteca de TISC.
Relacionamentos	Um relacionamento é um link entre dois observáveis ou dois SDOs ou Observável e SDO que descreve a maneira como os objetos estão relacionados. Os relacionamentos podem ser representados usando um objeto de relacionamento STIX (SRO) externo ou, em alguns casos, por meio de determinadas propriedades que armazenam uma referência de identificador que compreende um relacionamento incorporado. Para obter mais informações, consulte Objetos de relacionamentos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Separação de domínios e Central de segurança de inteligência contra ameaças

A separação de domínio é compatível com Central de segurança de inteligência contra ameaças. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

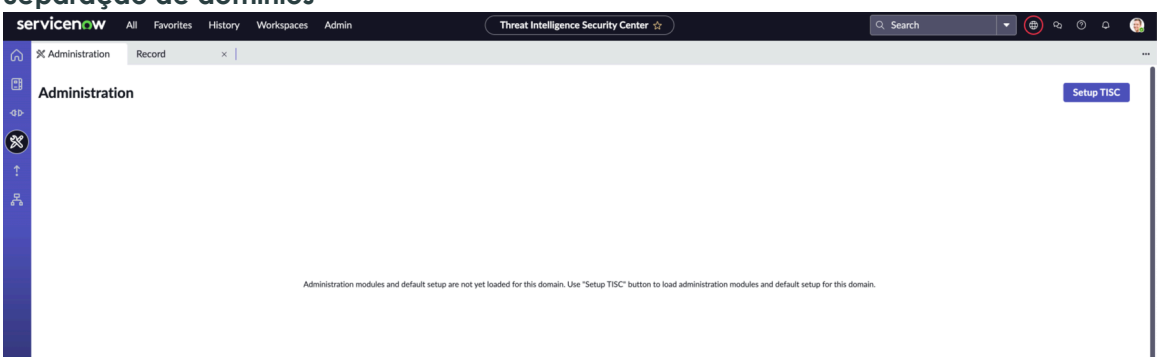
Visão geral

A Separação de domínios está habilitada para todos os recursos de Central de segurança de inteligência contra ameaças.

Como o Domain Separation funciona no Central de segurança de inteligência contra ameaças

- Todos os registros relacionados à configuração que são provisionados no sistema de base são enviados no domínio global. Caso a instância seja separada por domínio, os usuários verão um botão explícito **Configurar TISC** no módulo **Administração** do espaço de TISC. Clique neste botão para clonar as configurações de domínio global provisionadas do sistema de base nos respectivos domínios.

Separação de domínios



Nota: Os usuários só devem habilitar ou modificar registros de configuração específicos do domínio e não devem habilitar ou modificar registros de configuração no domínio global.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Algumas regras de notificação da plataforma (sysevent_email_action) são provisionadas no sistema base. Essas regras de notificação devem ser clonadas em domínios necessários e somente as regras de notificação específicas do domínio precisam ser habilitadas.

  Nota: Para obter mais informações sobre as notificações de regras, navegue até **Notificação do Sistema** > **Notificações** e filtre todas as regras de notificação de domínio global definidas nas tabelas que começam com o nome *sn_sec_tisc* para entender como os usuários podem identificar as regras de notificação de base que são provisionadas no sistema de base.

- Todas as configurações e dados ingeridos serão específicos para cada domínio, o que significa que os usuários de um domínio não poderão acessar dados de outro domínio.
- Configure um ambiente separado por domínio com esta aplicação instalando o plug-in Domain Support - Domain Extensions Installer.
- Há colunas de domínio adicionadas para todas as tabelas de aplicações do sistema de base.
- Usando a funcionalidade fornecida pela plataforma, os domínios de locatário gerenciam seus próprios dados de aplicação.
- A lógica de negócios e os processos que podem ser separados por domínio pelo proprietário da instância são iguais aos compatíveis com a plataforma.
- A lógica de negócios e os processos que podem ser administrados pelo domínio do locatário são os mesmos que a plataforma suporta.
- Você pode acessar a página Configuração na seção Administração. Clique no link fornecido na seção Administração para exibir a exibição Domain Separation.
- Para oferecer suporte à separação de domínio para os widgets usando indicadores do Performance Analytics (PA) no painel da página inicial do TISC, consulte o artigo da base de conhecimento KB1647990 para obter o procedimento detalhado.

Tabelas separadas por domínio

Todas as tabelas são separadas por domínio.

Casos de uso

Todos os recursos desta aplicação são separados por domínio.

Informações relacionadas

Domain Separation para provedores de serviço

Configurar Central de segurança de inteligência contra ameaças

Antes de usar o Central de segurança de inteligência contra ameaças, você deve baixá-lo da ServiceNow Store.

Funções instaladas

Revise as informações a seguir e verifique se você concluiu todas as tarefas para uma integração sem problemas. Abaixo está a lista de diferentes personas de usuário definidas para acessar e trabalhar com a aplicação:

- Analista de inteligência contra ameaças (sn_sec_tisc.analyst)
- Administrador de inteligência contra ameaças (sn_sec_tisc.admin)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Direitos aplicáveis a funções de TISC

Configuração	Descrição
Atribua e verifique as funções necessárias da Now Platform e da Central de segurança de inteligência contra ameaças.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • Como administrador, você deve instalar a aplicação TISC da ServiceNow Store e atribuir a função como sn_sec_tisc.admin. • Esta função sn_sec_tisc.admin executa as seguintes tarefas: ◦ Configura as fontes de dados para ingerir os dados. Para obter mais informações, consulte Feeds de inteligência contra ameaças. ◦ Configuramos as integrações necessárias para aprimorar os dados do observável no TISC. Para obter mais informações, consulte Integrações de aprimoramento de TISC. ◦ Configura funções de aprovação de importação de dados para importar dados usando o Assistente de importação. Para obter mais informações, consulte Como trabalhar com importações de dados. ◦ Configura a calculadora de pontuação de ameaça usando os critérios necessários para o cálculo automático da pontuação de ameaça de observáveis. Para obter mais informações, consulte Definir calculadora de pontuação de ameaça. ◦ Configura as taxonomias e valores de taxonomia necessários. Para obter mais informações, consulte Criando taxonomias. ◦ Configure o repositório do MITRE ATT&CK relevante para sua organização. Para obter mais informações, consulte MITRE-ATT&CK Repositório. **Nota:** Como um sn_sec_tisc.admin, você também pode atribuir a função sn_sec_tisc.analyst. • A função sn_sec_tisc.analyst executa as seguintes tarefas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Direitos aplicáveis a funções de TISC

Configuração	Descrição
	◦ Exibe a visão geral dos dados no sistema usando a página inicial do produto. Para obter mais informações, consulte Exibir página inicial da Central de segurança de inteligência contra ameaças. ◦ Importe dados para o sistema usando o botão Importar inteligência na página Biblioteca de ameaças. Para obter mais informações, consulte Central de segurança de inteligência contra ameaças Biblioteca. ◦ ▪ Pesquise nos dados presentes na aplicação usando a pesquisa fornecida na página Biblioteca de ameaças. ▪ Gerencia os dados ingeridos de várias origens na Biblioteca de ameaças. ▪ Executa várias ações de aprimoramento em observáveis. ▪ Cria e gerencia casos. Para obter mais informações, consulte Criação de casos usando o Workbench do analista de ameaças.

Plug-ins de dependência

Plug-in	Descrição
As seguintes aplicações são necessárias para a instalação desta aplicação: • Componentes do espaço comum da Gestão de casos de segurança [com.snc.escm.ws_commons]. • Threat Intelligence Support Common [com.snc.threat].	Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.

Exibir página inicial da Central de segurança de inteligência contra ameaças

Use a página inicial do TISC, que é a página principal, para visualizar os dados relacionados à inteligência contra ameaças.

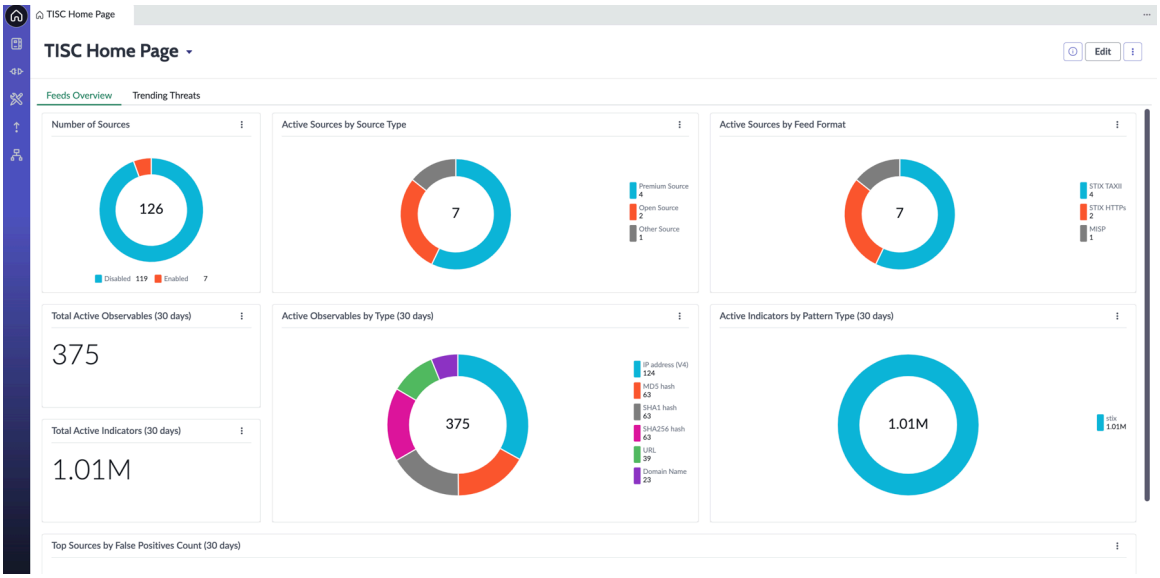
Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página inicial do TISC é exibida.



2. Exiba a página inicial do TISC com dados de widgets diferentes.
   A exibição da página inicial consiste em duas guias diferentes: **Visão geral de feeds** e **Ameaças**em alta . O conteúdo da página inicial vem de várias fontes, como observáveis, indicadores e feeds de dados.

   a. **Visão geral de feeds**: esta guia fornece uma visão geral de alto nível das diferentes origens em que os dados são ingeridos e das origens que estão configuradas para a ingestão de dados.

Visão geral de feeds

Nome do widget	Descrição	Ação
Número de origens	Exibe o número de origens por status, como rascunho, habilitado e desabilitado no sistema.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Origens ativas por tipo de origem	Exibe a distribuição de origens ativas por tipo de origem.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Origens ativas por formato de feed	Exibe o número de origens habilitadas por tipo de feed.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Total de observáveis ativos (30 dias)	Exibe as 10 principais origens por volume de registros de inteligência que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Observáveis ativos por tipo	Exibe o volume total superior de agregados de	Quando este widget é clicado, a página de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do widget	Descrição	Ação
	observáveis que foram criados nos últimos 30 dias.	detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Indicadores ativos por tipo de padrão	Exibe o volume total de agregados de indicador por tipo de padrão que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Total de indicadores ativos (30 dias)	Exibe o volume total de agregados de indicadores que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Principais origens por contagem de falso-positivos (30 dias)	Exibe o volume total por de observáveis falso-positivos que foram criados nos últimos 30 dias.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.

b. **Ameaças**em alta: esta guia fornece uma visão geral de alto nível das ameaças em alta.

Visão geral de feeds

Nome do widget	Descrição	Ação
Relatórios mais recentes (10 principais)	Exibe a lista de relatórios e links - 10 principais ordenados por data de publicação.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Feeds RSS mais recentes (10 principais)	Exibe a lista de feeds RSS e links - 10 principais ordenados por data de publicação.	Quando este widget é clicado, a página da lista é aberta com os registros filtrados.
Observáveis ativos por intervalo de pontuação de ameaça (30 dias)	Exibe a contagem de observáveis que foram criados nos últimos 30 dias distribuídos por intervalos de pontuação de ameaça.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Observáveis ativos por reputação (30 dias)	Exibe a contagem de observáveis que foram criados nos últimos 30 dias distribuídos por reputação.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Principais marcadores (30 dias)	Exibe os principais marcadores nos registros criados nos últimos 30 dias com base na frequência de uso.	Quando este widget é clicado, a página de detalhes de KPI do widget para o filtro selecionado é aberta em uma nova guia.
Setores mais direcionados (30 dias)	Exibe os 10 principais setores classificados por atividades	Quando este widget é clicado, a página de detalhes de KPI do widget

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do widget	Descrição	Ação
	relatadas que foram criadas nos últimos 30 dias.	para o filtro selecionado é aberta em uma nova guia.

Integração da Central de segurança de inteligência contra ameaças

Use esta seção para entender as Central de segurança de inteligência contra ameaças integrações.

A seção **Integrações** inclui os seguintes submódulos.

Integrações

Nome do módulo	Descrição
Catálogo	Todos os feeds de inteligência contra ameaças e integrações de aprimoramento disponíveis são mostrados como blocos/ cartões aqui. Os usuários não terão a capacidade de criar um novo feed ou integração a partir desta seção.
Feeds de ameaças	Esta seção contém os detalhes relacionados somente aos feeds de Inteligência contra ameaças e os usuários poderão configurar novos feeds de inteligência contra ameaças a partir desta seção.
Integrações de aprimoramentos	Esta seção contém os detalhes relacionados somente às integrações de aprimoramento e os usuários poderão configurar as integrações de aprimoramento disponíveis nesta seção. **Nota:** A seção Integrações de aprimoramento só ficará visível se pelo menos um plug-in de integração de aprimoramento estiver instalado.

Tradução automática

Central de segurança de inteligência contra ameaças Catálogo

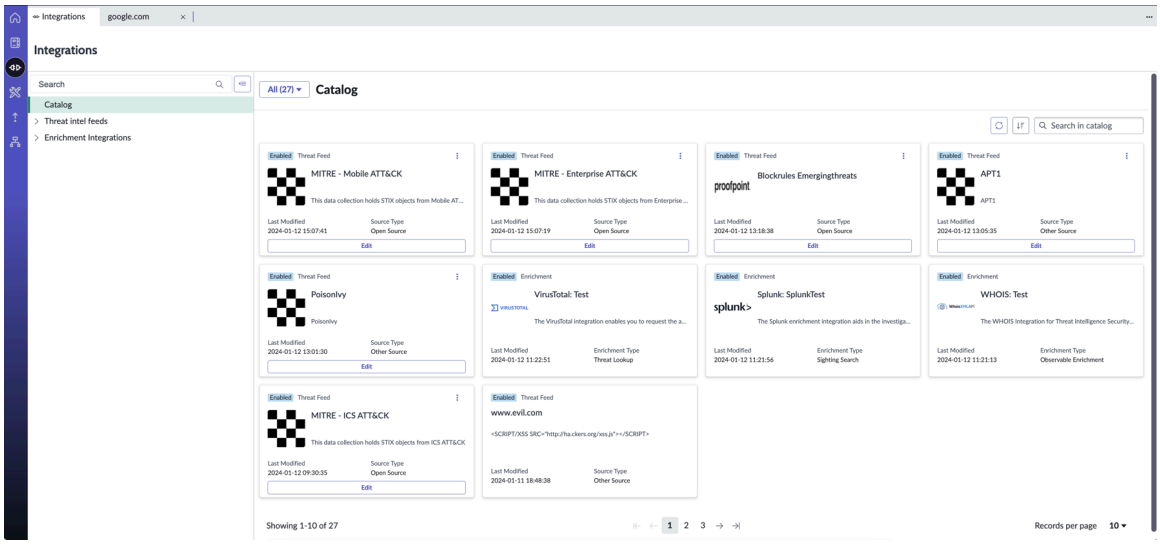
O Catálogo Central de segurança de inteligência contra ameaças é uma lista selecionada de feeds de Inteligência contra ameaças e integrações de aprimoramento disponíveis na aplicação para você habilitá-los após adicionar as informações necessárias e programar o feed para ingerir automaticamente dados de Inteligência contra ameaças em uma frequência definida.

Como um sn_sec_tisc.admin, você também pode pesquisar e editar as configurações de origem existentes, habilitar ou desabilitar e excluir as configurações do Catálogo. Qualquer nova fonte de dados adicionada ao Catálogo aparecerá como um novo cartão de configuração no Catálogo.

Função necessária:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_sec_tisc.admin (criar/atualizar)
- sn_sec_tisc.analyst (leitura)



Nota: Os cartões no catálogo são diferenciados por seu rótulo, que está presente na parte superior do feed de ameaças/enriquecimentodo cartão.

Ações na exibição do Catálogo

A exibição de Catálogo permite que você execute as seguintes ações.

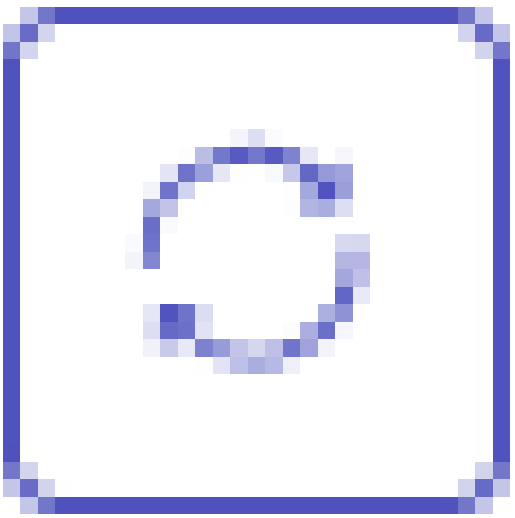
Ações na exibição do Catálogo

Ação	Descrição
Todos	Use este menu suspenso para filtrar feeds e integrações com base no estado atual. Você pode filtrar com base nos seguintes estados: • **Todos**: exibe todos os feeds e integrações na página. Esta é a opção padrão. • **Habilitado**: exibe todos os feeds e integrações que estão em um estado habilitado. • **Desabilitado**: exibe todos os feeds e integrações que estão em um estado desabilitado. • **Rascunho**: exibe todos os feeds e integrações que estão em estado de rascunho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações na exibição do Catálogo

Ação	Descrição
	Use esta ação para atualizar o Catálogo.
	Use esta ação para classificar todos os feeds e integrações com base no seguinte: • **Última modificação (recente)** • **Última modificação (mais antiga)** • **Nome (A-Z)** • **Nome (Z-A)**
Pesquisar no catálogo	Use esta ação para pesquisar feeds/ integrações com base no nome e na descrição no catálogo.

Feeds de inteligência contra ameaças

Use Feeds de inteligência contra ameaças para adicionar, editar ou remover fontes de dados de feed de Inteligência contra ameaças.

Os feeds de fonte de dados estão disponíveis no Catálogo de informações sobre ameaças na seção Integrações.

O catálogo de feeds de inteligência contra ameaças foi criado para mostrar as fontes de dados de feed disponíveis na forma de blocos e tem a capacidade de filtrar, pesquisar e navegar até os detalhes da configuração de origem e executar várias ações.

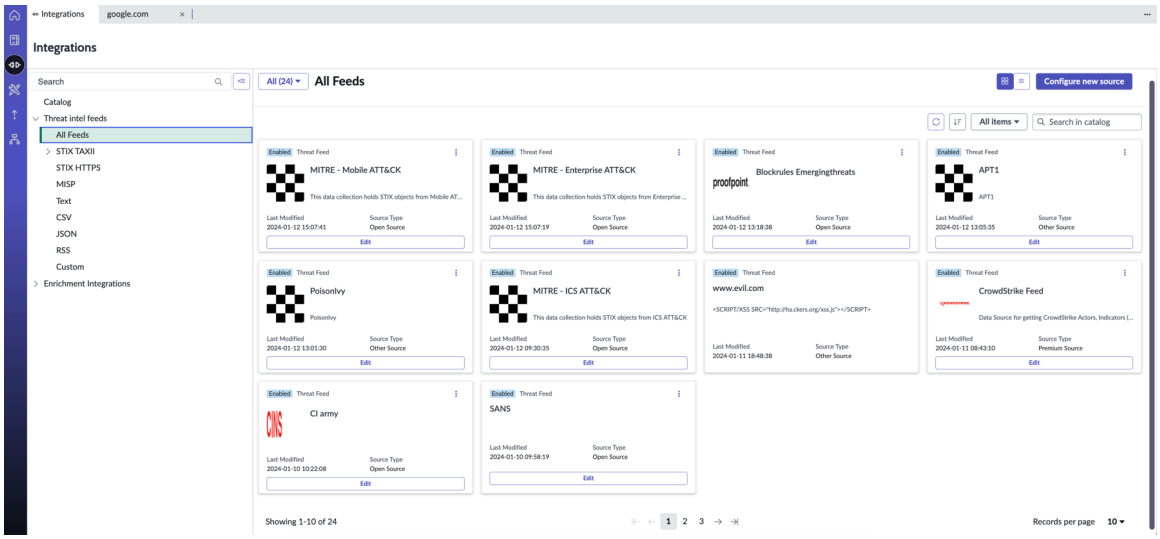
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Todos os Feeds

O sistema base inclui uma série de cartões para cada um dos feeds que você pode habilitar e usar.

Os feeds podem ser exibidos navegando até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações** > **Feeds de informações sobre ameaças** > **Todos os Feeds**.



Ações na exibição Todos os feeds

A seção Todos os feeds permite que você execute as ações a seguir.

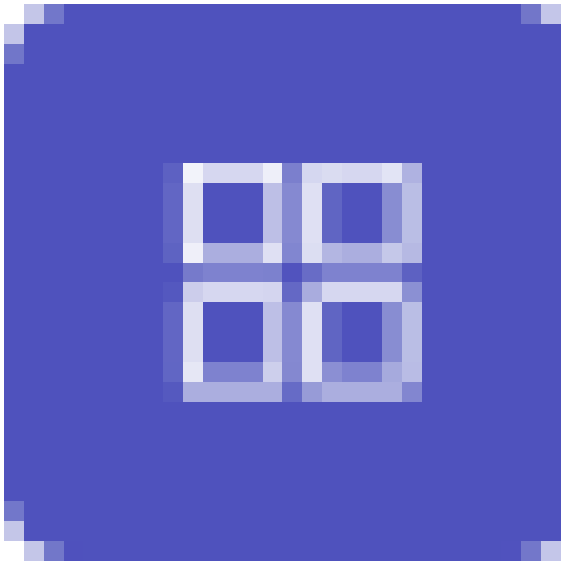
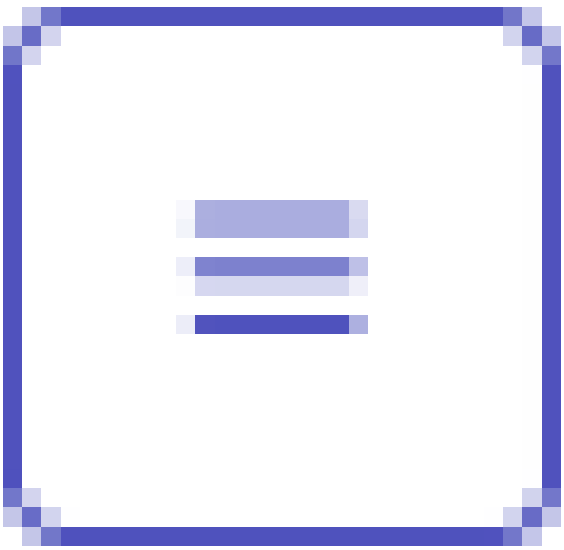
Ações na exibição de todas as integrações

Ação	Descrição
Todos	Use este menu suspenso para filtrar feeds com base no estado atual. Você pode filtrar com base nos seguintes estados: • **Todos**: exibe todos os feeds da página. Esta é a opção padrão. • **Habilitado**: exibe todos os feeds que estão em um estado habilitado. • **Desabilitado**: exibe todos os feeds que estão em um estado desabilitado. • **Rascunho**: exibe todos os feeds que estão em estado de rascunho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

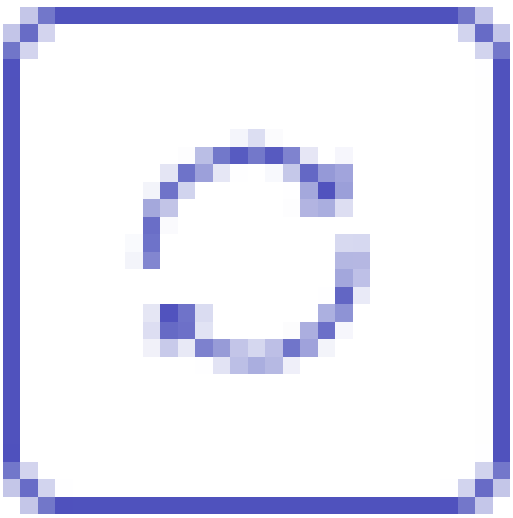
Ações na exibição de todas as integrações

Ação	Descrição
	Use esta ação para exibir todos os feeds na forma de cartões.
	Use esta ação para exibir todos os feeds na forma de uma exibição de lista.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações na exibição de todas as integrações

Ação	Descrição
	Use esta ação para atualizar a página.
	Use esta ação para classificar todas as integrações com base no seguinte: • **Última modificação (recente)** • **Última modificação (mais antiga)** • **Nome (A-Z)** • **Nome (Z-A)**
Todos os itens	Use esta ação para filtrar e listar os blocos de feed de inteligência contra ameaças por tipo de origem ou tipo de feed. **Tipo de origem**: • Código aberto • Outra origem • Origem Premium **Tipo de feed**: • CSV • Feed personalizado • JSON

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

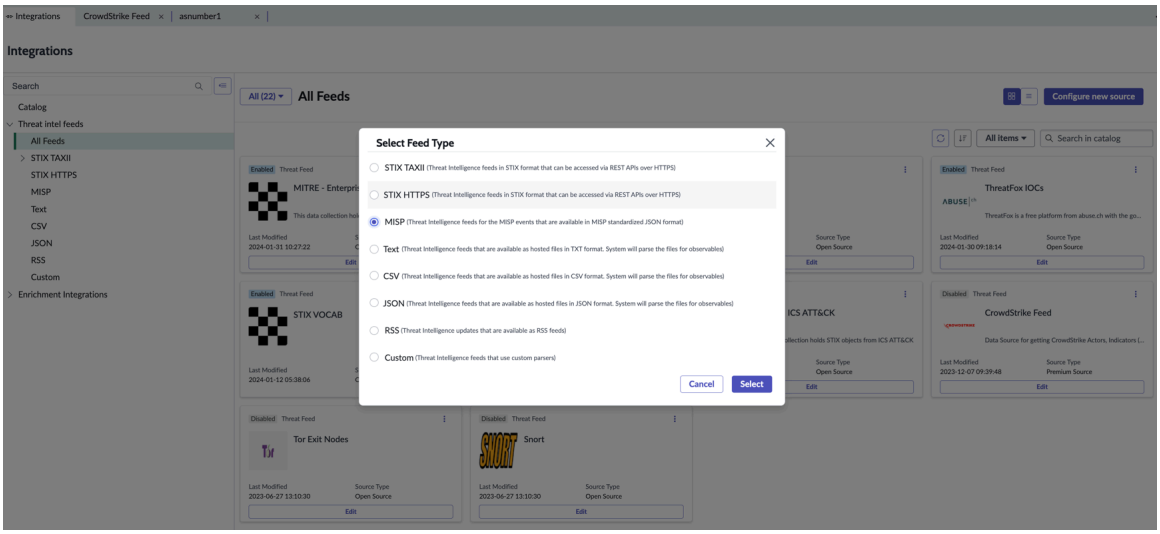
Ações na exibição de todas as integrações

Ação	Descrição
	• MISP • RSS • HTTPs do STIX • Texto
Pesquisar no catálogo	Use esta ação para pesquisar feeds com base no nome e na descrição no catálogo.

Configurar nova fonte de dados do feed de inteligência contra ameaças

Para configurar uma nova fonte de dados de feed de inteligência contra ameaças, siga o procedimento:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecionar **Feeds de informações sobre ameaças** > **Todos os Feeds**.
4. Clique **em Configurar nova origem**. Os vários tipos de feed são exibidos.



5. Selecione o respectivo tipo de feed. Por exemplo, MISP.
6. Clique em **"Selecionar"**.
7. No formulário, preencha os campos.

Criar nova fonte de dados

Campo	Descrição
Nome	Insira um nome para o feed.
Descrição	Descrição do feed.
Tipo de feed	O tipo de feed. Por exemplo, MISP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por padrão, este valor é exibido com base no tipo de feed que você selecionou no Catálogo.
Logotipo	Anexe o logotipo do feed de origem.
Setor	Selecione a categoria do setor, como Aeroespacial, Agrícola e assim por diante, para a qual a fonte de dados do feed se aplica.
Tipo de Origem	Selecione o tipo de origem na lista de tipos de origem disponíveis. A lista de origens disponíveis é: ◦ Governo ◦ ISACs ◦ Código aberto ◦ Origem Premium ◦ Outra origem

Preencha os campos na seção Configuração, conforme apropriado.

Configuração

Campo	Descrição
Período de expiração (dias)	Insira o período de expiração do feed em dias. Por exemplo, 180 dias. **Nota:** Quaisquer que sejam os dados ingeridos da origem, eles expirarão 180 dias após a ingestão.
Usar Mensagem REST	Marque a caixa de seleção **Usar Mensagem REST** se precisar usar a funcionalidade Mensagem REST/Método REST fornecida por Now Platform. Se esta caixa de seleção não estiver marcada, a aplicação usará o endpoint fornecido em **URL do endpoint REST** para buscar os dados do feed. Para obter mais informações, consulte Serviço web REST de saída na documentação Now Platform. **Nota:** Os campos Mensagem REST e Método REST são obrigatórios ao selecionar a mensagem REST.
Mensagem REST	Selecione o registro de Mensagem REST na lista de registros de mensagens REST que já estão configurados na instância. Para obter mais informações, consulte Serviço

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	web REST de saída na documentação da Now Platform. **Nota:** Selecione este valor quando precisar exibir cabeçalhos específicos e definir os registros relacionados ao REST usando a opção de mensagem REST.
Método REST	Selecione Método REST na lista de Métodos REST disponíveis configurados para a Mensagem REST selecionada. Para obter mais informações, consulte Serviço web REST de saída na documentação da Now Platform.
Confiança	Defina a confiança de todos os registros aplicáveis que são ingeridos por meio deste feed específico. **Nota:** Defina a confiança entre 0 e 100 para esta origem.
URL do endpoint REST	Insira a URL do endpoint REST em que os dados são hospedados pela fonte de dados.
Autenticação Necessária	Marque esta caixa de seleção se a autenticação for necessária para sua nova fonte de dados. **Nota:** Adicione uma declaração mencionando que isso só se aplica quando a URL do endpoint REST estiver sendo usada para recuperar os dados.
Tipo de autenticação	O tipo de autenticação do feed de origem. A seguir estão os tipos de autenticação que são configurados e provisionados no sistema de base para os usuários: ◦ ID de API/Chave de API ◦ ID da API/segredo da API ◦ Chave de API ◦ Chave de API/segredo de API ◦ Nome de usuário da API/senha da API/ chave da API ◦ Autenticação básica

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os tipos de autenticação no sistema de base para o tipo de feed de origem personalizado são ID do cliente e Segredo do cliente.
Cabeçalhos a serem passados com a solicitação	Todos os cabeçalhos a serem passados com as solicitações podem ser fornecidos em Mapeamento de cabeçalho de solicitação. O cabeçalho deve ser fornecido em par de chave-valor separado por dois pontos (':'). Cada par de valores de chave de cabeçalho deve ser fornecido em uma nova linha. Para fornecer parâmetros de autenticação como valores de cabeçalho, coloque o rótulo de autenticação necessário entre '${' e '}$'. Por exemplo, x-api-key:${Chave de API}$.
Avançado	Marque esta caixa de seleção para definir o script de integração personalizado e o script do processador de relatório. **Nota:** Quando você marcar esta caixa de seleção, os campos **Script de integração** e **Processador de relatório** serão exibidos para você selecionar os scripts personalizados.
Script de integração	O script de integração invoca uma chamada para a URL do endpoint REST usando os parâmetros de autenticação e os cabeçalhos conforme configurados no feed e, em seguida, o script busca os dados que estão disponíveis no feed específico. No sistema de base, a seguir estão as inclusões de scripts personalizados, que são provisionadas na aplicação para os scripts de integrações: ◦ FeedDatasourceIntegrationBase ◦ MITRESourceIntegration ◦ RSSFeedDatasourceIntegration ◦ SimpleFeedDatasourceIntegration ◦ SimpleMISPFeedDatasourceIntegration O script de integração padrão é baseado no tipo de feed selecionado. Por exemplo, se você selecionar o tipo de feed MISP, que é um formato padrão para processar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	e buscar os dados, o script de integrações será **SimpleFeedDatasourceIntegration**. **Nota:** Para os scripts de integração personalizada, você pode criar uma inclusão de script estendendo **FeedDatasourceIntegrationBase** e substituindo os métodos necessários.
Processador de relatórios	O script do processador de relatório processa os dados obtidos do feed usando o script de integração. No sistema de base, a seguir estão as inclusões de scripts personalizados, que são provisionadas na aplicação para os scripts de integrações: ◦ FeedDatasourceResponseProcessor ◦ MITRECollectionDataProcessor ◦ RSSFeedDatasourceResponseProcessor ◦ SimpleFeedDatasourceResponseProcessor ◦ SimpleMISPFeedDatasourceResponseProcessor ◦ TAXIIV2CollectionDataProcessor O processador de relatório padrão para STIX HTTPS é **TAXIIV2CollectionDataProcessor**. Por padrão, esta opção é exibida e você não pode modificar ou selecionar nenhum outro processador de relatório.

Preencha os campos na seção Programação, conforme apropriado.

Agendamento

Campo	Descrição
Executar	Defina a frequência com que você deseja ingerir os registros. O feed será executado com base no intervalo de programação do trabalho. Os intervalos de trabalho disponíveis são: ◦ Diariamente ◦ Semanalmente ◦ Mensalmente ◦ Periodicamente ◦ Uma vez

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Sob demanda ◦ Calendário comercial: início da entrada ◦ Calendário comercial: fim da entrada **Nota:** Por padrão, a frequência é definida como Sob demanda. Para obter mais informações, consulte Trabalhos agendados e como Executar automaticamente um script de sua escolha .
Buscar dados de	A data de início a partir da qual os dados precisaram ser obtidos. Este campo deve ser definido com a hora a partir da qual os dados precisam ser ingeridos da origem correspondente. Depois que este campo for definido, a próxima execução de ingestão buscará os dados do tempo configurado e as execuções de ingestão consecutivas buscarão dados incrementais. Por exemplo, a Origem está programada para ingerir os dados a cada hora. Se o usuário definir **Buscar dados de** como 12 de janeiro às 6h em 12 de janeiro às 9h30, o acionamento da ingestão em 12 de janeiro às 10h buscará os dados de 12 de janeiro às 6h a 12 de janeiro às 10h. A próxima ingestão que é acionada às 11h buscará somente os dados incrementais de 12 de janeiro às 10h a 12 de janeiro às 11h. **Nota:** Isso significa que as execuções programadas buscarão dados de forma incremental a partir da data especificada.

Marcadores

Campo	Descrição
Selecionar marcadores	Use os marcadores para anotar ou marcar registros que são ingeridos no sistema a partir desta origem. Comece a inserir o nome do marcador na barra de **pesquisa** para escolher os marcadores disponíveis na aplicação ou insira um novo nome de marcador e clique em **Adicionar** para atribuí-lo à origem.

8. Clique na ação **Salvar** para armazenar e criar o feed.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os detalhes fornecidos são validados e, por padrão, o status dos feeds está desabilitado.

9. (Opcional) Clique na ação **Salvar como rascunho** para armazenar somente as configurações de feed como rascunho. Os usuários não podem habilitar um feed quando ele é salvo como rascunho.

   Se você não tiver certeza sobre os detalhes da configuração, poderá usar a opção **Salvar como rascunho**. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.

10. Para habilitar o feed, clique em **Habilitar**.

    O feed foi habilitado com sucesso. Você também pode habilitar, desabilitar ou excluir um feed específico usando o menu **Ações** do bloco de feed necessário na página **Catálogo** ou **Feeds de informações sobre ameaças**.

    Nota: Se a Frequência de **execução** estiver definida como **Sob demanda** na seção **Programação** da página do formulário da fonte de dados, sempre que você habilitar a integração, um aviso de mensagem será exibido alertando os usuários de que agora eles habilitaram a origem com sucesso. Você deve mudar a frequência de execução para habilitar a configuração de origem para ingerir dados automaticamente.

11. Clique em **Habilitar** para habilitar o registro.

    Depois que o registro da fonte de dados do feed estiver habilitado, você poderá executar o registro para executar a integração.

    Nota: O registro da fonte de dados é rotulado e indicado como **habilitado**. Da mesma forma, você pode desabilitar o feed da fonte de dados clicando no botão **Desabilitar**.

12. Clique em **Excluir** para excluir o registro da fonte de dados do feed.
13. Selecione a seção **Executar integrações** para verificar os detalhes da execução.

Nota: O procedimento de configuração da fonte de dados de feed acima é o mesmo para todos os outros tipos de fonte de dados de feed, exceto para STIX TAXII. Para obter mais informações sobre como o STIX TAXII está configurado, consulte Configurar um novo feed TAXII.

Tipos de feeds de informações sobre ameaças

Estes são os tipos de feeds de inteligência contra ameaças que podem ser configurados e habilitados:

Feeds de inteligência contra ameaças

Tipo	Descrição
Feeds TAXII	Feeds que estão disponíveis no formato Coleções STIX/TAXII.
HTTPS do STIX	Feeds de inteligência contra ameaças no formato STIX que podem ser acessados por meio de REST APIs no protocolo HTTPS.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feeds de inteligência contra ameaças

Tipo	Descrição
MISP	Feeds que estão no MISP Formatar feeds.
Texto	Feeds que estão disponíveis como arquivos hospedados em formato de texto. **Nota:** O sistema analisará os arquivos em busca de URL, domínio, nome do arquivo, hashes e o endereço IP somente será extraído e nenhum outro tipo de observável será extraído.
CSV	Feeds que estão disponíveis como arquivos hospedados no formato CSV. **Nota:** O sistema analisará os arquivos em busca de URL, domínio, nome do arquivo, hashes e o endereço IP somente será extraído e nenhum outro tipo de observável será extraído.
JSON	Feeds que estão disponíveis como arquivos hospedados no formato JSON. **Nota:** O sistema analisará os arquivos em busca de URL, domínio, nome do arquivo, hashes e o endereço IP somente será extraído e nenhum outro tipo de observável será extraído.
RSS	Feeds que estão disponíveis no formato RSS. A aplicação armazenará os dados como registros de feed RSS.
Personalizado	Feeds que são configurados usando analisadores personalizados. **Nota:** O sistema analisará os arquivos em busca de URL, domínio, nome do arquivo, hashes e o endereço IP somente será extraído e nenhum outro tipo de observável será extraído.

Para as próximas etapas do procedimento, consulte a respectiva seção para configurar cada tipo de feed específico. Feeds de inteligência contra ameaças.

Exibir feeds de informações sobre ameaças

Esta seção apresenta os feeds de informações sobre ameaças que estão configurados no sistema de base.

Exibir feeds STIX TAXII

Exibir os feeds STIX TAXII configurados no sistema de base.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione **STIX TAXII**.
   Os feeds de MISP no sistema de base são descritos na tabela a seguir.

Feed de ameaças	Descrição	URL
Cyware TAXII	O Cyware Threat Intelligence eXchange (CTIX) é uma plataforma projetada para facilitar o compartilhamento de inteligência contra ameaças cibernéticas entre organizações.	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordedFuture TAXII	A Recorded Future é uma plataforma em nuvem de inteligência contra ameaças independente que permite que as organizações identifiquem e mitiguem ameaças em domínios cibernéticos, de cadeia de suprimentos, físicos e de fraude.	https://api.recordedfuture.com/taxii2
Pulsedive TAXII	A Pulsedive é uma plataforma de inteligência contra ameaças que fornece uma ampla variedade de serviços e ferramentas de inteligência contra ameaças cibernéticas para as organizações.	https://pulsedive.com/taxii2/api/

4. Clique em **Editar** para editar o feed.

Exibir feeds HTTPs STIX

Exiba os feeds HTTPs STIX configurados no sistema de base.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione **HTTPs STIX**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tabela a seguir descreve os feeds STIX HTTPs no sistema de base.

ThreatFeed	Descrição	URL
MITRE – Mobile ATT&CK	Esta coleta de dados contém objetos STIX do Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE – ICS ATT&CK	Esta coleta de dados contém objetos STIX do ICS ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE – Enterprise ATT&CK	Esta coleta de dados contém objetos STIX do Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Clique em **Editar** para editar o feed e fazer as atualizações necessárias.

Exibir feeds de MISP

Exiba os feeds de MISP configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione **MISP**.
   Os feeds de MISP no sistema de base são descritos na tabela a seguir.

Feed de ameaças	Descrição	URL
Feed do OSINT da Intel sobre ameaças da DigitalSide	Fonte de dados para buscar informações da Inteligência contra ameaças cibernéticas de código aberto do feed do DigitalSide Threat-Intel OSINT, que se baseia principalmente na análise de malware e em URLs, IPs e domínios comprometidos.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
IOCs de esgotamento de URL	URLHaus é um projeto de abuso.ch com o objetivo de compartilhar URLs mal-intencionados que estão sendo usados para distribuição de malware.	https://urlhaus.abuse.ch/downloads/misp/manifest.json

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
Malware Bazaar	O MalwareBazaar é um projeto do abus.ch com o objetivo de compartilhar amostras de malware com a comunidade de infosec, fornecedores de AV e provedores de inteligência contra ameaças.	https://bazaar.abuse.ch/downloads/misp/manifest.json
IOCs do ThreatFox	O ThreatFox é uma plataforma gratuita da Abuse.ch com o objetivo de compartilhar indicadores de comprometimento (IOCs) associados a malware com a comunidade de infosec, fornecedores de antivírus e provedores de inteligência contra ameaças.	https://threatfox.abuse.ch/downloads/misp/manifest.json

4. Clique em **Editar** para editar o feed.

Exibir feeds de texto

Exiba os feeds de texto configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione a opção **Texto**.
   A seguir está uma lista dos feeds de texto configurados no sistema de base.

Feed de ameaças	Descrição	URL
IPs de força bruta de Haley	Fornece uma lista de endereços IP da máquina invasora durante os últimos 2 anos, classificados por endereço IP	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Regras de bloqueio Ameaças emergentes	A Inteligência contra ameaças emergentes (ET) fornece feeds de informações de ameaças acionáveis para identificar IPs envolvidos em atividades suspeitas e mal-intencionadas.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Nuug Pop3 Groper Web	Lista de hosts que tentaram e falharam ao fazer logon	https://home.nuug.no/%7Epeter/pop3gropers.txt

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	no serviço pop3 em bsdly.net.	
Nós de saída do TOR	Os nós de saída do TOR podem ser usados para detectar tráfego proveniente da rede TOR.	https://www.dan.me.uk/torlist/?exit
Lista negra de IP do Talos Intelligence	A Talos foi formada pela combinação da equipe de pesquisa de vulnerabilidade da SourceFire, do grupo de comunicação e pesquisa de ameaças da Cisco e do grupo de aplicações seguras da Cisco. A experiência combinada é respaldada por uma infraestrutura sofisticada e pela incomparável telemetria de dados da Cisco que se estende por redes, endpoints, ambientes de nuvem, sistemas virtuais e tráfego diário de e-mail e web.	https://www.talosintelligence.com/documents/ip-blacklist
SANS	O ISC fornece um serviço gratuito de análise e aviso para milhares de usuários e organizações da Internet.	https://isc.sans.edu/feeds/topips.txt
Snort	O Snort é o principal Sistema de Prevenção de Intrusão (IPS) de código aberto do mundo. O Snort IPS usa uma série de regras que ajudam a definir atividades de rede mal-intencionadas.	https://snort.org/downloads/ip-block-list
Exercito de IC	A lista do CINS Arms é um subconjunto do conjunto de regras CINS Active Threat Intelligence e consiste em endereços IP que atendem a um de dois critérios básicos: 1) O fator de pontuação recente do Rogue Packet do IP é muito ruim ou 2) O IP desarmou um designado número de alertas "confiáveis" em um determinado número de Sentinels implantados em todo o mundo.	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	IPs brutos para as listas de bloqueios do firewall. Eles	https://rules.emergingthreats.net/

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	vêm de: redes de spam identificadas por SpamHaus (www.spamHaus.org), principais invasores listados por DShield (www.dshield.org) e Abuse.ch	fwrules/emerging-Block-IPs.txt
Lista de bloqueios Greensnow	O GreenSnow é uma equipe que consiste nos melhores especialistas em segurança de computadores. O GreenSnow coleta um grande número de IPs de diferentes computadores localizados em todo o mundo. O GreenSnow é comparado ao SpamHaus.org para ataques de qualquer tipo, exceto spam.	https://blocklist.greensnow.co/greensnow.txt
Exercito de IC	A lista do CINS Arms é um subconjunto do conjunto de regras CINS Active Threat Intelligence e consiste em endereços IP que atendem a um de dois critérios básicos: 1) O fator de pontuação recente do Rogue Packet do IP é muito ruim ou 2) O IP desarmou um designado número de alertas "confiáveis" em um determinado número de Sentinels implantados em todo o mundo.	https://cinsscore.com/list/ci-badguys.txt
Lista de bloqueios	www.blocklist.de é um serviço gratuito e voluntário fornecido por um especialista em fraudes/abusos, cujos servidores são frequentemente atacados via SSH-, Mail-Login-, FTP-, Webserver- e outros serviços.	https://lists.blocklist.de/lists/all.txt
Nós de saída do TOR	Os nós de saída do TOR podem ser usados para detectar tráfego proveniente da rede TOR.	https://www.dan.me.uk/torlist/?exit
IPs de BOT de Botscout	O BotScout ajuda a impedir que scripts da web automatizados, conhecidos como "bots",	http://botscout.com/last_caught_cache.txt

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	sejam registrados em fóruns, poluindo bancos de dados, espalhando spam e abusando de formulários em sites.	
VNC RFB do plano de dados	Endereços IP identificados como iniciando sessões de buffer de quadro remoto do VNC.	https://dataplane.org/signals/vncrfb.txt
Login TELNET do plano de dados	Endereços IP identificados como tentativas de login por meio da autenticação de senha TELNET.	https://dataplane.org/signals/telnetlogin.txt
Autenticação de senha SSH do plano de dados	Endereços IP identificados como tentativas de login por meio da autenticação de senha SSH.	https://dataplane.org/signals/sshpwauth.txt
Conexão do cliente SSH do plano de dados	Endereços IP identificados como executando negociações de protocolo de cliente SSH.	https://dataplane.org/signals/sshclient.txt
Regras de bloqueio Ameaças emergentes	A Inteligência contra ameaças emergentes (ET) fornece feeds de informações de ameaças acionáveis para identificar IPs envolvidos em atividades suspeitas e mal-intencionadas.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Saudação SMTP do plano de dados	Endereços IP identificados como clientes SMTP que emitiam comandos HELO ou EHLO não solicitados.	https://dataplane.org/signals/smtpgreet.txt
Consulta SIP do plano de dados	Endereços IP identificados como enviando consultas de OPÇÕES DE SIP.	https://dataplane.org/signals/sipquery.txt
Protocolo IP do plano de dados 41	Endereços IP identificados como retransmissão do protocolo IPv4 aberto 41 (ou seja, IPv6 sobre IPv4).	https://dataplane.org/signals/proto41.txt
Convite do SIP do plano de dados	Endereços IP identificados como enviando operações de CONVITE SIP.	https://dataplane.org/signals/sipinvitation.txt
Versão do CH TXT do DNS do plano de dados.bind	Endereços IP identificados como enviando consultas DNS CH TXT VERSION.BIND.	https://dataplane.org/signals/dnsversion.txt
TCP de DNS do plano de dados	Endereços IP identificados como enviando consultas	https://dataplane.org/signals/dnstcp.txt

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
	de DNS sobre a porta TCP 53.	
Recursão de DNS do plano de dados desejada EM QUALQUER	Endereços IP identificados como enviando consultas DNS recursivas EM QUALQUER.	https://dataplane.org/signals/dnsrdany.txt
Recursão de DNS do plano de dados desejada	Endereços IP identificados como enviando consultas DNS recursivas.	https://dataplane.org/signals/dnsrd.txt
Banco de dados de phishing dos links de phishing ativos do GitHub	Fonte de dados para buscar links de phishing ativos do banco de dados de phishing disponível no GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
Banco de dados de phishing dos domínios ativos do GitHub	Fonte de dados para buscar domínios ativos do banco de dados de phishing disponível no GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
Banco de dados de phishing de IPs ativos do GitHub	Fonte de dados para buscar IPs ativos do banco de dados de phishing disponível no GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Bots da lista de bloqueios	Todos os endereços IP que foram relatados nas últimas 48 horas como tendo executado ataques nos ataques de RFI, REG-Bots, IRC-Bots ou BadBots.	https://lists.blocklist.de/lists/bots.txt
Ataques do Apache na lista de bloqueios	Todos os endereços IP que foram relatados nas últimas 48 horas como tendo executado ataques no serviço Apache, Apache-DDOS, RFI-Ataques.	https://lists.blocklist.de/lists/apache.txt
Lista de bloqueios de Voip por Scopserv	Recupere a lista de ips na lista de bloqueios da lista de bloqueios de Voip.	http://voipbl.org/update/?dm=bl
Lista de bloqueios de domínio do Threatview	Domínios maliciosos identificados para phishing/serviço de malware/comando e controle.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Lista de bloqueios de hash do Threatview MD5	Hashes MD5 de arquivos mal-intencionados ou associados a malware, ransomware, ferramentas de invasão, bots etc.	https://threatview.io/Downloads/MD5-HASH-ALL.txt

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Feed de ameaças	Descrição	URL
Lista de bloqueios de URL do Threatview	URLs maliciosos que atendem a malware, phishing, botnets e C2.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Lista de bloqueios de hash de arquivo SHA do Threatview	Hashes SHA de arquivos conhecidos ou vinculados à execução de malware.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Lista de bloqueios de IP do Threatview	Lista de bloqueios de IPs maliciosos para endereços IP inválidos conhecidos.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Feed de busca do Threatview C2	Infraestrutura que hospeda servidores de comando e controle encontrados durante a busca proativa pelo Threatview.io	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
Feed de ameaças OSINT do Threatview	Indicadores maliciosos de comprometimento coletados da origem OSINT - Twitter e Pastebin.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. Clique em **Editar** para editar o feed.

Exibir feeds CSV

Exiba os feeds CSV configurados no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione **CSV**.
   Os feeds CSV no sistema de base são explicados na tabela a seguir.

ThreatFeed	Descrição	URL
Lista negra de certificados SSL da Abuse.ch	A lista de bloqueios de certificados SSL (CSV) é um CSV que contém a impressão digital SHA1 de todos os certificados SSL na lista de bloqueios em SSLBL.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Lista de bloqueios de IP de botnet C2	Um certificado SSL pode ser associado a um ou mais servidores (combinação de endereço IP:porta). O SSLBL coleta endereços IP que estão sendo executados com um certificado SSL na lista de bloqueios em	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ThreatFeed	Descrição	URL
	SSLBL. Normalmente, são servidores Botnet Command&Control (C&C). Portanto, o SSLBL publica uma lista de bloqueios contendo esses IPs que podem ser usados para detectar tráfego de botnet C2 de máquinas infectadas para a Internet, saindo da rede.	
Phishtank on-line	N/D	https://data.phishtank.com/data/online-valid.csv

4. Clique em **Editar** para editar o feed.

Exibir feed personalizado

Exiba o feed personalizado que é enviado no sistema de base.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione **Personalizado**.
   A tabela a seguir lista Feed personalizado pronto para uso.

ThreatFeed	Descrição	URL
Feed do CrowdStrike	Origem para obter dados de ator, observável e relatórios do CrowdStrike.	https://api.crowdstrike.com

4. Clique em **Editar** para editar o feed.

Exibir feed de ameaças premium do CrowdStrike

Exiba o feed de ameaças premium recém-adicionado para o tipo personalizado de feeds. Cada feed premium que usa o gerenciador de fonte de dados requer integrações de ponto.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

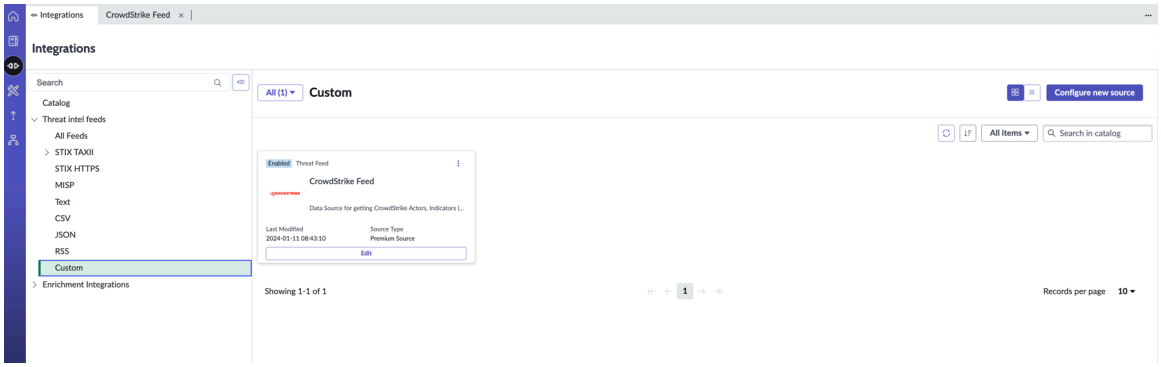
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecione **Personalizado**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no cartão **Feed do CrowdStrike**.

> **Nota:** Por padrão, o feed do CrowdStrike está desabilitado. Você deve editar as configurações para habilitar o feed.



5. Faça o detalhamento ativo até a seção **Detalhes da configuração**.
6. Insira a **URL base**, o**IDdo cliente e o Segredo do cliente**.

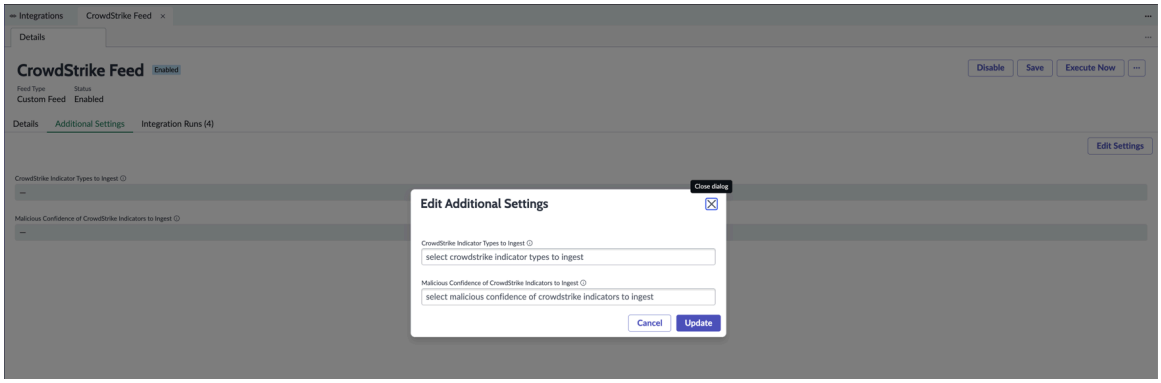
> **Nota:**
>
> a. **URL base**: cada nuvem do CrowdStrike tem uma URL base diferente. Ao fazer solicitações à API do CrowdStrike, use a URL base que corresponde à nuvem em que o CrowdStrike está hospedado.
>
> b. Você deve gerar seu ID de cliente e segredo do cliente, caso não os tenha. Para obter mais informações sobre o ID do cliente e o segredo do cliente, consulte a seção Definir seu primeiro cliente de API .
>
> c. Obtenha o ID do cliente e o segredo do cliente do CrowdStrike para os escopos necessários. Abaixo estão os escopos necessários para o ID do cliente e o segredo do cliente do Crowdstrike:
>
> - Indicadores (Inteligência Falcon)
> - Atores (Falcon Intelligence)
> - Relatórios (Falcon Intelligence)

7. Navegue até **Configurações adicionais** específicas para o CrowdStrike A integração do feed de ameaças pode ser usada para filtrar dados que são ingeridos da origem.

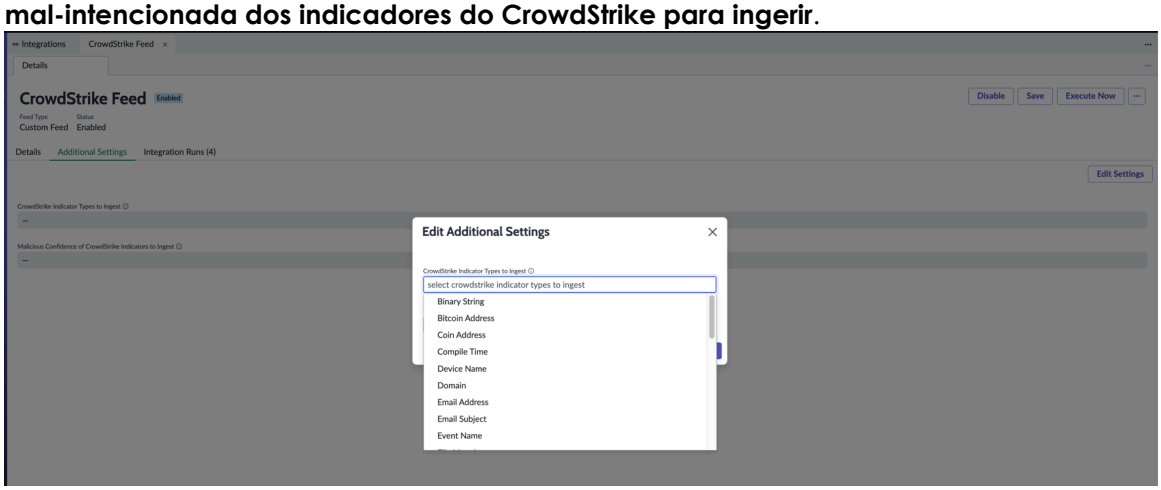
8. Clique **em Editar configurações**.

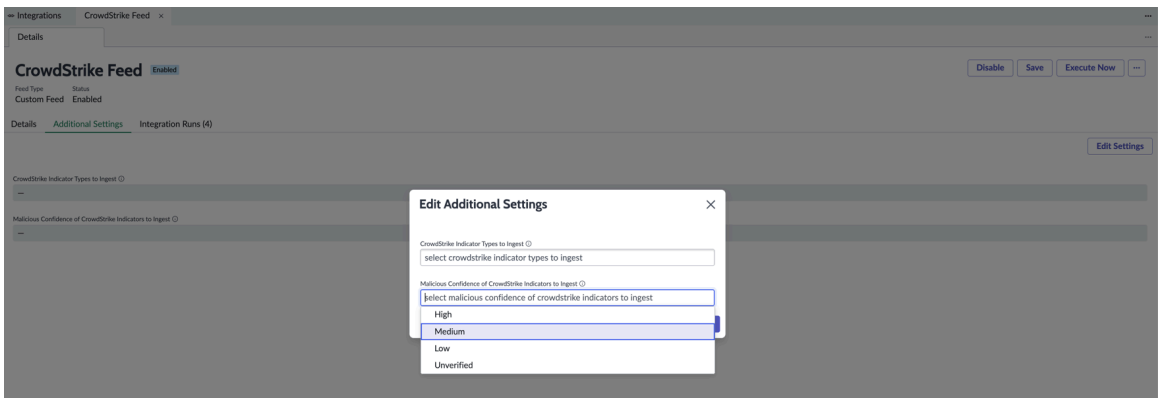
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Selecione uma das opções: **Tipos de indicador de Crowd-Strike para ingerir** ou **Confiança mal-intencionada dos indicadores do CrowdStrike para ingerir**.





Tradução automática

Nota:

a. Tipos deindicador do CrowdStrike a serem ingeridos: somente os tipos de indicador selecionados seriam ingeridos do CrowdStrike ao buscar os indicadores atualizados (os indicadores do CrowdStrike são mapeados para observáveis no TISC). Se for deixado em branco, indicadores de todos os tipos serão incluídos.

b. Confiança mal-intencionada de indicadores do CrowdStrike para ingestão: somente o indicador selecionado com confiança mal-intencionada selecionada seria ingerido do CrowdStrike ao buscar os indicadores atualizados (os indicadores no CrowdStrike são mapeados para observáveis no TISC). Se deixado em branco, serão ingeridos indicadores de toda a confiança mal-intencionada.

10. Selecione os valores necessários para cada opção. Com base nisso, os indicadores correspondentes serão ingeridos.

11. Clique em **Atualizar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

12. Clique em **Habilitar**.

> **Nota:** O feed premium é igual aos outros feeds, exceto a resposta que é analisada durante a configuração. Uma resposta específica é analisada para o CrowdStrike adicionando o ID do cliente e o segredo do cliente.

Que tipo de dados é obtido do CrowdStrike:

a. Indicadores do CrowdStrike que são atualizados após o tempo de ingestão configurado. Esses indicadores do CrowdStrike serão mapeados para observáveis no TISC. Abaixo estão os tipos de indicador que são ingeridos no TISC:
   - Hash SHA256
   - Hash MD5
   - Hash SHA1
   - URL
   - Domínio
   - Endereço IP
   - Nome de Mutex
   - Nome de arquivo
   - Endereço de e-mail
   - Nome de usuário
   - Bloco de endereço IP

b. Atores de ameaça do CrowdStrike que são atualizados após o tempo de ingestão configurado. Esses agentes do CrowdStrike serão mapeados para agentes de ameaça em nosso sistema.

c. Relatórios do CrowdStrike que são atualizados após o tempo de ingestão configurado. Esses relatórios do CrowdStrike serão mapeados para relatórios de ameaças em nosso sistema.

d. Também buscamos os dados abaixo, além das entidades mencionadas acima.
   i. Atores/relatórios/indicadores de ameaças que estão relacionados aos indicadores ingeridos acima.
   ii. Atores/indicadores de ameaças relacionados a todos os relatórios ingeridos como parte da ingestão atual.

Propriedades do sistema para CrowdStrike

A seguir detalhamos as propriedades do sistema para o CrowdStrike.

1. sn_sec_tisc.crowdstrike_actor_batch_size: indica o número de agentes a serem extraídos em uma única chamada de API. Observação: aplicável somente quando a integração não encontra o necessário presente no sistema.
   - Tipo: inteiro
   - Valor: 250
2. sn_sec_tisc.crowdstrike_api_limit: número de registros a serem buscados por vez no CrowdStrike. Quanto maior o número, mais memória será consumida para processar a carga.
   - Tipo: inteiro
   - Valor: 1000

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. sn_sec_tisc.crowdstrike_indicator_batch_size: denota o número de indicadores a serem extraídos em uma única chamada de API. Observação: aplicável somente quando a integração não encontra o necessário presente no sistema.
   - Tipo: inteiro
   - Valor: 150
4. sn_sec_tisc.crowdstrike_offset_limit_total: o total permitido de deslocamento e limite da API do CrowdStrike.
   - Tipo: inteiro
   - Valor: 50000
5. sn_sec_tisc.crowdstrike_report_batch_size: indica o número de relatórios a serem extraídos em uma única chamada de API. Observação: aplicável somente quando a integração não encontra o necessário presente no sistema.
   - Tipo: inteiro
   - Valor: 50

Noções básicas sobre STIX TAXII

A Expressão de informações sobre ameaças estruturadas (STIX) é uma linguagem e um formato de serialização usados para trocar inteligência contra ameaças cibernéticas (CTI). O Trusted Automated Exchange of Intelligence Information (TAXII) é um protocolo usado para trocar inteligência contra ameaças cibernéticas (CTI) por HTTPS.

Com o STIX, todos os aspectos de suspeita, comprometimento e atribuição são representados como objetos e relacionamentos descritivos. As informações do STIX podem ser representadas visualmente para um analista ou armazenadas como JSON para serem lidas rapidamente pela máquina.

A Inteligência contra ameaças cibernéticas (CTI) foi criada para definir um conjunto de representações e protocolos de informações para atender à necessidade de modelar, analisar e compartilhar informações sobre ameaças cibernéticas. O CTI tem como foco principal o desenvolvimento e a padronização da Expressão de informações de ameaças estruturadas (STIX) e da Troca automatizada confiável de informações de indicadores (TAXII).

Configurar um novo feed TAXII

Você pode manter feeds TAXII para compartilhar informações no formato STIX. Cada feed TAXII contém uma ou mais coleções TAXII.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações**.
3. Selecionar **Feeds de informações sobre ameaças** > **STIX TAXII** > **Feeds TAXII**.

   Nota: Configure o feed TAXII para servir como um perfil para todas as Coleções TAXII em.

4. Clique **em Configurar nova origem**.
   A página Configurar novo feed TAXII é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

Criar nova fonte de dados

Campo	Descrição
Nome	Insira um nome para o feed.
Descrição	Descrição do feed.
Tipo de Origem	O tipo de origem, como código aberto, origem premium e assim por diante, fornecido para o feed. Os tipos de origem disponíveis são: ◦ Governo ◦ ISACs ◦ Código aberto ◦ Origem Premium ◦ Outra origem
Logotipo	Anexe o logotipo do feed de origem.
Setor	Selecione a categoria do setor, como Aeroespacial, Agrícola e assim por diante, para a qual a fonte de dados do feed se aplica.

Preencha os campos na seção Configuração, conforme apropriado.

Configuração

Campo	Descrição
Versão de TAXII	Selecione a Versão TAXII do servidor TAXII que precisa ser configurada. As versões compatíveis são 2.0 e 2.1.
Tipo de Configuração	Forneça um tipo de configuração para buscar coleções TAXII. Os valores disponíveis são: ◦ **URL do serviço de descoberta**: escolha a URL do serviço de descoberta para buscar coleções de todas as raízes de API disponíveis no serviço de descoberta do servidor TAXII. ◦ **URL raiz da API**: escolha a URL raiz da API para buscar coleções da raiz da API específica do servidor TAXII.
Autenticação	Selecione a opção necessária na lista suspensa se a autenticação for necessária. As opções disponíveis são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Nenhum**: selecione esta opção se não houver autenticação necessária. ◦ **Básico**: selecione esta opção para fornecer o nome de usuário e a senha. ◦ **Chave de API**: selecione esta opção para fornecer uma chave de API. ◦ **Escolha uma mensagem REST**: selecione esta opção para qualquer outro tipo de autenticação. As opções de mensagem REST são: ▪ **Usar mensagem REST**: marque esta caixa se precisar de uma mensagem REST para criar uma mensagem REST de pré-compilação. Se você não selecionar, será usado o valor no campo de endpoint. Clique no ícone de pesquisa e selecione a mensagem REST na lista. ▪ **Método REST**: marque esta caixa se precisar de um método REST. Clique no ícone de pesquisa e selecione o método REST na lista. **Nota:** Os campos Mensagem REST e Método REST se tornam disponíveis quando a opção Mensagem REST é selecionada.
URL	Insira a URL do serviço de descoberta do servidor TAXII ou a URL raiz da API específica com base no tipo de configuração selecionado.
Seção avançada	
Avançado	Marque a caixa de seleção para escolher um script de integração e um processador de relatório diferentes. Verifique se os scripts escolhidos são compatíveis com a versão TAXII selecionada. Com base na versão e na autenticação TAXII, esses scripts são preenchidos automaticamente por padrão.
Script de integração	Invoca uma chamada para a REST Endpoint URL API usando os parâmetros de autenticação, como tipo de autenticação: nome de usuário/senha/chave de API e os cabeçalhos a serem passados com a solicitação e, em seguida, o script busca os observáveis ou indicadores de dados STIX que estão disponíveis para o feed específico.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os dados obtidos são somente os dados brutos (nenhum registro é criado) que serão anexados ao processo de integração e podem ser exibidos na seção **Execução de integração**. No sistema de base, a seguir estão as inclusões de scripts personalizados, que são provisionadas na aplicação para os scripts de integrações: ◦ TAXIIV2_0QueryParamAPIKeyIntegrationScript ◦ TAXIIV2_0BasicAuthIntegrationScript ◦ TAXIIV2_1QueryParamAPIKeyIntegrationScript ◦ TAXIIV2_1BasicAuthIntegrationScript O script de integração padrão é baseado no tipo de feed selecionado. As inclusões de script executam uma chamada REST simples, salvam a resposta como um anexo e retornam o anexo para o processador.
Processador de relatórios	O processador de relatório invoca uma chamada para a URL do endpoint REST. No sistema de base abaixo estão as inclusões de scripts personalizadas, que são provisionadas na aplicação para os scripts de integrações, **TAXIIV2CollectionDataProcessor**.

Preencha os campos na seção Programação, conforme apropriado.

Agendamento

Campo	Descrição
Frequência de execução de coletas	O intervalo de programação que será aplicado aos registros de coleta TAXII. A frequência de execução de uma coleta TAXII pode ser modificada na exibição do formulário de coleta TAXII, se necessário. **Nota:** Esta configuração será aplicada como padrão a todas as coleções TAXII obtidas. Há uma opção para substituir a configuração em Coleções TAXII, se necessário. Para obter mais informações, consulte Trabalhos agendados e como Executar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	automaticamente um script de sua escolha .
Buscar dados de	A data de início a partir da qual os dados precisaram ser obtidos. Este campo deve ser definido com a hora a partir da qual os dados precisam ser ingeridos da origem correspondente. Depois que este campo for definido, a próxima execução de ingestão buscará os dados do tempo configurado e as execuções de ingestão consecutivas buscarão dados incrementais. Por exemplo, a Origem está programada para ingerir os dados a cada hora. Se o usuário definir **Buscar dados de** como 12 de janeiro às 6h em 12 de janeiro às 9h30, o acionamento da ingestão em 12 de janeiro às 10h buscará os dados de 12 de janeiro às 6h a 12 de janeiro às 10h. A próxima ingestão que é acionada às 11h buscará somente os dados incrementais de 12 de janeiro às 10h a 12 de janeiro às 11h. **Nota:** Isso significa que as execuções programadas buscarão dados de forma incremental a partir da data especificada.

6. Clique **em Validar conexão**
   Uma mensagem informativa é exibida informando que a conexão do feed TAXII foi bem-sucedida. Para buscar as coleções, prossiga para a próxima etapa.
7. Clique **em Obter cobranças TAXII**.

   Nota: Se houver erros, será exibida uma mensagem de erro informando que ocorreu um erro ao buscar coleções TAXII e verificar os logs para obter mais detalhes.

   As Coleções TAXII são exibidas na seção Coleções TAXII e estão desabilitadas por padrão.
8. Habilite as coleções TAXII para recuperar os objetos STIX disponíveis nessas coleções TAXII.

Integrações de aprimoramento de TISC

O sistema base Central de segurança de inteligência contra ameaças não inclui integrações pré-configuradas. Esta seção fornece instruções para configurar integrações ServiceNow e de terceiros.

Importante:

Verifique se você instalou as integrações de aplicativos de terceiros necessárias. Você pode ver os observáveis, a pesquisa de detecções e os detalhes da pesquisa de ameaças somente para os aplicativos de terceiros instalados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

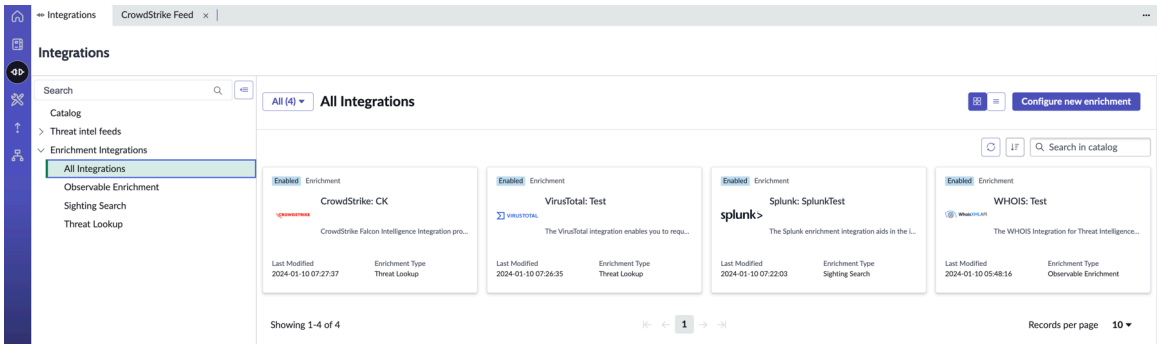
Todas as configurações de integração

Todas as integrações são aplicações separadas que precisam ser instaladas. O TISC oferece suporte a integrações com fornecedores de terceiros. Todas as integrações instaladas podem ser configuradas aqui.

Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

A seção de cada tipo de enriquecimento ficará visível somente se pelo menos uma das integrações correspondentes para esse tipo de enriquecimento estiver instalada. Por exemplo, a seção **Pesquisa de ameaças** ficará visível em **Integrações de aprimoramento** somente se pelo menos uma integração de pesquisa de ameaças estiver instalada.

Os cartões de integração configurados podem ser exibidos navegando até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.



Ações na exibição Todas as integrações

A exibição Todas as integrações permite que você execute as ações a seguir.

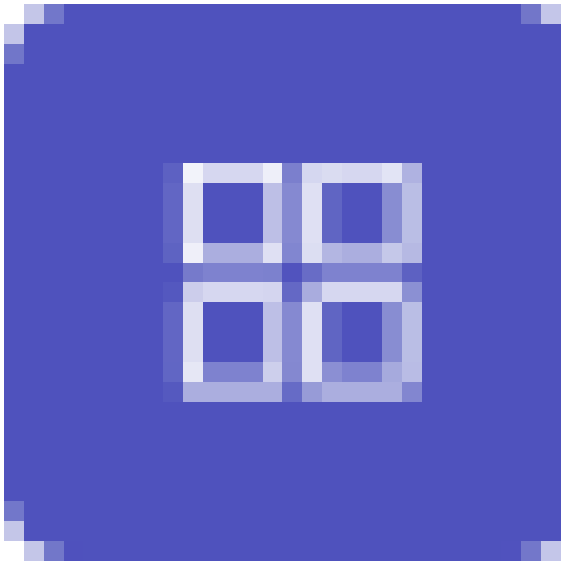
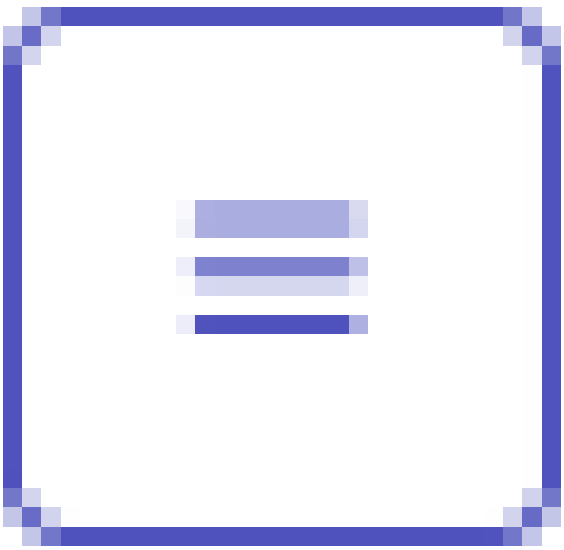
Ações na exibição de todas as integrações

Ação	Descrição
Todos	Use este menu suspenso para filtrar integrações com base no estado atual. Você pode filtrar com base nos seguintes estados: • **Todos**: exibe todas as integrações na página. Esta é a opção padrão. • **Habilitado**: exibe todas as integrações que estão em um estado habilitado. • **Desabilitado**: exibe todas as integrações que estão em um estado desabilitado. • **Rascunho**: exibe todas as integrações que estão em estado de rascunho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

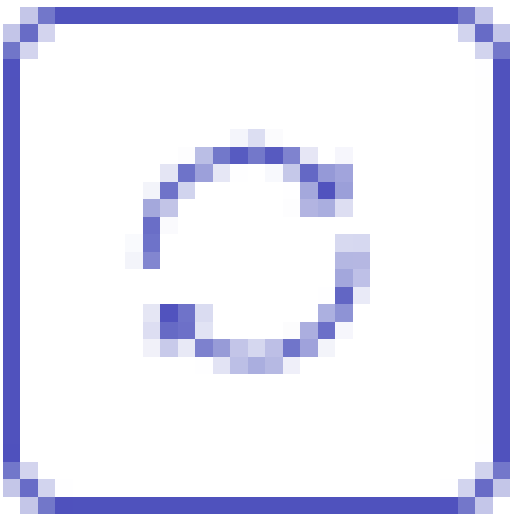
Ações na exibição de todas as integrações

Ação	Descrição
	Use esta ação para exibir todas as integrações na forma de cartões.
	Use esta ação para exibir todas as integrações na forma de listas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações na exibição de todas as integrações

Ação	Descrição
	Use esta ação para atualizar a página Todas as integrações.
	Use esta ação para classificar todas as integrações com base no seguinte: • **Última modificação (recente)** • **Última modificação (mais antiga)** • **Nome (A-Z)** • **Nome (Z-A)**
Pesquisar no catálogo	Use esta ação para pesquisar integrações configuradas com base no nome e na descrição no catálogo.

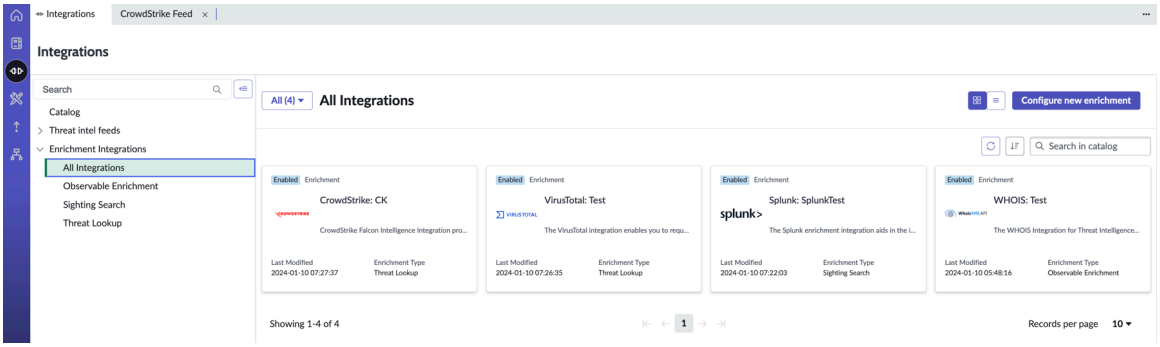
Configurar novo enriquecimento da exibição Todas as integrações

Você pode configurar novos aprimoramentos na exibição Todas as integrações ou diretamente nas seções Aprimoramento de observável, Pesquisa de detecções ou Pesquisa de ameaças, respectivamente. Para configurar o novo enriquecimento de todas as exibições de todas as integrações, execute as etapas a seguir.

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações** e selecione a seção **Todas as integrações**.

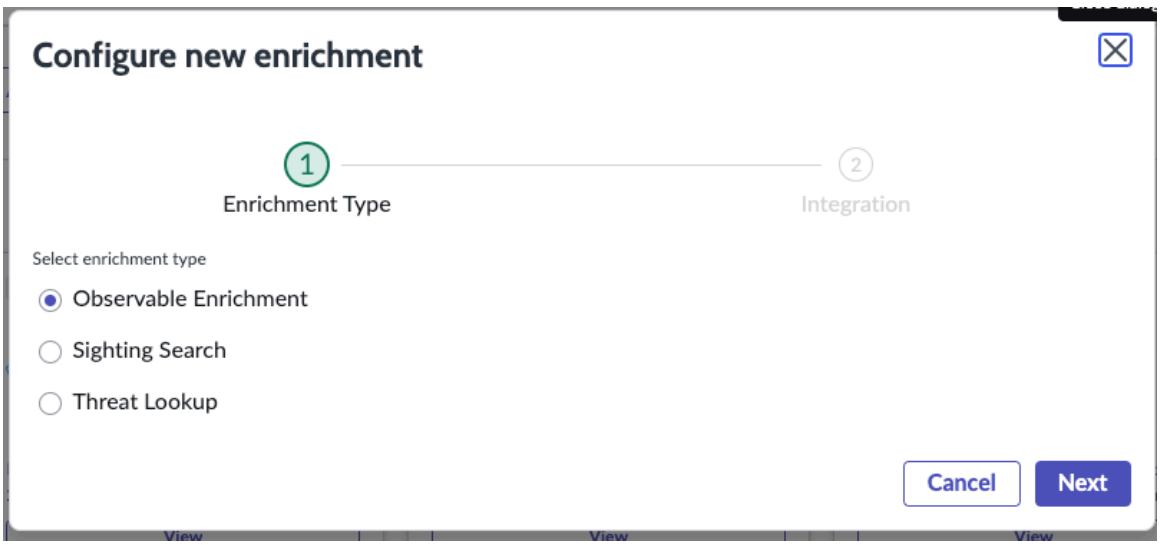
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique na ação **Configurar nova enriquecimento**.

   O pop-up Configurar novo aprimoramento aparece com três tipos de aprimoramento, que são Aprimoramento observável, Pesquisa de detecções ou Pesquisa de ameaças. Você precisa escolher o tipo de enriquecimento que deseja configurar.



4. Selecione um tipo de enriquecimento e clique em **Avançar**.

   Isso leva você ao pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que deseja configurar.

5. Selecione uma integração na lista de integrações disponíveis e clique em **Selecionar**.

   Isso leva você para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, integração WHOIS.

6. No formulário Criar nova integração, preencha os campos.

Configurar o novo formulário de integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `WHOIS1`.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	previamente por padrão. Por exemplo, `WHOIS`.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Aprimoramento de observável. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão. Os seguintes tipos de integração são compatíveis: ◦ Aprimoramento de Observável ◦ Pesquisa de detecções ◦ Pesquisa de ameaças
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.

7. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.

   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente de API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes integrações.

8. Clique na ação **Salvar** para armazenar e criar a configuração de integração de aprimoramento.

   Os detalhes fornecidos são validados e, por padrão, o status da integração de aprimoramento está desabilitado.

9. (Opcional) Clique na ação **Salvar como rascunho** para armazenar somente as configurações de integração como rascunho. Os usuários não podem habilitar uma integração quando ela é salva como rascunho

   Se você não tiver certeza sobre os detalhes da configuração, poderá usar a opção **Salvar como rascunho**. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.

10. Para habilitar a integração de aprimoramento, clique em **Habilitar**.

    A integração de aprimoramento foi habilitada com sucesso.

11. Você também pode habilitar, desabilitar ou excluir uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessário na página Catálogo ou na página Integrações de aprimoramento.

Configurar aprimoramento de observável

Você pode executar o aprimoramento da inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações executadas dependem daquelas que você ativou.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Central de segurança de inteligência contra ameaças oferece suporte ao aprimoramento de observável somente para a integração WHOIS a partir de agora. Para obter mais informações, consulte Configurar e habilitar a integração Whois.

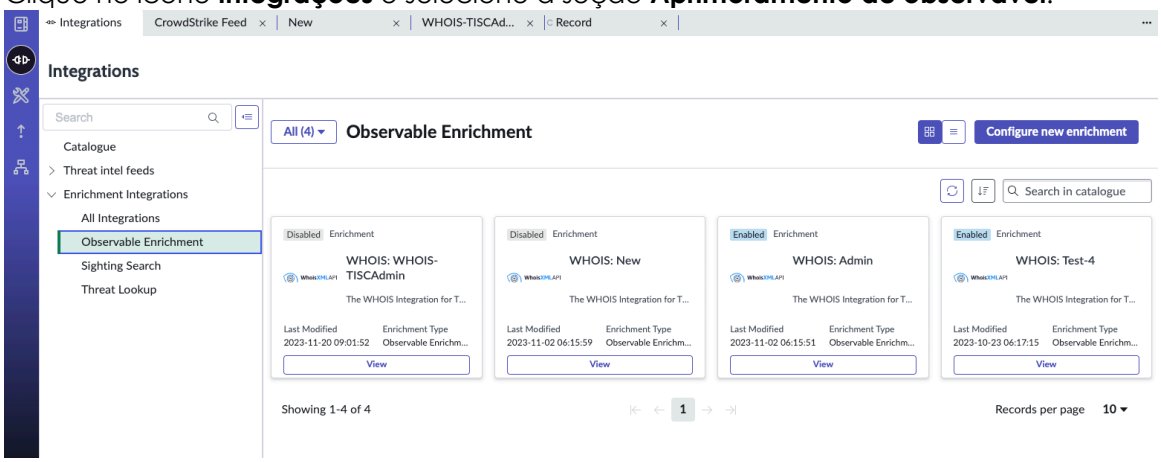
Nota: O módulo Integrações de aprimoramento só será mostrado se pelo menos uma das integrações que oferecem suporte a qualquer uma das capacidades estiver instalada na aplicação.

Por Que e Quando Desempenhar Esta Tarefa

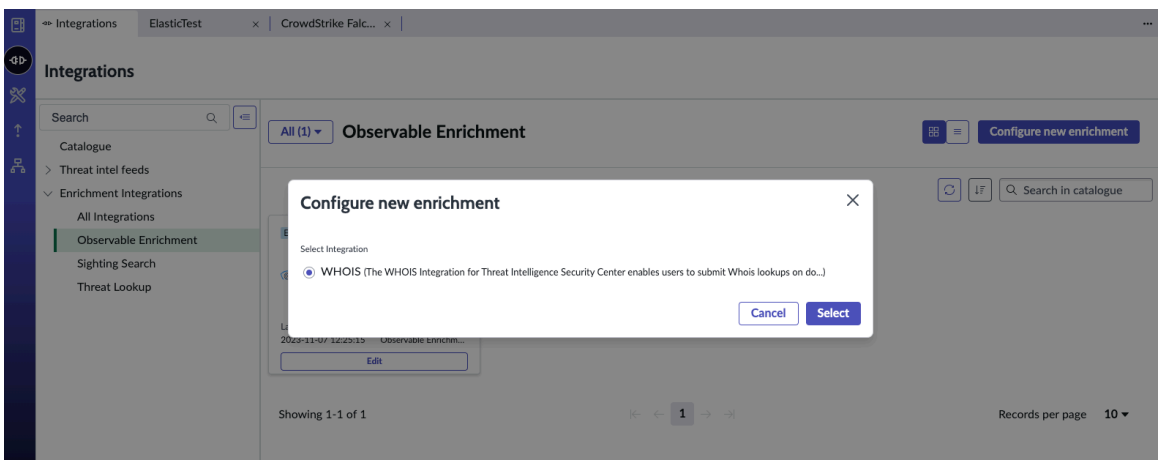
A seção Aprimoramento de observável contém somente as integrações com o tipo de integração como enriquecimento de observável. Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações** e selecione a seção **Aprimoramento de observável**.



3. Clique na ação **Configurar nova enriquecimento**.
   Isso leva você ao pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que precisa configurar.
4. Selecione uma integração na lista de integrações disponíveis e clique em **Selecionar**.
   Isso leva você para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, integração WHOIS.

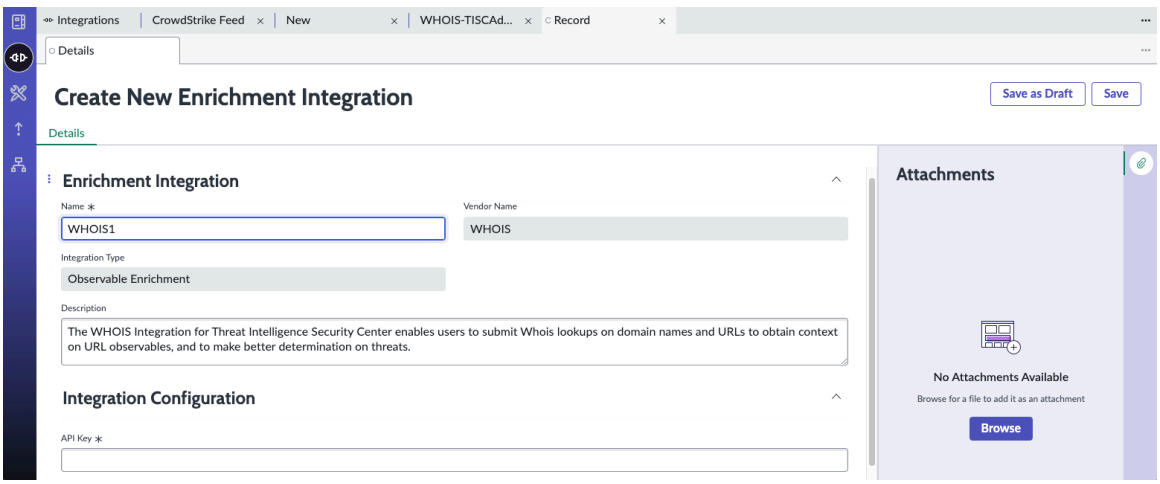


5. No formulário Criar nova integração, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Integração de aprimoramento	
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `WHOIS1`.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `WHOIS`.
Tipo de Integração	Tipo de integração que você selecionou, que é Aprimoramento de Observável. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão.
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.



6. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.
   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente de API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes apps.
7. Clique na ação **Salvar** para armazenar e criar a nova configuração de integração de aprimoramento.
   Depois de clicar na ação **Salvar** ou **Habilitar**, a integração é validada usando as configurações de integração fornecidas. Por padrão, o status da integração de aprimoramento é definido como desabilitado.
8. Clique **em Salvar como ação de rascunho** para armazenar somente as atualizações feitas na configuração de aprimoramento e não criá-las.
   Se você não tiver certeza sobre os detalhes da configuração, poderá usar a opção **Salvar como rascunho**. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
9. Para habilitar a integração de aprimoramento, clique em **Habilitar**.
   A integração de aprimoramento foi habilitada com sucesso. Você também pode habilitar, desabilitar ou excluir uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessário na página Catálogo ou na página Integrações de aprimoramento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar pesquisa de detecções

Você pode executar a pesquisa de detecções em um ou vários observáveis para determinar o número de vezes que os observáveis são avistados nos logs da sua organização. Você pode executar a pesquisa de detecções em observáveis dentro de um número selecionado de dias ou dentro de um intervalo de datas.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Nota: O módulo Integrações de aprimoramento só será mostrado se pelo menos uma das integrações que oferecem suporte a qualquer uma das capacidades estiver instalada na aplicação.

O Central de segurança de inteligência contra ameaças é compatível com a Pesquisa de detecções somente para as seguintes integrações:

- Pesquisa do Splunk
- ElasticSearch

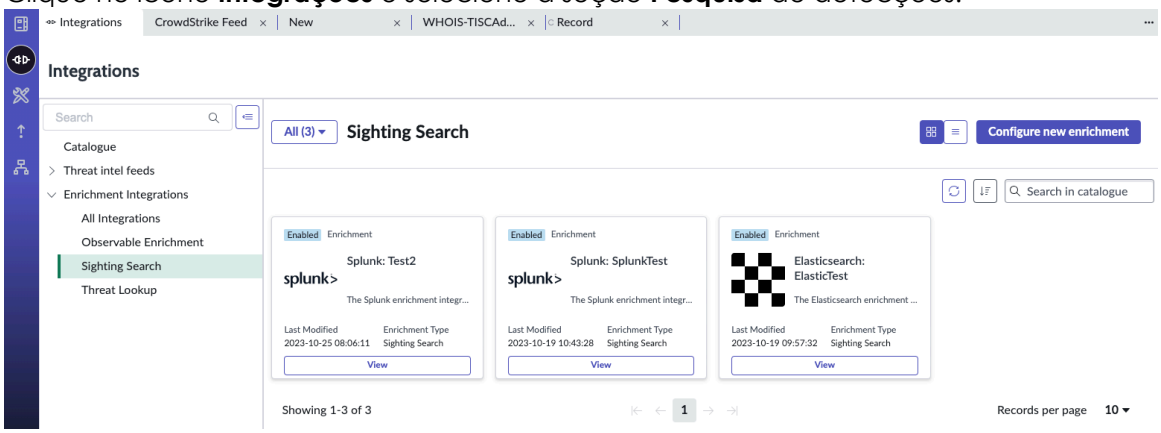
Por Que e Quando Desempenhar Esta Tarefa

A seção Pesquisa de detecções contém somente as integrações com o tipo de integração como pesquisa de detecções.

Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Procedimento

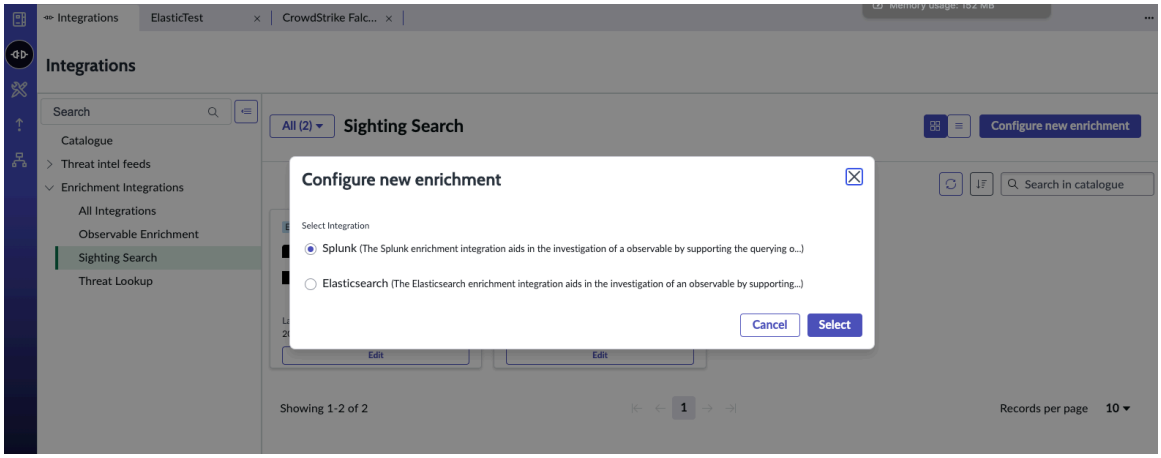
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações** e selecione a seção **Pesquisa** de detecções.



3. Clique na ação **Configurar nova enriquecimento**.
   Isso leva você ao pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que precisa configurar.
4. Selecione uma integração na lista de integrações disponíveis e clique em **Selecionar**.
   Isso leva você para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, integração Splunk.

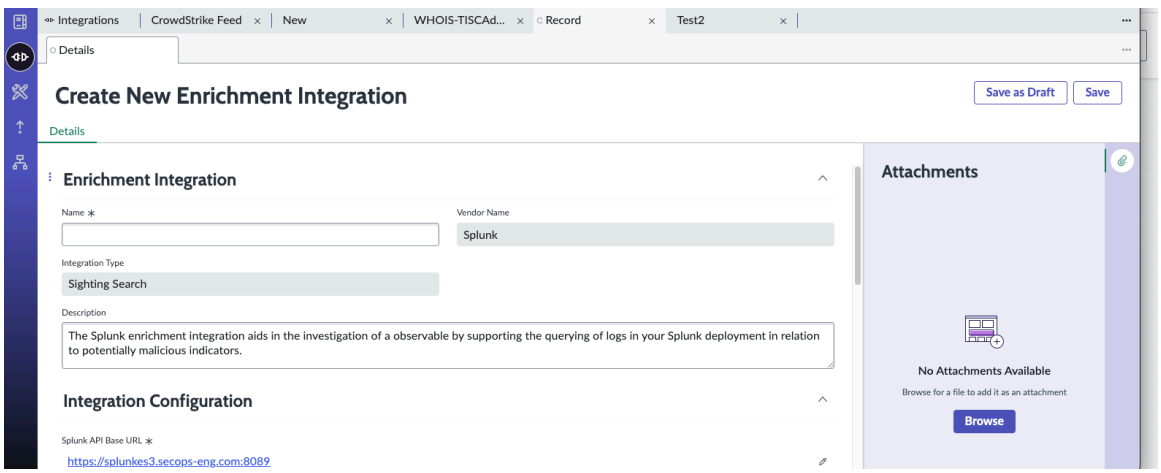
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. No formulário Criar nova integração, preencha os campos.

Campo	Descrição
Integração de aprimoramento	
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `Splunk-1`.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `Splunk`.
Tipo de Integração	Tipo de integração que você selecionou, que é Pesquisa de detecções. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão.
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.



6. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.
A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente de API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes apps.

7. Clique na ação **Salvar** para armazenar e criar a nova configuração de integração de aprimoramento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os detalhes fornecidos são validados e, por padrão, o status da integração de aprimoramento está desabilitado.

8. Clique **em Salvar como ação de rascunho** para armazenar somente as atualizações feitas na configuração de aprimoramento e não criá-las.
   Se você não tiver certeza sobre os detalhes da configuração, poderá usar a opção **Salvar como rascunho**. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
9. Para habilitar a integração de aprimoramento, clique em **Habilitar**.
   A integração de aprimoramento foi habilitada com sucesso. Você também pode habilitar uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessária na página Catálogo ou na página Todas as integrações.

Definir consultas para pesquisa de detecções

Você pode usar configurações de pesquisa de detecções para definir as consultas usadas para encontrar a predominância de observáveis em seu ambiente como parte da investigação observável.

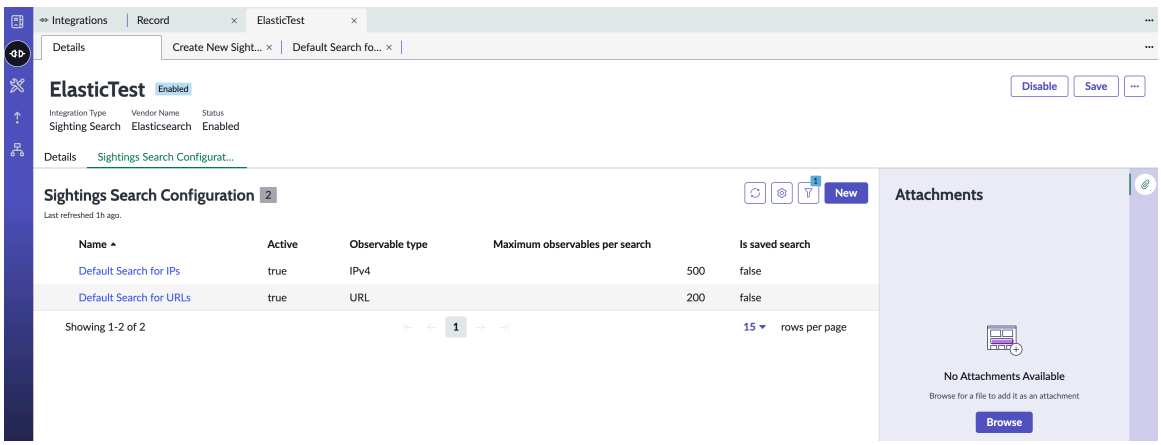
Exibir consultas para pesquisa de detecções

Função necessária: sn_sec_tisc.admin

Para exibir as configurações de pesquisa de detecções, execute as seguintes etapas:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de detecções**.
3. Procure a integração cuja configuração de pesquisa de detecções você deseja exibir e clique em **Editar**.
4. Selecione a guia **Configurações de pesquisa** de detecções.

   Você pode exibir a lista de configurações de pesquisa de detecções.



5. Clique na configuração de pesquisa de detecções necessária para exibir os detalhes da configuração.
6. Para gerar uma consulta de pesquisa de detecções de teste, clique na ação **Gerar consulta de pesquisa de detecções de teste**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A ação **Gerar consulta de pesquisa de detecções de teste** só funcionaria se você tivesse configurado os parâmetros de consulta de pesquisa de detecções. Para obter mais informações, consulte Usando parâmetros de pesquisa de detecções.

7. No pop-up Gerar consulta de pesquisa de detecções de teste, insira ou cole vários observáveis usando vírgula, nova linha, tabulação ou barras verticais para gerar uma consulta de teste.
8. Clique em **Gerar** para gerar a consulta de pesquisa de detecções de teste.
9. Você também pode executar as seguintes ações na guia Configurações de pesquisa de detecções:
   a. Para atualizar a lista de configurações de pesquisa de detecções, clique no ícone de .
   b. Para executar uma ação de lista nas configurações de pesquisa de detecções, clique no ícone .

      Você pode executar as duas ações de lista a seguir:

      - **Editar colunas**: você pode usar esta ação para adicionar ou remover colunas existentes e modificar a ordem de acordo com seus requisitos.
      - **Redefinir larguras**: você pode usar esta ação para redefinir as larguras das colunas.

   c. Para filtrar as configurações de pesquisa de detecções com base nas condições, clique no ícone do .

      O valor 1 indica que uma condição é usada para a filtragem.

Criar configurações de pesquisa de detecção

Função necessária: sn_sec_tisc.admin

```
Maximum observables per search = "maximum number of observables that can
 be substituted in a single search query"

Search = "Search query that should be executed in sighting search source.
Search query can contain substitution variables that would be substituted
 with observables of specific type as configured in sighting search
 parameters when sighting search query is formed"
```

Para criar uma configuração de pesquisa de detecções, execute as seguintes etapas:

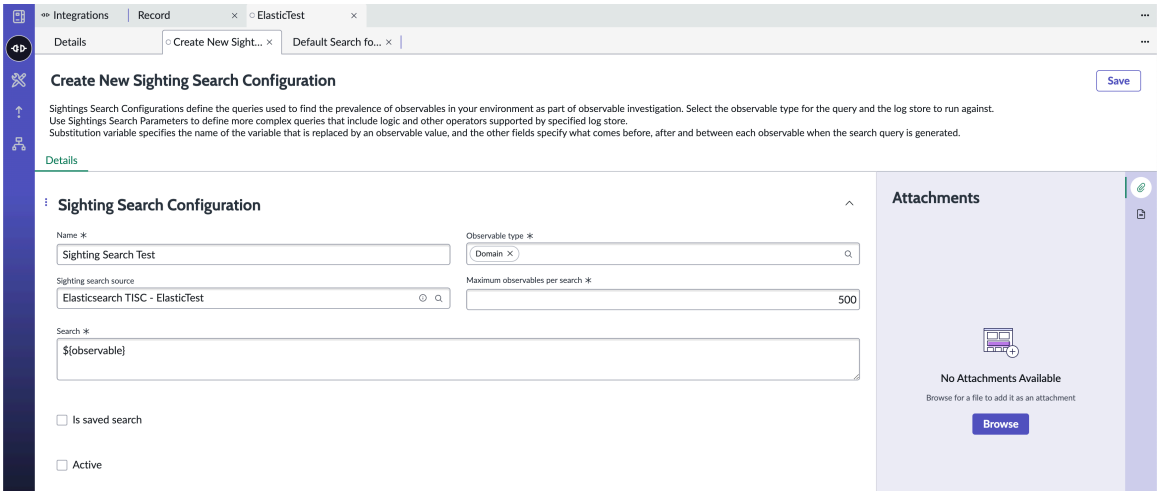
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de detecções**.
3. Procure a integração cuja configuração de pesquisa de detecções você deseja exibir e clique em **Editar**.
4. Selecione a guia **Configurações de pesquisa** de detecções.

   Você pode exibir a lista de configurações de pesquisa de detecções.

5. Para criar uma configuração de pesquisa de detecções, clique em **Novo**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. No formulário, preencha os campos.

Criar uma configuração de pesquisa de detecções

Campo	Descrição
Nome	Nome da configuração da pesquisa de detecções.
Tipo de observável	Define o tipo de categoria de observável.
Origem da pesquisa de detecções	Define a origem configurada para a integração.
Máximo de observáveis por pesquisa	O número de observáveis antes da consulta de pesquisa é dividido em várias consultas. Defina este valor como `500` para esta integração.
Pesquisar	Adicione uma cadeia de caracteres de pesquisa nativa para formar uma consulta. Por exemplo, `${observable}`.
Pesquisa salva	Executa uma pesquisa salva, ou seja, o campo Nome deve corresponder ao nome da pesquisa salva.
Ativo	A consulta será executada somente se a opção ativa estiver selecionada.

7. Clique em **Salvar**.

Usando parâmetros de pesquisa de detecções

Você pode usar parâmetros de pesquisa de detecções que definem consultas mais complexas, que incluem lógica e outros operadores compatíveis com o armazenamento de logs especificado.

Exibir parâmetros de pesquisa de detecções

Função necessária: sn_sec_tisc.admin

Para exibir os parâmetros de pesquisa de detecções, execute as seguintes etapas:

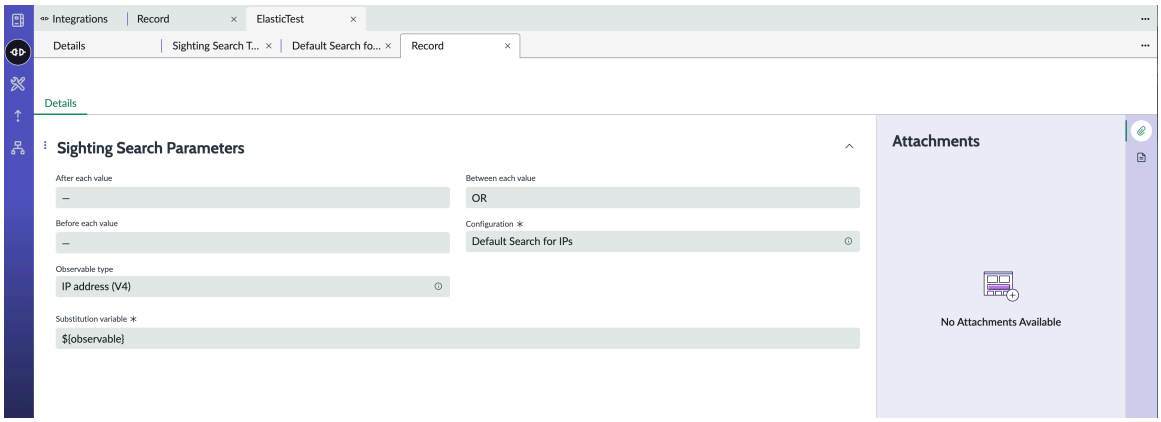
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de detecções**.
3. Procure a integração cuja configuração de pesquisa de detecções você deseja exibir e clique em **Editar**.
4. Selecione a guia **Configurações de pesquisa** de detecções.

   Você pode exibir a lista de configurações de pesquisa de detecções.

5. Clique na configuração de pesquisa de detecções necessária para exibir os detalhes da configuração.



6. Selecione a guia **Parâmetros de pesquisa** de detecções.

   Você pode exibir a lista de parâmetros de pesquisa de detecções.

7. Clique no parâmetro de pesquisa de detecções necessário para exibir os detalhes do parâmetro.
8. Você também pode executar as seguintes ações na guia Parâmetros de pesquisa de detecções:

   a. Para atualizar a lista de parâmetros de pesquisa de detecções, clique no ícone de .

   b. Para executar uma ação de lista nos parâmetros de pesquisa de detecções, clique no ícone .

      Editar colunas: você pode usar esta ação para adicionar ou remover colunas existentes e modificar a ordem de acordo com seus requisitos.

   c. Para filtrar os parâmetros de pesquisa de detecções com base nas condições, clique no ícone do .

      O valor 1 indica que uma condição é usada para a filtragem.

Criar parâmetro de pesquisa de detecções

`Exemplo para geração de consulta`

```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

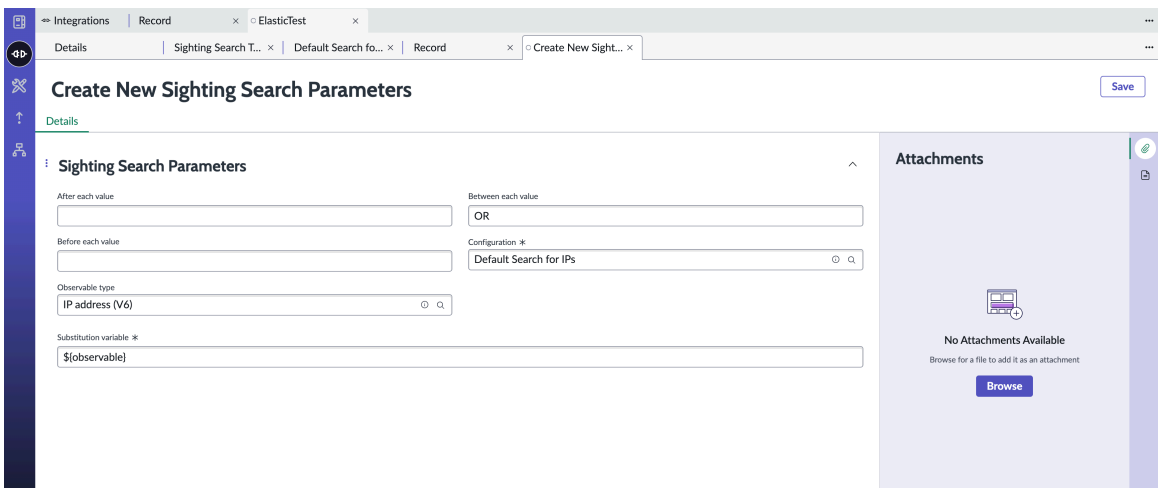
```
Query: {Before each Value}Obs1{After each Value}{Between each
 value}{Before each Value}Obs2{After each Value}


Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: "ip_address = 172.32.31.41
 OR ip_address = 192.168.10.12"
```

Para criar um parâmetro de pesquisa de detecções, execute as seguintes etapas:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Integrações**.
2. Na página Integrações, navegue até **Integrações de aprimoramento** > **Pesquisa de detecções**.
3. Procure a integração cuja configuração de pesquisa de detecções você deseja exibir e clique em **Editar**.
4. Selecione a guia **Configurações de pesquisa** de detecções.

   Você pode exibir a lista de configurações de pesquisa de detecções.
5. Clique na configuração de pesquisa de detecções necessária para exibir os detalhes da configuração.
6. Selecione a guia **Parâmetros de pesquisa** de detecções.

   Você pode exibir a lista de parâmetros de pesquisa de detecções.
7. Para criar um parâmetro de pesquisa de detecções, clique em **Novo**.



8. No formulário, preencha os campos.

Criar um parâmetro de pesquisa de detecções

Campo	Descrição
Após cada valor	O parâmetro de pesquisa de detecções após cada observável quando a consulta de pesquisa é gerada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Entre cada valor	O parâmetro de pesquisa de detecções entre cada observável quando a consulta de pesquisa é gerada. Por exemplo, OU.
Antes de cada valor	O parâmetro de pesquisa de detecções antes de cada observável quando a consulta de pesquisa é gerada.
Configuração	Os detalhes de configuração do parâmetro de pesquisa.
Tipo de observável	Define o tipo de categoria de observável.
Variável de substituição	Especifica o nome da variável que é substituída por um valor observável.

9. Clique em **Salvar**.

Configurar pesquisa de ameaças

Você pode configurar a pesquisa de ameaças para realizar uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pela Inteligência contra ameaças, os observáveis serão verificados quanto a malware e os resultados serão retornados. Você pode executar a pesquisa de ameaças em um ou mais observáveis para determinar a mal-intendência de um observável.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Nota: O módulo Integrações de aprimoramento só será mostrado se pelo menos uma das integrações que oferecem suporte a qualquer uma das capacidades estiver instalada na aplicação.

O Central de segurança de inteligência contra ameaças é compatível com a pesquisa de ameaças somente para as seguintes integrações:

- VirusTotal
- Inteligência do CrowdStrike

Para obter mais informações, consulte Pesquisa de ameaças.

Por Que e Quando Desempenhar Esta Tarefa
A seção Pesquisa de ameaças contém somente as integrações com o tipo de integração como pesquisa de ameaças.

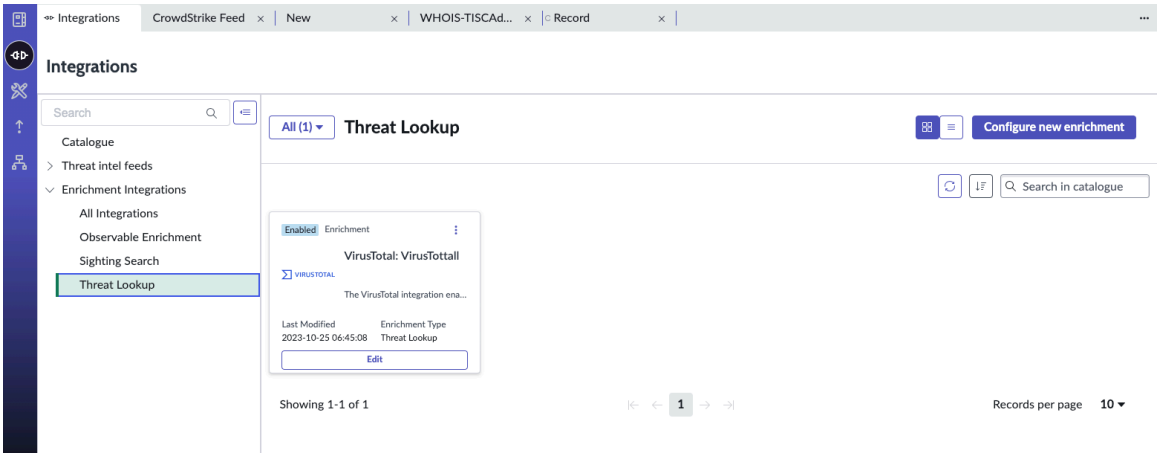
Esta seção exibe cartões para cada uma das implementações de integração configuradas que você pode ativar e usar.

Procedimento

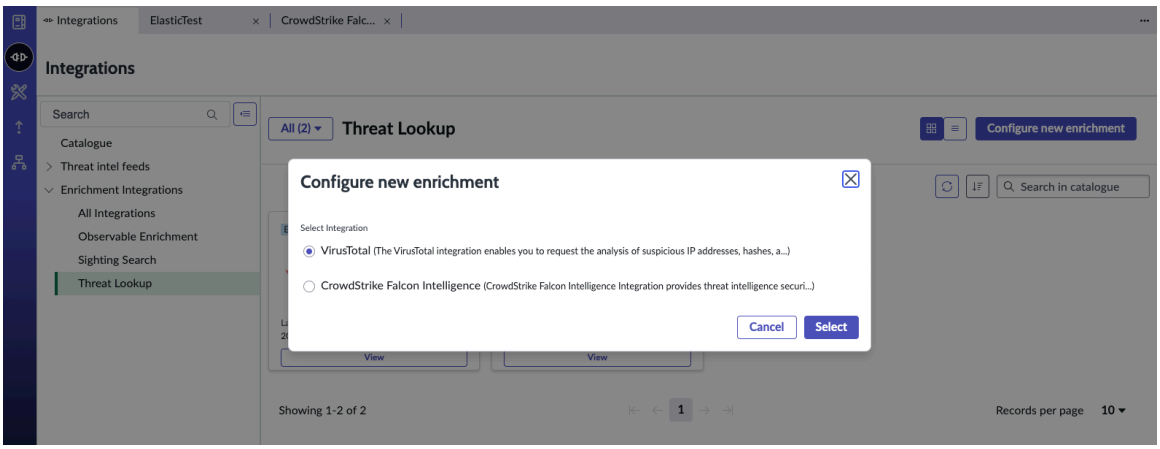
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Integrações** e selecione a seção **Pesquisa de ameaças**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique na ação **Configurar nova enriquecimento**.
   Isso leva você ao pop-up que exibe as integrações disponíveis. Você precisa escolher a integração que precisa configurar.
4. Selecione e integração na lista de integrações disponíveis e clique em **Selecionar**.
   Isso leva você para a página Criar nova integração de aprimoramento da integração selecionada. Esta página é preenchida previamente com detalhes da integração selecionada por padrão. Por exemplo, integração VirusTotal.

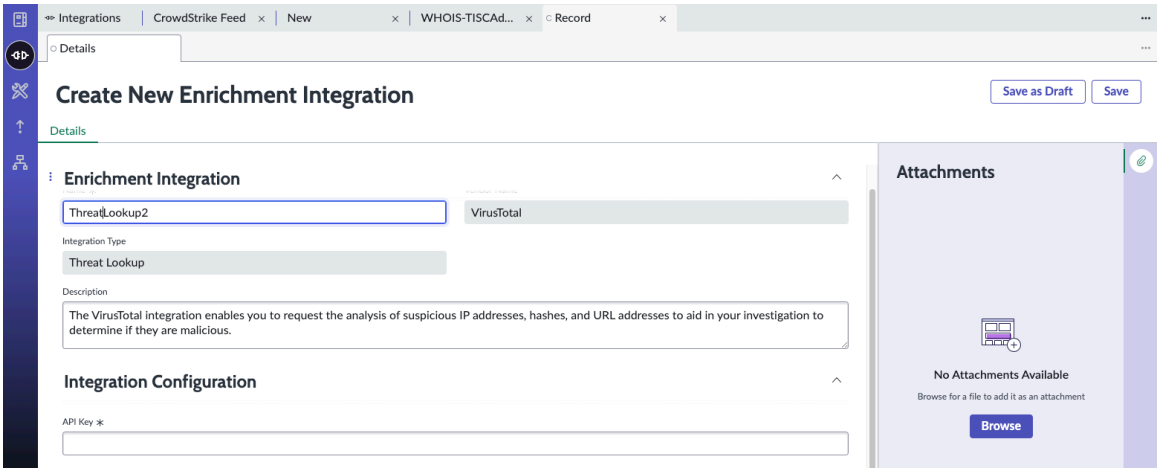


5. No formulário Criar nova integração, preencha os campos.

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, `VirusTotal-1`.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos previamente por padrão. Por exemplo, `VirusTotal`.
Tipo de Integração	Tipo de integração que você selecionou, que é Pesquisa de ameaças. Os detalhes do tipo de integração selecionado são preenchidos previamente por padrão.
Descrição	Insira uma descrição exclusiva para a nova integração de aprimoramento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na seção Configuração de integração, configure os detalhes da integração com base em seus requisitos.
   A seção Configuração de integração inclui detalhes de configuração, como chave de API, ID ou segredo do cliente de API, nome de usuário, senha e assim por diante, que você precisa preencher. Esses detalhes de configuração variam para diferentes apps.
7. Clique na ação **Salvar** para armazenar e criar a nova configuração de integração de aprimoramento.
   Os detalhes fornecidos são validados e, por padrão, o status da integração de aprimoramento está desabilitado.
8. Clique **em Salvar como ação de rascunho** para armazenar somente as atualizações feitas na configuração de aprimoramento e não criá-las.
   Se você não tiver certeza sobre os detalhes da configuração, poderá usar a opção **Salvar como rascunho**. Depois de obter os detalhes da configuração, você pode preencher as informações restantes na versão de rascunho e criá-la.
9. Para habilitar a integração de aprimoramento, clique em **Habilitar**.
   A integração de aprimoramento foi habilitada com sucesso. Você também pode habilitar, desabilitar ou excluir uma integração de aprimoramento específica usando o menu Ações do bloco de integração necessário na página Catálogo ou na página Integrações de aprimoramento.

Exibir calculadoras de reputação de pesquisa de ameaças

Você pode exibir a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis da sua integração.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

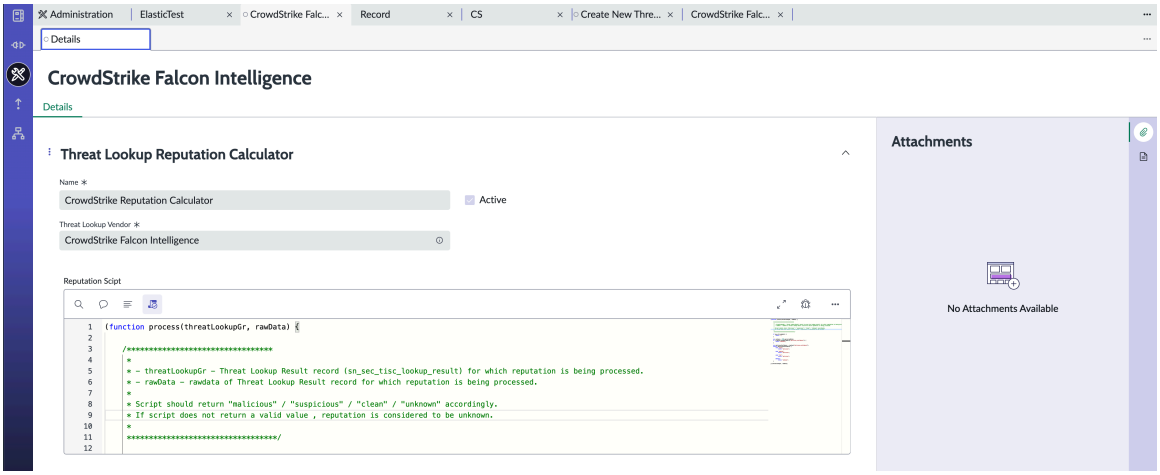
Para saber mais sobre as Calculadoras de reputação de pesquisa de ameaças, consulte Gerenciamento da calculadora de reputação de pesquisa de ameaças.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecione a seção **Calculadora de reputação de pesquisa de ameaças**.
   Você pode exibir a lista de calculadoras de reputação de pesquisa de ameaças.
3. Clique na Calculadora de reputação de pesquisa de ameaças necessária para exibir os detalhes da calculadora.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Você também pode executar as seguintes ações na seção Calculadora de reputação de pesquisa de ameaças:

   a. Para atualizar a lista de calculadoras de reputação de pesquisa de ameaças, clique no ícone de .

   b. Para executar uma ação de lista nas calculadoras de reputação de pesquisa de ameaças, clique no ícone .

      Você pode executar as duas ações de lista a seguir:

      - **Editar colunas**: você pode usar esta ação para adicionar ou remover colunas existentes e modificar a ordem de acordo com seus requisitos.
      - **Redefinir larguras**: você pode usar esta ação para redefinir as larguras das colunas.

   c. Para filtrar calculadoras de reputação de pesquisa de ameaças com base em condições, clique no ícone do .

      O valor 1 indica que uma condição é usada para a filtragem.

Referências de TISC API

A tabela a seguir fornece as referências de endpoints de API que ajudam nos aprimoramentos.

APIs de TISC

API	Descrição
API do TISC - POST /sn_sec_tisc/threat_intel_data/observables	Esta API recupera os dados dos observáveis, incluindo os relacionamentos entre os observáveis e outros dados de inteligência contra ameaças associados.
API do TISC - POST /sn_sec_tisc/threat_intel_data/add_observables	Esta API adiciona observáveis válidos à aplicação Central de segurança de inteligência contra ameaças (TISC) criando registros de origem de observável.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os endpoints da API do TISC, consulte API do TISC na seção de referência da REST API na implementação da API e referência em docs.servicenow.com.

Integrações de TISC

Esta seção fornece instruções para configurar e habilitar as integrações de Inteligência contra ameaças.

Aprimoramento de Observável

O fluxo de trabalho Enriquecer observável WhoIs executa o enriquecimento em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pela integração da API WhoisXML, os observáveis serão aprimorados.

Nota: A Central de segurança de inteligência contra ameaças oferece suporte ao aprimoramento de observável somente para a integração WHOIS.

Integração Whois

A integração Whois permite que você envie pesquisas Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para determinar melhor as ameaças.

Configurar e habilitar a integração Whois

Antes de usar a integração do Whois, você deve baixá-la da ServiceNow Store e ter uma conta válida do Whois.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Os plug-ins de integração do observável Whois e Central de segurança de inteligência contra ameaças são necessários.

Procedimento

1. Usando sua instância, acesse **a Central de segurança de inteligência contra ameaças**.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Aprimoramento de Observável**.
6. No cartão **WHOIS**, clique em **Configurar novo aprimoramento** para configurar a integração **WHOIS**.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, WHOIS.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, WHOIS.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da nova integração de aprimoramento. Por exemplo, a descrição da integração WHOIS é: A integração WHOIS para Central de segurança de inteligência contra ameaças permite que os usuários enviem pesquisas Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para determinar melhor as ameaças.

8. Faça o detalhamento ativo até a seção **Configuração de integração**.
9. Insira (ou cole) a **chave de API** que você adquiriu no site WHOIS.
10. Clique em **Salvar**.
    Os detalhes da integração são validados e, por padrão, o status da integração WHOIS está desabilitado.
11. Clique em **Habilitar** para habilitar a integração WHOIS.

Resultados
Depois de configurado, o WHOIS pode ser selecionado para executar aprimoramentos em observáveis na Central de segurança de inteligência contra ameaças.

Integração com Shodan

O Shodan é um mecanismo de pesquisa que analisa informações da faixa de serviço de dispositivos conectados em todo o mundo.

A integração do Shodan executa o enriquecimento nos seguintes observáveis:

- Endereços IP
- URLs
- Domínios

Configurar e habilitar a integração do Shodan

Antes de usar a integração do Shodan, você deve baixá-la da ServiceNow Store.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Usando sua instância, acesse **a Central de segurança de inteligência contra ameaças**.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Aprimoramento de Observável**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. No cartão **Shodan**, clique em **Configurar novo aprimoramento** para configurar a integração.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, Shodan.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos automaticamente e, por padrão, este campo será somente leitura. Por exemplo, Shodan.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Aprimoramento de observável.
Descrição	Insira a descrição da nova integração de aprimoramento. Por exemplo, a descrição da integração do Shodan é: O Shodan ajuda a analisar informações de faixa de dispositivos conectados em todo o mundo.

8. Faça o detalhamento ativo até a seção **Configuração de integração**.
9. Insira (ou cole) a **chave de API** que você adquiriu no portal Shodan.
10. Clique em **Salvar**.
    Os detalhes da integração são validados e, por padrão, o status é desabilitado.
11. Clique em **Habilitar** para habilitar a integração.

Pesquisa de detecções

Esta seção descreve as integrações do TISC Sighting Search e do Elastic Search.

Introdução à integração do Elasticsearch

A integração de aprimoramento do Elasticsearch pesquisa seus logs e adiciona informações de detecções relevantes aos seus observáveis.

Configurar e habilitar a integração do Elasticsearch

O Elasticsearch é um mecanismo distribuído de pesquisa e análise RESTful que se integra facilmente às Operações de segurança.

Antes de Iniciar

Antes de poder usar o Elasticsearch, você deve baixá-lo da ServiceNow Store.

Função necessária: sn_sec_tisc.admin

- O plug-in Central de segurança de inteligência contra ameaças deve ser instalado e ativado para que você possa usar a integração do Elasticsearch.
- Obtenha a URL base da API do Elasticsearch, a URL base do Kibana, o nome de usuário e a senha no seu perfil do Elasticsearch.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Usando sua instância, acesse **a Central de segurança de inteligência contra ameaças**.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de detecções**

   Nota: As integrações configuradas aparecem como uma série de cartões.

6. No cartão do **Elasticsearch**, clique em **Configurar novo aprimoramento** para configurar a integração do **Elasticsearch**.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a configuração de pesquisa de detecções.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, Elasticsearch.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da integração do Elasticsearch. Por exemplo, a integração de aprimoramento do Elasticsearch ajuda na investigação de um observável, oferecendo suporte à consulta de logs em sua implantação do Elasticsearch.
Configuração de Integração	
URL de Base da API Elasticsearch	A URL base que você adquiriu no site do Elasticsearch.
URL base do Kibana	A URL base do Kibana. [Opcional] Links para uma instância do Kibana, quando disponíveis.
Nome de usuário	Seu nome de usuário do Intel Elasticsearch.
Senha	Sua senha do Intel Elasticsearch.
Índice do Elasticsearch	O índice do Elasticsearch. Estes, por sua vez, conterão documentos exclusivos para cada índice. Os índices são identificados por nomes minúsculos que se referem a ações que são ações executadas (como pesquisar e excluir).
Campo do intervalo de datas	O carimbo de data/hora da configuração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do número de linhas de dados brutos nas propriedades do Security Incident Response .
MID Server	Selecione Qualquer para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o Editor de fluxo de trabalho.

8. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o status da integração do Elasticsearch está desabilitado.
9. Clique em **Habilitar** para habilitar a integração do Elasticsearch.

Resultados
Depois de configurado, o Elasticsearch pode ser selecionado para executar pesquisa de detecções em observáveis na Central de segurança de inteligência contra ameaças.

Introdução à integração de pesquisa do Splunk

O software Splunk pesquisa, monitora e analisa big data gerado por máquina e se integra facilmente às Operações de segurança. Antes de poder usar a integração Splunk Sighting Search, você deve baixá-la da ServiceNow Store.

Configurar e habilitar a integração do Splunk

A integração do Splunk Enrichment pesquisa seus logs e adiciona informações de detecção relevantes.

Antes de Iniciar
Antes de poder usar o Splunk Search, você deve baixá-lo da ServiceNow Store.

Função necessária: sn_sec_tisc.admin

- O plug-in Central de segurança de inteligência contra ameaças deve ser instalado e ativado para que você possa usar a integração do Splunk Search.
- Obtenha o Splunk e a Pesquisa do Splunk e obtenha a URL Base da API, a URL do Link, o Nome de Usuário e a Senha da sua instância do Splunk.

Procedimento

1. Usando sua instância, acesse **a Central de segurança de inteligência contra ameaças**.
2. Baixe a integração do ServiceNow Store.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Quando a instalação estiver concluída, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de detecções**
   As integrações configuradas aparecem como uma série de cartões.
6. No cartão **Pesquisa do Splunk**, clique em **Configurar novo aprimoramento** para configurar a integração da **Pesquisa do Splunk**.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a configuração de pesquisa de detecções.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, Splunk.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da integração do Splunk. Por exemplo, a integração de aprimoramento do Splunk ajuda na investigação de um observável, oferecendo suporte à consulta de logs em sua implantação do Splunk em relação a indicadores potencialmente maliciosos.
Configuração de Integração	
URL base da API Splunk	A URL base que você adquiriu do site Splunk.
URL do Link	[Opcional] A URL do link que vincula à interface da Web do Splunk, quando disponível.
Nome de usuário	Seu nome de usuário do Intel Elasticsearch.
Senha	Sua senha do Intel Elasticsearch.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os primeiros resultados que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do número de linhas de dados brutos nas propriedades do Security Incident Response .
Implantação no Local	O ambiente implantado no local.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
MID Server	Selecione Qualquer para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota: A configuração desta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o Editor de fluxo de trabalho.

8. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o status da integração do Splunk está desabilitado.
9. Clique em **Habilitar** para habilitar a integração do Splunk.

Resultados

Depois de configurado, o Splunk pode ser selecionado para executar pesquisas de detecções em observáveis na Central de segurança de inteligência contra ameaças.

Pesquisa de ameaças

O fluxo de trabalho de pesquisa de ameaças - VirusTotal e CrowdStrike Falcon executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo VirusTotal e também pelo CrowdStrike, os observáveis serão verificados quanto a malware e os resultados serão retornados.

Integração de TISC VirusTotal

A integração do TISC VirusTotal permite que você solicite a análise de endereços IP, arquivos, hashes de arquivo e endereços URL suspeitos para ajudar em sua investigação para determinar se eles são mal-intencionados.

Configurar e habilitar a integração VirusTotal

Antes de poder usar a integração VirusTotal, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

O plug-in Central de segurança de inteligência contra ameaças é necessário para ativar a integração do VirusTotal.

Procedimento

1. Usando sua instância, acesse **a Central de segurança de inteligência contra ameaças**.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, acesse o VirusTotal e obtenha a chave de API no seu perfil do VirusTotal.
4. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
5. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
6. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de ameaças**
7. Clique em **Configurar novo aprimoramento** para configurar a integração do **VirusTotal**.
8. Preencha os campos no formulário Configurar novo aprimoramento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, VirusTotal.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, VirusTotal.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da nova integração de aprimoramento.

9. Faça o detalhamento ativo até a seção **Configuração de integração**.
10. Insira (ou cole) a **chave de API** que você adquiriu no site VirusTotal.
11. Clique em **Salvar**.
    Os detalhes da integração são validados e, por padrão, o status da integração do VirusTotal está desabilitado.
12. Clique em **Habilitar** para habilitar a integração do VirusTotal.

Resultados
Depois de configurado, o VirusTotal pode ser selecionado para executar pesquisas em observáveis na Central de segurança de inteligência contra ameaças.

TISC Integração do CrowdStrike Falcon Intelligence

O CrowdStrike Falcon Intelligence fornece inteligência de segurança cibernética que se integra facilmente às Operações de segurança.

Nota:

O plug-in Central de segurança de inteligência contra ameaças é necessário para implementar a integração do CrowdStrike Falcon Intelligence.

Configurar e habilitar a integração do CrowdStrike Falcon Intelligence

Antes de poder usar o CrowdStrike Falcon Intelligence, você deve baixá-lo da ServiceNow Store e adicionar o ID de cliente e o segredo do cliente apropriados.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

- A aplicação Central de segurança de inteligência contra ameaças deve ser instalada e ativada.
- Obtenha o ID do cliente da API e o segredo do cliente da API no seu perfil do CrowdStrike Falcon Intelligence.
- Nos Escopos de API do portal do CrowdStrike Falcon Intelligence, habilite a configuração Leitura para Indicadores (Falcon Intelligence).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Usando sua instância, acesse **a Central de segurança de inteligência contra ameaças**.
2. Baixe a integração do ServiceNow Store.
3. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
4. Selecionar **Integrações** > **Integrações de aprimoramento** > **Todas as integrações**.
5. Como alternativa, você pode navegar até **Integrações** > **Integrações de aprimoramento** > **Todas as integrações** > **Pesquisa de ameaças**.
6. Clique em **Configurar novo** aprimoramento para configurar a integração **do CrowdStrike Falcon Intelligence**.
7. Preencha os campos no formulário Configurar novo aprimoramento.

Integração de aprimoramento

Campo	Descrição
Nome	Insira um nome para a nova integração de aprimoramento. Por exemplo, CrowdStrike Falcon Intelligence.
Nome do fornecedor	Nome do fornecedor Os detalhes do fornecedor selecionado são preenchidos por padrão. Por exemplo, CrowdStrike Falcon Intelligence.
Tipo de Integração	Tipo de integração que você selecionou. Por exemplo, Pesquisa de ameaças.
Descrição	Insira a descrição da nova integração de aprimoramento.
Configuração de Integração	
ID de cliente	O ID do cliente que você obteve do CrowdStrike.
Segredo do cliente	A chave secreta do cliente que você obteve do CrowdStrike.

8. Clique em **Salvar**.
   Os detalhes da integração são validados e, por padrão, o status da integração do CrowdStrike Falcon Intelligence está desabilitado.
9. Clique em **Habilitar** para habilitar a integração do CrowdStrike Falcon Intelligence.

Resultados

Depois de configurado, o CrowdStrike Falcon Intelligence pode ser selecionado para realizar pesquisas em observáveis na Central de segurança de inteligência contra ameaças.

TISC integration with SIR Workspace

A integração de TISC com SIR anexa automaticamente o contexto nos observáveis no espaço de trabalho de incidente de segurança para os analistas de segurança. Todos os novos observáveis do SIR podem ser enviados para o TISC para análise posterior pela equipe de CTI usando as ações de IU fornecidas nas telas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Além disso, todos os resultados de aprimoramento produzidos a partir de integrações disponíveis somente no SIR também podem ser enviados usando as ações de IU fornecidas no espaço de trabalho.

Administração

Usando a navegação à esquerda para navegar até o módulo Administração na Central de segurança de inteligência contra ameaças e exibir os seguintes módulos de administração de dados de TISC, para definir regras de filtragem e aprovação, definir pontuação de ameaça e gerenciar notificações.

Administração de dados

Módulo	Descrição
Mecanismo de regras	Esta seção consiste nas seguintes regras necessárias durante o gerenciamento de dados: 1. **Regras de aprovação de importações de dados**: defina as regras de aprovação e integre o fluxo de aprovação na seção Inteligência de importação após o envio da importação de dados. 2. **Regras de filtragem de entrada**: crie regras de filtro para filtrar os dados dos registros de origem de entrada. 3. **Regra de pontuação**de ameaça: personalize a calculadora de pontuação de ameaça que atribui pontuação de ameaça aos observáveis.
Listas de controle de segurança	Este módulo ajuda você com os controles de segurança: 1. **Lista de permissões** 2. **Lista de proibições** 3. **Lista de observação**
Taxonomias	Este módulo ajuda a criar taxonomias para os registros de fonte de dados.
Notificações	Este módulo define como gerenciar notificações por e-mail.
Modelos	Este módulo resume como criar modelos de relatório em tempo de design e experiência de tempo de execução.

Definição de regras de aprovação de importações de dados

Use esta seção para definir as regras de aprovação e integrar o fluxo de aprovação na seção Inteligência de importação após o envio da importação de dados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Administração** no espaço.
3. Ir para **Mecanismo de regras** > **Regras de aprovação de importações de dados**.
4. Selecione **Regra de aprovação para importações de dados**.

   No sistema base, **a Regra de aprovação para importações de dados** é a regra de aprovação padrão provisionada para permitir que os usuários ativem o fluxo de trabalho de aprovação.

5. Insira pelo menos um nome de usuário ou grupo de usuários para cada seção **Selecionar usuário ou grupo que requer aprovação** e **Selecionar aprovador(es)**.
6. Clique no botão **Habilitar** para habilitar o fluxo de aprovação para as importações de dados.

   Quando habilitadas, as importações de dados estarão na fila de aprovação para o aprovador aprovar ou rejeitar o processamento de dados. O aprovador revisará as mudanças feitas pelo analista e aprovará ou rejeitará a solicitação de importação de dados.

   Nota: Uma notificação por e-mail é enviada aos usuários ou grupos de usuários informando que o trabalho de importação foi processado e aprovado ou rejeitado.

Definição de regras de expiração

Defina regras de expiração para vários observáveis ou uma combinação de vários objetos de origem ou origem de indicadores que são criados no TISC.

Antes de Iniciar

Cada origem criada na aplicação tem um período de expiração. Os feeds de dados usam técnicas como o período de expiração baseado em tempo para aumentar a ingestão de dados. No TISC, as regras de expiração definem o tempo de expiração de um conjunto específico de fontes de dados ou conjunto de tipos de objetos ou tipos de observáveis.

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Regras de expiração**.
   A página Regras de expiração é exibida.
3. Clique em **Nova**.

Campo	Descrição
Nome	Insira um nome para a regra de expiração.
Descrição	Insira uma descrição para a regra de expiração.
Período de expiração (dias)	Especifique o tempo após o qual os dados ingeridos devem expirar ou ser considerados desatualizados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Insira o período de expiração do observável em dias. Por exemplo, 100 dias. **Nota:** Quaisquer que sejam os dados ingeridos da origem, eles expirarão 100 dias após a ingestão.
Fontes de dados	Indica a regra de expiração da fonte de dados atual. Selecione a lista de fontes de dados na pesquisa. **Nota:** Não selecione este campo e certifique-se de deixá-lo em branco se quiser selecionar todas as fontes de dados. Se você quiser selecionar o indicador como um objeto, deverá selecionar o objeto e, em seguida, selecionar o valor **Tipo de registros** como **Indicador**. **Nota:** Por padrão, uma regra de expiração de exemplo sn_sec_tisc_m2m_entity_rules é provisionada para os usuários no sistema de base. Para observáveis, esta amostra de regra de expiração estará no estado desabilitado. Você deve habilitar e ativar a regra. Para aplicar a regra nos registros de origem, você deve habilitar a regra.
Categoria	Indica o tipo de categoria de regra de expiração para a fonte de dados atual. Selecione o tipo de categoria na lista suspensa, como observável ou objeto.
Tipo de registros	Selecione o tipo de registros.

4. Clique em **Habilitar** para habilitar a regra de expiração depois de criar uma nova regra. Se você não habilitar a regra de expiração, a regra não será aplicada ao registro de origem.

Nota:

- Sempre que você habilita uma regra de expiração, uma verificação de duplicação acontece em segundo plano para verificar se há alguma regra duplicada no sistema com a mesma combinação de fontes de dados e tipo de registros. Em caso afirmativo, a aplicação solicitará uma mensagem informativa de que a regra já contém a mesma combinação de fonte de dados e categoria de objeto e que você deve modificar a combinação existente para habilitar a regra.
- Uma regra de expiração de amostra é provisionada para os usuários no sistema de base e esta **regra de expiração de amostra** para observável estará no estado desabilitado por padrão e você deve habilitar e ativar a regra.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Salvar**.
6. Clique em **Excluir** se quiser excluir qualquer regra de expiração.

Regras de expiração para registros de origem

As regras de expiração são basicamente úteis para definir o tempo de expiração dos registros de origem. O registro agregado herda o tempo de expiração mais alto dos registros de origens correspondentes.

Como as regras são aplicadas

Example: O tipo de registro de origem de entrada é malware do tipo de fonte de dados como CrowdStrike

Processo de avaliação de regra com base nas regras fornecidas para aplicar tempos de expiração aos registros de origem:

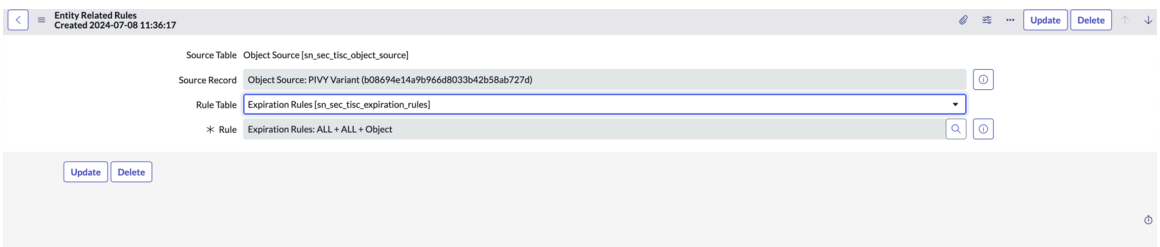
1. **Buscar todas as regras habilitadas:** a aplicação começa verificando todas as regras que estão habilitadas no momento.
2. Verifique a combinação de regras específica:

   Procure uma regra que corresponda especificamente à combinação de:

   - **Tipo de fonte de dados**: CrowdStrike
   - **Tipo de registros**: malware
3. **Prioridade com base nas combinações de regras correspondentes:**

   Se houver uma regra em que o tipo de fonte de dados for **CrowdStrike** e o tipo de registro for **Malware**, essa regra terá precedência. O tempo de expiração especificado nesta regra será aplicado.

4. **Regras de fallback:**
   a. Se nenhuma regra corresponder à combinação **CrowdStrike e Malware**, o sistema verificará se há uma regra em que o tipo de fonte de dados seja **CrowdStrike** e o tipo de registro seja **Todos**.
   b. Se nenhuma regra for encontrada, ele procurará uma regra em que o tipo de fonte de dados seja **Todos** e o tipo de registro seja **Malware**.
   c. Por fim, se nenhuma das regras acima existir, o padrão será uma regra em que o tipo de fonte de dados e o tipo de registro são **Todos**.
5. Se nenhuma dessas regras existir no sistema, nenhuma regra de expiração será aplicada aos registros de origem. Nesse caso, navegue até a tabela abaixo (mostrada na captura de tela) para verificar a combinação de regras que foram aplicadas aos objetos.



6. **Exclusão de fontes de dados:**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Suponha que, se uma fonte de dados que tem as regras de expiração associadas a ela for excluída, a exclusão poderá ser restrita ou não permitida até que essas regras sejam abordadas. Isso garante que não haja inconsistências na aplicação de políticas de expiração.

Definição de regras de filtragem

Crie regras de filtragem para filtrar qualquer tipo de dados ou qualquer tipo de dados de registros de origem de entrada. Usando o Gerenciador de fonte de dados, vários feeds, como dados STIX e feed RSS, são configurados e, para filtrar os dados dos feeds configurados, você precisa definir determinadas regras de filtragem.

Antes de Iniciar

Quando você está definindo uma regra de filtragem, essa regra é aplicada somente ao conjunto de dados de origem em que uma regra é aplicada para filtrar registros durante a ingestão e importação de dados.

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

Regras de filtragem são criadas e aplicadas em um registro de origem para processar outras etapas. O sistema base fornece a **regra de filtragem de amostra** para os usuários com uma regra predefinida para filtrar os observáveis ingeridos, dados de indicadores ou entidades/objetos.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Detalhar até **Mecanismo de regras** > **Regras de filtragem de entrada**.
3. Clique em **Novo** para definir regras de filtragem.
   A página Criar novas regras de filtro de entrada é exibida.
4. No formulário, preencha os campos.

Definir regras de filtragem

Campo	Descrição
Nome	Nome da nova regra de filtragem.
Descrição	Descrição resumida da regra de filtragem.
Ordem	A prioridade da regra de filtragem. Este campo indica a ordem na qual as regras de filtragem são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de filtragem com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100 para a regra de filtragem do sistema de base.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Fontes de dados	Selecione o tipo de fonte de dados na lista de pesquisa.
Tabela	Selecione o tipo de tabela ao qual você deseja aplicar o filtro. Por exemplo, Origem do observável, Origem do indicador e Origem do objeto.
Tipo de filtro (somente quando a tabela selecionada for Origem de observáveis)	Os tipos de filtro contêm duas opções com base nas quais você pode aplicar o filtro. ◦ Filtrar com base nas condições ◦ Filtro com base em lista
Tipo de filtro (filtro baseado na condição)	Condições de filtro no Construtor de condições. Essas condições são baseadas na tabela de origem. Por exemplo, Origem do indicador e Origem do objeto têm apenas o tipo de filtro: Filtro baseado em condição. Para adicionar mais condições, clique em **E** ou **OU**. Se **E** for selecionado, todas as condições deverão ser atendidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novo conjunto de condições**.
Tipo de filtro (filtro baseado na lista)	Se os observáveis de entrada corresponderem às entradas na lista selecionada, serão filtrados. **Nota:** Essas regras de filtragem não se aplicam a Importações de dados que usam a Inteligência de importação e as opções disponíveis são Lista de permissões, Lista de proibições e Lista de observação.

Depois que a regra de filtragem estiver habilitada nos dados ingeridos, o resultado poderá ser exibido nas guias a seguir como diferentes registros filtrados.

a. **Registros de observáveis filtrados**: filtra e lista os registros de observáveis.

b. **Registros de indicadores filtrados**: filtra e lista os registros de indicadores.

c. **Registros de objetos filtrados**: filtra e lista os registros de objetos.

Nota: Para aplicar as regras de filtragem com base em marcadores adicionados aos registros de origem, selecione a opção Marcadores de **TISC** no construtor de condições de filtro.

Calculadora de pontuação de ameaça personalizada no TISC

A Calculadora de pontuação de ameaça personalizada permite definir e calcular uma pontuação de gravidade de ameaça de um observável com base nos critérios definidos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pelo usuário, o que fornece uma pontuação de inteligência transparente dos observáveis. A pontuação de ameaça é calculada automaticamente para registros de observáveis.

Definir calculadora de pontuação de ameaça

Defina a pontuação de ameaça para os registros de observável que são gerados com base nos parâmetros definidos pelo usuário. O sistema base é provisionado com uma regra de pontuação de ameaça, que pode ser personalizada e habilitada de acordo.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Nota: Por padrão, a regra de pontuação de ameaça estará inativa. Você precisa habilitar a regra para ver a pontuação de observáveis.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Ir para **Regra de pontuação de ameaça**.
   A página da Calculadora de pontuação de ameaça é exibida.

Importante:

- Na aplicação, no sistema de base, há uma regra de pontuação que é provisionada para que os usuários exibam, editem ou modifiquem a pontuação da ameaça, mas o usuário não pode criar uma nova regra ou excluir a regra de pontuação de ameaça predefinida.
- As mudanças serão aplicadas a todos os novos observáveis ou atualizações dos observáveis a partir desse ponto. Para redefinir pontuações históricas, eles devem usar a opção de recálculo.

3. No formulário, os campos a seguir contêm os valores predefinidos.

Padrão de Calculadora de pontuação de ameaça

Campo	Descrição
Nome	Nome do valor de pontuação da ameaça. Por exemplo, Calculadora de pontuação de ameaça.
Descrição	Descrição do registro de pontuação de ameaça. Por exemplo, Calcula a pontuação de ameaça com base na soma ponderada de pontuações de critérios predefinidos.
Ponderação geral (aplicável ao construtor de critérios)	Este campo não é editável e exibe a ponderação geral calculada pelo sistema com base na ponderação correspondente aos critérios habilitados.
Critérios de pontuação	Indica os critérios de pontuação para um observável. A seguir estão as duas opções disponíveis para definir os critérios de pontuação de ameaça:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Construtor de critérios**: Use esta opção para adicionar, editar ou remover e habilitar e desabilitar critérios que contribuem para o cálculo da pontuação de ameaça e garantir que a ponderação agregada total seja de 100%. ◦ **Usar script (Avançado)**: o recurso de script é um recurso avançado para criar um script personalizado que deve retornar a pontuação de ameaça no intervalo de 0 a 100.

Abaixo estão as opções disponíveis para definir os **critérios de pontuação**:

◦ Criador de critérios

◦ Usar script (Avançado)

A seguir está o procedimento para o Construtor de critérios:

Nota: Você pode editar ou modificar os critérios existentes ou adicionar novos critérios.

a. Selecione o tipo de critérios.
Por exemplo, Adicionar novos critérios.

b. Selecione a **Tabela** para a qual os critérios estão configurados.
A lista de valores na lista suspensa são Observáveis, Ator da ameaça, Campanha, Local, Identidade, Vulnerabilidade, Evento de ameaça, Incidente de segurança e Agregados. Quando você seleciona uma dessas opções na lista suspensa, uma condição é aplicada. Essa condição garante que somente registros relacionados ao valor selecionado sejam exibidos ou calculados.

Nota:

- Se o Observável selecionado, a condição será aplicada ao registro do observável para o qual a pontuação de ameaça será calculada. Se a tabela selecionada não for observável, a condição será aplicada somente se os registros estiverem relacionados ao observável para o qual a pontuação de ameaça será calculada.
- Uma tabela agregada adicional é adicionada para definir as pontuações com base no número de relações que estão associadas aos observáveis. Por exemplo, selecione a Tabela: Agregados e o valor do campo: Agentes de ameaça para um observável, se houver mais de dois agentes de ameaça, defina a pontuação e aplique as condições conforme aplicável.
- Por exemplo, se você quiser definir uma pontuação para um ou mais agentes de ameaça associados a um observável, selecione o campo como Nº de agentes de ameaça, defina a pontuação desejada e aplique as condições conforme aplicável.

c. Selecione o **Campo** na tabela selecionada acima.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Insira a **ponderação** dos critérios entre 0 e 100.
A ponderação geral de todos os critérios deve ser de 100%.

e. Insira o nome e a descrição resumida dos critérios.

f. Marque a caixa de seleção **Habilitar critérios de pontuação** para habilitar os critérios de pontuação.

g. Defina as **Condições** e defina a pontuação das condições.

h. Você também pode adicionar novas condições usando o botão **Nova condição** e excluir a condição usando o ícone **Excluir critérios**.

i. Clique em **Adicionar** para adicionar os critérios configurados.

Aqui está um exemplo de definição de uma condição para uma pontuação de ameaça:

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. Clique no botão Recalcular **histórico** para recalcular a pontuação da ameaça.
Se houver mudanças na regra de pontuação de ameaça, você deverá aplicar novamente a regra de pontuação aos observáveis que têm a pontuação de ameaça já calculada no passado. Use o botão Recalcular **histórico** para acionar o trabalho de recálculo.

Nota:

- Uma mensagem de confirmação é exibida para você executar a ação, `Este é um processo de longa execução que é executado em segundo plano. Você não poderá fazer mudanças até que o processo seja concluído. Tem certeza de que deseja executar esta ação?`
- Para todos os eventos de atualização que estão sendo gerados para observáveis como parte do **histórico**de recálculo , o processamento de webhooks está desabilitado e, caso você queira habilitar, modifique esta propriedade do sistema `webhook_ignore_threat_score_reapply`.

5. Clique em **OK**.

Importante: Esta ação acionará um trabalho de longa execução e o sistema não permitirá que você faça mais mudanças na regra de pontuação de ameaça até que o trabalho seja concluído. Para obter mais informações sobre como a configuração do trabalho em segundo plano é definida, consulte Configuração da estrutura de trabalho em segundo plano da Resposta a vulnerabilidades .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está o **script Usar script (Avançado)** : use este script para criar um script personalizado que deve retornar a pontuação de ameaça dentro do intervalo de 0 a 100.

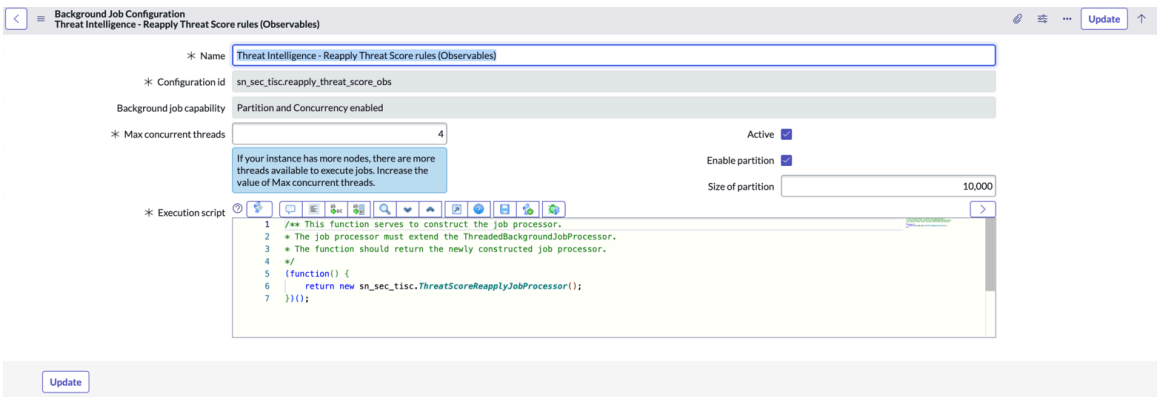
O campo de script avançado é preenchido automaticamente com uma função que usa os parâmetros **atuais** e **agregados** e essa função deve retornar a pontuação de ameaça no intervalo de 0 a 100.

Aqui, o parâmetro atual é o objeto GlideRecord da entidade (observável) para o qual a pontuação de ameaça está sendo calculada. Para os observáveis, corresponde ao GlideRecord da tabela sn_sec_tisc_observable. O parâmetro agregados é um objeto GlideRecord do registro da tabela sn_sec_tisc_aggregates que é usado para acessar as contagens de registros dos vários tipos de registro associados (como campanhas ou identidades) à entidade principal (observável).

Exemplo de exemplo do script na opção avançada:

```
answer = (function threatScoreCalculator(current, aggregates) {

    // return the threat score in the range of 0-100
    var threatSeverity = current.getValue("threat_severity");
    if(threatSeverity == "high")
     return 80;
    else {
        let associatedCampaigns =
 aggregates.getValue("num_of_campaigns");
        if(associatedCampaigns > 0)
            return 50;
    }
    return 0;

})(current, aggregates);
```

Para sua referência, abaixo está a captura de tela que mostra o processo de configuração do trabalho em segundo plano de pontuação de ameaça.



Definição de listas de controle de segurança

Use este recurso para adicionar ou remover observáveis em massa.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Ir para **Listas de controle de segurança**.
   Por exemplo, adicionar observáveis à lista de permissões e ir para a opção Lista de permissões.
3. Selecione **Lista de permissões**.
4. Selecione o tipo de Observáveis, como Endereço IP, Arquivo e assim por diante, para adicionar à lista de permissões.
5. Clique em **Adicionar**.
   A **lista Selecionar observáveis para permitir** é exibida.
6. Selecione todos os observáveis que precisam ser adicionados à lista de permissões.
7. Clique **em Adicionar à lista de permissões**.
   Os observáveis selecionados são adicionados.
8. Da mesma forma, selecione **Adicionar à lista de proibições** para adicionar os observáveis à lista removida.
9. Selecione **Adicionar à lista** de observação para adicionar os observáveis à lista de observação.

   Nota: Você pode adicionar diretamente os observáveis à lista de permissões, lista de proibições ou lista de observação diretamente na página de exibição do formulário Observáveis, que está disponível acima da faixa do formulário.

10. Para verificar, navegue até Informações sobre **ameaças Biblioteca**.
11. Selecione o tipo de observável que foi adicionado à lista de permissões.
    O observável é indicado como adicionado à lista de permissões.

    Nota: A lista de permissões e a lista de proibições são mutuamente exclusivas e o sistema garantirá automaticamente que um observável na lista de permissões não faça parte da lista de proibições e vice-versa.

Criando taxonomias

Crie taxonomias para os registros de fonte de dados.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração** > **Taxonomias**.
2. Clique em **Nova**.
3. Insira o **Nome**.
4. Habilite ou desabilite o **status** da taxonomia usando as ações de formulário Habilitar ou desabilitar.

   Nota: As taxonomias desativadas não estarão disponíveis para seleção de registros em que as taxonomias sejam aplicáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Vá para a seção **Valores** de taxonomia para adicionar valores de taxonomia.
6. Clique em **Novo** para abrir a nova exibição do formulário de valor de taxonomia e insira a **taxonomia** e o **valor**.
7. Clique em **Salvar**.
8. Por exemplo, navegue até **Biblioteca de informações sobre ameaças** > **Observáveis** para verificar as taxonomias do registro de observáveis.
9. Navegue até a seção **Marcadores e taxonomias** em qualquer página de formulário de observável e selecione a taxonomia recém-criada.

Nota: Você também pode adicionar marcadores e taxonomias na exibição de lista da biblioteca de informações sobre ameaças.

Gerenciamento da calculadora de reputação de pesquisa de ameaças

Você pode usar a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis com base nas respostas recebidas do fornecedor de pesquisa de ameaças.

Você pode criar uma Calculadora de descoberta de pesquisa de ameaças para sua integração e usar um script para determinar como deseja identificar as várias descobertas de observáveis. A Calculadora de descoberta de pesquisa de ameaças inclui um script de exemplo que vem com o sistema de base, que você pode usar para identificar as descobertas observáveis ou pode modificar este script de acordo com seus requisitos.

Para integrações de terceiros que fornecem os resultados calculados, a Calculadora de descoberta de pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema de base.

Acumular resultados de pesquisa de ameaças

Quando você tem vários resultados de pesquisa de ameaças para um observável de vários fornecedores de integração, os resultados de pesquisa de ameaças recentes de todos os fornecedores são considerados e as descobertas gerais do observável são marcadas da seguinte forma:

Descobertas de pesquisa de ameaças de acúmulo

Descoberta de observável mais recente	Descoberta observável geral
Mal-intencionado	Se um dos fornecedores de integração relatar o observável como malicioso, a descoberta geral do observável será marcada como mal-intencionada.
Suspeito	Se nenhum dos fornecedores de integração relatar o observável como malicioso, um deles o relatará como suspeito e a descoberta geral do observável será marcada como suspeita.
Limpar	Se todos os fornecedores de integração relatarem o observável como Limpo, a descoberta geral do observável será marcada como Limpo.
Desconhecido	Se nenhum dos fornecedores de integração relatar o observável como malicioso ou suspeito e um deles o

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descobertas de pesquisa de ameaças de acúmulo

Descoberta de observável mais recente	Descoberta observável geral
	relatar como desconhecido, a descoberta geral do observável será marcada como desconhecida.

Exibir calculadoras de reputação de pesquisa de ameaças

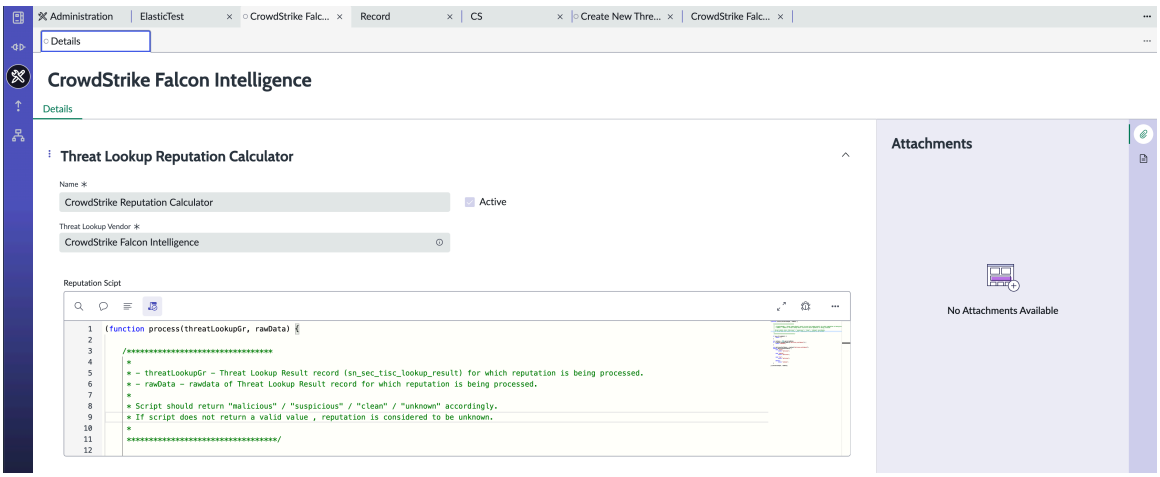
Você pode exibir a Calculadora de descoberta de pesquisa de ameaças para determinar como a reputação do observável é calculada com base na resposta do fornecedor de pesquisa de ameaças específico.

Função necessária: sn_sec_tisc.admin

Para exibir a Calculadora de reputação de pesquisa de ameaças, execute as seguintes etapas:

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecione a seção **Calculadora de reputação de pesquisa de ameaças**.

   Você pode exibir a lista de calculadoras de reputação de pesquisa de ameaças.
3. Clique na Calculadora de reputação de pesquisa de ameaças necessária para exibir os detalhes da calculadora.



Criar calculadora de reputação de pesquisa de ameaças

Função necessária: sn_sec_tisc.admin

Nota: Somente uma calculadora de pesquisa de ameaças pode estar ativa a qualquer momento por fornecedor de pesquisa de ameaças.

Para criar uma calculadora de reputação de pesquisa de ameaças, execute as seguintes etapas:

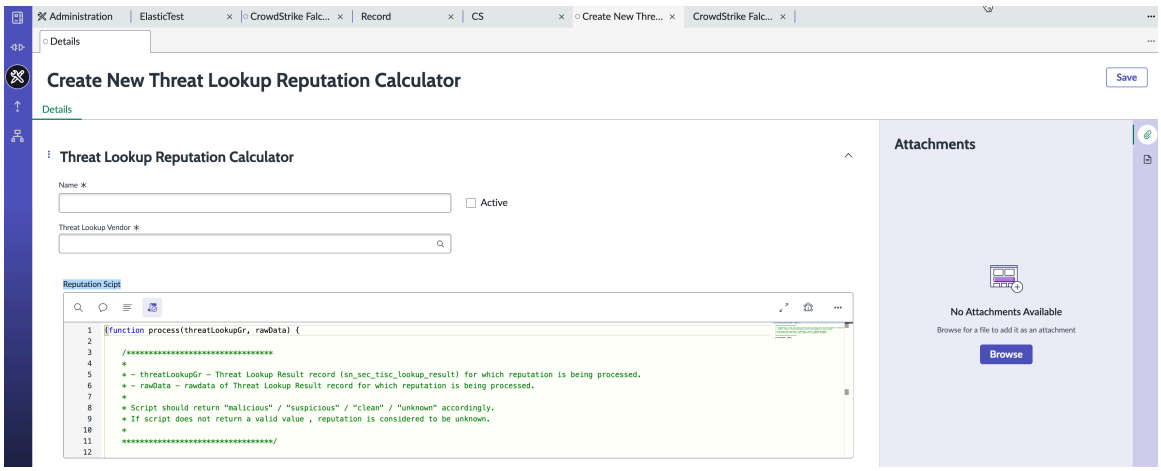
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecione a seção **Calculadora de reputação de pesquisa de ameaças**.

   Você pode exibir a lista de calculadoras de reputação de pesquisa de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Para criar uma calculadora de reputação de pesquisa de ameaças, clique em **Novo**.



4. No formulário, preencha os campos.

Criar uma calculadora de reputação de pesquisa de ameaças

Campo	Descrição
Nome	Nome da calculadora de reputação de pesquisa de ameaças.
Ativo	O cálculo de pesquisa de ameaças será executado somente se a opção Ativo estiver selecionada.
Fornecedor da pesquisa de ameaças	Nome do fornecedor da pesquisa de ameaças. Por exemplo, `CrowdStrike Falcon Intelligence`.
Script de reputação	Editor de script para determinar como você deseja identificar as várias descobertas observáveis. Cada integração de pesquisa de ameaças vem com um script base para calcular a reputação de pesquisa de ameaças.

5. Clique em **Salvar**.

Gerenciar notificações por e-mail

Use ServiceNow Notificações para criar e gerenciar notificações por e-mail do sistema e exibir logs de e-mail.

Notificações por e-mail

Use notificações por e-mail para enviar aos usuários selecionados notificações por e-mail sobre tarefas específicas na aplicação, como atualizações para observáveis/indicadores/ vários outros objetos.

Função necessária: administrador

Nota: Como administrador do sistema, você pode exibir, criar ou editar os detalhes da regra de notificação por e-mail na exibição clássica da aplicação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Central de segurança de inteligência contra ameaças fornece notificações por e-mail orientadas por regras que são enviadas para endereços de e-mail individuais ou uma lista de endereços de e-mail. Normalmente, as informações de disseminação de informações sobre ameaças para usuários internos são enviadas normalmente na forma de um e-mail. O processo envolve a entrega dos dados de inteligência contra ameaças aos usuários de acordo com o formato e as linhas do tempo especificados.

As notificações por e-mail permitem que os administradores especifiquem:

- Quando enviar a notificação
- Quem recebe a notificação
- Qual o conteúdo da notificação

Nota: Se você quiser fazer mudanças, precisará configurar para quem o e-mail deve ser enviado, modificando as regras do sistema de base com base em seus requisitos.

Para obter mais informações, consulte Criar uma notificação por e-mail na seção Administração da Now Platform da documentação.

A tabela a seguir detalha as regras de notificação por e-mail que são provisionadas no sistema de base.

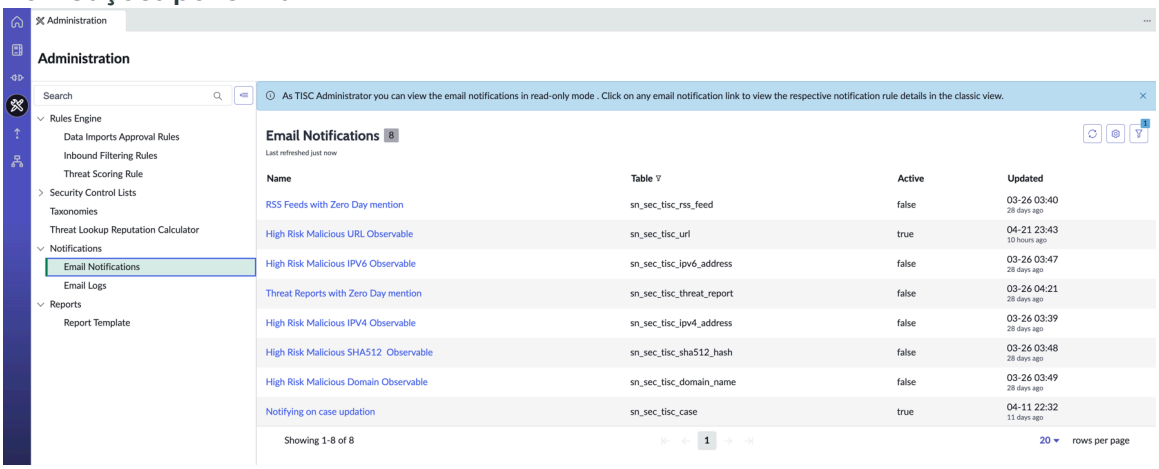
Notificações por e-mail

Nome	Tabela
Feeds RSS sem menção de dia	sn_sec_tisc_rss_feed
Observável de URL mal-intencionado de alto risco	sn_sec_tisc_url
Observável de IPV6 malicioso de alto risco	sn_sec_tisc_ipv6_address
Relatórios de ameaças com menção de dia zero	sn_sec_tisc_threat_report
Observável de IPV4 malicioso de alto risco	sn_sec_tisc_ipv4_address
Observável SHA512 malicioso de alto risco	sn_sec_tisc_sha512_hash
Observável de domínio malicioso de alto risco	sn_sec_tisc_domain_name
Notificação sobre atualização de caso	sn_sec_tisc_case

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificações por e-mail



Nota: Clicar em cada notificação por e-mail levará você para a IU clássica, para que você possa realizar as ações necessárias, como exibir, editar ou criar as notificações.

Logs de e-mail

Esta seção fornece uma visibilidade clara para os administradores de TISC sobre os e-mails que são enviados usando as regras de notificação por e-mail configuradas.

Alcance de logs e notificações por e-mail

O TISC fornece diferentes escopos para acessar, exibir ou modificar notificações por e-mail e logs com base em diferentes personas.

Nota:

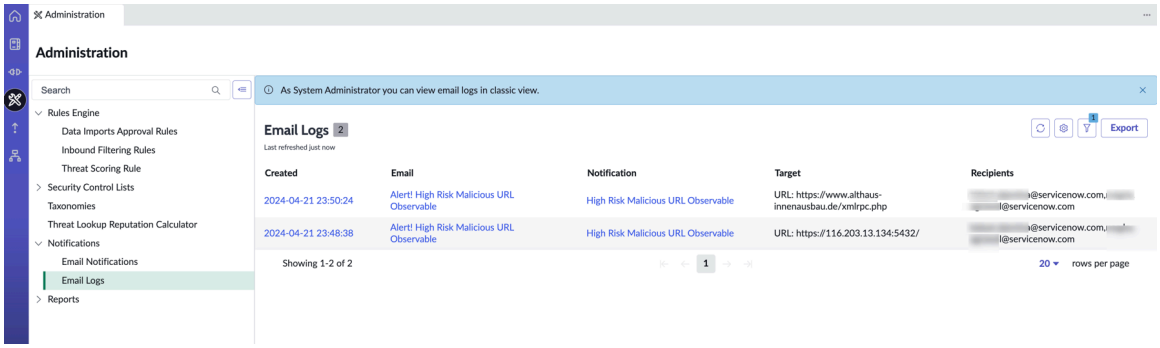
Persona	Níveis de acesso
Administrador de TISC (sn_sec_tisc.admin)	Como um sn_sec_tisc.admin, você só pode exibir as notificações por e-mail que estão configuradas para TISC. **Nota:** Clique nos hiperlinks dos logs de e-mail para navegar até a IU clássica e exibir essas notificações.
Administrador do sistema (admin)	Como administrador, você pode criar, exibir e editar as notificações na IU clássica. **Nota:** Clique nos hiperlinks de logs de e-mail para navegar até a IU clássica para exibir e criar essas notificações.

Nota: O administrador do TISC e o administrador do sistema podem usar os filtros e pesquisar os logs de e-mail.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Logs de E-mail



Modelos de relatório

Define a capacidade de reutilizar os modelos de relatório que podem ser compartilhados no grupo de usuários para gerar relatórios de forma rápida e consistente.

Use este recurso para criar diferentes tipos de modelos de relatório, que podem ser aplicados a casos que fornecem o status de investigação em andamento relevante para qualquer ameaça à sua organização e ajudam a gerar relatórios sobre o mesmo.

Esta seção explica como implementar a emissão de relatórios de CTI no nível de caso e também fornece experiências de administrador (design de modelo) e analista (tempo de execução).

Você pode adicionar campos de formulário de tarefa de caso personalizado ou listas relacionadas ao modelo de relatório que são referência com pontos. Além disso, você pode formatar e configurar o relatório com base em seus requisitos usando vários elementos de relatório.

Função necessária: sn_sec_tisc.admin

A tabela a seguir explica alguns modelos de relatório que são provisionados no sistema de base.

Modelo de relatório

Nome	Descrição
Relatório de status do caso - Perfil de agente da ameaça	O relatório foi projetado para fornecer um status sobre a investigação de caso em andamento relacionada a um agente de ameaça que tenta entender o contexto e a relevância da ameaça para a organização; comportamento adversário e objetivos em potencial; enriquecimento de IOC; Malware e ferramentas associados; TTPs observados; Diferença dos TTPs existentes – novas capacidades líquidas, pequenas modificações etc.
Resumo executivo	O relatório foi projetado para informar os tomadores de decisão sênior sobre um risco específico. O foco está no público executivo e no suporte a problemas estratégicos que explicam por que e como, em vez de o quê e quando. Todos os

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de relatório

Nome	Descrição
	detalhes técnicos e apêndices em apoio à escrita narrativa longa não serão incluídos neste relatório.
Resumo pós-investigação - Perfil do agente da ameaça	O relatório foi projetado para fornecer contexto e relevância da ameaça para a organização; comportamento adversário e objetivos em potencial; enriquecimento de IOC; Malware e ferramentas associados; TTPs observados; Diferença dos TTPs existentes – novas capacidades líquidas, pequenas modificações etc.

Nota: Por padrão, esses relatórios estão no estado publicado e no modo somente leitura. Como os modelos de relatório estarão no modo somente leitura, os usuários não poderão fazer edições nos modelos e os analistas não poderão gerar os relatórios, pois os modelos de relatório serão desabilitados.

Criar um novo modelo de relatório

Crie um novo modelo de relatório de caso de acordo com as necessidades de negócios da sua organização.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Relatórios** > **Modelo de relatório**.
   Esta seção exibe os modelos disponíveis no sistema de base e também os modelos publicados. Você pode escolher qualquer modelo desejado para trabalhar com os relatórios.

   Nota: Nesta seção, você também pode excluir os modelos, se necessário.

3. Clique em **Nova**.
4. Insira o nome e a descrição do modelo.
5. Clique em **Salvar**.
   A seção Conteúdo do modelo é exibida.

   Nota: Sempre que você criar um novo modelo de relatório, o modelo estará no estado de rascunho, o que significa que a criação do modelo está em andamento e qualquer outro usuário não poderá exibir o modelo de relatório até que ele seja concluído.

6. Expanda o **conteúdo do modelo** para inserir os campos desejados no corpo do modelo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- O modelo que você está editando permite definir o corpo do modelo e selecionar as variáveis necessárias para adicionar à seção do editor de modelos. Os modelos são compatíveis com o editor de Rich Text (RTE) para que você possa controlar várias funções disponíveis, como recuo, tamanho da fonte, criação de tabelas, adição de imagens e vários outros recursos de formatação.
- Você também pode inserir imagens em seus modelos de relatório. Para isso, você precisa copiar e colar a imagem diretamente no modelo. Ao adicionar uma imagem, essa imagem é carregada como um anexo.
- Você pode carregar ou anexar uma imagem de até 698 pixels. Se a imagem estiver acima do tamanho definido, ela será ajustada automaticamente para o tamanho original. Essa restrição de tamanho de pixel ajudará a geração do relatório em PDF a ser exibida em um formato adequado e as imagens não serão truncadas no relatório.

7. Adicione os elementos necessários do caso.
8. Clique em **Salvar conteúdo** para salvar o conteúdo do novo modelo de relatório.
9. Clique em **Visualizar** para visualizar o formato do relatório e também para ver como um relatório é gerado quando você gera qualquer relatório de caso.

Nota:

- **Campos de caso**: sempre que você modificar o(s) modelo(s) de relatório, visualize o conteúdo adicionado ao modelo. Por exemplo, quando você está gerando um relatório de caso e deseja adicionar um campo chamado Descrição resumida, é possível selecionar esse campo nos campos de caso e, em seguida, esse campo é adicionado como uma variável no modelo de relatório. Quando um relatório é gerado para o analista, qualquer que seja a descrição resumida do caso, essa descrição será exibida no relatório.
- **Registros**: no modelo de relatório, você também pode adicionar os registros relacionados desse caso específico que são exibidos como artefatos do caso. Por exemplo, se você quiser ver quaisquer observáveis maliciosos no relatório das listas relacionadas a observáveis, poderá adicioná-los ao seu modelo de relatório. Esses registros relacionados são exibidos no formato de tabela
- **Scripts**: sempre que você quiser ver a data e a hora do relatório, poderá adicionar os scripts de data e hora **atuais** ao modelo de relatório e isso adicionará a data e a hora de criação do relatório.
- **MITRE ATT&CK**: exibe as técnicas associadas ao cartão MITRE no seu relatório.

Depois de adicionar todos os campos necessários relacionados ao caso ao modelo de relatório, você precisa publicar o modelo de relatório.

10. Clique em **Publicar** para publicar o modelo.
Uma mensagem de confirmação será exibida se você quiser publicar o modelo de relatório.

Nota: Quando você publica um modelo de relatório, esse modelo é habilitado para todos os usuários. Caso ele esteja desatualizado e você queira restringir a exibição do relatório para os usuários, poderá desabilitar o relatório publicado, o que significa que o modelo de relatório ficará oculto para os usuários. Você precisa habilitar novamente o relatório publicado para os usuários verem e usá-lo até então, ele ficará oculto para exibição.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Clique em **Excluir** para excluir o modelo de relatório caso você não queira esse modelo de relatório.
    Se você quiser renomear seu modelo de relatório, clique em **Editar** e modifique os campos desejados.

Propriedades do sistema para relatórios

As propriedades do sistema para relatórios são explicadas abaixo.

Propriedade	Descrição	Valor
sn_sec_reporting.max_list_columns_allowed	Limite o número de colunas que podem ser adicionadas ao renderizar listas em PDFs de relatório. Isso usará as colunas desde o início da exibição até o limite permitido.	5
sn_sec_reporting.report_default_style_object	Use esta propriedade para controlar o CSS de campos de formulário livre, painel esquerdo, listas de relatório.	(objeto JSON)
sn_sec_reporting.load_all_records	Carrega todos os registros das listas no relatório criado a partir de um modelo. "verdadeiro" carrega todos os registros e "falso" carrega o número específico de registros definidos pela propriedade sn_sec_reporting.reporting_list_records_count.	Falso
sn_sec_reporting.reporting_list_records_count	Carrega um número específico de registros no editor de relatórios.	20
sn_sec_tisc.sn_sec_tisc_case.default_sort_order	Controla se os URLs das listas serão violados ou não.	Verdadeiro
sn_sec_tisc.show_all_tactics_reporting	Se verdadeiro, mostrará todas as táticas (incluindo aquelas sem técnicas associadas ao caso) para as listas do MITRE renderizadas no relatório.	Falso
sn_sec_tisc.reporting_email_template	Define o modelo de e-mail para a tabela Caso (sn_sec_tisc_case) que será usada no relatório de compartilhamento.	SYS ID do modelo de e-mail b55e22c54324021060eee0ea78b8f2df
sn_sec_tisc.sn_sec_tisc_case.excluded_fields	Campos excluídos do caso nas opções do menu de relatório/modelo para substituir um campo.	(Lista de todos os campos de caso excluídos

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	Esta propriedade é usada para obter o registro de mensagem de IU correspondente para o rótulo de campos de caso nas opções de menu de relatório/modelo.	sn_sec_tisc_case_reporting_ctx_menu_field_h

Editar um modelo de relatório publicado

Edite os modelos de relatório.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > > **Administração**.
2. Selecionar **Relatórios** > **Modelo de relatório**.
3. Selecione o modelo de relatório necessário.
4. Clique no botão **Editar** que é exibido no modelo de relatório.

Nota:

Uma mensagem de confirmação exibe que, Você está editando um modelo publicado e deve republicá-lo para disponibilizá-lo em Relatórios de caso. Deseja continuar editando? o que significa que você precisa republicar o modelo editado depois de fazer as mudanças necessárias.

5. Clique em **Editar** na caixa de diálogo de confirmação.
6. Faça as mudanças necessárias adicionando os campos de conteúdo obrigatórios ou a lista relacionada.
7. Clique **em Salvar conteúdo**.
8. Clique no botão **Publicar** para publicar as mudanças.

Nota:

a. Você também pode visualizar o conteúdo do modelo de relatório antes de publicá-lo.

b. Uma mensagem de confirmação exibe que, Tem certeza de que deseja publicar este modelo? Clique em **Publicar** para continuar publicando o modelo de relatório.

c. Caso você queira excluir o modelo de relatório, clique em **Excluir** para excluir o modelo de relatório.

Duplicar um modelo de relatório

Duplique um modelo de relatório se quiser adicionar atualizações incrementais. Em seguida, você poderá criar uma cópia do modelo de relatório.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > > **Administração**.
2. Selecionar **Relatórios** > **Modelo de relatório**.
3. Selecione o modelo.
4. Clique em **Duplicar**.
   O conteúdo do modelo selecionado está duplicado e a cópia desse modelo é exibida. O modelo estará novamente no estado Rascunho. Você pode personalizar o conteúdo e renomear o modelo conforme necessário.
5. Edite ou modifique o conteúdo do modelo copiado.

Nota: Você também pode excluir os modelos de relatório caso não precise mais deles e criar novos modelos.

Trabalhando com Webhooks

Um webhook é uma solicitação HTTP, acionada por um evento no sistema de origem (TISC) e enviada para um sistema de destino (onde a URL do endpoint está presente), com uma carga de dados de eventos.

Esses webhooks em Central de segurança de inteligência contra ameaças são úteis para notificar a aplicação de destino sempre que ocorrerem os eventos.

No TISC, você pode fazer o seguinte:

- Configurar Webhooks
- Gerenciar gatilhos
- Mecanismo de nova tentativa
- Executar validação
- Gerenciar assinaturas

Propriedades do sistema para Webhooks

As propriedades do sistema para webhooks são explicadas abaixo.

Nome da Propriedade	Descrição	Tipo	Valor
sn_sec_tisc.webhook_ignore_threat_score_recalculation	Ignorar eventos de webhook acionados pelo histórico de recálculo de pontuação de ameaça.	Verdadeiro/Falso	Verdadeiro
sn_sec_tisc.webhook_max_batch_size	Número máximo de eventos a serem enviados como parte de uma solicitação de webhook. O tamanho do lote será limitado a 2000, mesmo se um valor	Inteiro	1000

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição	Tipo	Valor
	maior for definido nesta propriedade.		
sn_sec_tisc.webhook_retry_count	Número de vezes que uma solicitação com falha deve ser repetida antes de marcá-la como erro e passar para o próximo lote de eventos. A contagem de novas tentativas será limitada a 10, mesmo se um número maior estiver definido nesta propriedade.	Inteiro	5
sn_sec_tisc.webhook_retry_interval	Número de segundos de espera antes de tentar novamente um lote com falha. Isso aumentará exponencialmente com base na contagem de novas tentativas. Por exemplo, se retry_count for 3 e retry_interval for 30, as novas tentativas serão disparadas após 30, 60 e 120s. O intervalo de repetição inicial será limitado a 300 segundos, mesmo se um valor maior estiver definido nesta propriedade.	Inteiro	30

Tradução automática

Configurar webhooks

Configure um webhook para assinar eventos na Central de segurança de inteligência contra ameaças.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa

Os webhooks do TISC fornecem a capacidade de integração com ferramentas de segurança, como SIEM. Os usuários podem assinar vários eventos relacionados a diferentes artefatos, como observáveis, indicadores, malware ou agentes de ameaça. O TISC notifica as ferramentas de segurança (como o SIEM) quando uma nova inteligência contra

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ameaças está disponível ou quando quaisquer dados de inteligência contra ameaças existentes são atualizados ou excluídos no TISC.

Por exemplo, sempre que um novo observável é adicionado à inteligência contra ameaças, uma solicitação de carga é enviada para a configuração de URL do webhook. Essa solicitação de carga geralmente coleta as informações do observável e as fornece como informações adicionais para as ferramentas de segurança (como o SIEM).

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de Webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Clique em **Nova**.

Campo	Descrição
Nome	Insira um nome de webhook.
Descrição	Adicione a descrição do webhook.
Detalhes da Configuração	
Usar Mensagem REST	Marque a caixa de seleção **Usar Mensagem REST** se precisar usar a funcionalidade de Mensagem REST/Método REST fornecida pela Now Platform. Se esta caixa de seleção não estiver marcada, a aplicação usará o endpoint fornecido na URL do Webhook para enviar as informações do evento. Para obter mais informações, consulte Serviço web REST de saída na documentação da Now Platform.
Mensagem REST	Selecione o registro de Mensagem REST na lista de registros de mensagens REST que já estão configurados na instância. Para obter mais informações, consulte Serviço web REST de saída na documentação da Now Platform. **Nota:** Os campos Mensagem REST e Método REST são obrigatórios ao selecionar a mensagem REST.
Método REST	Selecione Método REST na lista de Métodos REST disponíveis configurados para a Mensagem REST selecionada. Para obter mais informações, consulte Serviço web REST de saída na documentação da Now Platform.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Somente métodos POST REST são compatíveis com webhooks.
URL do webhook	Um endpoint de webhook é um URL que recebe notificações de eventos de webhook.
Autenticação Necessária	Marque esta caixa de seleção se a autenticação for necessária. **Nota:** Isso só se aplica quando a URL do Webhook está sendo usada para recuperar os dados.
Tipo de autenticação	O tipo de autenticação do webhook. **Nota:** A partir de agora, somente o tipo de autenticação Básica é compatível.
Nome de usuário	Forneça um nome de usuário para o tipo de autenticação.
Senha	Forneça uma senha para o tipo de autenticação.
Cabeçalhos a serem passados com a solicitação	Todos os cabeçalhos a serem passados com as solicitações podem ser fornecidos em Mapeamento de cabeçalho de solicitação. O cabeçalho deve ser fornecido em par de chave-valor separado por dois pontos (':'). Cada par de valores de chave de cabeçalho deve ser fornecido em uma nova linha. Para fornecer parâmetros de autenticação como valores de cabeçalho, coloque o rótulo de autenticação necessário entre '${' e '}$'. Por exemplo, nome de usuário:${Nome de usuário}$.

Tradução automática

4. Clique **em Validar e Salvar**.
   Caso os detalhes da configuração estejam incorretos, o sistema validará automaticamente a conexão se os detalhes da configuração forem alterados e, em seguida, a aplicação exibirá uma mensagem de aviso informando que a validação do webhook falhou e você precisa verificar os detalhes da configuração e modificá-los adequadamente .

Nota:

- Para a validação do webhook, a carga de solicitação vazia é enviada para o endpoint e o usuário precisa garantir que o endpoint envie o código de resposta bem-sucedido (200) quando a solicitação vazia for passada para o endpoint do webhook configurado.
- Por padrão, qualquer webhook criado estará no estado desabilitado. Você precisa habilitar o webhook e ativá-lo. Um webhook de amostra é provisionado no sistema de base como uma referência para os usuários.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gatilhos de assinatura

Exibir a lista de todos os gatilhos de webhook inscritos para o webhook atual.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de Webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Selecione o webhook.
   A seção Gatilhos inscritos é exibida.
4. Clique no botão **Assinar** na seção Gatilho inscrito.
   A exibição de lista mostra todos os gatilhos de webhook habilitados na instância.
5. Selecione os gatilhos de webhook desejados e clique em **Assinar** na caixa de diálogo Gatilhos de webhook.
   Uma mensagem de confirmação é exibida informando que o webhook foi inscrito com sucesso nos gatilhos selecionados. A partir daqui, você também pode criar diretamente um novo gatilho e assinar o webhook.

   Nota: Você também pode **cancelar** a assinatura do webhook dos gatilhos selecionados.

Exibir logs de erro do webhook

Use esta seção de logs de erro para exibir todas as entradas de auditoria marcadas como erro no status de um webhook específico.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Por Que e Quando Desempenhar Esta Tarefa
Os logs de auditoria permitem que os usuários investiguem, depurem a execução e identifiquem a causa raiz da falha de execução.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de Webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Selecione o webhook.
4. Vá para **Logs de erro**.
5. Exiba os logs de erro.
   A exibição de lista mostra todos os logs de erro de um webhook específico.
6. Vá para a coluna **Lote**.
7. Clique em qualquer **ID de lote**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Cada log de erro está associado a um lote e, usando o ID do lote (da coluna Lote), você pode exibir o registro de lote associado. Clique em qualquer ID de lote e isso será aberto em uma guia separada. Cada ID de lote contém o número de lote do webhook, a mensagem de erro, o código de status da resposta, a contagem de novas tentativas, os dados de carga real e a lista de eventos que serão enviados para o webhook.

8. Clique **em Repetir lote** para tentar novamente os lotes com falha.
   Quando você clica neste botão, uma carga de solicitação é enviada (desses dados de lote específicos) para o endpoint do webhook configurado.

Nota: Esta ação está disponível somente para os registros em lote que têm erros de execução ou foram concluídos com sucesso e os registros que estão no estado de nova tentativa serão repetidos automaticamente.

Exibir lotes de webhook

Um registro em lote de webhook é criado para cada execução de webhook.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para reduzir o número de chamadas de API enviadas para os endpoints do webhook, o envio em lote de eventos é implementado nos webhooks. Para cada webhook, se houver vários eventos acionados quase ao mesmo tempo, todos esses eventos serão enviados como parte da mesma solicitação para o endpoint do webhook.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de Webhooks** > **Webhooks**.
   A página Webhooks é exibida.
3. Selecione o webhook.
4. Vá para **Logs de erro**.
5. Exiba os logs de erro.
   A exibição de lista mostra todos os logs de erro de um webhook específico.
6. Vá para a coluna **Lote**.
7. Clique em qualquer **ID de lote**.
   A página Batch do Webhook é exibida.

Nota: Todos os lotes são armazenados na tabela `sn_sec_tisc_webhook_batch`.

Abaixo está o exemplo de formato de carga que o endpoint do webhook recebe:

```
{
    "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
    "events": [
        {
            "record": "Observable",
            "record_fields": {
                "is_false_positive": "false",
                "reputation": "malicious",
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
                "sys_updated_on": "2024-07-22T14:31:26.000Z",
                "type": "url",
                "sys_updated_by": "admin",
                "sys_created_on": "2024-07-04T06:45:20.000Z",
                "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
                "is_defanged": "false",
                "sys_created_by": "SecCommon.System",
                "tags": "Enriched",
                "taxonomies": "T1: V1",
                "domain": "urlhaus.abuse.ch",
                "status": "active",
                "source_count": "1",
                "threat_score": "20",
                "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
                "value": "https://urlhaus.abuse.ch/url/2578255/",
                "confidence": "89",
                "expiration_time": "2025-10-07T07:13:18.000Z",
                "tlp": "CLEAR"
            },
            "trigger": {
                "name": "Observable Update",
                "type": "UPDATE",
                "trigger_time": "2024-07-22T14:31:26.000Z",
                "trigger_fields": [
                    {
                        "field_name": "reputation",
                        "previous_value": null,
                        "current_value": "malicious"
                    }
                ]
            }
        },
        {
            "record": "Observable",
            "record_fields": {
                "is_false_positive": "false",
                "reputation": "malicious",
                "sys_updated_on": "2024-07-22T14:31:19.000Z",
                "type": "url",
                "sys_updated_by": "admin",
                "sys_created_on": "2024-07-04T06:45:20.000Z",
                "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
                "is_defanged": "false",
                "sys_created_by": "SecCommon.System",
                "tags": "Enriched",
                "taxonomies": "T1: V1",
                "domain": "urlhaus.abuse.ch",
                "status": "active",
                "source_count": "1",
                "threat_score": "20",
                "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
                "value": "https://urlhaus.abuse.ch/url/2578264/",
                "confidence": "89",
                "expiration_time": "2025-10-07T07:13:18.000Z",
                "tlp": "CLEAR"
            },
            "trigger": {
```


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
                "name": "Observable Update",
                "type": "UPDATE",
                "trigger_time": "2024-07-22T14:31:19.000Z",
                "trigger_fields": [
                    {
                        "field_name": "reputation",
                        "previous_value": null,
                        "current_value": "malicious"
                    }
                ]
            }
        }
    ]
}
```


A tabela a seguir lista a estrutura de carga em lote e seus atributos que serão enviados aos usuários como carga de webhook:

Parâmetros na carga em lote	Tipo	Descrição
batch_id	Cadeia de caracteres	Especifica o identificador exclusivo de um lote.
eventos	Matriz de objetivos	Contém uma matriz de eventos que são acionados como parte desse webhook. Cada evento conterá o snapshot dos valores de campo no momento da geração do evento e também conterá as informações do gatilho. **Nota:** Para obter mais informações sobre como exibir os parâmetros no objeto de evento, consulte Gatilhos de webhook.

Nota:

8. Clique no botão **Repetir lote** para tentar novamente o lote com falha.

Nota: Você também pode acionar o lote de nova tentativa para os lotes concluídos.

Gatilhos de webhook

Os gatilhos de webhook são usados para filtrar as entidades de inteligência contra ameaças que precisam ser rastreadas para quaisquer mudanças de evento, como Criar, Atualizar e Excluir.

Antes de Iniciar
Função necessária: sn_sec_tisc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Configurações de Webhooks** > **Gatilhos**.
   A página Gatilhos de Webhooks é exibida.
3. Clique em **Nova**.

Campo	Descrição
Nome	Insira um nome de gatilho de webhook.
Descrição	Adicione a descrição do gatilho do webhook.
Tabela	Selecione a tabela para o gatilho do webhook.
Tipo de gatilho	Define se o gatilho de webhook configurado é um evento de criação/atualização/exclusão na tabela especificada. **Campos de gatilho**: isso é exibido quando você seleciona o **Tipo de gatilho: Atualizar**. Esta é a lista de campos no registro para o qual o evento de atualização precisa ser rastreado. Se estiver vazio, o evento será considerado para qualquer mudança de campo no registro. Por exemplo, se os campos de gatilho forem **Confiança** e **Reputação** para a tabela **Observáveis**, esse gatilho será considerado somente quando os campos de confiança ou reputação forem atualizados. **Nota:** Os campos selecionados nos Campos de exclusão não estarão disponíveis na seleção de Campos de gatilho. **Excluir**: se o **Tipo de gatilho: Excluir**, os Campos de exclusão não ficarão visíveis.
Campos de exclusão	Este é o conjunto de campos que são excluídos da carga do gatilho do webhook.
Condições do filtro	Condições opcionais que podem ser aplicadas para filtrar os registros de correspondência de qualquer gatilho de evento. Por exemplo, se a gravidade da ameaça for alta e o tipo de gatilho estiver definido como Atualizar na tabela do observável, somente os observáveis que foram alterados e em que a gravidade da ameaça é alta serão enviados para a URL do webhook.

4. Clique em **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, o gatilho é criado no estado desabilitado.

5. Clique em **Habilitar** para habilitar o gatilho e este gatilho estará disponível para os webhooks assinarem.

   Nota: Clique em **Desabilitar** para desabilitar o gatilho habilitado e desabilitar cancelará a assinatura de todos os webhooks associados deste gatilho.

6. Clique em **Exibir carga de amostra** para selecionar o registro.
   Exiba a carga de amostra desse gatilho de webhook específico. Com base na tabela selecionada, os registros dessa tabela especificada serão preenchidos na lista suspensa **Selecionar registro**. Selecione o registro para exibir a carga de amostra. A carga de amostra é mostrada no formato JSON. Os campos na carga estão listados abaixo.

7. Selecione o tipo de registro na lista suspensa.
   A carga útil será alterada automaticamente com base no registro selecionado.


```
{
    "record": "Observable",
    "record_fields": {
        "additional_context": "This could be a potential malicious IP.
 ",
        "attack_phases": "Lockheed Martin: Command and Control",
        "author": "Anomali",
        "confidence": "50",
        "description": "This could be a potential malicious IP. ",
        "expiration_time": "2024-12-01T00:00:00.000Z",
        "first_observed": "2024-01-01T00:00:00.000Z",
        "first_seen": "2024-01-01T00:00:00.000Z",
        "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
        "is_defanged": "false",
        "is_false_positive": "false",
        "last_observed": "2024-01-01T00:00:00.000Z",
        "last_seen": "2024-01-01T00:00:00.000Z",
        "reputation": "suspicious",
        "source_count": "1",
        "status": "active",
        "sys_created_by": "SecCommon.System",
        "sys_created_on": "2024-06-04T00:00:00.000Z",
        "sys_id": "30526b0a436a02102164e0ea78b8f210",
        "sys_updated_by": "system",
        "sys_updated_on": "2024-06-15T00:00:00.000Z",
        "tags": "critical",
        "taxonomies": "MITRE: T121",
        "threat_level": "medium",
        "threat_score": "24",
        "threat_severity": "medium",
        "tlp": "CLEAR",
        "type": "ip_v4_address",
        "usage_categories": "APT",
        "value": "116.98.170.70"
    },
    "trigger": {
        "name": "Observable Update",
        "type": "UPDATE",
        "trigger_time": "2024-07-26T07:27:29.000Z",
        "trigger_fields": [
            {
```


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
                "field_name": "confidence",
                "previous_value": "30",
                "current_value": "50"
            }
        ]
    }
}
```

Lista de parâmetros na carga do gatilho

Parâmetro na carga do gatilho	Tipo	Descrição
registro	Cadeia de caracteres	Especifica o tipo de registro, como Observável ou Indicador.
registros_campos	Objeto	Especifica o snapshot dos campos de registro quando o evento é gerado. Para obter a lista de campos compatíveis, consulte a tabela na seção abaixo.
gatilho	Objeto	Especifica as informações do gatilho correspondente.
trigger.name	Cadeia de caracteres	Especifica o nome do gatilho
gatilho.tipo	Cadeia de caracteres	Especifica o tipo do gatilho. Os valores válidos são CRIAR, ATUALIZAR, EXCLUIR.
gatilho.tempo_gatilho	Data (no formato ISO com fuso horário UTC)	Especifica a hora em que o evento ocorreu no registro.
campos_gatilho	Matriz de objetivos	Disponível somente para o tipo de gatilho UPDATE. Ele especifica a lista de campos de gatilho que foram alterados como parte da ocorrência do evento. Os parâmetros dentro **de trigger_fields** são: ◦ **field_name**: fornece o nome do campo que foi alterado ◦ **opened_value**: fornece o valor anterior do campo. ◦ **current_value**: fornece o valor atual do campo.

Lista de campos compatíveis para criar e atualizar gatilhos

Tabela	Nome da Coluna	Rótulo da Coluna
Campanha	aliases	Aliases
Campanha	descrição	Descrição

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Campanha	first_seen	Visto pela primeira vez
Campanha	last_seen	Visto pela última vez
Campanha	nome	Nome
Campanha	objetivo	Objetivo
Indicador	adicional_context	Contexto adicional
Indicador	fases_ataque	Fases de ataque
Indicador	autor	Autor
Indicador	confiança	Confiança
Indicador	descrição	Descrição
Indicador	expiração_hora	Tempo de expiração
Indicador	first_detected	Detectado pela primeira vez
Indicador	first_observed	Observado pela primeira vez
Indicador	first_seen	Visto pela primeira vez
Indicador	ID	ID
Indicador	tipos_de_indicadores	Tipos de Indicador
Indicador	ioc_classification	Classificação IOC
Indicador	last_observed	Última observação
Indicador	last_seen	Visto pela última vez
Indicador	nome	Nome
Indicador	padrão	Padrão
Indicador	padrão_tipo	Tipo de padrão
Indicador	padrão_versão	Versão do padrão
Indicador	plataformas	Plataformas
Indicador	revogado	Revogado
Indicador	source_count	Nº de origens
Indicador	especificação_versão	Versão de especificação
Indicador	status	Status
Indicador	marcadores	Marcadores de TISC
Indicador	taxonomias	Taxonomias
Indicador	nível_de_ameaça	Nível de ameaça
Indicador	ameaça_severidade	Gravidade da ameaça
Indicador	TLP	TLP
Indicador	uso_categorias	Categorias de uso
Indicador	valid_from	Válido de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Indicador	válido_até	Válido Até
Malware	aliases	Aliases
Malware	fases_ataque	Fases de ataque
Malware	descrição	Descrição
Malware	executable_process_architectures	Arquiteturas de processo
Malware	first_seen	Visto pela primeira vez
Malware	implementação_idiomas	Idiomas de implementação
Malware	é_família	É família
Malware	last_seen	Visto pela última vez
Malware	malware_capacidades	Capacidades do malware
Malware	tipos_de_malware	Tipos de malware
Malware	nome	Nome
Objeto (campos de objeto comum)	adicional_context	Contexto adicional
Objeto (campos de objeto comum)	confiança	Confiança
Objeto (campos de objeto comum)	expiração_hora	Tempo de expiração
Objeto (campos de objeto comum)	ID	ID
Objeto (campos de objeto comum)	revogado	Revogado
Objeto (campos de objeto comum)	source_count	Nº de origens
Objeto (campos de objeto comum)	especificação_versão	Versão de especificação
Objeto (campos de objeto comum)	status	Status
Objeto (campos de objeto comum)	marcadores	Marcadores de TISC
Objeto (campos de objeto comum)	taxonomias	Taxonomias
Objeto (campos de objeto comum)	nível_de_ameaça	Nível de ameaça
Objeto (campos de objeto comum)	ameaça_severidade	Gravidade da ameaça
Objeto (campos de objeto comum)	TLP	TLP
Observável	adicional_context	Contexto adicional
Observável	fases_ataque	Fases de ataque

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Observável	autor	Autor
Observável	confiança	Confiança
Observável	descrição	Descrição
Observável	expiração_hora	Tempo de expiração
Observável	first_observed	Observado pela primeira vez
Observável	first_seen	Visto pela primeira vez
Observável	ID	ID
Observável	está_deformado	Está danificado
Observável	é_falso_positivo	É falso-positivo
Observável	last_observed	Última observação
Observável	last_seen	Visto pela última vez
Observável	reputação	Reputação
Observável	source_count	Nº de origens
Observável	status	Status
Observável	marcadores	Marcadores de TISC
Observável	taxonomias	Taxonomias
Observável	nível_de_ameaça	Nível de ameaça
Observável	pontuação_ameaça	Pontuação de ameaça
Observável	ameaça_severidade	Gravidade da ameaça
Observável	TLP	TLP
Observável	tipo	Tipo
Observável	uso_categorias	Categorias de uso
Observável	valor	Valor
Agente da ameaça	aliases	Aliases
Agente da ameaça	descrição	Descrição
Agente da ameaça	first_seen	Visto pela primeira vez
Agente da ameaça	objetivos	Objetivos
Agente da ameaça	last_seen	Visto pela última vez
Agente da ameaça	nome	Nome
Agente da ameaça	motivações_pessoais	Motivações pessoais
Agente da ameaça	motivação_primária	Motivação primária
Agente da ameaça	resource_level	Nível de recurso
Agente da ameaça	motivações_secundárias	Motivações secundárias
Agente da ameaça	sofisticação	Sofisticação

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Agente da ameaça	Ameaça_ator_roles	Funções de agente da ameaça
Agente da ameaça	ameaça_actor_types	Tipos de Agente da Ameaça
Relatório de ameaças	descrição	Descrição
Relatório de ameaças	nome	Nome
Relatório de ameaças	publicado	Publicado
Relatório de ameaças	tipos_de_relatórios	Tipos de relatório
Vulnerabilidade	software_afetado	Software afetado
Vulnerabilidade	descrição	Descrição
Vulnerabilidade	exploração_status	Status de exploração
Vulnerabilidade	exploit_exist	Explorar Itens Existentes
Vulnerabilidade	nome	Nome
Vulnerabilidade	publicado	Publicado
Vulnerabilidade	registro_último_modificado	Última modificação do registro
Vulnerabilidade	severidade	Gravidade

Abaixo está a lista de campos do sistema aplicáveis que são comuns a todas as entidades e são compatíveis com a Carga do gatilho do Webhook para gatilhos de criação e atualização.

- sys_id (SYS ID)
- sys_created_on (Criado)
- sys_created_by (Criado por)
- sys_updated_on (Atualizado)
- sys_updated_by (Atualizado por)

Nota: Para Excluir, somente sys_id (SYS ID) é enviado para a URL do endpoint do webhook como parte da carga útil e outros campos do sistema não são compatíveis.

Lista de campos compatíveis com o gatilho Excluir

Tabela	Nome da Coluna	Rótulo da Coluna
Observável	tipo	Tipo
Observável	valor	Valor
Indicador	nome	Nome
Indicador	padrão	Padrão
Indicador	padrão_tipo	Tipo de padrão
Indicador	valid_from	Válido de
Campanha	nome	Nome

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Nome da Coluna	Rótulo da Coluna
Malware	é_família	É família
Malware	nome	Nome
Agente da ameaça	nome	Nome
Relatório de ameaças	nome	Nome
Relatório de ameaças	publicado	Publicado
Vulnerabilidade	nome	Nome
Vulnerabilidade	severidade	Gravidade

Como trabalhar com fluxos automatizados

Use estas etapas definidas para saber como você pode usar os fluxos automatizados no TISC e seus recursos.

Crie fluxos que são executados com funções de TISC. No TISC, os fluxos são criados para o seguinte:

- Aprimoramento automatizado de IOC
- Analisar, avaliar e disseminar nos IoCs relacionados à ameaça
- Analise, avalie os IoCs relacionados à ameaça e crie um incidente.
- Suporte à gestão de vulnerabilidades.
- Acompanhamento de vulnerabilidades de dia zero.

Nota: Todos os fluxos são modelos enviados no estado de rascunho para que os usuários personalizem ou copiem de acordo com suas próprias necessidades.

Ações reutilizáveis

Ação de fluxo	Descrição
Adicionar marcador à entidade	Adicionar marcador a uma entidade que o suporta (observável/indicador/objeto).
Remover marcador da entidade	Removendo marcador para uma entidade que o suporta (observável/indicador/objeto).
Verificar se o endereço IP está no intervalo CIDR	Verificando se um endereço IP está dentro de um intervalo CIDR.
Verificar se o endereço IP está no intervalo	Verificando se um endereço IP está entre os intervalos de e para.

Aprimoramento automatizado de IOC

Saiba como automatizar o enriquecimento de IOCs usando fluxos quando eles corresponderem a um determinado critério.

Antes de Iniciar
Função necessária:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Automatizar o enriquecimento de gatilhos de IOC somente quando:

- o tipo do observável é um nome de domínio, endereço IPv4 ou endereço IPv6.
- o observável está em um estado processado.
- o observável não tem os marcadores aprimorados ou Ignorar aprimoramento.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos Automatizados**.
3. Selecione o link de ação **Aprimoramento de IOC automatizado** para exibir os detalhes da regra respectiva no Flow Designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

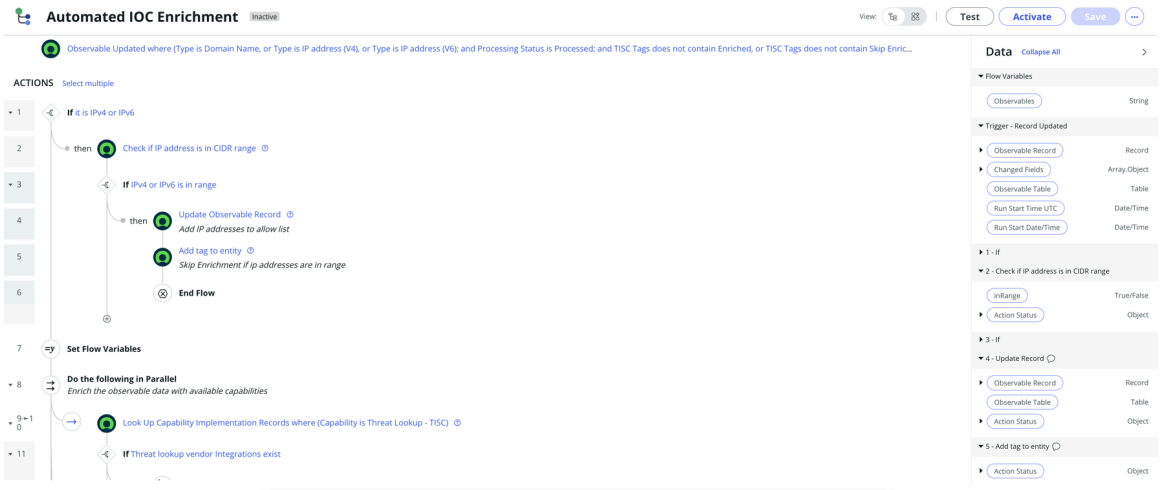
```
Observable Updated where (Type is Domain Name, or Type is IP address
 (V4), or Type is IP address (V6); and Processing Status is Processed;
 and TISC Tags does not contain Enriched, or TISC Tags does not contain
 Skip Enrichment, or TISC Tags does not contain Potential New Threat)
```

5. **Se o observável for um endereço IPv4 ou IPv6 e estiver dentro de um intervalo CIDR permitido:**
   a. Adicione o observável à lista de permissões.
   b. Atualize os marcadores de observáveis para Ignorar aprimoramento.
   c. Encerre o fluxo para este observável.
6. **Caso contrário, aprimore os dados do observável com os recursos disponíveis:**
   a. Execute pesquisa de ameaças e pesquisa de detecções para coletar informações adicionais sobre o observável.
   b. Atualize o observável com dados aprimorados.
   c. Adicione um marcador **Aprimorado** para indicar que o IOC foi processado.
7. **Além disso, se a reputação dos observáveis estiver limpa, então:**
   a. Marque o observável como falso-positivo e inativo.
8. **Else, se a reputação do observável for desconhecida**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Adicione o marcador **Não ameaça potencial e aprimorado** para indicar que não é uma ameaça.



Analisar, avaliar e disseminar observáveis

Aprenda a analisar e disseminar observáveis que estão relacionados à ameaça.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Sempre que um aprimoramento de pesquisa de detecções é solicitado, ele retorna sem detecções.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos Automatizados**.
3. Selecione **Analisar, avaliar e disseminar nos IoCs relacionados ao link de ação de ameaça** para exibir os respectivos detalhes da regra no Flow Designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

```
Sighting Created where (Sighting count is 0)
```

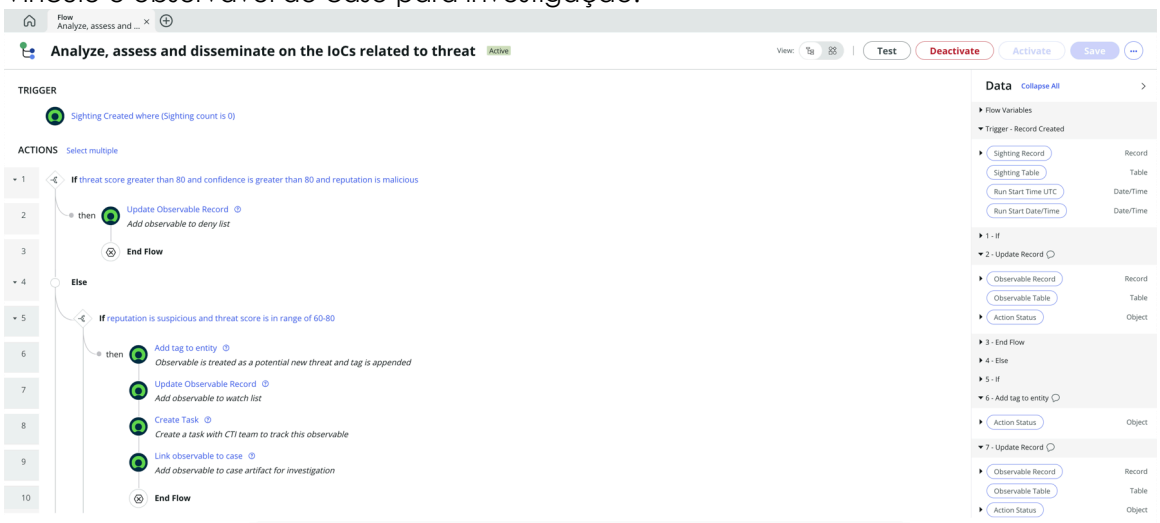
5. **O observável tem uma pontuação de ameaça maior que 80, confiança maior que 80 e reputação é mal-intencionada:**
   a. Adicione o observável à lista de proibições.
   b. Encerre o fluxo para este observável.
6. **Do contrário, a reputação do observável é suspeita e a pontuação da ameaça está no intervalo de 60 a 80:**
   a. Adicione um marcador chamado Possível nova ameaça.
   b. Adicione o observável à lista de observação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Crie uma tarefa de caso com a equipe de CTI para rastrear este observável e analisar melhor.

d. Vincule o observável ao caso para investigação.



Analisar e avaliar IoCs de ameaças

Aprenda a analisar IOCs que são uma ameaça e notificar a equipe de incidentes de segurança.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Sempre que um aprimoramento da pesquisa de detecções for solicitado:

- se o observável for avistado (contagem > 0) e
- A reputação do observável é mal-intencionada e
- A pontuação de ameaça do observável é > 80 e
- Confiança do observável > 80

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos Automatizados**.
3. Selecione **Analisar, avalie os IoCs relacionados à ameaça e crie o link de ação de incidente** para exibir os respectivos detalhes da regra no Flow Designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

```
Sighting Created where (Sighting count greater than 0, and Observable.
 Reputation is Malicious, and Observable. Threat Score greater than 80,
 and Observable. Confidence greater than 80)
```

Tradução automática

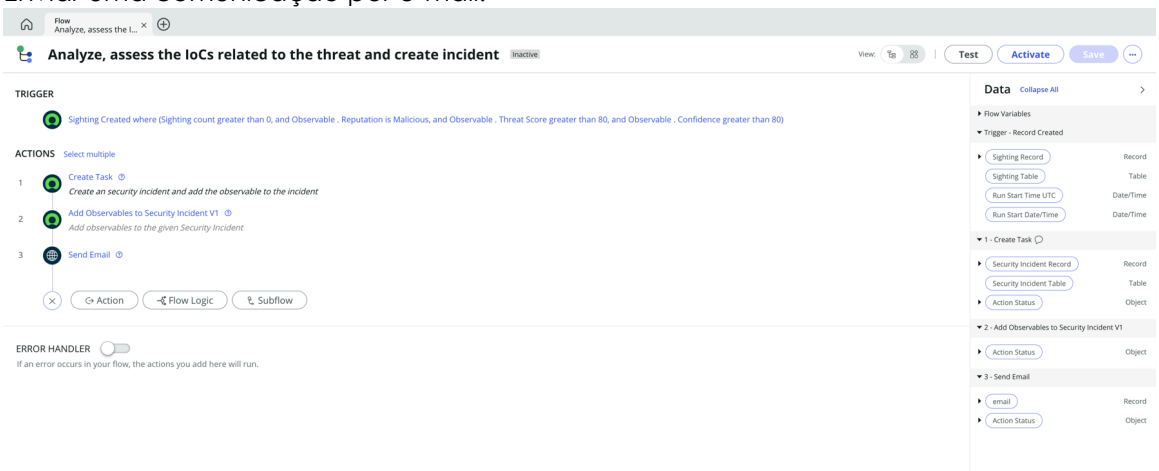
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Se a detecção foi criada em que (contagem de detecções maior que 0 e observável. A reputação é mal-intencionada e observável. Pontuação de ameaça maior que 80 e observável. Confiança maior que 80), então:**

   a. Crie um incidente de segurança e adicione o observável ao incidente.

   b. Adicionar observáveis ao incidente de segurança V1.

   c. Enviar uma comunicação por e-mail.



Suporte para gestão de vulnerabilidades

Saiba como uma nova vulnerabilidade é criada no TISC com uma vulnerabilidade relacionada no VR.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Quando uma nova vulnerabilidade é criada no TISC e há uma vulnerabilidade relacionada no VR.

- Se a pontuação de vulnerabilidade de VR (v2) for > 8 OU a pontuação de vulnerabilidade de VR (v3) for > 8.
- O total de IVs associados a ele é maior que 0.

Procedimento

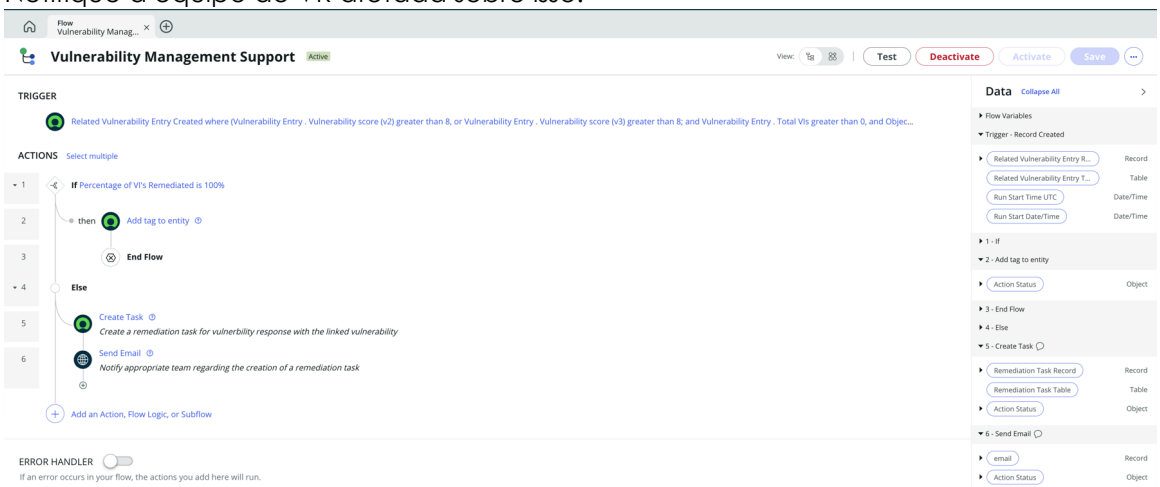
1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos Automatizados**.
3. Selecione o link de ação **Suporte de gestão de vulnerabilidades** para exibir os detalhes da regra respectiva no Flow Designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

```
When new vulnerability is created in TISC and there is a related
 vulnerability in VR.
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Se a porcentagem do total de IVs corrigidos associados a essa vulnerabilidade for 100%, então:**
   a. Adicione um marcador chamado Corrigido ao observável.
6. **Caso contrário, aprimore os dados do observável com os recursos disponíveis:**
   a. Crie uma tarefa de correção para VR.
   b. Notifique a equipe de VR afetada sobre isso.



Rastreamento de vulnerabilidades de dia zero

Aprenda a analisar feeds RSS que entram no sistema.

Antes de Iniciar

Função necessária:

- Administrador do sistema (exibir, criar ou editar)
- sn_sec_tisc.admin (exibição)

Por Que e Quando Desempenhar Esta Tarefa

Sempre que um novo feed RSS for criado no sistema e tiver uma menção de "Dia zero" no título ou na descrição.

Procedimento

1. Navegar até **Todos** > **Central de segurança de inteligência contra ameaças** > **Administração**.
2. Selecionar **Fluxos Automatizados**.
3. Selecione o link de **acompanhamento de vulnerabilidade de dia zero** para exibir os detalhes da regra respectiva no Flow Designer.
4. Exiba a ação do Flow Designer para o seguinte gatilho:

```
RSS Feed Created where (Title contains zero day, or Description
 contains zero day, or Title contains zero_day, or Description
 contains zero_day, or Title contains zero-day, or Description contains
 zero-day)
```

5. **Se o observável for um endereço IPv4 ou IPv6 e estiver dentro de um intervalo CIDR permitido:**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Crie um caso para a equipe de TISC, junto com uma tarefa de correção para a equipe de VR.

b. Notifique as equipes de TISC e de VR envolvidas.

Tabelas de fluxos automatizados

As tabelas a seguir ajudam a entender as tabelas de relacionamento entre entidades e tabelas de enriquecimento que são usadas em fluxos automatizados.

Tabelas de relacionamento entre entidades

Tabela	Entidade
Observável de indicador relacionado	sn_sec_tisc_m2m_indicator_observable
Indicador relacionado	sn_sec_tisc_m2m_indicator
Observável relacionado	sn_sec_tisc_m2m_observável
Relacionamento objeto-objeto	sn_sec_tisc_m2m_object
Objeto do indicador relacionado	sn_sec_tisc_m2m_object_indicator
Relacionamento objeto-observável	sn_sec_tisc_m2m_object_observable

Tabela de aprimoramento

Tabela	Entidade
Resultados da Pesquisa de ameaças	sn_sec_tisc_lookup_result
Detecções	sn_sec_tisc_sighting
Resultados de Aprimoramento do Observável	sn_sec_tisc_observable_enrichment_result

Como trabalhar com importações de dados

As importações de dados permitem que você exiba todos os registros que estão sendo processados para o trabalho de importação e também lista os trabalhos de importação que estão aguardando aprovações.

Exibição de todas as importações

Use esta seção para exibir todos os registros importados que são exibidos na exibição de lista para todos os usuários.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações**.
2. Selecionar **Importações de dados** > **Todas as importações**
   Esta página exibe todos os registros que estão sendo processados para o trabalho de importação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Abra qualquer registro para exibir o status do processo de importação.

> **Nota:** Você também pode clicar em **Nova importação** para criar um novo registro de importação. Depois de clicar neste botão, a aplicação direcionará você para a página **Importar inteligência**. Para obter mais informações sobre como criar novos registros, consulte a seção Importar inteligência contra ameaças e prossiga com o respectivo tipo de importação.

Exibição das minhas importações

Use esta seção para exibir os registros de importação criados pelo usuário conectado.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações**.
2. Selecionar **Importações de dados** > **Minhas importações**
   Esta página exibe todos os registros desses registros de importação que são categorizados para processamento adicional do trabalho de importação.
3. Abra qualquer registro para exibir o status do processo de importação.

> **Nota:** Você também pode clicar em **Nova importação** para criar um novo registro de importação. Depois de clicar neste botão, a aplicação direcionará você para a página **Importar inteligência**. Para obter mais informações sobre como criar novos registros, consulte a seção Importar inteligência contra ameaças e prossiga com o respectivo tipo de importação.

4. Exibir o resumo dos registros de importação.

> **Nota:** Caso algum dos trabalhos de importação não tenha sido enviado, você pode **Enviar** os registros para processamento posterior e enviá-los para aprovação. Se a aprovação não for necessária para esse trabalho de importação específico, esses registros serão processados automaticamente.

Exibição das minhas aprovações

Use esta seção para revisar e aprovar os registros do trabalho de importação.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Importações**.
2. Selecionar **Importações de dados** > **Minhas aprovações**
   Esta página exibe todos os registros de importação que estão aguardando aprovação do usuário conectado.
3. Abra qualquer registro para aprovar ou rejeitar o registro de importação.
4. Clique em **Aprovar** para aprovar o registro do trabalho de importação.
   A caixa de diálogo **Aprovar importação** é exibida e uma mensagem de confirmação é exibida se as importações selecionadas devem ser aprovadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Uma notificação por e-mail é enviada aos respectivos usuários de que o trabalho de importação que estava em andamento foi aprovado. Para obter mais informações sobre regras de aprovação, consulte Definição de regras de aprovação de importações de dados.

5. Selecione **Aprovar** na caixa de diálogo.
   Uma notificação por e-mail é enviada ao usuário que criou o trabalho de importação e o trabalho de importação que estava em andamento agora está aprovado.
6. Clique em **Rejeitar** para rejeitar um registro.

Nota:

- Você pode revisar e reenviar o trabalho de importação rejeitado. Certifique-se de adicionar comentários para rejeição.
- Uma notificação por e-mail é enviada ao usuário que criou o trabalho de importação quando o trabalho de importação que estava em andamento é rejeitado.
- Uma notificação por e-mail é enviada aos aprovadores que solicitam a aprovação.

Importar inteligência contra ameaças

Use este recurso para adicionar ou importar os dados de inteligência contra ameaças manualmente para o repositório.

Os seguintes formatos de importação são compatíveis com o processo de importação de dados de inteligência:

1. Importar do arquivo estruturado
2. Importar do formato padrão
3. Importar de texto simples
4. Importar do arquivo (não estruturado)

Importar dados usando arquivo estruturado

Carregue os dados estruturados nos formatos de arquivo compatíveis, como CSV, XLSX ou XLS.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca de informações sobre ameaças é exibida.
2. Clique **em Importar inteligência**.
3. Clique **em Importar do cartão de arquivo estruturado**.

Importante: Ao importar os dados de inteligência contra ameaças nos formatos de arquivo compatíveis, como TXT, CSV, STIX 2.x JSON, MISP JSON ou arquivo estruturado, o tamanho do arquivo é limitado a 5 MB. O limite de caracteres para texto bruto é limitado a 10.000.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

Campo	Descrição
Escolha uma opção	Selecione a opção necessária na lista suspensa, como Observáveis ou Indicadores. ◦ **Observáveis**: selecione os dados de observáveis a serem importados. **Nota:** Selecione esta opção se estiver importando dados de observáveis. Além disso, não modifique os cabeçalhos das colunas no arquivo. Os campos obrigatórios são Valor e Tipo, e outros são opcionais. Além disso, insira a data/hora no formato AAAA-MM-DDThh:mm:ssZ. ◦ **Indicadores**: selecione os dados de indicadores a serem importados. **Nota:** Selecione esta opção se estiver importando dados de indicadores. Além disso, não modifique os cabeçalhos das colunas no arquivo. Os campos obrigatórios para indicadores são Padrão, Tipo de padrãoe Válido de e outros são opcionais. Além disso, insira a data/hora no formato AAAA-MM-DDThh:mm:ssZ.
Visualizar e baixar arquivo de amostra para Indicadores	Use este link para baixar o arquivo de amostra usando o link Visualizar e carregar os dados estruturados em um formato de arquivo compatível, como CSV, XLS ou XLSX. **Nota:** Os cabeçalhos de coluna devem corresponder exatamente aos cabeçalhos. Os campos Valor e Tipo são necessários para cada observável no arquivo. Os campos restantes são opcionais, onde Visto pela primeira vez e Visto pela última vez devem estar em números e ter a hora do período em milissegundos.
Carregar arquivo	Clique neste link para carregar os dados do arquivo no formato de arquivo de estrutura recomendado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Você só pode carregar um arquivo por vez. Para adicionar um novo arquivo, você deve remover o existente e adicionar um novo arquivo.
Definir definições	
TLP	Selecione o indicador TLP (Traffic Light Protocol) na lista suspensa a ser aplicado aos registros importados. O TLP está no TISC e é rotulado com cores diferentes para garantir que os dados confidenciais sejam compartilhados com os usuários pretendidos. ◦ CLEAR: as informações podem ser compartilhadas sem restrições. ◦ VERMELHO ◦ ÂMBAR+ESTRITO ◦ ÂMBAR ◦ VERDE
Confiança (0–100)	Defina o valor de confiança entre 0 e 100 para os registros importados.
Período de expiração (dias)	Insira o período de expiração dos registros importados. **Nota:** Este é um campo obrigatório.
Marcadores	
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador na barra de **pesquisa** para escolher os marcadores disponíveis no sistema ou insira um novo nome de marcador e clique em **Adicionar** para atribuí-lo à origem.
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia para os dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência de ameaças. Por exemplo, nomenclatura CAPEC. Para obter mais informações, consulte Criando taxonomias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: As opções de valor de taxonomia mudam com base na taxonomia selecionada.
Substituir valor de origem	Marque esta caixa de seleção se quiser substituir os valores de origem de TLP, Confiança, Expiração, Marcadores e Taxonomias pelos valores configurados. Se você não marcar esta caixa de seleção, os valores configurados serão aplicados se não estiverem vazios.

5. Clique em **Avançar**.
6. Revise os dados antes do envio para processamento.

   Nota: A revisão de registros importados não é compatível com a opção STIX.

   Depois de clicar em **Avançar**, você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo apresenta todos os registros que precisam ser importados.

   O usuário pode executar qualquer tipo de atividade e vários usuários podem colaborar usando a seção de comentários, que está disponível no menu contextual à direita. A lista de registros importados será renderizada quando o arquivo inteiro ou o texto bruto for processado. O processamento de importação de arquivos grandes levará mais tempo e, durante o processamento, você também poderá verificar o status, revisar e enviar na página de registro de importação.

   Nota: Todos os registros que falham nas validações são ignorados no processo de importação e esses registros não são exibidos na página Revisar e enviar para processamento posterior.

7. Clique em **Atualizar tipo** e selecione o tipo para atualizar qualquer tipo de registros importados.
8. Clique em **Excluir** para excluir qualquer tipo de registros importados.
9. Clique em **Enviar**.

   Nota: Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não precisar do processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente ao enviar a solicitação.

10. Clique em **Exibir status** para exibir o status do registro de importação ou clique em **Concluído**.
    O registro exibe o status processado quando os dados são importados para processamento.
11. Clique em **Cancelar** para anular o processo de importação.
12. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar dados usando o formato padrão

Carregue os dados padrão nos formatos de arquivo compatíveis, como STIX 2.x JSON, MISP JSON.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca de informações sobre ameaças é exibida.
2. Clique **em Importar inteligência**.
3. Clique **em Importar do cartão de arquivo padrão**.

> **Importante:** Ao importar os dados de inteligência contra ameaças nos formatos de arquivo compatíveis, como TXT, CSV, STIX 2.x JSON, MISP JSON ou arquivo estruturado, o tamanho do arquivo é limitado a 5 MB. O limite de caracteres para texto bruto é limitado a 10.000.

4. No formulário, preencha os campos.

Campo	Descrição
Formato do arquivo	Selecione a opção necessária na lista suspensa, como STIX 2.x JSON ou MISP JSON. ◦ **STIX 2.x JSON**: selecione o formato em STIX 2.x JSON para importar. ◦ **MISP JSON**: selecione o formato no formato MISP JSON para importar.
Carregar arquivo	Clique neste link para carregar os dados no formato de arquivo padrão.
Definir definições	
TLP	Selecione o indicador TLP na lista suspensa a ser aplicado aos registros importados.
Confiança (0–100)	Defina o valor de confiança.
Período de expiração (dias)	Insira o período de expiração dos registros importados. **Nota:** Este é um campo obrigatório.
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador na barra de pesquisa para escolher os marcadores disponíveis no sistema ou insira um novo nome de marcador e clique em Adicionar para atribuí-lo à origem.
Taxonomia	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecionar uma taxonomia	Selecione a taxonomia para os dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência de ameaças. Por exemplo, nomenclatura CAPEC. Para obter mais informações, consulte Criando taxonomias.
Selecionar valores de taxonomia	Indica os valores de taxonomia associados à taxonomia.
Substituir valor de origem	Marque esta caixa de seleção se quiser substituir os valores de origem para TLP, Confiança, Expiração, Marcadores e Taxonomias dos valores configurados. Se você não marcar esta caixa de seleção, os valores padrão serão aplicados.

5. Clique em **Avançar**.
6. Revise os dados antes do envio para processamento.

   Nota: A revisão de registros importados não é compatível com a opção STIX.

   Depois de clicar em **Avançar**, você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo apresenta todos os registros que precisam ser importados.

   O usuário pode executar qualquer tipo de atividade e vários usuários podem colaborar usando a seção de comentários, que está disponível no menu contextual à direita.

   Nota: Todos os registros que falham nas validações são ignorados no processo de importação e esses registros não são exibidos na página Revisar e enviar para processamento posterior.

7. Clique em **Atualizar tipo** e selecione o tipo para atualizar qualquer tipo de registros importados.
8. Clique em **Excluir** para excluir qualquer tipo de registros importados.
9. Clique em **Enviar**.

   Nota:

   Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não precisar do processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente ao enviar a solicitação.

10. Clique em **Exibir status** para exibir o status do registro ou clique em **Concluído**.
    O registro exibe o status processado depois de processado.
11. Clique em **Cancelar** para anular o processo de importação.
12. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar dados usando texto bruto

Importe os dados dos observáveis copiando e colando o texto bruto ou inserindo o texto livre.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca de informações sobre ameaças é exibida.
2. Clique **em Importar inteligência**.

> **Importante:**
> - Todos os caracteres danificadores serão limpos como parte da análise e extração de observáveis.
> - Para esta opção de texto colado, somente URL, domínio, nome de arquivo, hashes e endereço IP serão extraídos e nenhum outro tipo de observável será extraído para a importação de dados e, no caso de tais tipos de observáveis, como registro, tipos de diretório, esses serão ser ignorado na importação.

3. Clique **em Importar do cartão de texto bruto**.

> **Importante:** Ao importar os dados de inteligência contra ameaças no formato de texto bruto, os caracteres são limitados a 10.000. A opção de texto bruto pode ser usada como uma solução alternativa para extrair os observáveis do PDF.

4. No formulário, preencha os campos.

Campo	Descrição
Caixa de texto de dados brutos	Insira ou copie e cole o texto bruto aqui nesta caixa de texto. **Nota:** Você só pode inserir ou colar o texto bruto em até 10.000 caracteres.
Definir definições	
TLP	Selecione o indicador TLP na lista suspensa a ser aplicado aos registros importados.
Confiança (0–100)	Defina o valor de confiança.
Período de expiração (dias)	Insira o período de expiração dos registros importados. **Nota:** Este é um campo obrigatório.
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador na barra de pesquisa para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	escolher os marcadores disponíveis no sistema ou insira um novo nome de marcador e clique em Adicionar para atribuí-lo à origem.
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia para os dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência de ameaças. Por exemplo, nomenclatura CAPEC. Para obter mais informações, consulte Criando taxonomias.

5. Clique em **Avançar**.
6. Revise os dados antes do envio para processamento.

   Depois de clicar em **Avançar**, você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo apresenta todos os registros que precisam ser importados.

   O usuário pode executar qualquer tipo de atividade e vários usuários podem colaborar usando a seção de comentários, que está disponível no menu contextual à direita.

   Nota: Todos os registros que falham nas validações são ignorados no processo de importação e esses registros não são exibidos na página Revisar e enviar para processamento posterior.

7. Clique em **Atualizar tipo** e selecione o tipo para atualizar qualquer tipo de registros importados.
8. Clique em **Excluir** para excluir qualquer tipo de registros importados.
9. Clique em **Enviar**.

   Nota: Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não precisar do processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente ao enviar a solicitação.

10. Clique em **Exibir status** para exibir o status do registro ou clique em **Concluído**.
    O registro exibe o status processado depois de processado.
11. Clique em **Cancelar** para anular o processo de importação.
12. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Importar dados usando o formato de arquivo não estruturado

Carregue os dados em um formato não estruturado compatível com formatos de arquivo como TXT, CSV, JSON, XLS, XLSX.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
   A página Biblioteca de informações sobre ameaças é exibida.
2. Clique **em Importar inteligência**.

Importante:

- Todos os caracteres danificadores serão limpos como parte da análise e extração de observáveis.
- Para esta opção de formato de arquivo não estruturado, somente URL, domínio, nome do arquivo, hashes e endereço IP serão extraídos e nenhum outro tipo de observável será extraído para a importação de dados e, no caso de tais tipos de observáveis, como registro, tipos de diretório, esses será ignorado na importação.

3. Clique no cartão **Importar do arquivo (não estruturado)**.

Nota: Ao importar os dados de inteligência contra ameaças nos formatos de arquivo compatíveis, como TXT, CSV, STIX 2.x JSON, MISP JSON ou arquivo estruturado, o tamanho do arquivo é limitado a 5 MB.

4. No formulário, preencha os campos.

Campo	Descrição
Carregar arquivo	Clique neste link para carregar os dados no formato de arquivo padrão.
Definir definições	
TLP	Selecione o indicador TLP na lista suspensa a ser aplicado aos registros importados.
Confiança (0–100)	Defina o valor de confiança.
Período de expiração (dias)	Insira o período de expiração dos observáveis associados. **Nota:** Este é um campo obrigatório.
Adicionar marcadores	Use os marcadores para anotar ou marcar registros ingeridos no sistema a partir desta origem. Comece a digitar o nome do marcador na barra de pesquisa para escolher os marcadores disponíveis no sistema ou insira um novo nome de marcador e clique em Adicionar para atribuí-lo à origem.
Taxonomia	
Selecionar uma taxonomia	Selecione a taxonomia para os dados importados. Usando taxonomias, defina dicionários que podem ser usados como taxonomias atribuídas a registros de inteligência de ameaças. Por exemplo,

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	nomenclatura CAPEC. Para obter mais informações, consulte Criando taxonomias.

5. Revise os dados antes do envio para processamento.

   Depois de clicar em **Avançar**, você pode ver o resumo de todas as informações que o usuário forneceu na seção acima e a seção abaixo apresenta todos os registros que precisam ser importados.

   O usuário pode executar qualquer tipo de atividade e vários usuários podem colaborar usando a seção de comentários, que está disponível no menu contextual à direita.

   Nota: Os formatos compatíveis para importar os dados são TXT, CSV, JSON, XLS e todos os registros que falham nas validações são ignorados no processo de importação e esses registros não são exibidos na página Revisar e enviar para processamento.

6. Clique em **Atualizar tipo** e selecione o tipo para atualizar qualquer tipo de registros importados.
7. Clique em **Excluir** para excluir qualquer tipo de registros importados.
8. Clique em **Enviar**.

   Nota: Depois de enviar o registro de importação, o usuário será direcionado ao aprovador para aprovar o registro de importação correspondente com base nas regras de aprovação configuradas. Se o usuário atual que está criando o registro não precisar do processo de aprovação, o registro passará pelo processo de aprovação automática, o trabalho de importação será aprovado automaticamente ao enviar a solicitação.

9. Clique em **Exibir status** para exibir o status do registro ou clique em **Concluído**. O registro exibe o status processado quando o envio é bem-sucedido.
10. Clique em **Cancelar** para anular o processo de importação.
11. Clique em **Voltar** para voltar à página anterior e revisar o registro, se necessário.

Workbench do analista de ameaça

A página Workbench do analista de ameaças consiste em casos e tarefas de caso que estão em Analistas de ameaças e sua equipe.

Use o recurso **Gestão** de casos para criar e rastrear as investigações de ameaças e atividades de análise.

Durante as investigações de ameaças, os analistas coletam os dados de registros de inteligência interna, como observáveis, agentes de ameaças, campanhas e assim por diante.

Visão geral do workbench

A página Visão geral do workbench consiste nas tarefas de caso e nos casos que estão sob os analistas de ameaças e sua equipe.

A visão geral lista todos os casos em aberto e seus status, o que ajuda os analistas a gerenciar sua carga de trabalho e priorizar suas investigações.

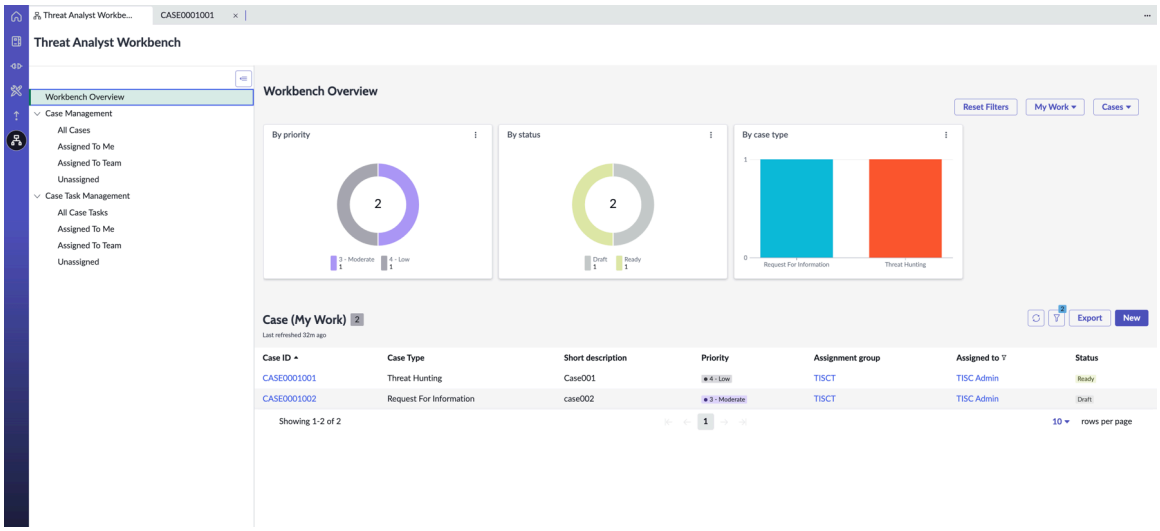
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_sec_tisc.analyst, sn_sec_tisc.admin

Depois que o caso for criado, os analistas atribuirão as tarefas de caso a outros analistas ou equipes para investigação adicional e também colaborarão com eles para compartilhar informações e insights.

Existem vários widgets presentes em cada filtro agrupado por prioridade, status e tipo de caso que estão nas filas dos analistas de ameaças e na fila da equipe de analistas de ameaças.



Quando os filtros são aplicados nos widgets, a metade inferior da página de visão geral é preenchida com os casos ou tarefas de caso correspondentes apresentados como itens de lista. Para remover os filtros aplicados, clique em **Redefinir filtros** para redefinir para a exibição original.

Usando esta página, os analistas e administradores de ameaças podem exibir seu trabalho, o trabalho das equipes e qualquer trabalho não atribuído. Você pode navegar até a lista suspensa. As opções disponíveis são:

- Meu trabalho: selecione esta opção para exibir o trabalho atribuído a você.
- Trabalho da minha equipe: selecione esta opção para exibir o trabalho da sua equipe atribuído a todos os grupos dos quais você faz parte.
- Trabalho não atribuído: selecione esta opção para exibir o caso ou a tarefa de caso que não estão atribuídos. Para atribuir o caso ou a tarefa de caso, você deve acessar a exibição do formulário e atribuir os usuários ou grupos de usuários ao caso e à(s) tarefa(s) de caso.

Você também pode exibir casos e tarefas de caso diretamente na Visão geral do workbench que estão atribuídos a você. Por padrão, a exibição de caso é exibida. Você pode usar o menu suspenso e selecionar as tarefas de caso se quiser exibir as tarefas de caso por prioridade e status.

Criação de casos usando o Workbench do analista de ameaças

Os casos são usados para rastrear informações sobre uma campanha ou agente de ameaça que ameaça sua organização. Depois que um caso é criado, você pode adicionar artefatos que permitem revisar e analisar todas as informações relacionadas a um único caso ou tarefa de caso.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst, sn_sec_tisc.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Clique em **Nova**.
5. Preencha os campos, se for o caso.

Criar novo caso

Campo	Descrição
ID do caso	Um identificador exclusivo para o caso. Este é o ID gerado pelo sistema.
Descrição resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.
Descrição	Uma descrição detalhada, incluindo informações relevantes sobre o caso, como histórico, qual análise é necessária e resultados esperados.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado. As opções possíveis para a investigação são: ◦ Busca de ameaças ◦ Solicitação de informações ◦ Caso de gestão de vulnerabilidade ◦ Caso de conformidade ◦ Caso de resposta do incidente ◦ Caso de colaboração ◦ Outros
Prioridade	Uma avaliação da gravidade da solicitação ou do problema.
Grupo de atribuição	O grupo atribuído responsável por trabalhar no caso.
Status	O status atual do caso.
Atribuído a	O analista responsável por trabalhar em um caso.
Data de vencimento	A data e a hora em que a tarefa deve ser concluída ou encerrada.
Colaboradores	A lista de designados acumulada de tarefas e deve ser possível adicionar sobre ela.
TLP	Valor exclusivo que indica a configuração de confidencialidade dos dados por TLP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Lista de observação	Quando um usuário é adicionado à lista de observação, a pessoa recebe notificações por e-mail sobre mudanças de status e prioridade.
Impor restrição	Marque esta caixa de seleção para modificar membros do grupo permitido e membros permitidos. Para obter mais informações, consulte Restrições impostas para caso(s).

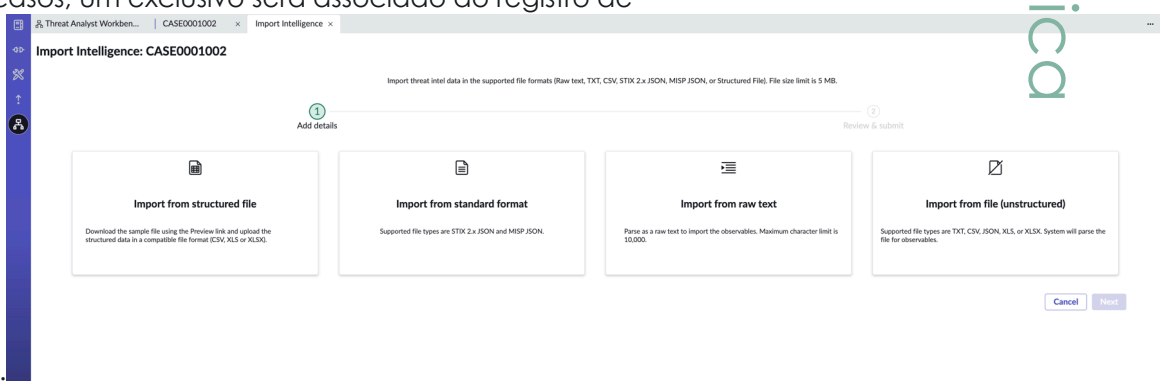
6. Preencha os campos na seção Informações, conforme apropriado.

Informações

Campo	Descrição
Anotações	Quaisquer anotações adicionais relacionadas à investigação de ameaças.
Recomendações ou ações	Quaisquer recomendações ou ações relacionadas à investigação de ameaças.
Análise e descobertas	Insira a análise e as descobertas relacionadas à investigação de ameaças.
Resumo do fechamento	Adicione o resumo de fechamento das descobertas.

7. Clique em **Salvar**.
Depois que o registro tiver sido salvo, você poderá clicar na guia **Importar inteligência** para importar os dados de inteligência contra ameaças usando o recurso **Importar inteligência**.

Nota: Se você estiver importando e processando dados da Gestão de casos, um exclusivo será associado ao registro de importação.



Restrições impostas para caso(s)

Use este recurso para restringir um caso e fornecer uma lista de grupos e usuários que podem acessá-lo.

Função necessária:

- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Considerações principais

1. Restringir um caso e fornecer uma lista de grupos/usuários que podem acessá-lo.
2. Habilite o campo "Impor restrição" presente na página do formulário de caso.
3. Modifique membros do grupo permitido e membros permitidos.
4. Depois que um caso é marcado como restrito, somente membros de grupos permitidos, membros da lista de usuários permitidos e usuários com a função sn_sec-tisc.admin podem acessar este caso.
5. Conceda acesso à função sn_sec_tisc.restriction_access_manager, que é necessária para ler/gravar o campo Impor restrição. Se você for um analista que não tem essa função, não poderá ver a opção Impor restrição para caso(s) ou tarefa(s) de caso.
6. O analista assign_to existente e o analista que o marcou como restrito também perderão o acesso se não tiverem a permissão necessária.
7. A restrição de caso na equipe de CTI é implementada caso a caso. Membros permitidos podemacessar casos restritos se estiverem na lista de permitidos. Incluí-los em uma das listas de casos permitidos não significa que eles possam acessar todos os outros casos restritos.
8. Se o caso estiver marcado como restrito e os membros permitidos ou o grupo permitido for deixado em branco, somente sn_sec_tisc.admin poderá acessar esses casos restritos.
9. Somente grupos CTI são permitidos no campo **Grupo permitido**. Um usuário com a função sn_sec_tisc.analyst é permitido na lista de **Membros permitidos**.

Nota: Uma anotação de trabalho será publicada se um caso for marcado como restrito.

Controles de acesso para casos e tarefas de caso

Permitir controles de acesso específicos para um caso ou tarefa de caso.

Controle de acesso	Descrição
Acesso de leitura	Os usuários externos adicionados aqui terão acesso para exibir o formulário de caso, mas não poderão editar nenhum campo no caso nem executar nenhuma ação.
Acesso privilegiado	Os usuários externos adicionados aqui terão acesso para editar qualquer campo no formulário de caso, mas não terão permissão para executar orquestrações.

Acesso de usuários externos ou tarefas de caso

Controles de acesso de usuário externo são necessários para controlar o acesso em um caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de caso atribuídas a usuários externos

1. É recomendável que o usuário acesse o espaço do TISC e exiba somente os módulos de tarefas de caso.
2. O usuário externo só pode ver as tarefas de caso atribuídas a esse usuário específico ou aos grupos aos quais o usuário pertence.
3. O usuário externo deve ser capaz de reatribuir a tarefa dentro do grupo ao qual o usuário pertence.

Nota: Usuário externo é qualquer usuário que esteja fora da equipe de CTI.

Por padrão, a seção de controle de acesso de usuário externo não está visível e o usuário precisa de uma função adicional. Além disso, a seção de controle de acesso de usuário externo não deve estar visível para usuários externos que tenham acesso privilegiado ou de leitura em um caso.

Nota: Os usuários externos acessam o espaço de TISC e aqueles que têm visibilidade dos módulos Caso e Tarefas de caso. O usuário verá somente os casos para os quais ele tem acesso (de leitura ou privilegiado).

Funções para atribuir acesso de usuário externo

Função	Descrição
sn_sec_tisc.special_access_read_manager	• O usuário com esta função poderá ver a seção. • Será capaz de editar o campo Acesso de leitura. • A função é atribuída ao administrador de informações sobre ameaças por padrão e pode ser atribuída a outros usuários na equipe de CTI.
sn_sec_tisc.special_access_write_manager	• O usuário com esta função poderá ver a seção. • Poderá editar o campo Acesso privilegiado. • A função é atribuída ao administrador de informações sobre ameaças por padrão e pode ser atribuída a outros usuários na equipe de CTI.

Associar técnica de MITRE

Associe uma ou mais técnicas MITRE a um caso.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Clique no botão **Associar técnica do MITRE**.
6. Clique em **Adicionar matriz** para associar a técnica MITRE.
   A caixa de diálogo **Associar técnica MITRE ao caso** é exibida.
7. Selecione a **Matriz**.
   Todas as matrizes habilitadas serão exibidas para você selecionar a Matriz.
8. Selecione a tática nas listas suspensas.
   Todas as táticas associadas a uma matriz serão exibidas.

   Nota: Caso você queira adicionar mais táticas, clique em **Adicionar tática**. As táticas selecionadas anteriormente não serão mais exibidas na lista suspensa se você estiver adicionando uma nova tática.

9. Selecione a **técnica**.
   Todas as técnicas associadas à tática selecionada serão exibidas. Caso você esteja adicionando mais táticas, poderá selecionar as técnicas associadas para essas táticas selecionadas.
10. Clique em **Salvar**.
    Se você quiser excluir todos os dados associados à matriz, clique em **Excluir matriz**. Esta ação removerá somente os dados da matriz associados, mas a matriz permanecerá no repositório do MITRE ATT&CK.

    O registro de dados de matriz associado é exibido na seção Cartão do MITRE ATT&CK. Na exibição do cartão:

    Nota: Você pode alternar entre várias matrizes na lista suspensa Matriz.

    a. A primeira linha da exibição do cartão exibe todas as táticas associadas à matriz selecionada no momento.
    b. Cada cartão de tática mostra o nome da tática e o número de técnicas dessa tática mapeadas para o registro de caso atual.
    c. Todas as técnicas associadas a esse caso são mostradas verticalmente em cada tática. Você pode clicar em qualquer técnica para exibir a exibição do formulário de técnica.
11. Clique em **Mostrar ID** para mostrar os IDs de todas as técnicas associadas.

    Nota: Cada cartão de técnica mostra o nome e o ID da técnica somente quando a **opção Mostrar ID** está habilitada.

12. Clique em **Atualizar** para atualizar a exibição do cartão.
    Você pode exibir o carimbo de data/hora da última atualização da matriz selecionada.

    Nota: Clique no ícone pop-out para exibir o cartão de matriz associado em uma nova guia.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar tarefa de caso usando o Workbench do analista de ameaças

Crie tarefas de caso para associar a caso(s).

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst, sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Gestão de tarefas do caso** > **Tarefas de todos os casos**.
   Todas as tarefas de caso são exibidas.
4. Clique em **Nova**.
5. Preencha os campos, se for o caso.

Criar nova tarefa de caso

Campo	Descrição
ID da tarefa	Um identificador exclusivo para a tarefa de caso. Este é o ID gerado pelo sistema.
Descrição resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.
Descrição	Uma descrição detalhada, incluindo informações relevantes sobre a tarefa de caso, como histórico, qual análise é necessária e resultados esperados.
ID do caso primário	Selecione o ID do caso primário na pesquisa.
Prioridade	Uma avaliação da gravidade da solicitação ou do problema.
Grupo de atribuição	O grupo atribuído responsável por trabalhar na tarefa de caso.
Status	O status atual da tarefa de caso.
Atribuído a	O analista que é responsável por trabalhar em uma tarefa de caso.
Data de vencimento	A data e a hora em que a tarefa de caso deve ser concluída ou encerrada.
TLP	Valor exclusivo que indica a configuração de confidencialidade dos dados por TLP.
Impor restrição	Como um sn_sec_tisc_admin, marque esta caixa de seleção para modificar membros do grupo permitido e membros permitidos. Para obter mais informações, consulte Restrições impostas para caso(s).

6. Preencha os campos na seção Informações, conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Quaisquer anotações adicionais relacionadas à investigação de ameaças.
Fechamento	Adicione o resumo de fechamento das descobertas.

7. Clique em **Salvar**.
   Sua tarefa de caso será associada ao seu caso.

> **Nota:** Depois de salvar a tarefa de caso, você pode adicionar marcadores e taxonomias à tarefa. Para obter mais informações, consulte Criando taxonomias.

Adicionar artefatos a casos ou tarefas de caso

Depois de criar um caso, você pode exibir ou adicionar artefatos, como incidentes de segurança, ICs e indicadores de comprometimento, ao caso. Esses artefatos atuam como pistas na resolução do caso.

Antes de Iniciar

Função necessária: administrador

> **Nota:** Os artefatos estão disponíveis somente para os casos existentes. Para observáveis e indicadores, os artefatos também podem ser adicionados ou associados a um caso do trabalho de importação usando o botão Importar inteligência. Para obter mais informações sobre como importar, consulte Importar inteligência contra ameaças

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso ou tarefa de caso.
5. Acesse a guia **Artefatos**.
   Os artefatos associados são exibidos como as listas relacionadas a esse caso específico ou tarefa de caso.
6. Vincular ou desvincular os registros do caso ou da tarefa de caso.

> **Nota:** Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.

A tabela a seguir lista as listas relacionadas a artefatos relacionados ao(s) caso(s) ou tarefa(s) de caso:

Registros relacionados

Lista relacionada	Descrição
Técnicas MITRE	Liste as técnicas MITRE relacionadas ao(s) caso(s).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Observável	Lista de observáveis relacionados a esses casos ou tarefas de caso.
Indicadores	Lista de indicadores relacionados a esses casos ou tarefas de caso.
Padrões de ataque	Lista de padrões de ataque relacionados a esses casos ou tarefas de caso.
Campanhas	Liste as campanhas relacionadas a esses casos ou tarefas de caso.
Linha de ação	Liste o curso de ações relacionadas a esses casos ou tarefas de caso.
Componentes de dados	Lista de componentes de dados relacionados a esses casos ou tarefas de caso.
Grupos de ameaças	Liste os agrupamentos de ameaças relacionados a esses casos ou tarefas de caso.
Identidades	Liste as identidades relacionadas a esses casos ou tarefas de caso.
Infraestrutura	Liste a infraestrutura, como sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados que estejam relacionados a estes casos ou tarefas de caso.
Conjuntos de intrusão	Liste os conjuntos de intrusão, como um conjunto de comportamentos adversários e recursos com propriedades comuns que estão relacionados a esses casos ou tarefas de caso.
Locais	Liste os registros de locais relacionados a esses casos ou tarefas de caso.
Malware	Liste os registros de origem de malware que estão relacionados a esses casos ou tarefas de caso.
Definições de marcação	Listar os registros de definições de marcação relacionados a esses casos ou tarefas de caso.
Anotações de ameaça	Listar os registros de definições de marcação relacionados a esses casos ou tarefas de caso.
Dados observados	Liste os dados observados que estão relacionados a esses casos ou tarefas de caso.
Opiniões sobre ameaças	Liste as opiniões de ameaças relacionadas a esses casos ou tarefas de caso.
Relatórios de ameaças	Listar os relatórios de ameaças relacionados a esses casos ou tarefas de caso.
Detecções	Lista de detecções relacionadas a estes casos ou tarefas de caso.
Agentes da ameaça	Liste os agentes de ameaça que estão relacionados a estes casos ou tarefas de caso.
Ferramentas	Listar as ferramentas relacionadas a esses casos ou tarefas de caso.
Vulnerabilidades	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente que esteja relacionado a estes casos ou tarefas de caso.
Casos Relacionados	Lista os casos relacionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Tarefas do caso relacionado	Lista as tarefas de caso relacionadas.
Incidentes de segurança	Liste os incidentes de segurança relacionados a esses casos ou tarefas de caso.
Itens de configuração afetados	Liste os itens de configuração afetados que estão relacionados a esses casos ou tarefas de caso.
Serviços afetados	Liste os serviços afetados que estão relacionados a esses casos ou tarefas de caso.
Ativos afetados	Liste os ativos afetados que estão relacionados a esses casos ou tarefas de caso.
Entradas de Vulnerabilidade	Liste as entradas de vulnerabilidade relacionadas a esses casos ou tarefas de caso.

Executar ações de aprimoramento em um caso

Use esta seção para entender como as ações de aprimoramento são realizadas em caso(s).

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

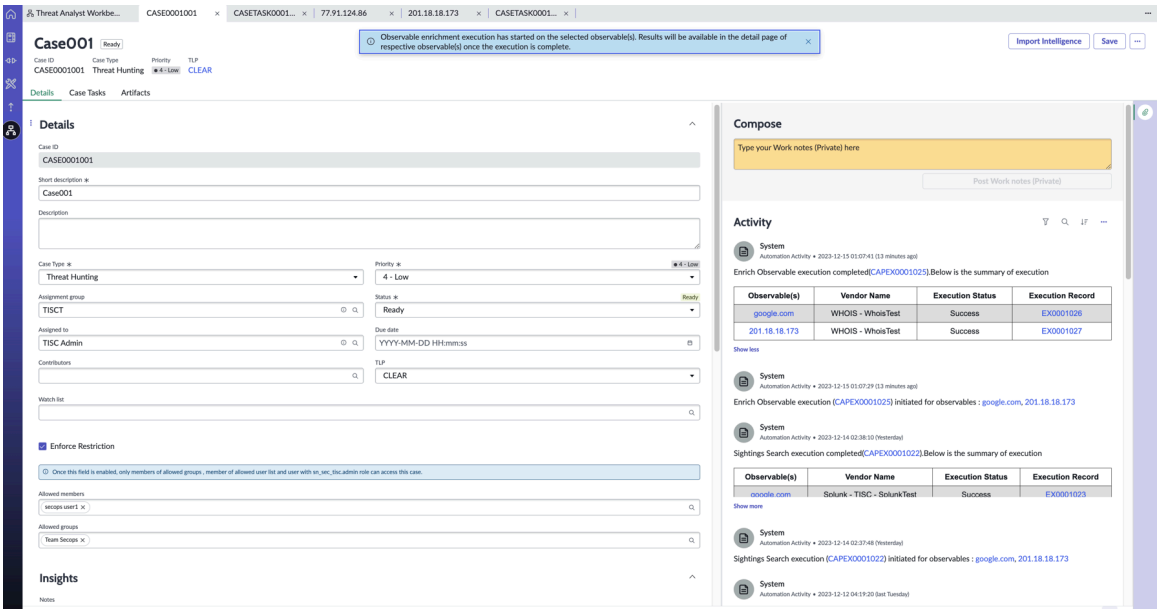
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso ou tarefa de caso.
5. Acesse a guia **Artefatos**.
6. Selecione a lista relacionada de Observáveis.
7. Selecione um ou mais observáveis.
8. Clique em qualquer Ação de aprimoramento na lista suspensa.
9. Selecione as implementações disponíveis.
10. Clique em **Enviar**.
    Por exemplo, Executar pesquisa de ameaças. A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida informando que a execução de aprimoramento do observável foi iniciada no(s) observável(is) selecionado(s). Os resultados estarão disponíveis na página de detalhes dos respectivos observáveis quando a execução for concluída.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Depois que a execução é iniciada ou concluída, uma anotação de trabalho é publicada no fluxo de atividades da exibição do formulário.



Exibir relatórios de caso

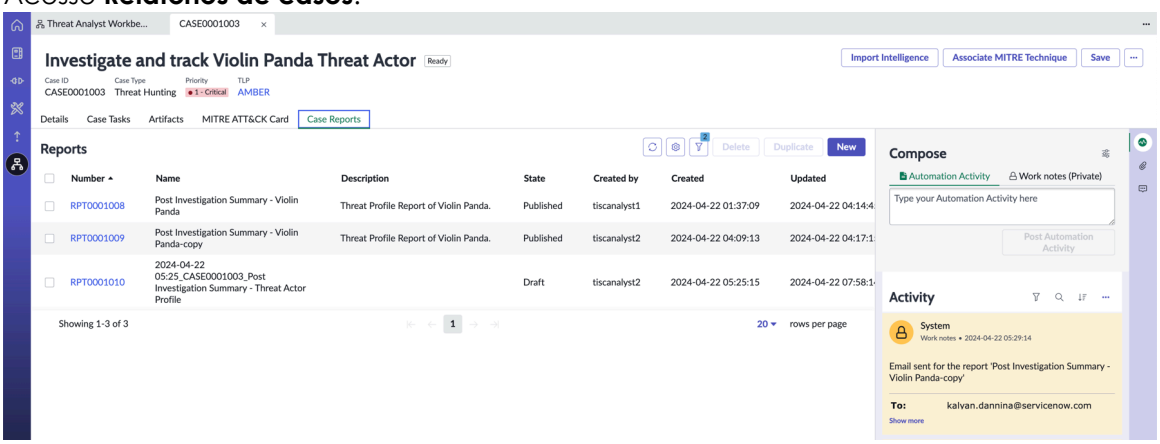
Use o recurso de relatórios de casos para gerar relatórios relacionados aos casos. Esses relatórios incluem um relatório pós-investigação ou um relatório resumido executivo.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Acesse **Relatórios de casos**.

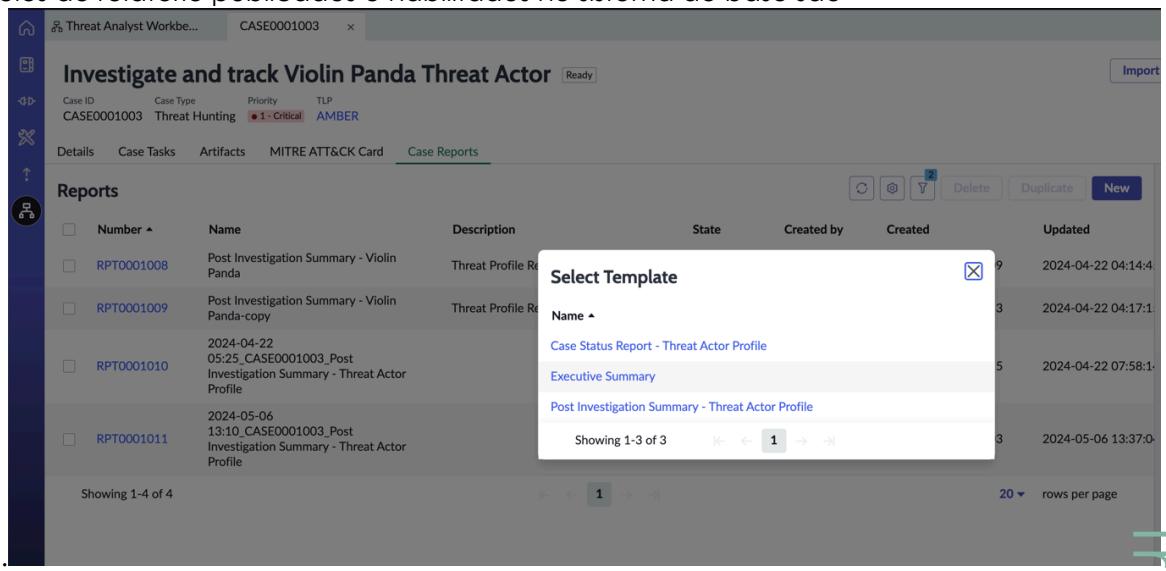


Nota: Você pode excluir os relatórios da lista, criar uma cópia duplicada dos relatórios existentes e personalizar seu próprio relatório.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Nova**.
   Os modelos de relatório publicados e habilitados no sistema de base são exibidos.



7. Selecione o modelo de relatório desejado.
   O modelo de relatório selecionado para o tipo de relatório é gerado. Além disso, aqui, depois que o relatório é publicado, isso significa que um grupo maior de usuários pode exibi-lo, mas se o relatório estiver no estado de rascunho, esse relatório ficará oculto para os usuários. Como analista, você só pode exibir os relatórios publicados, mas não os relatórios no estado de rascunho.

   Nota:
   - Caso você queira adicionar mais campos, selecione os campos e adicione-os diretamente ao relatório de caso.
   - Se você quiser adicionar uma lista relacionada, por exemplo, uma lista de observáveis, selecione Observáveis. Todos os observáveis associados a esse caso específico serão listados. Selecione um ou mais observáveis e clique em **Adicionar**. Você também pode filtrar o observável necessário e adicioná-lo ao seu caso.

8. Clique em **Salvar conteúdo** para salvar o conteúdo do seu relatório.
9. Clique em **Visualizar** para visualizar o relatório.

   Nota: Você pode fazer o seguinte:
   - **Maximize** a janela do relatório.
   - **Baixe** o relatório usando o ícone de **download**.
   - Destaque o relatório em uma nova guia, caso a altura ou o tamanho do relatório tenham uma melhor experiência de exibição.
   - **Edite** o Nome do relatório e a Descrição do relatório.
   - **Publicar** o relatório.

10. Clique no botão **Editar conteúdo** para republicar o relatório.

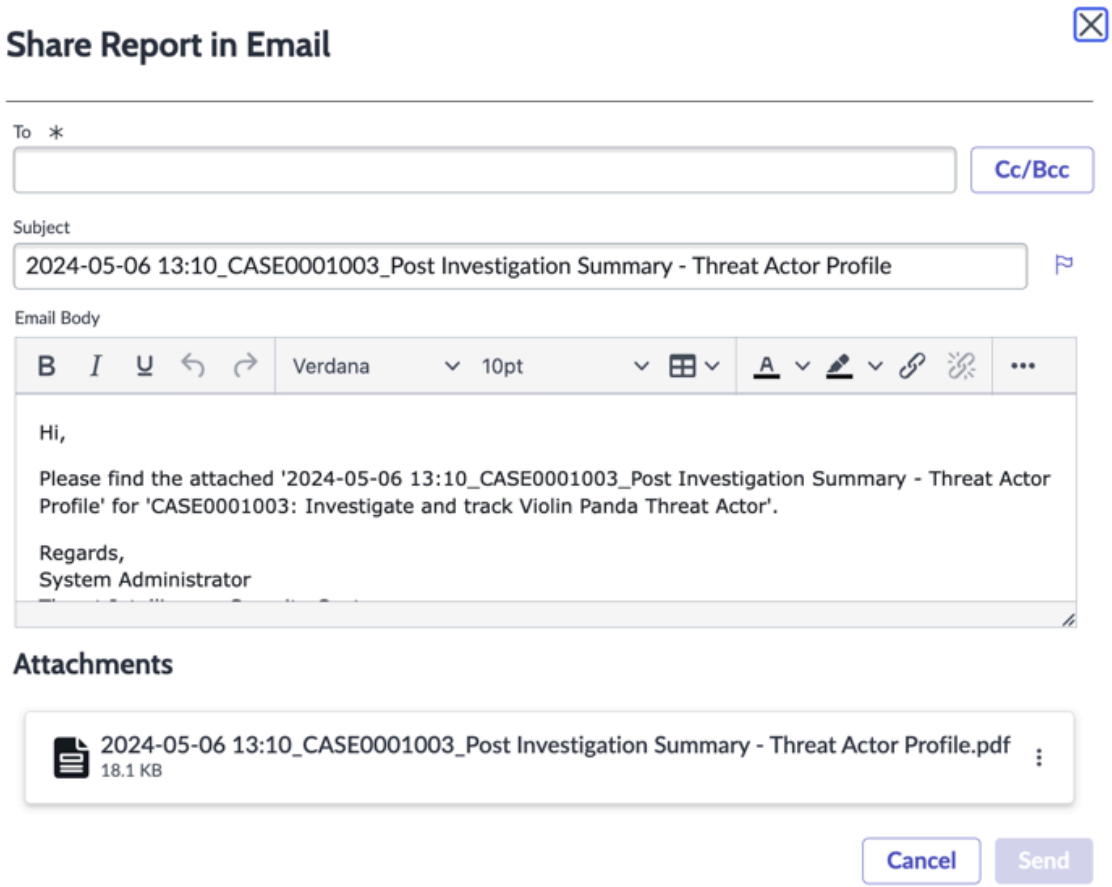
    Nota: Uma mensagem de aviso será exibida para você compartilhar o relatório:

    Você deve republicar o relatório depois de fazer mudanças para baixar ou compartilhar o relatório. Deseja continuar editando?

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Clique em **Editar**.
    Se você quiser editar o relatório, poderá continuar editando o relatório conforme explicado ou poderá publicar o relatório. Depois de publicado, o relatório será somente leitura.
12. Clique em **Compartilhar relatório em e-mail** para compartilhar o relatório.
    Ao compartilhar o relatório, o relatório em PDF gerado é anexado como um anexo ao e-



    mail.
13. Adicione os campos de e-mail necessários, como Para (com quem você deseja compartilhar o relatório), CC e CCO
14. Marque o e-mail como importante, se necessário.
15. Clique em **Enviar**.
    O relatório será compartilhado com o grupo maior de usuários.

Carregar anexos de arquivo seguros

Use esta seção para entender como carregar anexos de arquivo seguros para o(s) caso(s).

Antes de Iniciar

Função necessária: sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

Nota: As listas relacionadas a Arquivos seguros só são exibidas quando você tem a função de usuário, sn_sec_tisc.secure_file_access.

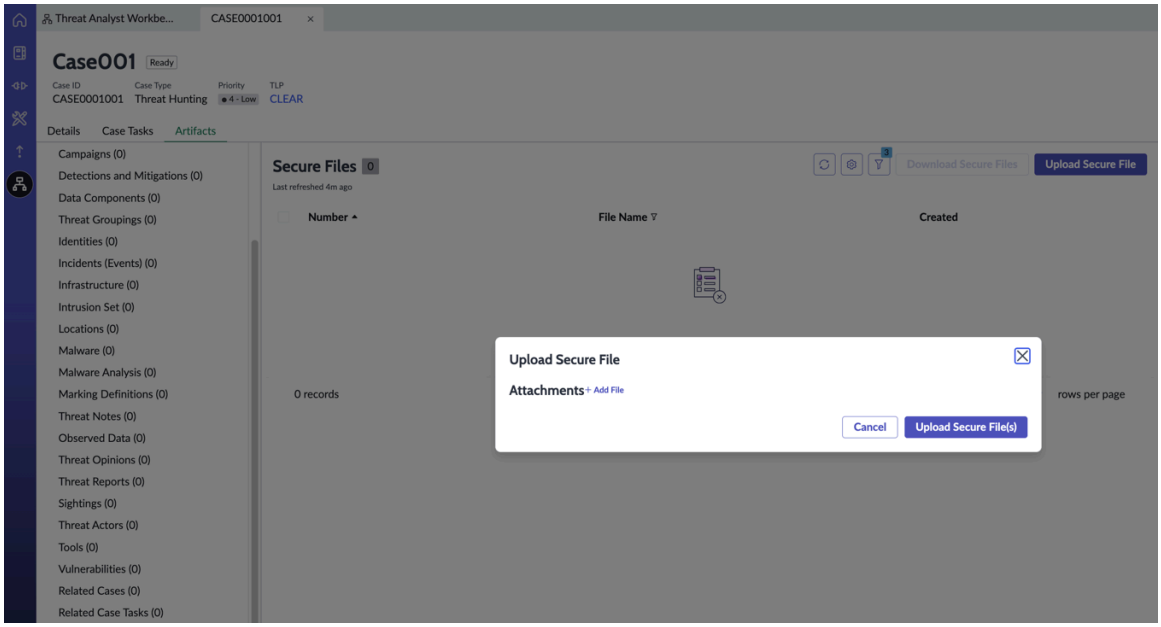
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Ir para **Gestão de casos** > **Todos os Casos**.
   Todos os casos são exibidos.
4. Selecione qualquer caso.
5. Ir para **Artefatos** > **Arquivos seguros** listas relacionadas.
6. Clique no botão **Carregar arquivo seguro**.
7. Clique em **Adicionar arquivo** para adicionar os anexos.
8. Selecione os arquivos e clique no botão **Carregar arquivo(s) seguro(s)**.
   Os anexos de arquivo foram carregados.



9. Clique em **Baixar arquivos seguros** para baixar os anexos.
   Os anexos estão disponíveis no formato zip.
10. Como alternativa, você pode baixar o arquivo navegando até a página de detalhes do registro de arquivo seguro.

Nota:

- Todos os anexos seguros são criptografados e armazenados no sistema usando a Estrutura de gestão de chaves (KMF). Para obter mais informações, consulte Criptografia de anexo .
- Se os usuários tiverem assinatura do *ServiceNow Integration Hub* **Instalador do pacote profissional**, os arquivos seguros serão compactados no formato zip e também criptografados e armazenados

Central de segurança de inteligência contra ameaças Biblioteca

Uma biblioteca de ameaças é definida como um grupo de objetos e entidades organizados que atendem às organizações com informações estruturadas e não estruturadas de ameaças à segurança.

As informações sobre a ameaça estão disponíveis na forma de feeds. Os feeds fornecem dados valiosos sobre ameaças de fontes como STIX, MISP e assim por diante, que listam entidades de inteligência contra ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A biblioteca da Central de segurança de inteligência contra ameaças explica como navegar pelos dados, executando pesquisas básicas e avançadas e regras de filtragem, invocar o assistente de importação, adicionar manualmente registros de inteligência contra ameaças, executar as ações necessárias, como adicionar à lista de permissões, listas de proibições e listas de observação .

A exibição detalhada fornece informações para os registros de inteligência e, nas exibições de lista, você pode executar ações rápidas em um ou mais registros.

Noções básicas sobre o modelo de dados

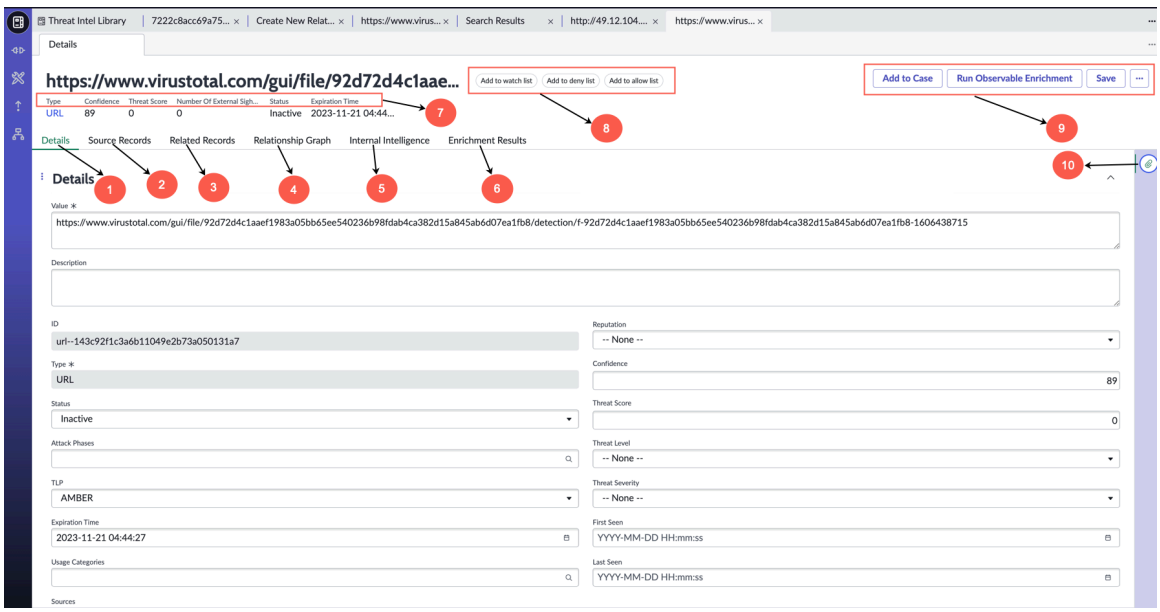
O modelo de dados e a arquitetura do módulo da central de segurança de inteligência contra ameaças foram projetados para oferecer suporte a capacidades da plataforma de inteligência contra ameaças e diferentes exibições de segurança que fornecem dados detalhados para analistas de ameaças.

O modelo de dados tem as estruturas de dados que são representadas como objetos no repositório de inteligência contra ameaças.

TISC Exibição do formulário Objetos da biblioteca

A página inicial de objetos Central de segurança de inteligência contra ameaças consiste nos seguintes recursos.

Use ou navegue até as seções a seguir e saiba mais sobre cada SDOs em detalhes.



TISC exibição de formulário de objetos da biblioteca

Ordem	Menu/Guia	Descrição
1	Guia **Detalhes**	Use esta seção para exibir ou editar os SDOs na exibição de formulário.
2	Guia**Registros de origem**	Os registros de origem contribuem para um registro agregado conforme exibido na exibição de formulário. Esses registros de origem são

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição de formulário de objetos da biblioteca

Ordem	Menu/Guia	Descrição
		criados automaticamente a partir de feeds ou criados manualmente pelo usuário.
3	Guia **Registros relacionados**	Lista todos os registros relacionados associados ao SDO.
4	Guia**Gráfico de relacionamento**	Representação visual dos objetos relacionados.
5	Guia**Inteligência interna**	Lista os registros de inteligência interna dos objetos associados.
6	Guia**Resultados de aprimoramento**	Lista as integrações de aprimoramento associadas aos objetos.
7	**Faixa de formulário**	Esta é uma seção somente leitura que contém os campos-chave, como Tipo, Confiança, Pontuação de ameaça, Número de detecções, Status e Tempo de expiração.
8	**Ações de IU da faixa de formulário**	Estas são as listas de controle de segurança que estão disponíveis para você clicar caso precise adicioná-las à lista de permissões, removê-las da lista de permissões (lista de proibições) ou adicioná-las à lista de observação com base nos observáveis. Clique para: • adicionar à lista de observação • adicionar à lista de proibições • adicionar à lista de permissões **Nota:** As ações de formulário são aplicáveis somente a observáveis.
9	**Ações de IU do formulário**	As ações de IU de formulário disponíveis são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição de formulário de objetos da biblioteca

Ordem	Menu/Guia	Descrição
		1. **Adicionar ao caso**: adicione os objetos ao caso. 2. **Executar aprimoramento de observável**: execute os aprimoramentos nos objetos selecionados. 3. **Salvar**: salva o registro. 4. **Excluir**: exclui o registro.
10	**Menu contextual direito**	Fornece acesso fácil aos controles rápidos, como anexos, anotações e assim por diante, com base nas tarefas associadas a esse objeto. Esta opção está disponível nas duas guias restantes para o analista de ameaças acessar sempre que necessário. O menu contextual fornece navegação fácil para:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição de formulário de objetos da biblioteca

Ordem	Menu/Guia	Descrição
		1. **Anexos**: anexe qualquer arquivo relacionado aos objetos. **Nota:** Sempre que você cria um novo observável, indicadores ou quaisquer objetos ou exibe os objetos existentes, o painel **Anexos** é exibido por padrão na respectiva exibição de formulário. Você pode clicar no ícone **Anexos** no menu contextual à direita ou ir para **Preferências** > **Espaços** e desabilite **Mostrar a barra lateral**. Para obter mais informações, consulte Configuração das preferências do Espaço do Next Experience . 2. **Informações**: adicione informações adicionais relacionadas aos observáveis ou indicadores associados a esse objeto.
N/D	**Pesquisar no Navegador**	Use esta função de pesquisa para pesquisar vários objetos na biblioteca de informações sobre ameaças (TI). Por exemplo, você pode pesquisar todos os registros de observáveis no módulo de biblioteca de TI.
N/D	**Pesquisar na biblioteca de inteligência contra ameaças**	Use esta função de pesquisa para pesquisar os registros de origem em várias origens com base em seus critérios de pesquisa. Os resultados serão exibidos em uma guia separada **Resultados** de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

TISC exibição de formulário de objetos da biblioteca

Ordem	Menu/Guia	Descrição
		Por exemplo, para um endereço IP 104.227.137.35, se você precisar pesquisar os registros, inserindo 104.*, a pesquisa restringirá os registros e exibirá os registros que contêm o endereço IP que começa com 104 na guia separada **Resultados** da pesquisa. • Você também pode modificar as palavras-chave de pesquisa existentes nos critérios de pesquisa na mesma página de resultados de pesquisa sem voltar para a página Biblioteca de ameaças. • Da mesma forma, você também pode pesquisar com base no nome e na descrição de qualquer registro específico. • Depois que os registros forem filtrados e listados, você poderá clicar na exibição de lista para acessar o respectivo registro em uma nova guia.

Tradução automática

Repositório de biblioteca de TISC

O repositório IoC contém objetos STIX, cada um desses objetos contém uma informação específica.

Observáveis

Os observáveis representam propriedades com monitoramento de estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes .

A seguir estão os tipos de observáveis disponíveis na aplicação:

- Artefato
- Número do AS
- Diretório
- Nome do domínio

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço de e-mail
- Mensagem do e-mail
- Assunto do E-mail
- Arquivo
- Endereço IPv4
- CIDR de IPv4
- Endereço de IPv6
- CIDR de IPv6
- Endereço MAC
- Hash MD5
- Nome de Mutex
- Rede
- Outro observável
- Processo
- Hash SHA1
- Hash SHA256
- Hash SHA512
- Software
- URL
- Conta de usuário
- Chave de Registro do Windows
- Certificado X.509

Definir um observável

Os observáveis podem ser recuperados da ingestão de feed programada ou do assistente de importação. No entanto, você pode criar observáveis, conforme necessário.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Clique em **Nova**.
3. Selecione o **tipo de observável**.
   O formulário de registro Criar novo observável é exibido.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

4. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Sempre que você cria um novo observável ou exibe os observáveis existentes, o painel **Anexos** é exibido por padrão na exibição do formulário. Você pode clicar no ícone Anexos no menu contextual à direita ou ir para **Preferências** > **Espaços** e desabilite **Mostrar a barra lateral**. Para obter mais informações, consulte Configuração das preferências do Espaço do Next Experience .

Seção de detalhes

Campo	Descrição
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável.
Descrição	Descrição do registro do observável.
Autor	Insira o nome.
Tipo	O tipo de classificação de observável, como endereço IP, nome de domínio, artefato, diretório, arquivo ou hash. Por padrão, isso é exibido quando você seleciona o novo registro.
Status	O status ativo ou inativo do observável.
Fases de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
TLP	Valor exclusivo que indica a configuração de confidencialidade dos dados por TLP.
Reputação	Especifica a reputação mal-intencionada do observável.
Status	Insira o status do observável, se ativo ou inativo.
Pontuação de ameaça	Indica a pontuação de ameaça para esse observável.
Tempo de expiração	Especifica o tempo de expiração do registro do observável.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Confiança	Insira a confiança para este registro de observável. A propriedade de confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Impedir atualizações do sistema	Definir este sinalizador como verdadeiro impedirá que o sistema substitua valores de campos no registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
É falso-positivo	Um sinalizador booliano que indica se o observável foi identificado como falso-positivo.

Atributos

Campo	Descrição
Resolve para	Especifica uma lista de referências a um ou mais endereços IP ou nomes de domínio para os quais o nome de domínio é resolvido.
É FQDN	Um nome de domínio totalmente qualificado (FQDN) é o endereço completo de um host ou computador da Internet. Ele fornece sua localização exata no sistema de nomes de domínio (DNS), especificando o nome do host, o nome do domínio e o domínio de nível superior (TLD).

Informações adicionais

Campo	Descrição
Nível de ameaça	Indica o nível de ameaça do registro do observável.
Visto pela primeira vez	A hora em que este registro observável foi visto pela primeira vez executando atividades mal-intencionadas.
Gravidade da ameaça	Indica a gravidade da ameaça do registro do observável.
Visto pela última vez	A hora em que este registro de observável foi visto pela última vez executando atividades mal-intencionadas.
Categorias de uso	Categorias nas quais o observável se enquadra, como botnet ou phishing.
Fases de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
Contexto adicional	Adicione qualquer contexto adicional.
Origens	Especifica a origem da ameaça a partir da qual este registro é criado.

Importante: **Pontuação relatada pela origem**: este campo contém o valor agregado das pontuações de ameaça relatadas pelas origens das quais o observável é ingerido. Para ver este campo no formulário de registro do observável, você deve adicioná-lo manualmente, pois ele não está disponível por padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributos

Campo	Descrição
Resolve para	Especifica uma lista de referências a um ou mais endereços IP ou nomes de domínio para os quais o nome de domínio é resolvido.
É FQDN	Um nome de domínio totalmente qualificado (FQDN) é o endereço completo de um host ou computador da Internet. Ele fornece sua localização exata no sistema de nomes de domínio (DNS), especificando o nome do host, o nome do domínio e o domínio de nível superior (TLD).

Nota: Os atributos**Resolve para** e **É FQDN** são aplicáveis somente ao tipo **Nome de domínio** de observáveis.

Atributos de tipo de observável

Nome de Atributo	Tipos de Atributo
Artefato	◦ Chave de descriptografia ◦ Algoritmo de criptografia ◦ Hash MD5 ◦ Tipo de MIME ◦ Hash SHA1 ◦ Hash SHA256 ◦ Hash SHA512 ◦ URL
Número do AS	◦ Nome ◦ RIR
Diretório	◦ Hora de criação do diretório ◦ Hora do último acesso ao diretório ◦ Hora da última modificação do diretório ◦ Caminho codificado
Nome do domínio	◦ É FQDN ◦ Resolve para
Endereço de e-mail	◦ Nome de exibição ◦ Corpo do E-mail ◦ Destinatários de e-mail Cco ◦ Destinatários de e-mail Cc ◦ Destinatários de e-mail Para

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
	◦ Remetente do e-mail ◦ Assunto do E-mail ◦ Data de envio
Arquivo	◦ Informações adicionais ◦ Nome do arquivo codificado ◦ Hora de criação do arquivo ◦ Hora do último acesso ao arquivo ◦ Hora da última modificação do arquivo ◦ Número Mágico do Nome do Arquivo ◦ Hash MD5 ◦ Tipo de MIME ◦ Hash SHA1 ◦ Hash SHA256 ◦ Hash SHA512
Endereço IPv4	◦ Número do AS ◦ Endereço MAC
CIDR de IPv4	◦ Número do AS ◦ Endereço MAC
Endereço de IPv6	◦ Número do AS ◦ Endereço MAC
CIDR de IPv6	◦ Número do AS ◦ Endereço MAC
Rede	◦ Bytes de destino ◦ Contagem de pacotes de destino ◦ Porta de Destino ◦ Hora de término ◦ Tamanho do corpo da mensagem HTTP ◦ Cabeçalho da solicitação HTTP ◦ Método de solicitação HTTP ◦ Valor da solicitação HTTP ◦ Versão da solicitação HTTP ◦ Byte de código ICMP ◦ Byte de tipo ICMP ◦ Está ativo na rede ◦ É bloqueio de soquete

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
	◦ É escuta de soquete ◦ Protocolos de rede ◦ Família de endereços de soquete ◦ Descritor de soquete ◦ Identificador de soquete ◦ Opções de soquete ◦ Contagem de bytes de origem do tipo de soquete ◦ Contagem de pacotes de origem ◦ Porta de Origem ◦ Hora de início ◦ Sinalizadores de destino de TCP ◦ Sinalizadores de origem de TCP
Processo	◦ ASLR habilitado ◦ Linha de comando ◦ Diretório de trabalho atual (CWD) ◦ DEP habilitada ◦ Variáveis do Ambiente ◦ Está oculto ◦ SID do responsável ◦ ID do Processo ◦ Prioridade ◦ Hora de criação do processo ◦ Descrições dos serviços ◦ Nome de exibição do serviço ◦ Nome do Grupo de serviço ◦ Nome do serviço ◦ Tipo de início do serviço ◦ Tipo de serviço de status do serviço ◦ Informação de inicialização ◦ Nível de integridade do Windows ◦ Título da janela
Software	◦ Enumeração de plataforma comum (CPE) ◦ Idiomas compatíveis ◦ Identificação de software (SWID) ◦ Versão do fornecedor

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
Conta de usuário	◦ Hora de criação da conta ◦ Hora de vencimento da conta ◦ Login da conta ◦ Tipo de Conta ◦ Informações adicionais ◦ Pode escalar privilégios ◦ Hora da última mudança de credenciais ◦ Nome para exibição ◦ Hora do primeiro login ◦ É conta desabilitada ◦ É privilegiado ◦ É conta de serviço ◦ Hora do último login ◦ ID do Usuário
Chave de Registro do Windows	◦ Chave modificada ◦ Valor do registro de tempo ◦ Contagem de subchaves
Certificado X.509	◦ Informações adicionais ◦ Identificador de chave de autoridade ◦ Restrições básicas ◦ Políticas de certificação ◦ Pontos de distribuição de CRL ◦ Uso de chave estendido ◦ Inibir qualquer política ◦ Emissor ◦ Nome alternativo do emissor ◦ É autoassinado ◦ Uso de chave ◦ Restrições de nome ◦ Restrições de política ◦ Mapeamentos de políticas ◦ Uso de chave privada válido a partir de ◦ Uso de chave privada válido até ◦ Algoritmo de assinatura ◦ Assunto ◦ Nome Alternativo do Assunto ◦ Atributos do diretório de assunto

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de Atributo	Tipos de Atributo
	◦ Identificador de chave do assunto ◦ Algoritmo de chave pública do assunto ◦ Expoente de chave pública do assunto ◦ Módulo de chave pública do assunto ◦ Válido de ◦ Válido Até ◦ Versão

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um registro de observável.

5. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
6. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um observável.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione a taxonomia associada a um observável.
Adicionar valores de taxonomia	Adicione os valores de taxonomia associados a um observável.

Registros de Origem

Campo	Descrição
Os detalhes dos registros de origem de um observável são exibidos, se houver.	

O que Fazer Depois

A tabela a seguir lista os registros relacionados aos observáveis:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Lista relacionada	Descrição
Observável	Lista de observáveis relacionados a este observável. **Nota:** Esta seção também contém os possíveis relacionamentos entre dois observáveis. Para obter mais informações, consulte Confirmar possível relacionamento observável-observável e consulte Definir relacionamentos observável-observável para obter os relacionamentos confirmados entre os dois observáveis.
Indicadores	Lista de indicadores relacionados a este observável.
Padrões de ataque	Lista de padrões de ataque relacionados a este observável.
Campanhas	Liste as campanhas relacionadas a este observável.
Infraestrutura	Liste a infraestrutura, como sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados que estejam relacionados a este observável.
Conjuntos de intrusão	Liste os conjuntos de intrusão, como um conjunto de comportamentos adversários e recursos com propriedades comuns que estão relacionados a este observável.
Malware	Liste os registros de origem de malware que estão relacionados a este observável.
Agentes da ameaça	Liste os agentes de ameaça que estão relacionados a este observável.
Eventos de ameaça	Liste os eventos de ameaça relacionados a este observável.
Vulnerabilidades	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente relacionado a este observável.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Além disso, na seção **Registros relacionados**, você pode confirmar os relacionamentos entre dois observáveis usando a seção **Possíveis relacionamentos** disponível na exibição de formulário de **observáveis**. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
3. Você pode adicionar observáveis a casos. Para obter mais informações, consulte Adicionar ao caso.
4. Você também pode executar ações de aprimoramento para observáveis. Para obter mais informações, consulte Executar ações de aprimoramento em um caso.

Registros de origem de observáveis

Os registros de origem contribuem para um registro agregado conforme exibido na exibição de formulário. Esses registros de origem são criados automaticamente a partir de feeds ou criados manualmente pelo usuário.

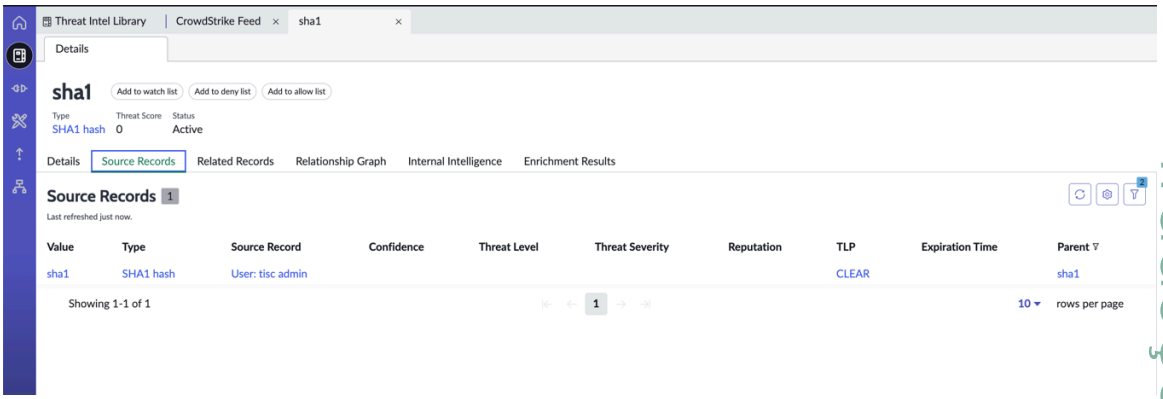
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Selecione um ou mais observáveis.
5. Vá para **Registros de origem**.
   Os registros de origem para um registro agregado são exibidos.



6. Exibir os registros.

Vincular registros relacionados a informações sobre ameaças

Vincule os registros relacionados aos objetos de inteligência de ameaças correspondentes.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro de observável como exemplo.
3. Acesse a seção **Registros relacionados**.
4. Selecione qualquer registro relacionado.
5. Clique em **Vincular**.
   A caixa de diálogo Vincular objetos é exibida.
6. Selecione os objetos na lista e clique no botão **Vincular**.
   Os objetos associados a um registro de observável serão vinculados e exibidos na exibição de lista de Registros relacionados.
7. Clique em **Salvar**.
   Clique no botão **Desvincular** para desvincular os objetos

Buscar dados de observáveis

Buscar os dados de registros relacionados a observáveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para **Observáveis**.
   Os observáveis relacionados associados a esse objeto selecionado são exibidos.
4. Selecione qualquer registro de observável.
   Se os observáveis fornecidos tiverem CVEs associados a ele, você poderá buscar seus dados vulneráveis relacionados automaticamente usando o botão fornecido, e esses registros associados serão exibidos na seção Contexto de negócios das vulnerabilidades.
5. Ir para **Inteligência interna** > **Entradas vulneráveis**.
   Os registros de CVEs associados aos observáveis são exibidos.
6. Selecione qualquer CVE e clique no botão **Buscar dados relacionados à vulnerabilidade**.

Nota:

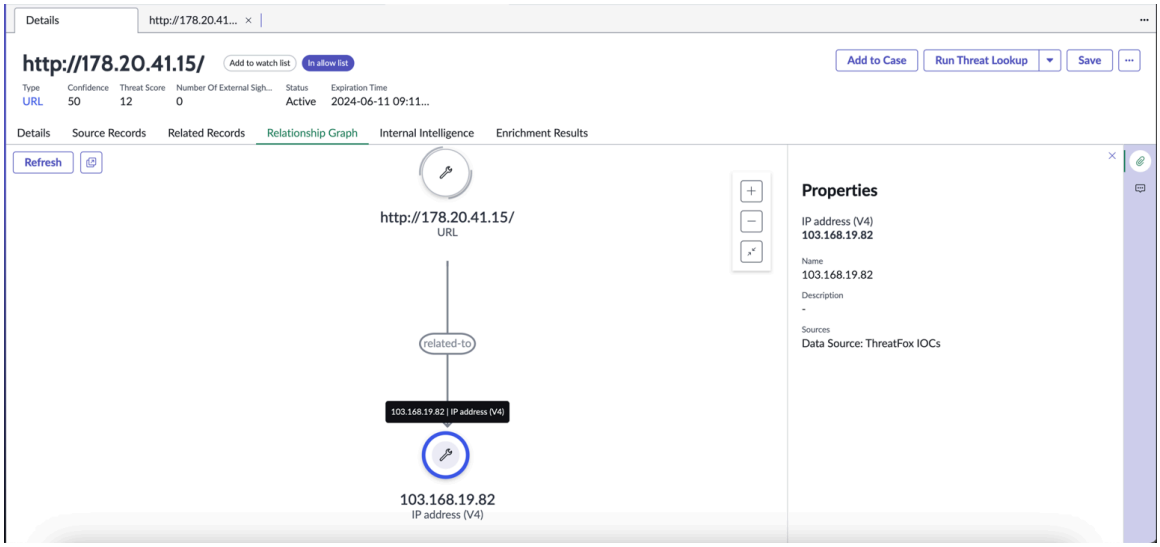
- Uma mensagem informativa exibe que Este objeto de vulnerabilidade específico não tem entradas vulneráveis associadas a ele. Você deve associar os objetos às entradas vulneráveis para buscar os dados. Para obter mais informações, consulte Buscar dados de vulnerabilidade sobre como vincular os registros e executar o trabalho agendado para buscar os dados. e para obter mais informações sobre trabalhos agendados, consulte Trabalhos agendados .
- Este botão acionará um trabalho agendado em segundo plano e os detalhes de início e execução do trabalho serão exibidos na seção Fluxo de atividades. Por exemplo, quando o trabalho é acionado, o fluxo de atividades exibe uma atividade que começou a buscar dados associados às entradas vulneráveis. O trabalho agendado em segundo plano verificará continuamente se há observáveis que tenham alguma entrada vulnerável associada ao observável e será executado automaticamente. Este trabalho agendado será executado a cada uma hora. no caso, se os registros não forem obtidos, você poderá vincular manualmente os registros e buscar os dados.

Exibir detalhes no Visualizador

Usando o Visualizador, você pode exibir os relacionamentos entre objetos, observáveis e indicadores, o que fornece contexto para você investigar mais. O Visualizador usa cores e ícones para ilustrar várias informações sobre os objetos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode fazer o seguinte:

- Aumente o zoom em qualquer objeto, ajuste-o à tela, arraste os nós ou fixe-os para enfocar um relacionamento específico.
- Clique em qualquer objeto para abrir o painel de detalhes. No painel de detalhes, você pode obter mais informações associadas ao objeto. Você pode exibir as propriedades do nó, como Objeto, Nome do objeto, Descrição e Origens. Por padrão, a seção de detalhes de cada nó do gráfico não é exibida e você precisa clicar em cada nó do gráfico para exibir os detalhes do nó selecionado.

  Nota: O Visualizador está disponível para todos os objetos de domínio STIX (SDOs), exceto os objetos de relatório e dados observados. Clique no botão Atualizar para atualizar o visualizador.

- Você também pode clicar no ícone pop-out para exibir o gráfico em uma janela muito maior.

Como trabalhar com registros de inteligência interna

Use este recurso para trabalhar com os dados de inteligência interna que são coletados do Configuration Database Management System (CMDB) na Central de segurança de inteligência contra ameaças.

Exibir registros de inteligência interna

Exiba os registros de inteligência interna coletados do CMDB, Security Incident Response (SIR), Vulnerability Response (VR) desses registros.

Antes de Iniciar

A seção Inteligência interna fornece o contexto de outras aplicações na plataforma, como SIR, VR e CMDB, para fornecer uma perspectiva mais ampla da ameaça aos analistas.

Função necessária: sn_sec_tisc.analyst

Nota: A guia Inteligência interna só está visível para observáveis e objetos de vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro de observável.
3. Acesse a guia **Inteligência interna**.
   A seção Inteligência interna é composta por três subseções, como Resposta a incidentes de segurança, Contexto de negócios e Resposta a vulnerabilidades.

   Nota: Você deve ter as respectivas aplicações instaladas em sua instância para que essas seções sejam listadas na guia **Inteligência interna**.

   a. **Security Incident Response**: exibe todos os incidentes vinculados aos observáveis associados e itens de vulnerabilidade.

   Nota: Os valores dos observáveis devem corresponder entre o incidente SIR e também dentro do TISC. Somente então os observáveis ou indicadores associados são listados na seção Resposta a incidentes de segurança. Você também pode vincular e desvincular os registros pesquisando os registros nos sistemas de origem. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.

   - Selecione qualquer registro para navegar e exibir os detalhes no sistema de origem. Por exemplo, Observáveis associados no Security Incident Response para buscar os registros de observáveis associados.
   - Como parte da versão atual, a seguir estão os dados de inteligência que você pode buscar nos registros de origem (SIR):
     - Observáveis Associados
     - Itens de vulnerabilidade

   b. **Contexto de negócios**: exibe os usuários afetados e quaisquer outros itens de configuração. Como parte da versão atual, a seguir estão os dados de inteligência que você pode buscar nos registros de origem (contexto de negócios):
   - Itens de configuração
   - Serviços afetados
   - Ativos afetados

   c. **Resposta a vulnerabilidades**: exibe os dados de inteligência de vulnerabilidades.

   Entradas de vulnerabilidade: esta opção corresponde às vulnerabilidades e busca os registros relacionados.

Executar ações de aprimoramento a partir do observável

Use esta seção para entender como as ações de aprimoramento são realizadas em observáveis e outros objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Ir para **Observáveis** > **Todos os observáveis**.
4. Clique em qualquer ação de aprimoramento no botão de divisão.
5. Selecione as implementações disponíveis.
6. Clique em **Enviar**.
   Por exemplo, Executar pesquisa de ameaças. A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida informando que a execução de aprimoramento do observável foi iniciada no(s) observável(is) selecionado(s). Os resultados estarão disponíveis na página de detalhes dos respectivos observáveis quando a execução for concluída.

Nota: Depois que a execução é iniciada ou concluída, uma anotação de trabalho é publicada no fluxo de atividades da exibição do formulário.

Adicionar ao caso

Adicione observáveis, indicadores ou outros objetos ao caso.

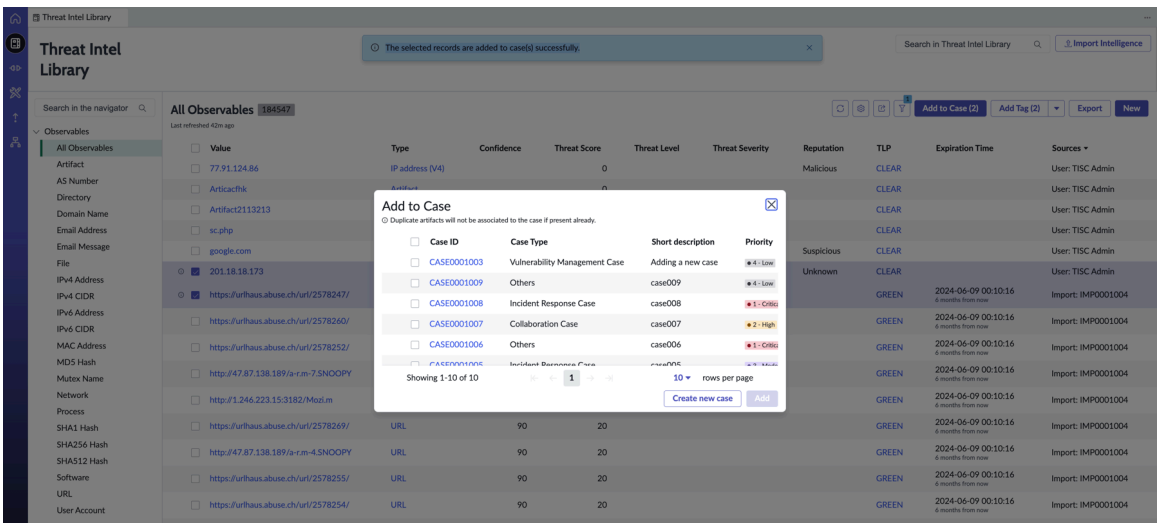
Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

A seguir está o procedimento que mostra como adicionar um caso a um registro de observável.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione o(s) observável(is).
3. Clique no botão **Adicionar ao caso**.
   Exibe somente os casos em que o registro ainda não está associado.



4. Verifique se deseja adicionar o registro aos casos existentes e, em caso afirmativo, selecione o caso existente. Caso contrário, clique em **Criar novo caso**.
   Crie um novo caso inserindo as seguintes informações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar novo caso

Campo	Descrição
ID do caso	Um identificador exclusivo para o caso. Este é o ID gerado pelo sistema.
Descrição resumida	Resumo da solicitação ou problema que está sendo investigado ou uma descrição resumida.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado. As opções possíveis para a investigação são: ◦ Busca de ameaças ◦ Solicitação de informações ◦ Caso de gestão de vulnerabilidade ◦ Caso de conformidade ◦ Caso de resposta do incidente ◦ Caso de colaboração ◦ Outros
Prioridade	Uma avaliação da gravidade da solicitação ou do problema.
Grupo de atribuição	O grupo atribuído responsável por trabalhar no caso.
Atribuído a	O analista responsável por trabalhar em um caso.

5. Clique em **Criar** se estiver criando um novo caso.

   Nota: O novo caso é adicionado à lista de casos existentes.

6. Selecione os casos recém-adicionados.
7. Clique em **Adicionar**.
   Uma mensagem informativa é exibida informando que os registros selecionados foram adicionados ao(s) caso(s) com sucesso.

Executar operações de aprimoramento no TISC

A tabela a seguir descreve as interações envolvidas na execução de diferentes operações de aprimoramento do TISC.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Telas do modal de TISC

Capacidade	Interações de estruturas de UX	Integrações compatíveis
Executar pesquisa de ameaças	Na tela 1 – Selecione a(s) implementação(ões) e envie. Não há entradas comuns ou entradas específicas de implementação aplicáveis a Executar pesquisa de ameaças.	• Total de vírus • Crowd-Strike Falcon Intelligence
Executar Pesquisa de detecções	Tela 1 – Selecionar implementações e Tela 2 – Entradas comuns são aplicáveis. A pesquisa de detecções usa a frequência de data e hora como entradas comuns em várias implementações do Splunk e outras integrações.	• Pesquisa elástica • Detecção do Splunk
Executar Aprimoramento Observável	Somente tela 1 – Selecionar implementações. Não há entradas comuns ou entradas específicas de implementação aplicáveis a Executar aprimoramento de observável.	• WHOIS • Shodan

Tradução automática

Executar Pesquisa de ameaças

Selecione uma ou mais implementações conforme aplicável para executar a pesquisa de ameaças em observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

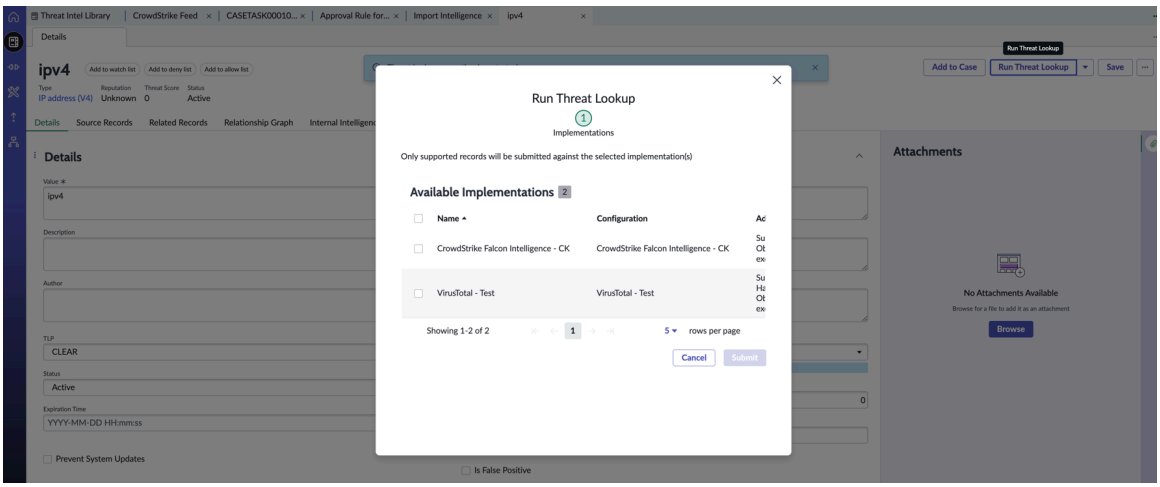
Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique **em Executar pesquisa de ameaças**.
   A tela Executar modal **de implementação de seleção** de pesquisa de ameaças é exibida.

> **Nota:** Executar pesquisa de ameaças realiza as pesquisas de inteligência contra ameaças para determinar se os observáveis estão associados a ameaças conhecidas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione as implementações necessárias na lista.



7. Clique em **Enviar**.
   A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida informando que a execução da pesquisa de ameaças foi iniciada.

Nota:

- Depois que a execução é iniciada ou concluída, uma anotação de trabalho é publicada no fluxo de atividades da exibição do formulário.
- Os resultados de aprimoramento enviados do espaço SIR podem ser encontrados na guia **Resultados** de aprimoramento da página de detalhes de observáveis correspondente no espaço do TISC.
- Os resultados de aprimoramento enviados do espaço SIR podem ser identificados usando o campo **Origem** da tabela de resultados de aprimoramento.

Executar Pesquisa de detecções

Execute a integração relacionada Executar pesquisa de detecções.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Para executar esta ação, selecione a implementação e adicione entradas de tempo de execução comuns que se apliquem a todas as implementações selecionadas, conforme aplicável.

Procedimento

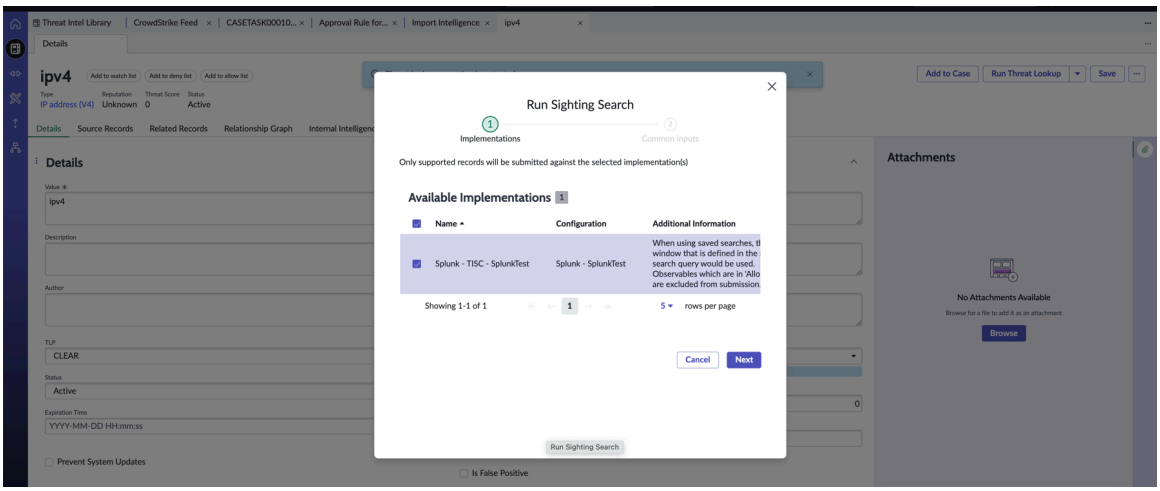
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique **em Executar pesquisa de detecções**.
   A tela do modal **Executar implementação de seleção de** pesquisa de detecções é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Executar pesquisa de detecções realiza as pesquisas de inteligência contra ameaças para determinar se os observáveis estão associados a ameaças conhecidas.

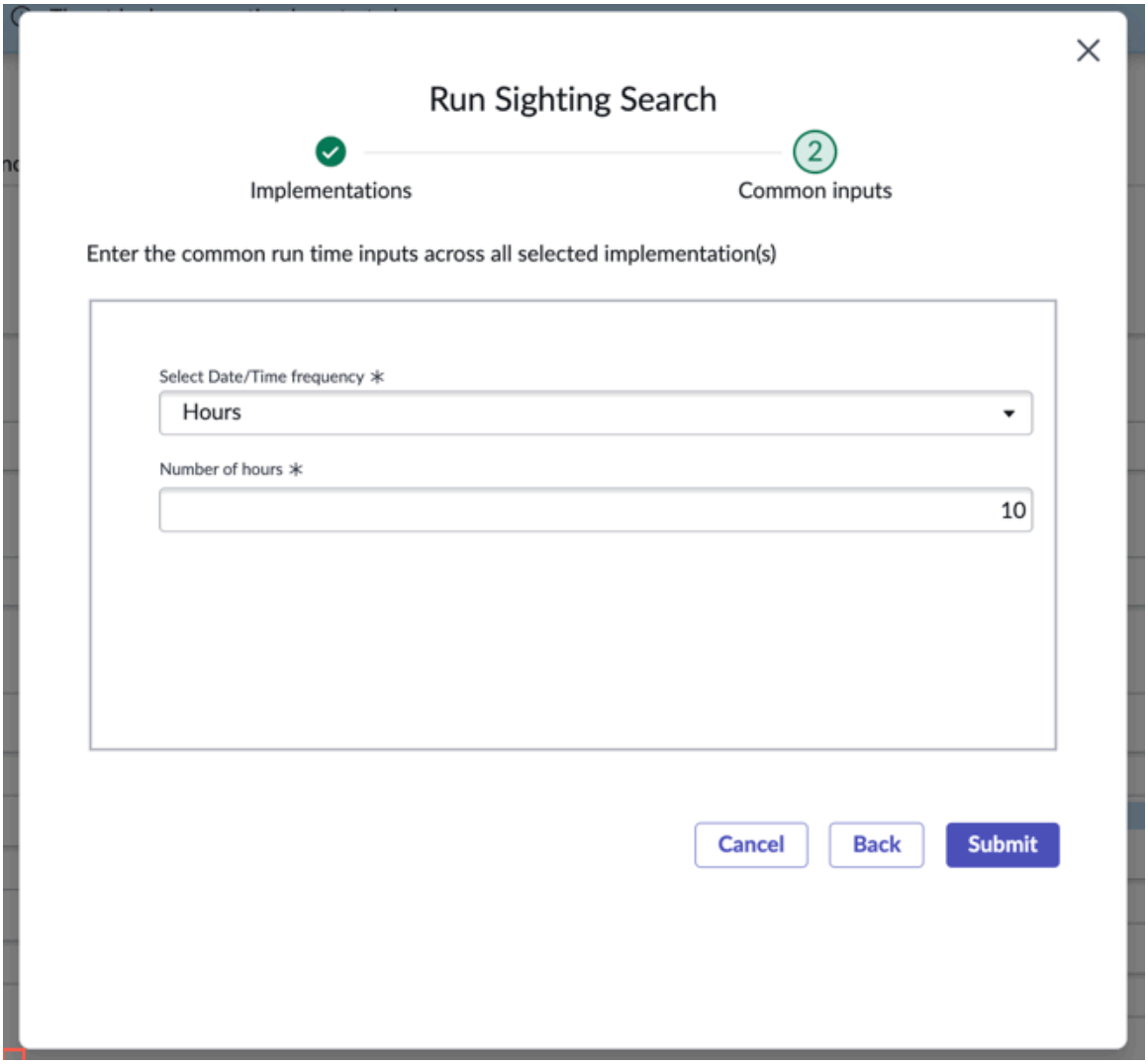
6. Selecione as implementações necessárias na lista.



7. Clique em **Avançar**.
8. Selecione o valor de entrada de tempo de execução comum, como Selecionar frequência de data/hora e Número de horas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Clique em **Enviar**.
   A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida informando que a execução Executar pesquisa de detecções foi iniciada.

Nota:

- Depois que a execução é iniciada ou concluída, uma anotação de trabalho é publicada no fluxo de atividades da exibição do formulário.
- Os resultados de aprimoramento enviados do espaço SIR podem ser encontrados na guia **Resultados** de aprimoramento da página de detalhes de observáveis correspondente no espaço do TISC.
- Os resultados de aprimoramento enviados do espaço SIR podem ser identificados usando o campo **Origem** da tabela de resultados de aprimoramento.

Executar Aprimoramento Observável

Selecione uma ou mais implementações conforme aplicável para executar a pesquisa de ameaças em observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Tradução automática

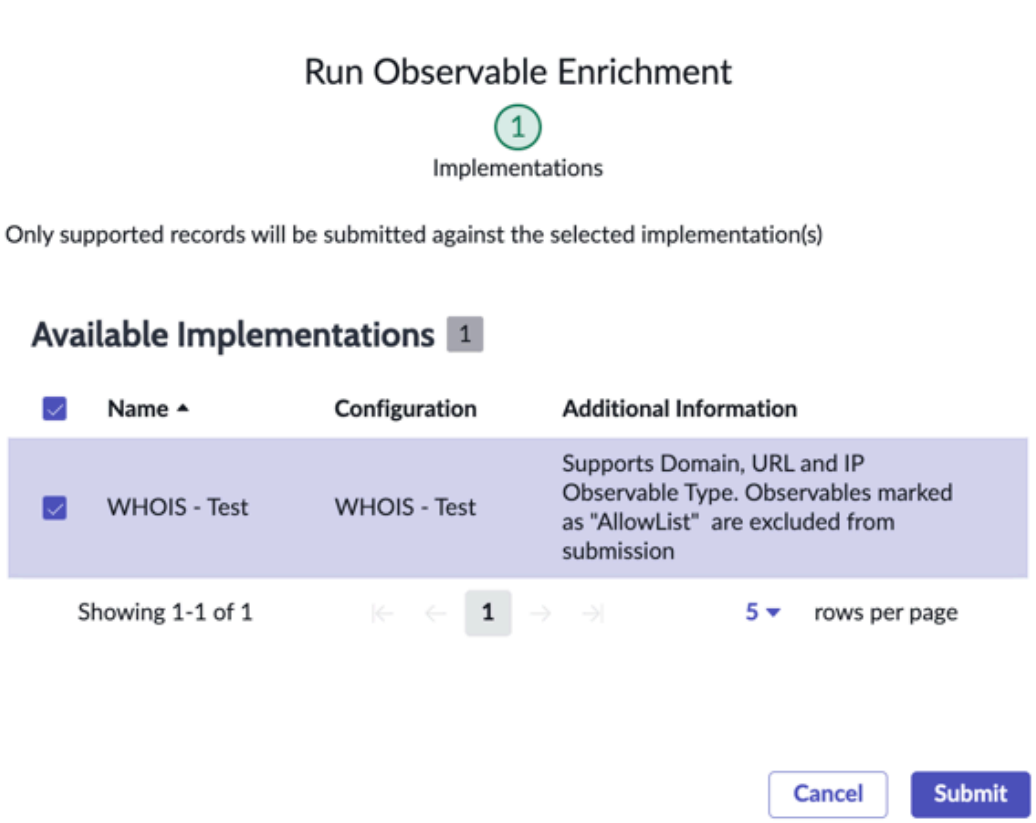
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Workbench do analista de ameaças**.
3. Ir para **Observáveis** > **Todos os observáveis**.
4. Abra qualquer registro observável.
5. Clique **em Executar aprimoramento de observável**.
   A tela do modal **Executar implementações de seleção de** aprimoramento de observável é exibida.

   Nota: Somente registros compatíveis serão enviados em relação às implementações selecionadas

6. Selecione as implementações necessárias (por exemplo, WHOIS) na lista.



7. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ação de aprimoramento selecionada será executada e uma mensagem informativa será exibida informando que a execução da pesquisa de ameaças foi iniciada.

Nota:

- Depois que a execução é iniciada ou concluída, uma anotação de trabalho é publicada no fluxo de atividades da exibição do formulário.
- Os resultados de aprimoramento enviados do espaço SIR podem ser encontrados na guia **Resultados** de aprimoramento da página de detalhes de observáveis correspondente no espaço do TISC.
- Os resultados de aprimoramento enviados do espaço SIR podem ser identificados usando o campo **Origem** da tabela de resultados de aprimoramento.

Exibir resultados de enriquecimento

Exiba observáveis, indicadores e vários resultados de aprimoramento de objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.admin

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Observáveis** > **Todos os observáveis**.
2. Selecione qualquer registro de observável.
3. Vá para a guia **Resultados** de aprimoramento.
   Os Resultados de aprimoramento exibem os resultados de aprimoramento das integrações de TISC.

Nome de enriquecimento	Descrição
Resultados da Pesquisa de ameaças	Lista todos os resultados de pesquisa de ameaças associados a um observável.
Detecções	Lista todas as vistas associadas a um observável.
Resultados de enriquecimento observável	Lista todos os resultados de aprimoramento de observável associados a um observável.

Indicadores

Indicadores são artefatos observados em uma rede ou sistema operacional que provavelmente indicam uma invasão. IoCs típicos são assinaturas de vírus e endereços IP, hashes MD5 de arquivos de malware ou URLs ou nomes de domínio.

Definir um indicador

Defina um indicador.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **Indicadores**.
2. Selecione **Indicador**.
3. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

4. No formulário, preencha os campos.

Seção de detalhes

Campo	Descrição
ID	ID exclusivo do indicador.
Descrição	Descrição do indicador.
Nome	Nome do indicador.
Padrão	O padrão de detecção para este indicador pode ser expresso como um padrão STIX.
Tipo de Padrão	A linguagem padrão usada neste indicador.
Versão do padrão	A versão da linguagem de padrões usada para os dados na propriedade de padrão que deve corresponder ao tipo de dados de padrão incluídos na propriedade de padrão.
Válido de	O tempo a partir do qual este indicador é considerado um indicador válido dos comportamentos que ele está relacionado ou representa.
Válido Até	O tempo após o qual este indicador não deve mais ser considerado um indicador válido dos comportamentos aos quais está relacionado ou representa.
Classificação IOC	A classificação IOC dos indicadores.
Tipos de Indicador	Indica as várias categorias do indicador.
Status	Indica o status dos indicadores.
Plataformas	Define as plataformas para as quais este indicador é aplicável.
TLP	Valor exclusivo que indica a configuração de confidencialidade dos dados por TLP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Fases de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
Confiança	Insira a confiança para este registro de indicador. A propriedade de confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Nível de ameaça	Indica o nível de ameaça do registro do indicador.
Tempo de expiração	Especifica o tempo de expiração do registro do indicador.
Gravidade da ameaça	Indica a gravidade da ameaça do registro do indicador.
Categorias de uso	Categorias nas quais o observável se enquadra, como botnet ou phishing.
Visto pela primeira vez	A hora em que este registro do indicador foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este registro de indicador foi visto pela última vez executando atividades mal-intencionadas.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um indicador.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este indicador.
Versão de especificação	A versão da especificação STIX usada para representar o indicador. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação	Especifica a hora em que o indicador é criado no sistema.
Atualizado	Especifica a hora em que o indicador é atualizado no sistema.
Extensões	Indica as extensões do indicador.
Processando Status	Representa o status de processamento deste indicador.

5. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
6. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um indicador.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione a taxonomia associada a um indicador.
Adicionar valores de taxonomia	Adicione os valores de taxonomia associados a um indicador.

Registros de Origem

Campo	Descrição
Os detalhes dos registros de origem de um indicador são exibidos, se houver.	

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos indicadores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Lista relacionada	Descrição
Referências de indicadores	Lista de referências externas que descreve este indicador.
Observáveis	Lista os registros de observáveis relacionados a este indicador.
Indicadores	Lista os indicadores relacionados a este indicador. **Nota:** Esta seção também contém os possíveis relacionamentos entre dois indicadores. Para obter mais informações, consulte Confirmar possíveis relacionamentos entre indicador e indicadore consulte Definir relacionamentos indicador-indicador para obter os relacionamentos confirmados entre os dois observáveis.
Itens de configuração	Lista os itens de configuração relacionados a este indicador.
Padrões de ataque	Lista a origem dos Padrões de ataque que descreve os métodos que os adversários usam para comprometer os destinos relacionados a este indicador.
Campanhas	Lista a origem das campanhas que descreve um conjunto de atividades mal-intencionadas ou ataques que ocorrem ao longo do tempo em relação a um conjunto específico de metas relacionadas a este indicador.
Detecções e mitigações	Lista as detecções e mitigações relacionadas a este indicador.
Identidades	Lista as identidades relacionadas a este indicador.
Infraestrutura	Lista a origem da infraestrutura que descreve todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque relacionado a este indicador.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns que estão relacionados a este indicador.
Locais	Lista os locais geográficos associados ao objeto.
Malware	Lista os registros de origem de malware que estão relacionados a este indicador.
Definições de marcação	Lista as definições de marcação associadas a este objeto.
Detecções	Lista os registros de origem de detecções associados a este objeto.
Agentes da ameaça	Lista as mudanças associadas ao observável.
Eventos de ameaça	Lista os observáveis relacionados que foram identificados pela origem da ameaça.
Ferramenta	Lista a ferramenta associada a este objeto.
Vulnerabilidades	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Além disso, na seção **Registros relacionados**, você pode confirmar os relacionamentos entre dois observáveis usando a seção **Relacionamentos potenciais** disponível na exibição do formulário de **Indicadores**. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
3. Você pode adicionar indicadores a casos. Para obter mais informações, consulte Adicionar ao caso.

Padrões de ataque

Padrões de ataque são um tipo de Táticas, técnicas e procedimentos (TTPs) que descrevem os métodos que os adversários tentam para comprometer os alvos.

Padrões de ataque são usados para ajudar a categorizar os ataques. Eles generalizam ataques específicos para os padrões que seguem e fornecem informações detalhadas sobre como os ataques são realizados.

Por exemplo, o Spear Phishing é um tipo comum de ataque em que um invasor envia uma mensagem de e-mail cuidadosamente criada para uma parte com a intenção de fazer com que ela clique em um link ou abra um anexo para entregar malware. Os Padrões de ataque são mais específicos, como Spear Phishing por um agente de ameaça específico (exemplo - que o destino venceu uma contestação) também pode ser um padrão de ataque.

Definir um padrão de ataque

Defina um padrão de ataque para ajudar os analistas de ameaças a categorizar os ataques.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para **Padrão de ataque**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de detalhes do padrão de ataque

Campo	Descrição
ID	ID exclusivo para um padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome para este padrão de ataque.
Descrição	Insira uma descrição para um padrão de ataque.
Aliases	Nomes alternativos para identificar este padrão de ataque.
Fase de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
Permissões necessárias	Selecione as permissões necessárias para este padrão de ataque.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este modo de padrão de ataque. A propriedade de confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Impedir atualizações do sistema	Definir este sinalizador como verdadeiro impedirá que o sistema substitua valores de campos no registro.

Importante: Depois de criar um novo registro de objeto, a caixa de seleção **Impedir atualizações do sistema** será exibida.

Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto, padrão de ataque. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação	Especifica a hora em que o registro é criado no sistema.
Atualizado	Especifica a hora em que o registro é modificado no sistema.
Extensões	Indica as extensões do padrão de ataque.
Processando Status	Representa o status de processamento deste objeto, padrão de ataque.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um observável.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a um padrão de ataque.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a um padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao padrão de ataque.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Campanha

A campanha é definida como um agrupamento de comportamentos adversários que descreve um conjunto de atividades ou ataques mal-intencionados, às vezes chamados de vagas, que ocorrem durante um período de tempo contra um conjunto específico de metas.

Definir campanha

Defina uma campanha para agrupar comportamentos adversários.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para o objeto de **campanha**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de campanha

Campo	Descrição
ID	ID exclusivo para um comportamento adversário.
Nome	Insira um nome para um comportamento adversário.
Descrição	Insira uma descrição para esta campanha.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Objetivo	O objetivo primário, objetivo, resultado desejado ou efeito pretendido da campanha. O que o agente da ameaça ou o conjunto de intrusão espera realizar com esta campanha.
Aliases	Nomes alternativos a serem identificados para esta campanha.
TLP	O Protocolo de semáforo (TLP) indica as informações confidenciais compartilhadas com o público correto. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade para este padrão de ataque.
Confiança	Insira a confiança para esta campanha.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para uma campanha.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta campanha.
Visto pela primeira vez	A hora em que este objeto foi visto pela primeira vez executando um comportamento adversário.
Visto pela última vez	A hora em que este objeto foi visto pela última vez executando um comportamento adversário.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação	Especifica a data e a hora em que o objeto foi criado na origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Extensões	Indica as extensões do padrão de ataque.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Processando Status	Representa o status de processamento deste objeto, campanha.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a uma campanha.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a uma campanha.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados à campanha.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à campanha.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Identidades	Lista de identidades associadas a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de Marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Linha de ação

Um curso de ação é uma ação realizada para impedir um ataque ou para responder a um ataque que está em andamento.

O curso de ações descreve respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls). Também pode descrever ações de nível superior, como treinamento de funcionários ou mudanças de política.

Por exemplo, um curso de ação para atenuar uma vulnerabilidade pode descrever a aplicação do patch que a corrige.

Definir curso de ação

Defina um curso de ação para impedir um ataque ou responder a um ataque que está em andamento.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para o objeto **Curso de ação**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de detalhes do curso de ação

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Nome	Insira um nome descritivo para este curso de ação.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o curso de ação, incluindo potencialmente sua finalidade e suas principais características.
Ação	Para capturar cursos de ação estruturados ou automatizados.
TLP	O Protocolo de semáforo (TLP) indica as informações confidenciais compartilhadas com o público correto. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade para este padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para um curso de ação.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.

Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados a um observável.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a um padrão de ataque.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a um padrão de ataque.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao curso de ação.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de Marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Identidade

As identidades representam indivíduos, organizações ou grupos reais e classes de indivíduos, sistemas ou grupos. As identidades se aplicam ao STIX 2.x.

Um SDO de identidade pode capturar informações básicas de identificação, informações de contato e os setores aos quais a identidade pertence. A identidade representa alvos de ataques, fontes de informações, criadores de objetos e identidades de agentes de ameaças.

Definir identidades

Defina identidades que representam indivíduos, organizações ou grupos reais.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para Objeto de **identidade**.
4. Clique em **Nova**.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

Exibição de detalhes de identidade

Campo	Descrição
ID	ID exclusivo de uma identidade.
Nome	Insira um nome descritivo para esta identidade. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o curso de ação, incluindo potencialmente sua finalidade e suas principais características.
Funções	A lista de funções que esta Identidade executa.
Classe da identidade	O tipo de entidade que esta identidade descreve. Por exemplo, indivíduo ou organização.
Setores	A lista de setores do setor aos quais esta identidade pertence.
Informações de contato	As informações de contato, como e-mail e número de telefone, desta identidade.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para esta identidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para a identidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional relacionado a esta identidade.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à identidade.
Adicionar marcadores	Adicionar novos marcadores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada à identidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados à identidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Registros relacionados

Campo	Descrição
Referências externas	Lista referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de Marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Infraestrutura

O SDO de infraestrutura representa um tipo de táticas, técnicas e procedimentos (TTPs). Eles descrevem todos os sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque. A infraestrutura se aplica ao STIX 2.x.

Os elementos de um ataque são representados por outros SDOs ou SCOs. No entanto, o SDO de infraestrutura representa um grupo nomeado de dados que constitui a infraestrutura.

Exemplos de infraestrutura incluem servidores C2 usados em um ataque, um dispositivo ou um servidor que faz parte de uma defesa ou servidores de banco de dados direcionados por um ataque.

Definir infraestrutura

Defina uma infraestrutura que são quaisquer sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para Objeto de **infraestrutura**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes da infraestrutura

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Nome	Insira um nome descritivo para este curso de ação. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a infraestrutura, incluindo potencialmente sua finalidade, como ela está sendo usada, como ela se relaciona com outras atividades de inteligência capturadas em objetos relacionados e suas principais características.
Tipos de infraestrutura	Descreve a categorização da infraestrutura.
Aliases	Nomes alternativos para identificar esta infraestrutura.
Fases de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Visto pela primeira vez	A hora em que esta infraestrutura foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta infraestrutura foi vista pela última vez executando atividades mal-intencionadas.
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta infraestrutura.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta infraestrutura.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a hora em que o registro é criado na origem.
Atualizado	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

Tradução automática

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à infraestrutura.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta infraestrutura.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta infraestrutura.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Conjunto de intrusão

Um conjunto de intrusão é um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns. Um conjunto de intrusão geralmente envolve uma única organização. O conjunto de intrusão se aplica ao STIX 2.x.

Um conjunto de intrusão pode capturar várias campanhas ou outras atividades. Essas atividades compartilham atributos que indicam um agente de ameaça comumente conhecido ou desconhecido.

A nova atividade pode ser atribuída a um conjunto de intrusão, mesmo se os agentes da ameaça por trás do ataque não forem conhecidos. Os agentes da ameaça podem passar de oferecer suporte a um conjunto de intrusão para oferecer suporte a outro ou podem oferecer suporte a vários conjuntos de intrusão.

Um conjunto de intrusão é o pacote de ataque inteiro e pode ser usado por um longo período em várias campanhas para atingir potencialmente várias finalidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir conjunto de intrusão

Defina um conjunto de intrusão que é um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para **Conjunto de intrusão**.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de detalhes do conjunto de intrusão

Campo	Descrição
ID	ID exclusivo de um conjunto de intrusão.
Nome	Insira um nome descritivo para este conjunto de intrusão. Ao se referir a uma entidade específica (um indivíduo ou organização), esta propriedade deve conter o nome canônico da entidade específica.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Nomes alternativos para identificar este conjunto de intrusão.
Objetivos	Os objetivos de alto nível deste Conjunto de Intrusão, ou seja, o que eles estão tentando fazer. Por exemplo, eles podem ter a motivação de obter ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito. Para fazer isso, eles podem executar campanhas específicas que tenham objetivos detalhados, como comprometer os sistemas de ponto de venda em um grande varejo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Visto pela primeira vez	A hora em que este conjunto de intrusão foi visto pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que este conjunto de intrusão foi visto pela última vez executando atividades mal-intencionadas.
Motivação primária	O principal motivo, motivação ou finalidade por trás deste Conjunto de Intrusão. A motivação é o motivo pelo qual o Conjunto de Intrusão deseja atingir o objetivo (o que eles estão tentando alcançar).
Motivações secundárias	Os motivos, motivações ou finalidades secundárias por trás deste Conjunto de Intrusão. Essas motivações podem existir como uma causa igual ou quase igual à motivação primária. No entanto, isso não substitui ou necessariamente amplia a motivação primária, mas pode indicar um contexto adicional. A posição na lista não tem importância.
Nível de recurso	Esta propriedade especifica o nível organizacional no qual este Conjunto de Intrusão normalmente funciona, o que por sua vez determina os recursos disponíveis para este Conjunto de Intrusão para uso em um ataque.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este conjunto de intrusão.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este conjunto de intrusão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este conjunto de intrusão.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o registro é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a hora em que o registro é criado na origem.
Atualizado	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao conjunto de intrusão.
Adicionar marcadores	Adicionar novos marcadores.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este conjunto de intrusão.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este conjunto de intrusão.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao conjunto de intrusão.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
	exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Local

Um local representa uma localização geográfica. Os locais são usados principalmente para fornecer contexto a outros SDOs. Os locais se aplicam ao STIX 2.x.

O local pode conter alguns ou todos os seguintes elementos: região (América do Norte), endereço cívico (Nova York, EUA), latitude e longitude.

O SDO do local pode estar relacionado a uma identidade ou conjunto de intrusão para indicar que a identidade ou o conjunto de intrusão está nesse local. Também pode estar relacionado a um malware ou padrão de ataque para indicar que a vítima está em um local específico.

Por exemplo, um Local pode ser usado em um relacionamento para descrever que o conjunto de intrusão Bourgeois Swallow se origina da Europa Oriental.

Pelo menos uma das seguintes propriedades ou conjuntos de propriedades deve ser fornecido:

- região
- país
- latitude e longitude

Definir local

Defina uma localização geográfica para fornecer mais contexto a outros SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para o objeto **Local**.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos

Exibição de detalhes de identidade

Campo	Descrição
ID	ID exclusivo do local.
Nome	Insira um nome descritivo para identificar o local.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
Latitude	A latitude do local em graus decimais. Números positivos descrevem latitudes ao norte do equador e números negativos descrevem latitudes ao sul do equador. O valor desta propriedade deve ser de -90,0 a 90,0, respectivamente.
Longitude	A longitude do local em graus decimais. Números positivos descrevem longitudes a leste do meridiano principal e números negativos descrevem longitudes a oeste do meridiano principal. O valor desta propriedade deve ser de -180,0 a 180,0, inclusive.
Precisão	Define a precisão das coordenadas especificadas pelas propriedades de latitude e longitude. Isso é medido em metros. A localização real pode estar em qualquer lugar até metros de precisão do ponto definido. Se esta propriedade não estiver presente, a precisão não será especificada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se esta propriedade estiver presente, as propriedades de latitude e longitude deverão estar presentes.
Região	A região em que este local está.
País	O país em que este local está.
Área administrativa	O estado, a província ou outra área administrativa subnacional em que este local está.
Cidade	A cidade em que este local está.
Endereço	O endereço que este local descreve. Esta propriedade inclui todos os aspectos ou partes do endereço.
CEP	O código postal em que este local está.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este local.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este local.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões deste local.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a hora em que o registro é criado na origem.
Atualizado	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao local.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este local.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este local.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao local.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Malware

Malware é um tipo de TTP que representa código mal-intencionado. Refere-se a um programa que é inserido secretamente em um sistema. O malware se aplica ao STIX 2.x.

A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

O Malware SDO caracteriza, identifica e categoriza instâncias e famílias de malware a partir de dados derivados da análise. Este SDO captura informações detalhadas sobre como o malware funciona e o que ele faz.

Definir malware

Defina um malware que representa um código mal-intencionado.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse Objeto de inteligência de ameaças de **malware**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes do malware

Campo	Descrição
ID	ID exclusivo para identificar a instância do malware.
Nome	Insira um nome para identificar a instância ou família de malware, conforme especificado pelo produtor do SDO. Para uma família de malware, o nome deve ser definido.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a instância ou família de malware, incluindo potencialmente sua finalidade e suas principais características.
Tipos de malware	Indica as várias categorias do malware.
É família	Marque esta caixa de seleção para especificar se o objeto representa uma família de malware ou uma instância de malware.
Aliases	Os nomes alternativos usados para identificar este malware ou família de malware.
Fases de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
Visto pela primeira vez	A hora em que esta instância ou família de malware foi vista pela primeira vez executando atividades mal-intencionadas.
Visto pela última vez	A hora em que esta instância ou família de malware foi vista pela última vez executando atividades mal-intencionadas
Arquiteturas de processo	Indica as arquiteturas de processo para este malware.
Idiomas de implementação	Indica os idiomas de implementação deste malware.
Capacidades do malware	As capacidades que podem ser exibidas por uma instância ou família de malware.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este malware.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para o registro de malware.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este registro de malware.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, malware.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.

Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao malware.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada ao malware.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados ao malware.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações relacionadas a este malware.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Análise de malware	Lista os registros de análise de malware associados a este objeto.
Malware	Lista os registros de malware associados a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Análise de malware

A análise de malware captura os metadados e os resultados de um malware. A análise de malware se aplica ao STIX 2.x.

A análise de malware inclui a análise estática ou dinâmica realizada em uma instância ou família de malware.

Definir análise de malware

Defina a análise de malware que captura os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento
1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para Objeto de **análise de malware**.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de detalhes da análise de malware

Campo	Descrição
ID	ID exclusivo para identificar a análise de malware.
Produto	O nome do mecanismo de análise ou produto que foi usado. Os nomes dos produtos DEVEM estar todos em minúsculas com palavras separadas por um hífen "-". Para casos em que o nome de um produto não pode ser especificado, um valor anonimizado deve ser usado.
Versão	A versão do produto de análise que foi usada para executar a análise.
VM da hospedagem	Uma descrição do ambiente da máquina virtual usada para hospedar o sistema operacional convidado, se aplicável, que foi usada para a análise dinâmica da instância ou família de malware. Se este valor não estiver incluído em conjunto com a propriedade operating_system_ref, isso significa que a análise dinâmica pode ter sido realizada em um estado bruto (ou seja, sem virtualização) ou que as informações foram editadas. O valor desta propriedade DEVE ser o identificador de um objeto de software do SCO.
Sistema operacional	O sistema operacional usado para a análise dinâmica da instância ou família de malware. Isso se aplica a sistemas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	operacionais virtualizados, bem como aos que são executados em Bare Metal. O valor desta propriedade DEVE ser o identificador de um objeto de software do SCO.
Versão da configuração	Os nomes alternativos usados para identificar este malware ou família de malware.
Módulos	Os módulos de análise específicos que foram usados e configurados no produto durante esta execução de análise.
Versão do mecanismo de análise	A versão do mecanismo de análise ou produto (incluindo mecanismos AV) que foi usada para executar a análise.
Versão da definição de análise	A versão das definições de análise usadas pela ferramenta de análise, incluindo ferramentas AV.
Análise iniciada	A data e a hora em que a análise de malware foi iniciada.
Análise finalizada	A data e a hora em que a análise de malware foi encerrada.
Resultado	O resultado da classificação conforme determinado pelo scanner ou pelo processo de análise da ferramenta.
Nome do resultado	O resultado da classificação ou o nome atribuído à instância de malware pela ferramenta de verificação.
Enviado	A data e a hora em que o malware foi enviado pela primeira vez para verificação ou análise. Este valor permanecerá constante enquanto a data verificada pode mudar. Por exemplo, quando o malware foi enviado para uma ferramenta de análise de vírus.
Observável analisado	Selecione o observável que foi analisado.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para esta análise de malware.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para o registro da família de malware.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este registro de malware.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, malware.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.

Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao malware.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada ao malware.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados ao malware.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Malware	Lista os registros de malware associados a este objeto.
Definições de Marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Detecção de objeto

As vistas denotam que um objeto foi visto. Os objetos podem ser um malware, uma ferramenta, um agente de ameaça e assim por diante.

As detecções rastreiam quem e o que é o alvo, como os ataques são realizados e para rastrear tendências no comportamento de ataque.

O objeto de relacionamento de detecção contém propriedades extras não presentes nos objetos de relacionamento genéricos. Essas propriedades extras representam dados específicos para relacionamentos de detecção.

Definir detecção de objeto

Defina a detecção de objeto que descreve que um objeto (malware, ferramenta, agente de ameaça e assim por diante) foi visto.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Objeto Objeto** de detecção.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Escolher entidade e valor

Campo	Descrição
Entidade	Selecione o registro de detecção do objeto de entidade. **Nota:** Durante qualquer nova criação de registro de detecções de objeto, um registro de relacionamento associado é necessário para agregação.
Detecção de	Indica que uma entidade ou indicador específico foi observado em um ambiente que pode ser uma indicação de uma possível ameaça. **Nota:** Selecione o registro relacionado à detecção que está associado ao objeto selecionado no campo Entidade para que os registros relacionados possam ser criados e agregados aos registros de detecção.

Exibição de Detalhes de detecção de objeto

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a detecção.
Visto pela primeira vez	O início da janela de tempo durante a qual o SDO referenciado pela propriedade foi detectado.
Visto pela última vez	O fim da janela de tempo durante a qual o SDO referenciado pelo qual a propriedade foi avistada.
Contagem	Se presente, deve ser um número inteiro entre 0 e 999,999,999 inclusive e representa o número de vezes que o SDO foi referenciado pelo qual a propriedade foi avistada.
É resumo	Indica se a Detecção deve ser considerada os dados de resumo. Os dados de resumo são uma agregação de relatórios de detecções anteriores e não devem ser considerados dados de origem primária.
É interno	Indica se a detecção é interna.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este conjunto de intrusão.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à identidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta infraestrutura.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta infraestrutura.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à detecção de objeto.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Objetos	Lista os objetos associados às detecções.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Dados observados

Os Dados observados transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os Objetos cibernéticos (SCOs) STIX. Os dados observados se aplicam ao STIX 2.x.

Dados observados capturam uma única observação de uma única entidade (arquivo, conexão de rede), bem como a agregação de várias observações de uma entidade.

Você pode usar os Dados observados sozinhos (sem relacionamentos) para transmitir dados brutos coletados de qualquer origem. As origens incluem relatórios de analistas, áreas restritas e ferramentas de detecção baseadas em host e rede.

Por exemplo, Dados observados podem capturar informações sobre um endereço IP, uma conexão de rede, um arquivo ou uma chave de registro. Dados observados não são uma asserção de inteligência, são simplesmente as informações brutas sem qualquer contexto para o que isso significa.

Definir dados observados

Transmite informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os Objetos cibernéticos (SCOs) STIX.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para Objeto de **dados observados**.
4. Clique em **Nova**.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

Exibição de detalhes dos dados observados

Campo	Descrição
ID	ID exclusivo para identificar os dados observados.
Observado pela primeira vez	A hora inicial em que os dados foram vistos.
Última observação	A última vez em que os dados foram vistos.
Contagem de observações	O número de vezes que cada objeto observável cibernético foi visto. O valor deve ser um número inteiro de 1 a 999,999,999.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança dos dados observados
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esses dados observados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esses dados observados.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Criação	Especifica a data e a hora em que o objeto é criado na origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Extensões	Indica as extensões do padrão de ataque.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados aos dados observados.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esses dados observados.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esses dados observados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos dados observados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Agente da ameaça

Os agentes da ameaça são indivíduos, grupos ou organizações que agem com intenção mal-intencionada. Os agentes da ameaça se aplicam ao STIX 2.x.

Um agente de ameaça não é um conjunto de intrusão, mas pode oferecer suporte ou ser afiliado a vários conjuntos de intrusão, grupos ou organizações ao longo do tempo.

Os agentes da ameaça usam seus recursos e os recursos de um conjunto de intrusão para conduzir ataques e executar campanhas contra metas.

Você pode identificar os agentes da ameaça por seus motivos, capacidades, objetivos, nível de sofisticação, atividades anteriores, recursos aos quais eles têm acesso e sua função na organização.

Definir agente da ameaça

Defina os agentes de ameaça que são indivíduos, grupos ou organizações que agem com intenção mal-intencionada.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Vá para Objeto de agente da **ameaça**.
4. Clique em **Nova**.

> **Nota:** Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de detalhes do agente da ameaça

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Nome	Insira um nome descritivo para identificar o local.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
Aliases	Uma lista de outros nomes para identificar este agente da ameaça.
Objetivos	Os objetivos de alto nível deste agente da ameaça, ou seja, o que ele está tentando fazer. Por exemplo, eles podem ter a motivação de obter ganhos pessoais, mas seu objetivo é roubar números de cartão de crédito.
Tipos de Agente da Ameaça	Os tipos deste agente de ameaça.
Funções de agente da ameaça	As várias funções de agente de ameaça para este objeto.
Visto pela primeira vez	A hora em que este agente de ameaça foi visto pela primeira vez. Esta propriedade é uma propriedade de resumo de dados de detecções e outros dados que podem ou não estar disponíveis no STIX. Se forem recebidas novas detecções anteriores ao carimbo de data/hora da primeira vista, o objeto poderá ser atualizado para considerar os novos dados.
Visto pela última vez	A hora em que este agente de ameaça foi visto pela última vez.
Motivação primária	O motivo, a motivação ou a finalidade primária por trás deste agente de ameaça. A motivação é o motivo pelo qual o agente da ameaça deseja atingir

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	o objetivo (o que ele está tentando alcançar). Por exemplo, um agente de ameaça com o objetivo de interromper o setor financeiro de um país pode ser movido por um sentimento de aversão ideológica ao capital.
Sofisticação	A habilidade, conhecimento específico, treinamento especial ou experiência que um agente de ameaça deve ter para executar o ataque.
Motivações secundárias	Esta propriedade especifica os motivos, motivações ou finalidades secundárias por trás deste agente de ameaça. Essas motivações podem existir como uma causa igual ou quase igual à motivação primária. No entanto, isso não substitui ou necessariamente amplia a motivação primária, mas pode indicar um contexto adicional. A posição na lista não tem importância.
Nível de recurso	O nível organizacional no qual este agente de ameaça normalmente trabalha, que por sua vez determina os recursos disponíveis para este agente de ameaça para uso em um ataque. Este atributo está vinculado à propriedade de sofisticação - um nível de recurso específico implica que o agente da ameaça tem acesso a pelo menos um nível de sofisticação específico.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este agente de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

Tradução automática

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

Importante: Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.

Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agente da ameaça.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agente de ameaça.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agente de ameaça.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agente da ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista de locais associados a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Detecções	Lista as vistas associadas a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Evento de ameaça

Um evento ou situação que tem o potencial de causar consequências ou impactos indesejáveis.

Um hacker que ataque um site é um evento de ameaça. Se os hackers conseguirem danificar qualquer site ou roubar informações, isso será definido como um evento de ameaça.

Definir evento de ameaça

Defina um evento de ameaça quando um evento que resulta em acesso não autorizado e aquisição de informações não públicas ou na interrupção ou uso indevido de qualquer sistema de informações.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto de **evento de ameaça**.
4. Clique em **Nova**.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

Exibição de detalhes do agente da ameaça

Campo	Descrição
ID	ID exclusivo de um curso de ação para evitar um evento de ameaça.
Nome	Insira um nome descritivo para identificar o evento de ameaça.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o evento de ameaça, incluindo potencialmente sua finalidade e suas principais características.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este agente de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao evento de ameaça.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este evento de ameaça.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este evento de ameaça.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao evento de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
	é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Grupo de ameaça

Um objeto de agrupamentos de ameaças afirma explicitamente que os objetos STIX referenciados têm um contexto compartilhado. Os agrupamentos de ameaças se aplicam ao STIX 2.x.

Um objeto de Agrupamentos de ameaças representa um conjunto de dados que, após análise suficiente, se desenvolve para transmitir um relatório de incidente ou ameaça como um objeto de relatório STIX. Por exemplo, um agrupamento pode ser usado para caracterizar uma investigação em andamento sobre um evento ou incidente de segurança.

Um objeto de agrupamentos de ameaças também pode ser usado para declarar que os objetos STIX referenciados estão relacionados a um processo de análise em andamento. Por exemplo, um analista de ameaças pode colaborar com outras pessoas em sua comunidade de confiança para examinar uma série de campanhas e indicadores.

O SDO de agrupamento de ameaças contém uma lista de referências a SDOs, SCOs e SROs, junto com uma declaração explícita do contexto compartilhado pelo conteúdo, uma descrição textual e o nome do agrupamento.

Definir agrupamento de ameaças

Defina agrupamentos de ameaças como objetos que têm um contexto compartilhado.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para Objeto de **agrupamento de ameaças**.
4. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Exibição de detalhes do agrupamento de ameaças

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir que um tipo de ataque de grupo de ameaças aconteça.
Nome	Insira um nome descritivo para identificar o grupo de ameaças.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o evento de ameaça, incluindo potencialmente sua finalidade e suas principais características.
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este agrupamento de ameaças.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agrupamento de ameaças.

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Anotação de ameaça

Uma anotação de ameaça transmite um texto informativo para fornecer análises adicionais não contidas nos objetos STIX, objetos de definição de marcação ou objetos de conteúdo de idioma aos quais a anotação está relacionada. As anotações de ameaça se aplicam ao STIX 2.x.

Por exemplo, um analista pode adicionar uma anotação a um objeto de campanha criado por outra organização. A anotação pode indicar que eles viram publicações relacionadas a essa campanha em um fórum de hackers.

As anotações geralmente são criadas por analistas humanos e são compostas de texto orientado por humanos. Elas contêm uma propriedade extra para capturar o autor que criou a anotação.

Definir anotação de ameaça

Defina anotações de ameaça que transmitem informações para fornecer contexto ou análise adicional que não está disponível em objetos existentes.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para **Anotação de ameaça**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes da anotação de ameaça

Campo	Descrição
ID	ID exclusivo de uma anotação de ameaça.
Resumo	Especifique um breve resumo do conteúdo da anotação.
Conteúdo	Especifica o conteúdo da anotação.
Autores	Especifica o nome do autor (por exemplo, um analista).
Confiança	Insira a confiança para este curso de ação.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta anotação de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à anotação de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
	é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de Marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Opinião sobre ameaças

Uma Opinião é uma avaliação da precisão das informações em um Objeto STIX produzida por uma entidade diferente. As opiniões sobre ameaças se aplicam ao STIX 2.x.

A propriedade de opinião captura o nível de acordo ou desacordo usando uma escala fixa. A escala fixa também oferece suporte a um mapeamento numérico para permitir operações estatísticas consistentes entre opiniões.

Por exemplo, um analista de uma organização consumidora pode dizer que "discorda totalmente" de um objeto de campanha e fornecer uma explicação sobre o motivo.

As opiniões são subjectivas e a especificação não aborda a melhor forma de as interpretar.

Os analistas humanos criam opiniões e são compostos por texto orientado por humanos. Eles contêm uma propriedade extra para capturar o autor que criou a opinião.

Definir opinião sobre ameaças

Defina opiniões de ameaças como uma avaliação da precisão das informações em um objeto STIX.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto **Opinião sobre ameaças**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes da opinião sobre ameaças

Campo	Descrição
ID	ID exclusivo para uma opinião sobre ameaças.
Opinião	A opinião do produtor sobre o objeto STIX.
Explicação	Especifica o conteúdo da opinião.
Autores	Especifica o nome do autor (por exemplo, um analista).
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este curso de ação.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta opinião de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta opinião de ameaça.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a hora em que o registro é criado na origem.
Atualizado	Especifica a hora em que o registro é modificado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à opinião sobre a ameaça.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta opinião de ameaça.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta opinião de ameaça.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à opinião de ameaça.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
	é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Relatório de ameaças

Relatórios de ameaças são coleções de inteligência contra ameaças com foco em um ou mais tópicos. Os relatórios de ameaças se aplicam ao STIX 2.x.

Os relatórios de ameaças incluem a descrição de um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar inteligência de ameaças relacionada para que ela possa ser publicada como uma história abrangente de ameaças cibernéticas.

O SDO do relatório de ameaças contém uma lista de referências a objetos STIX junto com uma descrição textual e o nome do relatório.

Definir relatório de ameaças

Defina relatórios de ameaças que descrevem um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto **Relatório de ameaças**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes do relatório de ameaças

Campo	Descrição
ID	Especifique um nome para identificar o relatório de ameaças.
Nome	Especifique um breve resumo do conteúdo da anotação.
Descrição	Uma descrição que fornece informações adicionais e contexto sobre o relatório.
Tipos de relatório	Especifica o nome do autor (por exemplo, um analista).
Publicado	A data em que este relatório foi publicado oficialmente pelo autor do relatório.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta anotação de ameaça.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este padrão de ataque.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos relatórios de ameaças.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
	é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de Marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Grupos de ameaças	Lista os agrupamentos de ameaças associados a este objeto.
Relatórios de ameaças	Lista os relatórios de ameaças associados a este objeto.
Ferramentas	Lista o software legítimo que é usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Ferramenta

As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques. As ferramentas se aplicam ao STIX 2.x.

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Por exemplo, ferramentas de acesso remoto (RDP) e ferramentas de verificação de rede (Nmap) são ferramentas que um agente de ameaça usa durante um ataque.

Definir ferramentas

Defina ferramentas como software legítimo que é usado para executar ataques.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Vá para Objeto de **ferramenta**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes das ferramentas

Campo	Descrição
ID	ID exclusivo para identificar uma ferramenta.
Nome	Insira um nome descritivo para identificar a ferramenta.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a ferramenta, incluindo potencialmente sua finalidade e suas principais características.
Tipos de Ferramentas	O(s) tipo(s) de ferramenta(s) descrito(s).
Aliases	Nomes alternativos usados para identificar esta Ferramenta.
Versão da ferramenta	O identificador de versão associado à ferramenta.
Fases de ataque	Representa a fase de ataque em uma cadeia de eliminação, como LM, MITRE ATT&CK.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta ferramenta.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta ferramenta.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados ao agrupamento de ameaças.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a este agrupamento de ameaças.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a este agrupamento de ameaças.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados às ferramentas.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Vulnerabilidade

Uma vulnerabilidade é uma fraqueza ou um defeito em um componente de software ou hardware que os invasores exploram. As vulnerabilidades se aplicam ao STIX 2.x.

A fraqueza ou defeito está nos requisitos, designs ou implementações do código encontrado em um componente de software ou hardware. Essa fraqueza é explorada diretamente para afetar negativamente a confidencialidade, a integridade ou a disponibilidade desse sistema.

CVE é uma lista de vulnerabilidades e exposições de segurança da informação que fornece nomes comuns para problemas conhecidos publicamente [CVE].

Por exemplo, se um malware explorar CVE-2015-12345, um objeto de malware poderá ser vinculado a um objeto de vulnerabilidade que faz referência a CVE-2015-12345.

Definir vulnerabilidade

Defina vulnerabilidade como uma fraqueza ou defeito em um componente de software ou hardware que os invasores exploram.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse Objeto de **vulnerabilidade**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes de vulnerabilidades

Campo	Descrição
ID	ID exclusivo para identificar uma vulnerabilidade.
Nome	Um nome usado para identificar a vulnerabilidade.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a vulnerabilidade, incluindo potencialmente sua finalidade e suas principais características.
Gravidade	Indica o grau normalizado de severidade desta vulnerabilidade
CVSS3.0	Indica o CVSS v3 para esta vulnerabilidade.
CVSS 2.0	Indica o CVSS v2 para esta vulnerabilidade.
Status de exploração	Indica o status de exploração associado a esta vulnerabilidade
Publicado	Indica quando a vulnerabilidade é publicada.
Última modificação do registro	Indica quando o registro foi modificado pela última vez.
Software afetado	Lista o software afetado associado à vulnerabilidade.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta vulnerabilidade.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à vulnerabilidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecionar taxonomia	Selecione uma taxonomia associada a esta vulnerabilidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta vulnerabilidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vulnerabilidade.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Definições de marketing	Lista as definições de marketing associadas a este objeto.
Detecções	Lista as vistas associadas a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
	exploram e que está associado a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Buscar dados de vulnerabilidade

Busque dados relacionados à vulnerabilidade, como itens de configuração, entradas vulneráveis e contexto de negócios.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse Objeto de **vulnerabilidade**.
   As vulnerabilidades relacionadas associadas a este objeto são exibidas.
4. Selecione o respectivo registro de vulnerabilidade.
   Se houver CVEs associados a ele, você poderá buscar os dados relacionados a vulnerabilidades automaticamente usando o botão fornecido, e esses registros associados serão exibidos na seção Contexto de negócios das Vulnerabilidades.
5. Ir para **Inteligência interna** > **Entradas vulneráveis**.
   Os registros de CVEs associados são exibidos.
6. Selecione qualquer CVE e clique no botão **Buscar dados relacionados à vulnerabilidade**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Este link associará automaticamente os registros e buscará esse contexto de negócios específico de registros.
- Caso não haja registros associados, será exibida uma mensagem informativa informando que Este objeto de vulnerabilidade específico não tem entradas vulneráveis associadas a ele. Você deve associar manualmente os objetos às entradas vulneráveis para buscar os dados.
- Este botão acionará um trabalho agendado em segundo plano e os detalhes de início e execução do trabalho serão exibidos na seção **Fluxo de atividades**. Por exemplo, quando o trabalho é acionado, o fluxo de atividades exibe uma atividade que começou a buscar dados associados às entradas vulneráveis. Para obter mais informações sobre como os trabalhos agendados são executados para buscar os dados, consulte Trabalhos agendados .

7. Clique em **Vincular** para vincular manualmente os objetos.
8. Selecione os registros a serem vinculados e busque os dados relacionados à vulnerabilidade usando o botão **Buscar dados relacionados à vulnerabilidade**. Quando você clicar neste botão, o trabalho em segundo plano será acionado e os dados serão obtidos automaticamente para a respectiva seção. Uma mensagem exibe que o trabalho para buscar dados associados às entradas vulneráveis foi iniciado. Você pode rastrear o status no fluxo de atividades e atualizar a lista quando o trabalho for concluído para verificar os resultados. Por exemplo, se os dados estiverem relacionados aos itens de configuração, você verificará os resultados na seção Itens de configuração. Para obter mais informações sobre como adicionar CVEs, consulte Adicionar CVEs a entradas de terceiros .

Nota: Da mesma forma, você pode buscar os dados de registros de observáveis. Para obter mais informações, consulte Buscar dados de vulnerabilidade.

Definição de marcação

O objeto de definição de marcação representa uma marcação específica. As marcações de dados normalmente representam requisitos de manipulação ou compartilhamento de dados.

Definir definição de marcação

Defina definições de marcação para manipular e compartilhar os requisitos dos dados.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto **Definição de marcação**.
4. Clique em **Nova**.

Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

Exibição de detalhes da origem da definição de marcação

Campo	Descrição
ID	ID exclusivo para identificar uma definição de marcação.
Nome	Um nome usado para identificar a definição de marcação.
Tipo de definição	A propriedade de tipo identifica o tipo de objeto. A propriedade definition_type identifica o tipo de definição de marcação.
Definição	A propriedade de definição contém o próprio objeto de marcação, por exemplo, TLP.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Confiança	Insira a confiança para este objeto. A propriedade de confiança identifica a confiança que o criador tem na exatidão de seus dados. O valor de confiança DEVE ser um número no intervalo de 0 a 100.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta definição de marcação.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta definição de marcação.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à vulnerabilidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta vulnerabilidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta vulnerabilidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vulnerabilidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Detecções e mitigações	Lista as detecções e mitigações associadas a este objeto.
Identidades	Lista as identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjuntos de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Análise de malware	Lista a análise mal-intencionada associada a este objeto.
Observáveis	Lista os observáveis associados a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista os indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Eventos de ameaça	Lista os eventos de ameaça associados a este objeto.
Grupos de ameaças	Lista os agrupamentos de ameaças associados a este objeto.
Anotações de ameaça	Lista as Anotações de ameaças associadas a este objeto.
Opiniões sobre ameaças	Lista as opiniões de ameaças associadas a este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Ferramentas	Lista as ferramentas associadas a este objeto.
Vulnerabilidades	Lista as vulnerabilidades associadas a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Componente de dados

Os componentes de dados são usados para identificar propriedades ou valores específicos de uma fonte de dados.

Definir componente de dados

Defina um componente de dados para identificar as propriedades ou valores de uma fonte de dados

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto **Componente de dados**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes do componente de dados

Campo	Descrição
ID	ID exclusivo para identificar um componente de dados.
Nome	Um nome usado para identificar o componente de dados.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a vulnerabilidade, incluindo potencialmente sua finalidade e suas principais características.
Fonte de dados	Indica o grau normalizado de severidade desta vulnerabilidade
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Confiança	Indica a confiança deste objeto. A confiança deve estar entre 0 e 100.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este componente de dados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para este componente de dados.
Versão de especificação	A versão da especificação STIX usada para representar este objeto. O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do componente de dados.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à vulnerabilidade.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta vulnerabilidade.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta vulnerabilidade.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao componente de dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros relacionados

Campo	Descrição
Padrões de ataque	Lista os padrões de ataque associados a este objeto.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Fontes de dados

As fontes de dados representam os vários assuntos/tópicos de informações que podem ser coletados por sensores/logs. As fontes de dados também incluem componentes de dados, que identificam propriedades/valores específicos de uma fonte de dados.

Definir fontes de dados

Defina uma fonte de dados para representar os vários assuntos ou tópicos de informações.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto **Fontes de dados**.
4. Clique em **Nova**.

   Nota: Sempre que você cria novos registros de objeto para observáveis, indicadores, entidades ou objetos, um registro de origem é criado e uma mensagem de aviso é exibida informando que o novo registro de objeto foi criado e o usuário é redirecionado para o registro agregado.

5. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes de vulnerabilidades

Campo	Descrição
ID	ID exclusivo para identificar a fonte de dados.
Nome	Um nome usado para identificar a fonte de dados.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre a fonte de dados, incluindo potencialmente sua finalidade e suas principais características.
Camadas de coleção	Indica a descrição de onde a fonte de dados pode ser coletada fisicamente, como host, rede, plano de controle de nuvem e assim por diante.
Plataformas	Indica que o sistema em que um adversário está operando pode ser um sistema operacional ou uma aplicação.
Colaboradores	Indica os colaboradores desta fonte de dados.
TLP	O TLP é usado para garantir que informações confidenciais sejam compartilhadas com o público apropriado. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para esta fonte de dados.

Informações adicionais

Campo	Descrição
Contexto adicional	Adicione qualquer contexto adicional para esta fonte de dados.
Versão de especificação	A versão da especificação STIX usada para representar este objeto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O valor desta propriedade deve ser 2.1 para objetos STIX definidos de acordo com esta especificação.
Idioma	Esta propriedade identifica o idioma do conteúdo de texto neste objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Extensões	Indica as extensões do padrão de ataque.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Processando Status	Representa o status de processamento deste objeto, curso de ação.
Criação	Especifica a data e a hora em que o objeto é criado na origem.
Atualizado	Especifica a data e a hora em que o objeto foi atualizado na origem.
Criado por ref	Esta propriedade especifica que o objeto de identidade que descreve a entidade criou este objeto.

6. Clique em **Salvar**.
   Depois de salvar, uma mensagem de aviso será exibida indicando que Um novo registro de observável foi criado. Clique em **Continuar** para editar o registro e criar novos relacionamentos.
7. Clique em **"Continuar"**.

> **Importante:** Depois de criar um novo registro de observável, a caixa de seleção **Impedir atualizações do sistema** será exibida.
>
> Marque esta caixa de seleção para impedir atualizações do sistema depois que o observável, o indicador ou os registros de objetos STIX forem criados.

Marcadores e taxonomias

Campo	Descrição
Marcadores	
Selecionar marcadores	Selecione os marcadores associados à fonte de dados.
Adicionar marcadores	Adicionar novos marcadores.
Taxonomias	
Selecionar taxonomia	Selecione uma taxonomia associada a esta fonte de dados.
Adicionar valores de taxonomia	Adicione valores de taxonomia associados a esta fonte de dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à fonte de dados.

Registros relacionados

Campo	Descrição
Referências externas	Lista as referências externas que se referem a informações não STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.

Nota:

1. Você pode vincular e desvincular os registros relacionados associados a este objeto. Para obter mais informações, consulte Vincular registros relacionados a informações sobre ameaças.
2. Os vários SDOs na biblioteca de TI também contêm os possíveis relacionamentos. Para estabelecer relacionamentos entre dois objetos quaisquer, use o link **Relacionamentos potenciais** da **Biblioteca de informações sobre ameaças** para confirmar os relacionamentos entre os objetos. Para obter mais informações, consulte Confirmar possíveis relacionamentos objeto-objeto.
3. Além disso, use a seção **Registros relacionados** na exibição de formulário de objetos para confirmar os relacionamentos entre dois objetos usando a seção **Relacionamentos potenciais** disponível na exibição de formulário. Para obter mais informações sobre, consulte Confirmar relacionamentos potenciais de registros relacionados.
4. Você pode adicionar objetos a casos. Para obter mais informações, consulte Adicionar ao caso.

Definir feeds RSS

Um feed de inteligência contra ameaças é um fluxo de dados contínuo em tempo real que reúne informações relacionadas a riscos ou ameaças cibernéticas. Os feeds RSS oferecem uma maneira fácil de manter-se atualizado com seus sites favoritos, como blogs ou notícias mais recentes sobre segurança cibernética.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse o objeto **Feeds RSS**.

   Nota: Os feeds ingeridos podem ser pesquisados usando esta seção, mas você não pode criar novos registros.

4. No formulário, os campos a seguir são preenchidos automaticamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de detalhes de feeds RSS

Campo	Descrição
Título	Título do feed RSS.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre os feeds RSS, incluindo potencialmente sua finalidade e suas principais características.
Link	Indica o link adicionado aos feeds RSS.
Origem	Especifica a origem do feed RSS a partir da qual este registro de objeto é criado.
Data de publicação	Indica quando o feed RSS é publicado.
Autor	Indica o autor do feed RSS.

5. Clique em **Salvar**.

Informações

Campo	Descrição
Anotações	Adicione anotações adicionais para este feed.

Informações adicionais

Campo	Descrição
URL da mídia	Indica o URL da mídia.
Comentários de feedback	Qualquer feedback adicional comenta sobre o feedback.

Objetos de relacionamentos

Use os objetos de relacionamentos para vincular dois observáveis ou um observável e o SDO para explicar como eles se relacionam entre si.

Os objetos de relacionamento STIX (SROs) representam tipos de relacionamentos entre vários objetos STIX. Os seguintes objetos de relacionamento estão disponíveis:

- **Relacionamento observável-observável**: este objeto define relacionamentos entre observáveis.
- **Relacionamento objeto-objeto**: este objeto define relacionamentos entre SDOs, exceto o objeto de indicador. Um exemplo de um relacionamento definido por objeto-objeto é que um padrão de ataque entrega um malware.
- **Relacionamento objeto-observável**: este objeto define relacionamentos entre SDOs e o objeto observável (SCO). Um exemplo de um relacionamento definido de objeto-observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.
- **Relacionamento entre objeto e indicador**: este objeto define os relacionamentos entre SDOs e o objeto do indicador.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Relacionamentos indicador-indicador**: este objeto define relacionamentos entre objetos de indicador.
- **Relacionamento indicador-observável**: este objeto define relacionamentos entre o objeto de indicador e outros SDOs. Um exemplo de um relacionamento definido por objeto-indicador é quando um indicador detecta evidências de uma campanha.

Relacionamentos de objeto

Objeto de relacionamento	Origem de exemplo	Exemplo de destino	Descrição de exemplo
Relacionamentos observável-observável	Endereço IP, nome do domínio		Este relacionamento descreve entre os observáveis.
Relacionamentos objeto-objeto	Padrão de ataque	Malware	Este relacionamento descreve que este padrão de ataque é usado para entregar esta instância de malware (ou família).
Relacionamentos objeto-observável			Este relacionamento descreve entre os objetos e os observáveis.
Relacionamentos objeto-indicador	Indicador	Padrão de ataque, Campanha, Infraestrutura, Conjunto de intrusão, Malware, Agente de ameaça, Ferramenta	Esse relacionamento descreve que o indicador pode detectar evidências do padrão de ataque, campanha, infraestrutura, conjunto de intrusão, malware, agente de ameaça ou ferramenta relacionada. A evidência pode não ser direta. Por exemplo, o indicador pode detectar evidências secundárias da campanha, como malware que é comumente usado por essa campanha específica.
Indicador - Relacionamentos do indicador	Infraestrutura	Dados observados	Este relacionamento descreve que o indicador é criado com base em informações de um

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos de objeto

Objeto de relacionamento	Origem de exemplo	Exemplo de destino	Descrição de exemplo
			objeto de dados observado. Um exemplo de um relacionamento definido de objeto-observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.
Indicador-Observável			Este relacionamento descreve entre os indicadores e os observáveis.

Definir relacionamentos observável-observável

Defina relacionamentos entre observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos** > **Observável-Observável**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Observável de origem	Selecione e defina o objeto de origem.
Observável de destino	Selecione e defina o objeto de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. As opções disponíveis são: Defina a direção do relacionamento, seja direta ou inversa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ◦ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Base para correlação	Nome da regra de correlação com base na qual o sistema identificou como os registros relacionados desse observável. Esta regra é preenchida automaticamente.

6. Clique em **Enviar**.

Definir relacionamentos objeto-objeto

Defina relacionamentos entre SDOs, exceto o objeto de indicador.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos** > **Objeto-objeto**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Objeto de origem	Selecione e defina o objeto de origem.
Tipo de objeto de origem	Define o tipo de objeto de origem.
Objeto de destino	Selecione e defina o objeto de destino.
Tipo de objeto de destino	Define o tipo de objeto de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa. ◦ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ◦ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Hora de início	Especifica a hora em que o relacionamento é criado.
Hora de Parada	Especifica a hora em que o relacionamento é interrompido ou removido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Uma breve descrição sobre os relacionamentos entre objetos.

6. Clique em **Enviar**.

Definir relacionamentos objeto-observável

Defina relacionamentos entre SDOs e o objeto observável (SCO).

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos** > **Objeto-observável**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Observável	Selecione e defina o observável.
Objeto	Selecione e defina o objeto.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa. ◦ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ◦ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Hora de início	Especifica a hora em que o relacionamento é criado.
Hora de Parada	Especifica a hora em que o relacionamento é interrompido ou removido.
Descrição	Uma breve descrição sobre os relacionamentos entre objetos.

6. Clique em **Enviar**.

Definir relacionamentos objeto-indicador

Defina relacionamentos entre o objeto do indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos** > **Indicador de objeto**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Indicador	Selecione e defina o indicador.
Objeto	Selecione e defina o objeto.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa. ◦ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ◦ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Hora de início	Especifica a hora em que o relacionamento é criado.
Hora de Parada	Especifica a hora em que o relacionamento é interrompido ou removido.
Descrição	Uma breve descrição sobre os relacionamentos entre objetos.

6. Clique em **Enviar**.

Definir relacionamentos indicador-indicador

Defina relacionamentos entre o objeto de indicador e outros Use os objetos de relacionamentos para vincular dois observáveis ou um observável e o SDO para explicar como eles se relacionam.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos** > **Indicador-Indicador**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Especifica a origem da ameaça a partir da qual este registro é criado.
Domínio	Define o escopo do registro do objeto. O valor neste campo é preenchido automaticamente.
Indicador de destino	Selecione e defina o objeto do indicador de destino.
Tipo de relacionamento	Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. Defina a direção do relacionamento, seja direta ou inversa. ◦ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ◦ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Indicador de origem	Selecione e defina o indicador de objeto de origem.

6. Clique em **Enviar**.

Definir relacionamentos entre indicador e observável

Defina relacionamentos entre o objeto do indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos** > **Indicador-Observável**.
4. Clique em **Nova**.
5. Preencha os campos no formulário conforme apropriado.

Campo	Descrição
Observável	Selecione e defina o observável.
Indicador	Selecione e defina o objeto do indicador.

6. Clique em **Enviar**.

Relacionamentos potenciais

A aplicação usa correlação automatizada para estabelecer relacionamentos potencialmente possíveis entre dois SDOs, dois observáveis ou um observável e SDO.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecione um ou mais registros potencialmente relacionados e aplique esta ação na IU, o que mudará ainda mais os registros para os relacionamentos confirmados e visíveis na seção Registros relacionados.
2. Todas as correlações confirmadas ingeridas ou criadas manualmente por um analista substituirão os possíveis relacionamentos criados pela correlação automática.

Confirmar possível relacionamento observável-observável

Use esta seção para confirmar os relacionamentos entre os observáveis.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos potenciais** > **Observável-Observável**.
4. Selecione o(s) registro(s) de observável(is).
5. Clique **em Confirmar relação**.
   Um registro de relacionamento potencial é idealmente criado e identificado com base em suas regras de correlação. Depois de confirmar o relacionamento, o registro de observáveis será movido para a seção Relacionamentos, o que significa que a relação entre observáveis e observáveis está confirmada. O registro mostra uma relação confirmada somente quando as regras de correlação são correspondidas. Por exemplo, um possível relacionamento pode ser criado quando dois observáveis do tipo URLs têm o mesmo nome de domínio.

   Como alternativa, você também pode criar um novo registro de observáveis vinculando os observáveis da lista de observáveis e confirmar os relacionamentos na guia de registros relacionados de cada observável.

   a. Abra qualquer registro de observável.

   b. Acesse a guia **Registros relacionados**.

   c. Clique no botão **Vincular**.

   d. Selecione um ou mais observáveis.

   e. Clique em **Vincular**.
      Isso criará um novo relacionamento entre o registro do observável selecionado e os observáveis recém-vinculados.

6. Clique em **Excluir** para excluir os relacionamentos.

Confirmar possíveis relacionamentos objeto-objeto

Defina os possíveis relacionamentos entre os objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos potenciais** > **Objeto-objeto**.
4. Selecione o registro do observável.
5. Clique **em Confirmar relação**.
   Um registro de relacionamento potencial é idealmente criado e identificado com base em suas regras de correlação. Depois de confirmar o relacionamento desta seção, o registro de observáveis será movido para a seção Relacionamentos, o que significa que a relação entre observáveis e observáveis está confirmada. O registro mostra uma relação confirmada somente quando as regras de correlação são correspondidas. Por exemplo, um possível relacionamento pode ser criado quando dois observáveis do tipo URLs têm o mesmo nome de domínio.

   Como alternativa, você também pode criar um novo registro de observáveis vinculando os observáveis da lista de observáveis e confirmar os relacionamentos na guia de registros relacionados de cada observável.

   a. Abra qualquer registro de observável.

   b. Acesse a guia **Registros relacionados**.

   c. Clique no botão **Vincular**.

   d. Selecione um ou mais observáveis.

   e. Clique em **Vincular**.
      Isso criará um novo relacionamento entre o registro do observável selecionado e os observáveis recém-vinculados.

6. Clique em **Excluir** para excluir os relacionamentos.

Confirmar possíveis relacionamentos entre indicador e indicador

Defina os possíveis relacionamentos entre os objetos.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Ir para **Relacionamentos potenciais** > **indicador-indicador**.
4. Selecione o registro do observável.
5. Clique **em Confirmar relação**.
   Um registro de relacionamento potencial é preferencialmente confirmado com base em regras de correlação automatizadas. Depois de confirmar o relacionamento, o registro de observáveis será movido para a seção Relacionamentos, o que significa que a relação entre observáveis e observáveis está confirmada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro mostra uma relação confirmada somente quando as regras de correlação são correspondidas. Por exemplo, um possível relacionamento é confirmado quando dois observáveis do tipo URLs têm o mesmo nome de domínio.

Como alternativa, você também pode criar um novo registro de observáveis vinculando os observáveis da lista de observáveis e confirmar os relacionamentos na guia de registros relacionados de cada observável.

a. Abra qualquer registro de observável.

b. Acesse a guia **Registros relacionados**.

c. Clique no botão **Vincular**.

d. Selecione um ou mais observáveis.

e. Clique em **Vincular**.
Isso criará um novo relacionamento entre o registro do observável selecionado e os observáveis recém-vinculados.

6. Clique em **Excluir** para excluir os relacionamentos.

Confirmar relacionamentos potenciais de registros relacionados

Confirme os relacionamentos entre os dois SDOs.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Navegar até **Espaços** > **Central de segurança de inteligência contra ameaças**.
2. Clique no ícone **Biblioteca de informações sobre ameaças** no espaço.
3. Acesse a seção **Registros relacionados**.
4. Expandir **relacionamentos potenciais**.
5. Abra qualquer registro, como observáveis, indicadores ou qualquer outro objeto que você deseja confirmar os relacionamentos entre dois SDOs.
6. Por exemplo, selecione aqui **Observáveis** na navegação à esquerda.
7. Selecione os registros de **observável** na lista.

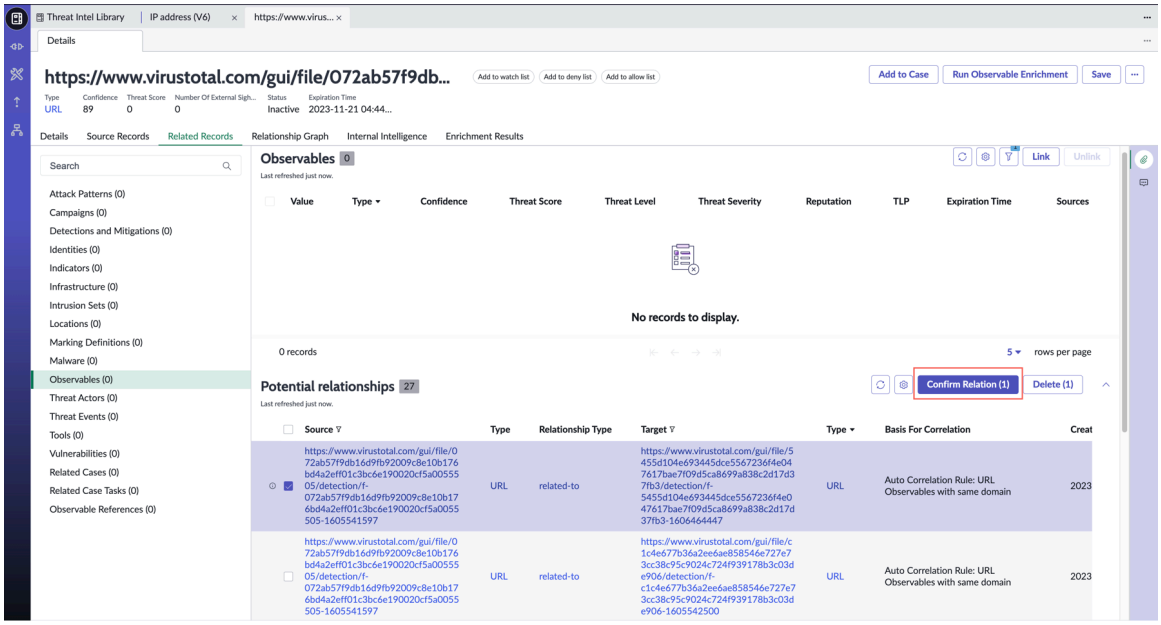
   Nota: A seção de lista mostra todos os registros de observáveis vinculados do observável associado.

8. Clique no botão **Confirmar relacionamentos** para confirmar os relacionamentos entre os objetos.

   Nota: Para obter mais informações, consulteObjetos de relacionamentos e Relacionamentos potenciais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Clique em **Excluir** para excluir os observáveis associados.
   Para obter informações sobre como os relacionamentos potenciais e os relacionamentos são estabelecidos entre os SDOs, consulte Relacionamentos potenciais e Objetos de relacionamentos.

Correlação automatizada

A correlação automatizada ajuda a identificar os relacionamentos entre observáveis, indicadores e objetos.

Com o processo de correlação, a aplicação estabelecerá automaticamente a correlação entre registros de inteligência contra ameaças com base nas regras predefinidas. Com base no tipo de regra que foi aplicada, o relacionamento pode ser um relacionamento confirmado ou um relacionamento em potencial. Se os relacionamentos entre os objetos forem confirmados, esses objetos serão exibidos automaticamente na exibição de detalhes desse objeto na seção **Registros relacionados**.

O seguinte descreve os relacionamentos e possíveis relacionamentos:

- **Relacionamentos**: use os objetos de relacionamentos para vincular dois observáveis ou um observável e o SDO para explicar como eles se relacionam entre si.
- **Relacionamentos potenciais**: use os relacionamentos potenciais para estabelecer relacionamentos potencialmente possíveis entre dois SDOs, dois observáveis ou um observável e SDO usando a correlação automatizada.

A seguir estão as regras de correlação predefinidas provisionadas no sistema de base:

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
Observáveis com o mesmo hash de arquivo	A regra compara os valores de hash dos observáveis (do mesmo tipo) e identifica se eles	A regra compara os valores de hash (do mesmo tipo) dos indicadores e identifica se eles	Cria um Relacionamento

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
	compartilham o mesmo hash.	compartilham o mesmo hash.	
Observáveis de URL com o mesmo domínio	A regra examina os pontos comuns na estrutura de URLs para identificar se eles compartilham o mesmo domínio base.	A regra examina os pontos comuns na estrutura de URLs - identifica se eles compartilham o mesmo domínio base e têm uma estrutura de subdiretórios semelhante.	Cria um relacionamento potencial
Observável encontrado como origem no objeto de rede	A regra corresponde ao valor do atributo de origem da rede com IPV4, IPV6 ou observáveis de nome de domínio no sistema e vincula como a origem do tráfego.	A regra corresponde ao valor do atributo de origem com IPV4, IPV6 ou observáveis de nome de domínio no sistema e vincula como origem de tráfego.	Cria um Relacionamento
Observável encontrado como destino no objeto de rede	A regra corresponde ao valor do atributo de destino da rede com IPV4, IPV6 ou observáveis de nome de domínio no sistema e links como o destino do tráfego.	A regra corresponde ao valor do atributo de origem com IPV4, IPV6 ou observáveis de nome de domínio no sistema e links como destino do tráfego.	Cria um Relacionamento
Relacionar observáveis com base na comunicação	Com base nos objetos de rede, a regra identifica todos os observáveis (IPV4, IPV6 e nome de domínio) que se comunicaram com o mesmo destino (IPV4, IPV6 ou nome de domínio) e estabelece um relacionamento entre esses observáveis. Além disso, observáveis relacionados (IPV4, IPV6 e nome de domínio) se estiverem relacionados ao mesmo objeto de	Na base dos objetos de rede, a regra identifica todos os indicadores que se comunicaram com o mesmo destino (IPV4, IPV6, mac-addr ou domain-name) e estabelece um relacionamento entre esses indicadores como conectados à mesma infraestrutura C2.	Cria um Relacionamento

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
	rede que a origem se comunica com o destino.		
Observáveis de domínio raiz relacionados a subdomínios	A regra vincula um domínio raiz a subdomínios e vice-versa para o tipo de domínio de observáveis.	A regra vincula um domínio raiz a subdomínios.	Cria um Relacionamento
Domínios relacionados a IPs com base em resoluções de DNS	Usando atributos domain-ipv4 ou domain-ipv6 de observáveis de domínio, a regra estabelece relacionamentos entre os domínios e os IPs.	Use os atributos domain-ipv4 ou domain-ipv6. A regra identifica todos os domínios ou subdomínios que são resolvidos para o mesmo endereço IP e estabelece relacionamentos entre os indicadores, indicando sua conexão com a mesma infraestrutura C2.	Cria um Relacionamento
Domínios correspondentes com certificados SSL	A regra analisa as informações do certificado SSL associadas aos observáveis do domínio e estabelece uma relação entre eles.	A regra analisa as informações do certificado SSL associadas aos indicadores e identifica que ambos os certificados são emitidos pela mesma autoridade de certificação e compartilham a mesma data de expiração e estabelece relacionamentos entre os indicadores, indicando sua conexão com a mesma infraestrutura C2 ou campanha de ameaça.	Cria um Relacionamento
Relacionar entidades com base em observáveis comuns	A regra compara se o mesmo observável está relacionado a duas entidades	A regra compara se o mesmo observável está relacionado a duas entidades diferentes e as	Cria um relacionamento potencial

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de correlação

Nome de Regra	Descrição de Regra	Definição de regra	Ação de regra
	diferentes e as relaciona entre si.	identifica como relacionadas entre si.	
Relacionar indicadores com base em observáveis comuns	A regra compara se o mesmo observável está relacionado a dois indicadores diferentes e os relaciona entre si.	A regra compara se o mesmo observável está relacionado a dois indicadores diferentes e os identifica como relacionados entre si.	Cria um relacionamento potencial
Relacionar indicadores com objetos com base em observáveis comuns	A regra compara se o mesmo observável está relacionado a indicadores e objetos e os relaciona entre si.	A regra compara se o mesmo observável está relacionado a dois indicadores diferentes e objetos e os identifica como relacionados entre si.	Cria um relacionamento potencial

MITRE-ATT&CK™ Repositório

O repositório MITRE-ATT&CK está disponível na Biblioteca de inteligência em que os dados das origens MITRE são ingeridos.

Os dados do MITRE que chegam ao repositório são armazenados em um repositório MITRE separado dos dados da Biblioteca de informações sobre ameaças, em que os dados do MITRE não são acumulados para o fluxo de agregação ou desduplicação e são independentes.

As fontes de dados disponíveis na aplicação são:

1. MITRE – Enterprise ATT&CK
2. MITRE – Mobile ATT&CK
3. MITRE – ICS ATT&CK

Os dados dessas origens são armazenados em um repositório MITRE separado na biblioteca de TI no sistema de base. No caso, se você quiser criar uma nova origem MITRE, configure uma origem personalizada. Para obter mais informações, consulte Exibir feed personalizado e, na exibição do formulário, clique na caixa de seleção **Avançado** e selecione o **Processador de relatório** como: **MITRECollectionDataProcessor**.

Gerenciar matrizes

Gerencie as matrizes que são importadas das coleções MITRE TAXII. Matrizes são uma coleção de táticas e técnicas. Você pode exibir as matrizes para revisar se suas coleções estão disponíveis no repositório MITRE-ATT&CK.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Depois de habilitar as fontes de dados de feed relacionadas ao MITRE ATT&CK que estão disponíveis no sistema de base, clique em **Executar agora** para executar as integrações e buscar as informações relacionadas ao MITRE.
   Para obter mais informações sobre como habilitar as integrações
2. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK**.
   Os registros relacionados ao MITRE ATT&CK são exibidos. Por padrão, todos os registros estão no estado habilitado.

   Nota: Você pode habilitar somente as matrizes relevantes para sua organização.

3. Selecione qualquer registro de matriz e clique em **Desabilitar** se quiser desabilitar qualquer registro específico.
4. Como alternativa, você pode criar um novo registro de matrizes clicando em **Novo** para manualmente para criar as matrizes do MITRE ATT&CK.
5. Preencha os campos corretamente.

Criar nova mitigação de MITRE - Detalhes

Campo	Descrição
Nome	Insira o nome da matriz.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Ativo	Marque esta caixa de seleção para ativar o registro de matriz.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este tipo de objeto.
Comentários	Adicione comentários que você possa ter.

Gerenciar técnicas

Gerencie as técnicas que são importadas das coleções MITRE TAXII. As técnicas contêm várias maneiras que os invasores desenvolveram para empregar uma determinada tática.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode revisar e desativar técnicas que não são relevantes para sua organização. No STIX, as técnicas são conhecidas como padrões de ataque.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

As técnicas representam como um adversário atinge um objetivo tático executando uma ação.

Procedimento

1. Depois de habilitar as fontes de dados de feed relacionadas ao MITRE ATT&CK que estão disponíveis no sistema de base, clique em **Executar agora** para executar as integrações e buscar as informações relacionadas ao MITRE.
   Para obter mais informações sobre como habilitar as integrações
2. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Técnicas**.
   Os registros de técnicas do MITRE ATT&CK são exibidos. Por padrão, todos os registros estão no estado habilitado.
3. Selecione qualquer registro de técnica e clique em **Desabilitar** se quiser desabilitar qualquer registro específico.
4. Como alternativa, você pode criar novos registros de técnicas clicando em **Novo** para criar manualmente as técnicas do MITRE ATT&CK.
5. Preencha os campos corretamente.

Criar nova mitigação de MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de uma técnica.
Nome	Insira o nome da técnica.
Origem	Especifica a origem da ameaça a partir da qual este registro é criado.
Plataformas	Adicione as plataformas necessárias.
Permissões necessárias	Adicione as permissões necessárias.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o conjunto de intrusão, incluindo potencialmente sua finalidade e suas principais características.
Detecção	A técnica de detecção é usada para identificar o acesso de adversários ou atividades não autorizadas em redes de computadores.
Informações	

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este tipo de objeto.
Comentários	Adicione comentários que você possa ter.

Gerenciar mitigações

Gerencie as mitigações que são importadas das coleções MITRE TAXII. As mitigações permitem que você evite que um adversário execute com sucesso técnicas ou subtécnicas contra sua organização. No STIX, as mitigações são conhecidas como curso de ações.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Depois de habilitar as fontes de dados de feed relacionadas ao MITRE ATT&CK que estão disponíveis no sistema de base, clique em **Executar agora** para executar as integrações e buscar as informações relacionadas ao MITRE.
   Para obter mais informações sobre como habilitar as integrações.
2. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Mitigações**.
   Clique em uma mitigação para exibir todas as informações associadas.
3. Clique em **Novo** para criar manualmente as mitigações do MITRE ATT&CK.
4. Preencha os campos corretamente.

Criar novas ferramentas do MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, incluindo potencialmente sua finalidade e suas principais características.
Colaboradores	Especifica os colaboradores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

5. Clique em **Salvar**.

Gerenciar grupos

Gerencie os grupos que são importados das coleções MITRE TAXII. Grupos são conjuntos de atividades de invasão relacionadas que são rastreados por um nome comum na comunidade de segurança. Os analistas rastreiam clusters de atividades usando vários termos, como grupos de ameaças, grupos de atividades, agentes de ameaças, conjuntos de intrusão e campanhas. No STIX, os grupos são conhecidos como conjuntos de intrusão.

Antes de Iniciar
Função necessária: sn_sec_tisc.analyst

Procedimento

1. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Grupos**.
   Você pode exibir os grupos listados.
2. Clique em **Novo** para criar manualmente os grupos do MITRE ATT&CK.
3. Preencha os campos corretamente.

Criar novos grupos de MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, incluindo potencialmente sua finalidade e suas principais características.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

4. Clique em **Salvar**.
5. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos**.

Gerenciar malware

Gerencie as informações de malware que você importou das coleções MITRE TAXII. É um tipo de TTP que representa código mal-intencionado.

Antes de Iniciar

Refere-se a um programa que é inserido secretamente em um sistema. A intenção de um malware é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicações ou sistema operacional (SO) da vítima.

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Grupos**.
   Você pode exibir os malwares listados.
2. Clique em um malware para exibir todas as informações associadas.
3. Clique em **Novo** para criar manualmente o malware MITRE ATT&CK.
4. Preencha os campos corretamente.

Criar novo malware MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, incluindo potencialmente sua finalidade e suas principais características.
Colaboradores	Especifica os colaboradores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

5. Clique em **Salvar**.
6. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos**.

Gerenciar ferramentas

Gerencie as informações de ferramentas que você importou das coleções MITRE TAXII. As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Por Que e Quando Desempenhar Esta Tarefa

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Ferramentas**.
   Você pode exibir as ferramentas listadas.
2. Clique em uma ferramenta para exibir todas as informações associadas.
3. Clique em **Novo** para criar manualmente as ferramentas do MITRE ATT&CK.
4. Preencha os campos corretamente.

Criar novas ferramentas do MITRE - Detalhes

Campo	Descrição
ID	ID exclusivo de um curso de ação para impedir um ataque.
Revogado	Indica que os objetos revogados não são mais considerados válidos pelo criador do objeto.
Nome	Insira um nome descritivo para identificar o objeto.
Origem	Especifica a origem da ameaça a partir da qual este registro de objeto é criado.
Aliases	Uma lista de outros nomes para identificar este objeto.
Hora de criação na origem	Especifica a hora em que o objeto é criado na origem.
Hora de modificação na origem	Especifica a hora em que o objeto é modificado na origem.
Descrição	Uma descrição que fornece mais detalhes e contexto sobre o objeto, incluindo potencialmente sua finalidade e suas principais características.
Colaboradores	Especifica os colaboradores.
Informações	
Anotações	Quaisquer informações adicionais relacionadas à mitigação.
Informações adicionais	
Contexto adicional	Adicione qualquer contexto adicional para este objeto.
Comentários	Adicione comentários para este objeto.

5. Clique em **Salvar**.
6. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciar relacionamentos de MITRE

Gerencie as informações de relacionamentos de MITRE que você importou das coleções de MITRE TAXII.

Antes de Iniciar

Função necessária: sn_sec_tisc.analyst

Procedimento

1. Para exibir os dados do repositório do MITRE ATT&CK, navegue até **Espaços** > **Central de segurança de inteligência contra ameaças** > **Biblioteca de informações sobre ameaças** > **MITRE ATT&CK** > **Relacionamentos**.
   Você pode exibir os relacionamentos listados.
2. Clique em qualquer objeto de origem para exibir todas as informações associadas.
3. Clique em **Novo** para criar manualmente os relacionamentos do MITRE ATT&CK.
4. Preencha os campos corretamente.

Criar novas ferramentas do MITRE - Detalhes

Campo	Descrição
Objeto MITRE de origem	Adicione o objeto MITRE de origem.
Objeto MITRE de destino	Adicione o objeto MITRE de destino.
Tipo de MITRE de origem	Insira o tipo MITRE de origem.
Tipo de MITRE do destino	Insira o tipo de MITRE de destino.
Tipo de relacionamento	Defina relacionamentos entre objetos. Uma descrição que fornece mais detalhes e contexto sobre o tipo de relacionamento. As opções disponíveis são: Defina a direção do relacionamento, seja direta ou inversa. ◦ Inverso - Este é o tipo de relacionamento entre o observável e o objeto. ◦ Direto - este é o tipo de relacionamento entre o objeto e o observável.
Origem	Selecione e defina o objeto de origem.
ID do relacionamento	Defina o ID do relacionamento.

5. Clique em **Salvar**.
6. Para exibir como esses objetos estão relacionados, clique em **Relacionamentos**.

Gestão e retenção de dados

Os dados são armazenados e gerenciados na instância do TISC de acordo com a estrutura de objetos da biblioteca TIDC para que os administradores exibam e configurem de acordo com a necessidade da organização.

O arquivamento e a restauração de dados são uma das principais funcionalidades para proteger os registros para uso futuro. As seções a seguir definem e explicam o processo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de arquivamento de TISC e a retenção de registros, já que a Inteligência contra ameaças contém grandes volumes de dados e registros.

Processo de arquivamento de dados

Os dados aumentam rapidamente nas tabelas com o aumento da adoção da plataforma. Algumas tabelas vêm com o sistema de base com várias políticas de gerenciamento de dados, mas outros usuários são necessários para implementá-las por conta própria.

Existem algumas maneiras diferentes de os usuários gerenciarem seus dados em tabelas:

- Excluir os dados
- Arquivar os dados

Nota: Se os usuários não adotarem nenhuma das maneiras de gerenciar seus dados, o uso aumentará com o tempo e os dados tendem a ficar muito maiores, o que terá um grande impacto no desempenho da instância da aplicação e também no armazenamento.

Regras de arquivamento para observáveis

As regras de arquivamento para observáveis provisionados no sistema de base estão listadas na seção abaixo.

- Mensagem de e-mail
- Hash SHA256
- Outro observável
- Hash SHA512
- Arquivo
- Hash SHA1
- Endereço de e-mail
- URL
- Número do AS
- Assunto do e-mail
- CIDR de IPv4
- Nome do Mutex
- Artefato
- Conta de usuário
- Chave de Registro do Windows
- Endereço IPv6
- Hash MD5
- Endereço IPv4
- Diretório
- Certificado X.509
- Regra de arquivamento de feed RSS
- Importa regras de arquivamento
- Processo do local

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modificar regras de arquivamento para observáveis

Modifique as regras de arquivamento para observáveis e exiba também uma estimativa do número de registros afetados pela regra.

Antes de Iniciar

Função necessária: administrador

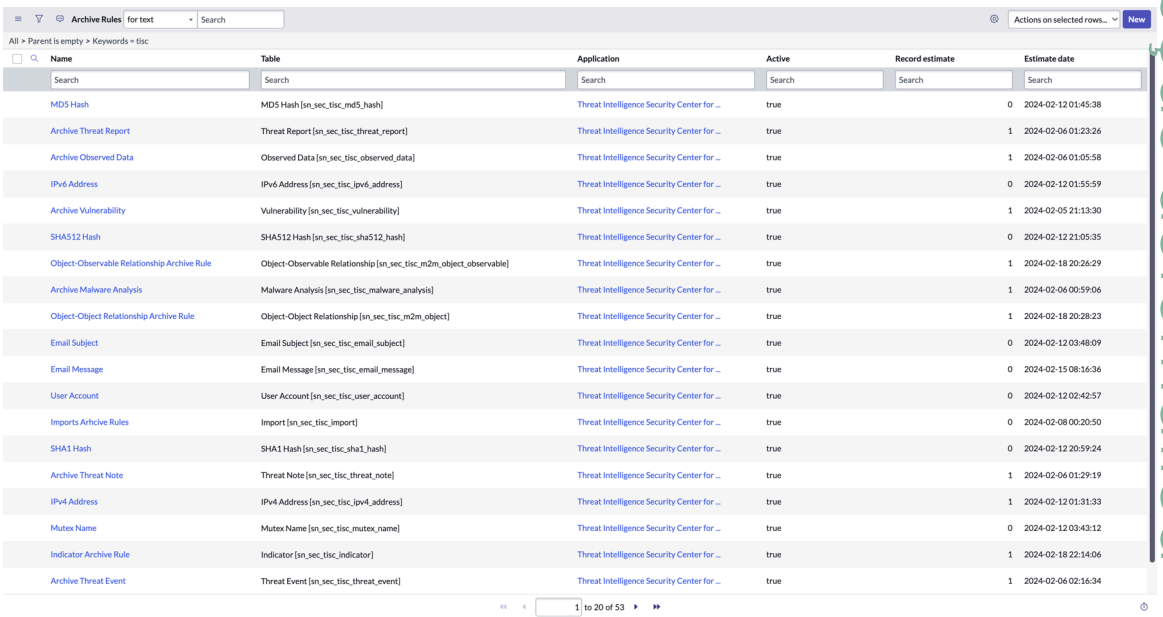
Por Que e Quando Desempenhar Esta Tarefa

As regras de arquivamento de amostra estão inativas por padrão.

A opção Histórico significativo e a condição devem ser sempre definidas como Falso para observáveis, indicadores, registros relacionados e objetos. Ao definir esta opção como falsa, você pode arquivar os registros, mas se esta opção estiver definida como verdadeira, isso significa que você não pode arquivar os registros, independentemente da definição das regras.

Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
   A lista de regras de arquivamento aplicáveis ao TISC é exibida. Essas regras de arquivamento são diferentes para cada tipo de objeto e são aplicáveis independentemente.



2. Selecione qualquer regra de arquivamento.
   Por exemplo, selecione Registro observável do diretório para ver a regra de arquivamento do sistema de base.
3. Clique **em Adicionar condição de filtro**.
4. Selecione a opção **Histórico significativo** e defina a condição como **Falso**.
   Ao definir esta opção como falsa, você pode arquivar os registros, mas se esta opção estiver definida como verdadeira, isso significa que você não pode arquivar os registros, independentemente da definição das regras.
5. Neste exemplo, defina o Status do observável como Inativo e o Tempo de expiração como 2 anos.
   Isso significa que o registro do observável pode ser arquivado quando o status é inativo e o período de expiração desse observável está definido como 2 anos e, portanto, qualquer coisa antes desse período a partir da data atual será arquivada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Cada regra de arquivamento é acionada a cada hora, portanto, qualquer mudança na regra é modificada a partir da hora do trabalho agendado. Caso você queira executar o trabalho explicitamente e não queira esperar até que o trabalho seja programado, modifique-o adequadamente. Siga as etapas abaixo.

6. Navegar até **Links relacionados** > **Recalcular estimativa**.

   A estimativa do registro foi recalculada e atualizada com o valor estimado.

   Nota: Se o valor da estimativa de registro for 0, os registros não serão arquivados, mas se o valor da estimativa de registro for 1, a aplicação identificará esse valor e esse registro será arquivado.

7. Selecione **Executar arquivo agora**.
8. Vá para a seção **Execução** de arquivamento abaixo para verificar o processo de execução de arquivamento.

   Nota: Você notará que o número total de registros arquivados é apenas um registro, já que o valor de estimativa de registro também é um.

9. Navegar até **Biblioteca de informações sobre ameaças** > **Observáveis**.
10. Pesquise o registro arquivado.
    O registro deve ter sido arquivado e não exibirá os resultados quando você pesquisar o registro.

    Nota:

    - Como parte das regras de arquivamento do TISC, toda a origem e seus registros relacionados que estão listados como parte dos registros relacionados arquivados também serão arquivados junto com o registro do observável agregado. Você pode fazer o detalhamento ativo da seção de log de arquivamento para ver a lista de registros arquivados que foram executados automaticamente em segundo plano e exibidos nesta seção.
    - Caso você queira exibir o registro arquivado, pesquise o registro nessa tabela relacionada. Simultaneamente, você também pode verificar o registro arquivado navegando até **Arquivamento do Sistema** > **Log de Arquivamento**. Exibe o número de registros arquivados.

Regras de arquivamento de objeto

As regras de arquivamento para observáveis provisionados no sistema de base estão listadas na seção abaixo.

As regras de arquivamento de amostra estão inativas por padrão.

A opção **Histórico significativo** e a condição devem ser sempre definidas como **Falso** para observáveis, indicadores, registros relacionados e objetos. Ao definir esta opção como falsa, você pode arquivar os registros, mas se esta opção estiver definida como verdadeira, isso significa que você não pode arquivar os registros, independentemente da definição das regras.

- Arquivar identidade
- Arquivar componente de dados
- Arquivar malware

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Arquivar detecções de objeto
- Ferramenta de arquivamento
- Arquivar evento de ameaça
- Arquivar padrão de ataque
- Arquivar agrupamento de ameaças
- Arquivar vulnerabilidade
- Arquivar infraestrutura
- Arquivar anotação de ameaça
- Arquivar linha de ação
- Arquivar agente da ameaça
- Arquivar relatório de ameaças
- Arquivar conjunto de intrusão
- Arquivar campanha
- Arquivar dados observados
- Arquivar definição de marcação
- Arquivar opinião sobre ameaças
- Arquivar análise de malware

Nota: Para arquivar objetos diferentes, siga o procedimento explicado aqui para Regras de arquivamento de observável Modificar regras de arquivamento para observáveis.

Regras de arquivamento de registros relacionados e indicadores

As regras de arquivamento para indicadores e registros relacionados que são provisionados no sistema de base estão listadas na seção abaixo.

As regras de arquivamento de amostra estão inativas por padrão.

A opção **Histórico significativo** e a condição devem ser sempre definidas como **Falso** para observáveis, indicadores, registros relacionados e objetos. Ao definir esta opção como falsa, você pode arquivar os registros, mas se esta opção estiver definida como verdadeira, isso significa que você não pode arquivar os registros, independentemente da definição das regras.

- **Indicador**: regra de arquivamento de indicador
- **Arquivamento de registros relacionados**:
  - Regra de arquivamento de observável relacionado
  - Regra de arquivamento de relacionamento objeto-objeto
  - Regra de arquivamento de relacionamento objeto-objeto
  - Regra de arquivamento de objeto de indicador relacionado
  - Regra de arquivamento do indicador relacionado
  - Regra de arquivamento de observável de indicador relacionado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para arquivar indicadores e registros relacionados, siga o procedimento explicado aqui para Regras de arquivamento de observável Modificar regras de arquivamento para observáveis.

Regras de arquivamento para registros relacionados

1. Para os registros relacionados, os registros são arquivados com base no objeto ou observável de origem e de destino.
2. O trabalho de programação **Atualizando coluna arquivada de relacionamento** é acionado e executado uma vez por dia.
3. Depois que o trabalho agendado é acionado e executado, as colunas arquivadas de origem e de destino são atualizadas de acordo nos registros relacionados.
4. As regras de arquivamento de relacionamento quando acionadas na próxima execução e identificam os registros com as colunas arquivadas de origem e de destino são definidas como verdadeiras e esses registros serão arquivados.

Programação de trabalho do arquivador

Depois que as regras de arquivamento estiverem configuradas e houver regras de arquivamento ativas, o trabalho do arquivador processará essas regras e arquivará os registros.

O trabalho agendado Arquivamento é configurado como um trabalho com intervalo de repetição de uma hora. Ele chama uma classe que entrega o thread para um thread em segundo plano chamado glide.db.archiver.

Para evitar que o processo de arquivamento consuma muitos recursos do sistema, as propriedades de arquivamento abaixo podem ser usadas para controlar quantos registros a regra de arquivamento processa em um intervalo.

Ao alterar as propriedades de arquivamento, o trabalho do Arquivador pode exceder a duração de 1 hora e você pode ter vários trabalhos de arquivamento executados.

Propriedades da regra de arquivamento

A seguir está a descrição das propriedades da regra de arquivamento.

Nome	Descrição	Tipo	Valor inteiro
glide.db.archive.batch_size	Controla quantos registros uma regra de arquivamento processa por trabalho em lote.	Inteiro	1000
glide.db.archive.sleep_time	Controla o tempo de espera entre cada execução de trabalho em lote de regra de arquivamento, em segundos.	Inteiro	1
glide.db.archive-.max_iterations	Controla o número máximo de trabalhos em lote a serem executados em uma hora.	Inteiro	10

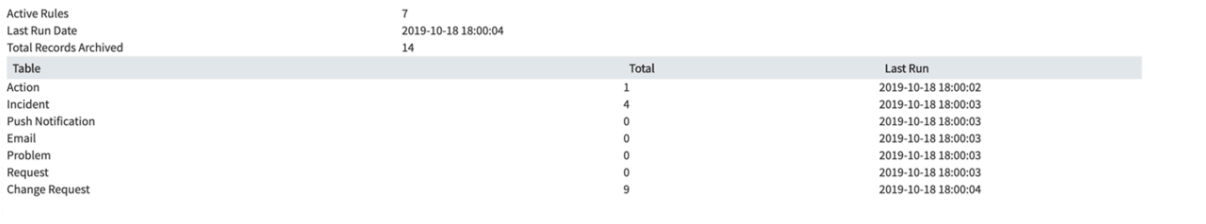
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página de diagnóstico de regras de arquivamento

Usando esta página, você pode exibir os detalhes do número de regras de arquivamento que estão ativas e o total de registros que foram arquivados e a última execução do trabalho de arquivamento.

Link para acessar a página Diagnóstico:

```
https://<your-instance>.service-now.com/ui_page.do?sys_id=71681edc9f3120007aaa207c7f4bcc2b
```



Active Rules	7
Last Run Date	2019-10-18 18:00:04
Total Records Archived	14

Table	Total	Last Run
Action	1	2019-10-18 18:00:02
Incident	4	2019-10-18 18:00:03
Push Notification	0	2019-10-18 18:00:03
Email	0	2019-10-18 18:00:03
Problem	0	2019-10-18 18:00:03
Request	0	2019-10-18 18:00:03
Change Request	9	2019-10-18 18:00:04

Procedimento de arquivamento

1. Carrega N registros que atendem aos critérios da regra de arquivamento (em que N é a propriedade do tamanho do lote).
2. Insira na tabela ar_*.
3. Exclua o registro da tabela original.
4. Crie uma entrada sys_archive_log.

Quando um registro é arquivado, uma entrada é feita na tabela Log de arquivamento (sys_archive_log) e o xml do registro é salvo como a carga.

Depuração

Algumas colunas são úteis na depuração: Execução de arquivamento, Arquivamento, Restaurado, ID e Tabela de origem.

1. **Execução de arquivamento**: fornecerá os detalhes de qual execução de arquivamento específica arquivou este registro.
2. **Arquivo**: a regra de arquivamento que atendeu à condição.
3. **Restaurado**: este campo ficará em branco se o registro não tiver sido restaurado. Se os registros tiverem sido restaurados, este campo conterá a data e a hora em que o registro foi restaurado.
4. **Da tabela**: a tabela da qual o registro foi removido.

Importante: A exclusão de uma entrada de log de arquivamento impede a restauração dos dados dos registros arquivados.

A presença de uma entrada no Log de Arquivamento é tudo de que o sistema precisa para saber que o registro foi arquivado uma vez (se foi restaurado), em qualquer caso, se foi ignorado, o que significa que o mecanismo de arquivamento não arquivará novamente algo que foi restaurado.

Registros e anexos relacionados também podem ser arquivados, já que na regra de arquivamento você pode especificar quais registros relacionados deseja arquivar. Se você restaurar o registro original, os registros relacionados também precisarão ser restaurados

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(isso não é automático, pois as tabelas de registros relacionados são independentes após o arquivamento).

Iniciar regra de destruição a partir de um script

Crie uma regra de destruição para excluir os registros arquivados e os registros relacionados após um determinado período de tempo.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

- `novo GlideArchiver().archiveDestroyByRule(xxxx); em que xxxx é o sys_id da regra de destruição.`
- Se você precisar corrigir as propriedades da regra de destruição em execução nos dados arquivados, consulte Regra de arquivamento e propriedades da regra de destruição .

Exiba as Regras de destruição dos registros arquivados:

Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Destruição de Arquivo**.
2. Selecione qualquer registro para exibir a regra de destruição.
   Com base no período de Duração do arquivamento, os registros são removidos da aplicação automaticamente. No caso, se você quiser executar manualmente a regra de destruição, **Executar Destruição de Arquivo Agora** ou se quiser modificar a Duração de arquivamento padrão, edite ou modifique o formulário de acordo.

   Nota: Para cada tabela, aplica-se uma regra de destruição individual.

Exibir regras de destruição no TISC

Exiba as regras de destruição que são provisionadas no sistema de base.

Antes de Iniciar

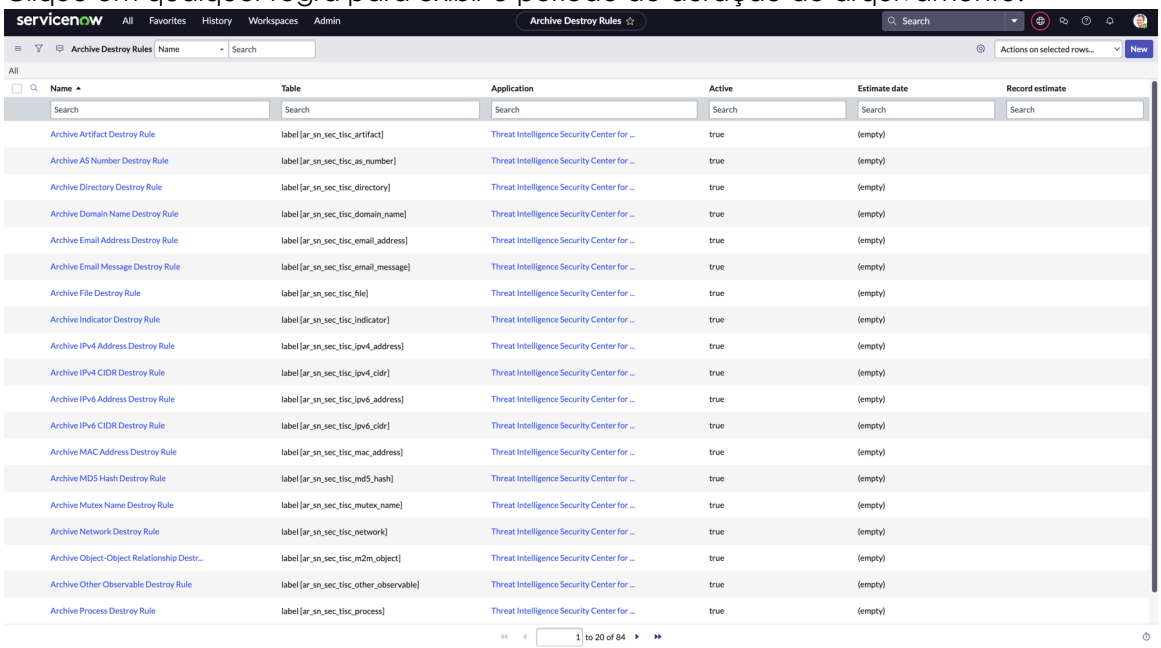
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Destruição de Arquivo**.
   A lista de regras de destruição aplicáveis ao TISC é exibida. Essas regras de destruição são diferentes para cada tipo de objeto e são aplicáveis independentemente.
2. Exiba as regras de destruição aplicáveis para TISC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em qualquer regra para exibir o período de duração do arquivamento.



Limitações de arquivamento de dados

Há um limite no tamanho de uma tabela de arquivamento que você pode criar para armazenar dados. O limite é baseado no tamanho dos dados, não na contagem de registros.

Se você receber um erro informando que uma tabela de arquivamento não pôde ser criada, isso pode estar relacionado a esta limitação de tamanho. Para obter mais informações, consulte Limites de tamanho da tabela de arquivamento de dados .

Regras de arquivamento de monitoramento

Esta seção ajuda a rastrear e monitorar as regras de arquivamento.

Descrição de Regra	Navegar até	Saída esperada
Threads de arquivamento ativos	**Arquivamento do Sistema** > **Status de Arquivamento**	• **Nome**: glde.db.archiver.xxxx em que xxxx é o sysid da regra de arquivamento correspondente. • **Valor**: iniciar com ativo ou ocioso
Andamento geral do arquivamento	**Arquivamento do Sistema** > **Regras de Arquivamento**	A coluna de estimativa informa quantos registros ainda precisam ser arquivados. Atualizado a cada hora antes da próxima iteração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descrição de Regra	Navegar até	Saída esperada
Andamento de arquivamento individual	**Arquivamento do Sistema** > **Regras de Arquivamento**	• **Duração**: cerca de 45 minutos. • **Total primário**: 30.000 por execução.

Recursos de aprendizado

Esta seção abaixo ajuda você a saber mais sobre o processo de arquivamento de dados e as práticas recomendadas.

Referências

Título de referência	Links de referência
Como restaurar vários registros relacionados arquivados de registros arquivados no modo em lote.	KB0819650
Arquivamento de dados: visão geral e perguntas frequentes	KB0785300
Arquivamento | Pesquisas do Splunk	KB0782324
Registros de documento de anexo órfãos devido ao arquivamento	KB0647663
Arquitetura de trabalho de arquivamento, configuração de regras de arquivamento, regras de destruição de arquivo	
Arquivamento de vários threads	KB0821186
Práticas recomendadas de arquivamento	KB0999731
Arquivamento de dados em docs.servicenow.com	Administração da Now Platform
Arquivar propriedades de regra e destruir regra em docs.servicenow.com	Administração da Now Platform
Arquivamento da gravação de TOI	Arquivamento
Vídeos de treinamento de desempenho	KB0960168

Tradução automática

Fluxo funcional de processamento de dados de TISC

A Central de segurança de inteligência contra ameaças (TISC) fornece uma solução que automatiza a coleta e o processamento de dados, o que ajuda a reduzir a carga sobre os analistas de informações sobre ameaças, evitando as etapas manuais envolvidas.

A Central de segurança de inteligência contra ameaças (TISC) coleta inteligência usando um dos seguintes métodos:

1. Ingestão de fontes de dados pré-configuradas e executadas em uma programação.
2. Analistas de informações sobre ameaças que importam dados usando o recurso Importar inteligência.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Criação manual de registros individuais na aplicação.

> **Nota:** Os dados coletados na aplicação serão processados para normalizar, desduplicar e agregar as informações antes de carregar na biblioteca de informações sobre ameaças.

Terminologia básica usada em Processamento de dados

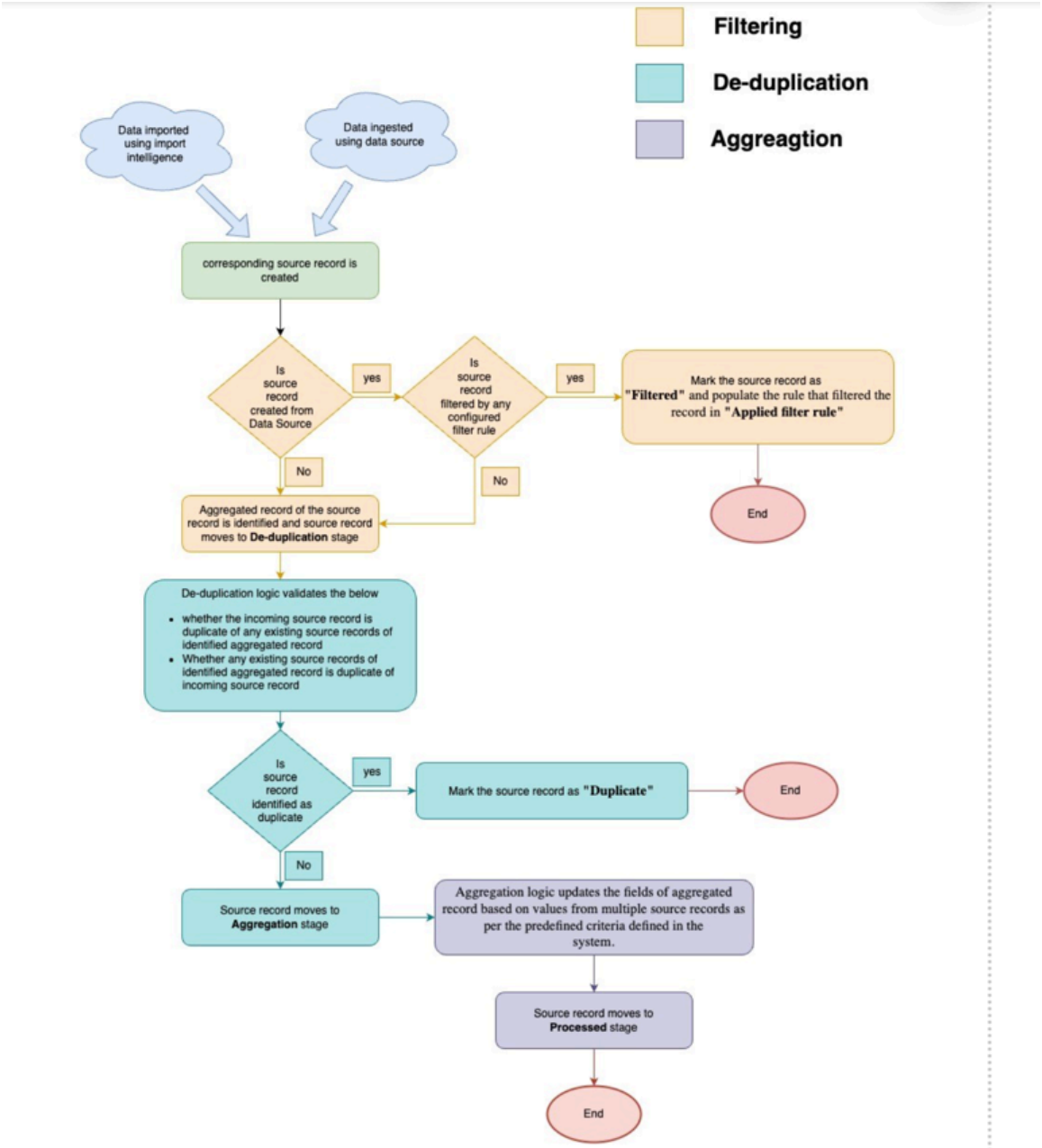
1. Tabelas de origem: as tabelas de origem contêm os dados relacionados às entidades que são obtidas de várias origens e, em seguida, os registros serão criados por cada origem.
2. Registros agregados: as tabelas de registros agregados contêm os dados relacionados a uma entidade específica, agregando os dados de todos os registros de origem de uma entidade específica.

Fluxo de dados de TISC

1. Em uma execução bem-sucedida de importação de inteligência/Fonte de dados, os registros seriam criados nas tabelas de origem correspondentes.
2. Depois que os dados chegam à tabela de origem, eles passam pela lógica de filtragem para validar se o registro deve ser filtrado com base nas **regras de filtragem de entrada**configuradas. (Consideremos SourceRecord1 como um registro de origem para nossa explicação).
3. Se o registro for filtrado por qualquer uma das regras de filtragem de entrada configuradas, o registro de origem correspondente (SourceRecord1) será marcado como **Filtrado** e a regra que filtrou o registro poderá ser encontrada em Regra de filtro aplicada.
4. Vamos supor que o registro de origem (SourceRecord1) seja agregado a AggregateRecord1.
5. Se o registro não for filtrado, ele será marcado para desduplicação, definindo o status de processamento como Pronto para desduplicação.
6. A lógica de desduplicação valida o seguinte:
   a. Se o registro de origem de entrada (SourceRecord1) for uma duplicata de quaisquer registros de origem existentes para AggregateRecord1.
   b. Qualquer um dos registros de origem existentes para AggregateRecord1 é uma duplicata do registro de origem de entrada (SourceRecord1).
7. Cada entidade tem campos e relacionamentos específicos com base nos quais o registro de origem é validado para duplicação.
8. Se o registro de origem de entrada (SourceRecord1) for uma duplicata de qualquer registro de origem existente de AggregateRecord1, o registro de origem de entrada (SourceRecord1) será marcado como Duplicado.
9. Se qualquer registro de origem existente (Registro de origem existente1) de AggregateRecord1 for identificado como duplicata do registro de origem de entrada (SourceRecord1), o registro de origem existente (Registro de origem existente1) será marcado como Duplicado e o registro de origem de entrada (SourceRecord1) será marcado para agregação definindo o status de processamento como Pronto para agregação.
10. Como parte da agregação, os campos do registro agregado AggregateRecord1 serão atualizados com base nos valores de vários registros de origem que serão agregados de acordo com os critérios predefinidos definidos no sistema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

Data Loss Prevention Incident Response

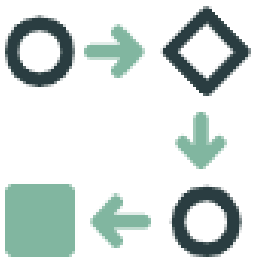
A aplicação Data Loss Prevention Incident Response (DLP IR) permite revisar e gerenciar o fluxo de trabalho de correção de incidentes do DLP de várias origens, como endpoint, rede, e-mail e nuvem.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Data Loss Prevention Incident Response

Explorar	Instalar e configurar	Administrar
		
Saiba mais sobre como analistas e administradores usam a Resposta a incidentes da DLP	Instalação e configuração da aplicação DLP Incident Response	Tarefas de administração sobre como gerenciar os incidentes do DLP na Now Platform
Uso	**Integrar**	
Atualize e gerencie incidentes aproveitando o Portal do usuário final da DLP, o Portal de operações da DLP e o Painel da DLP.	Amplie as capacidades da DLP integrando com aplicações de terceiros	

Exploração do Data Loss Prevention Incident Response

Explore a aplicação Data Loss Prevention Incident Response para saber como gerenciar informações confidenciais de seus clientes, como dados financeiros e proprietários, registros de saúde ou números de previdência social.

A perda de dados ocorre quando informações confidenciais ou sensíveis saem da rede corporativa como resultado de comunicação não autorizada. Com a aplicação DLP, você pode identificar, responder e proteger seus canais de perda de dados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao usar a aplicação Data Loss Prevention Incident Response, sua organização tem os seguintes benefícios principais:

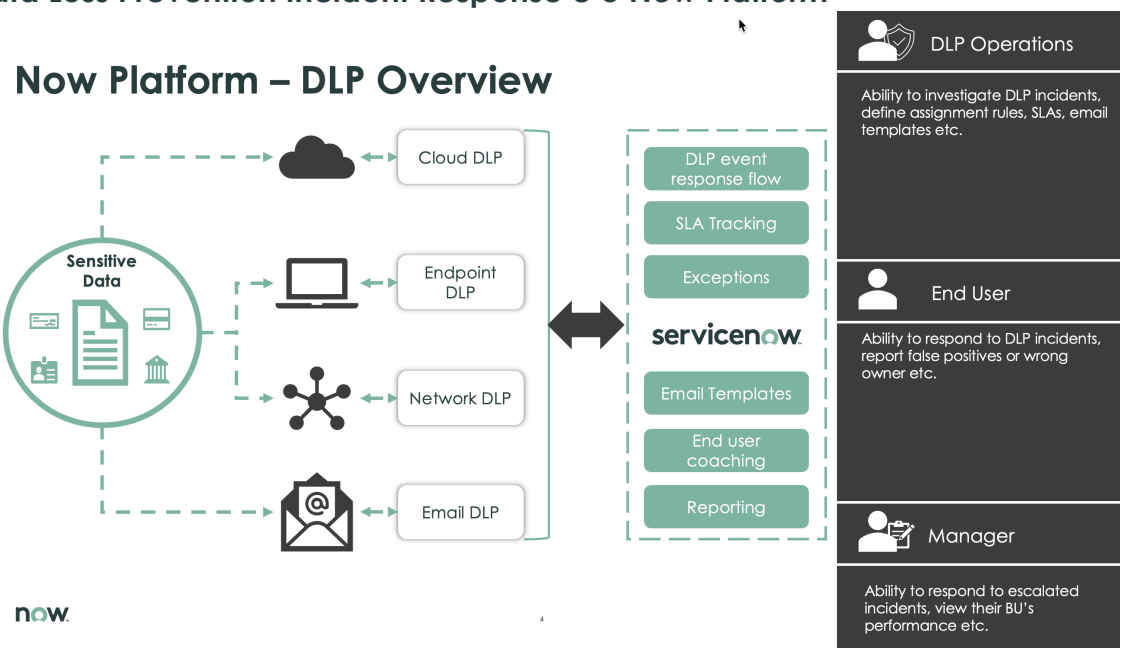
- Integre a várias soluções DLP de terceiros para obter uma exibição unificada dos incidentes no Now Platform.
- Monitore e atribua incidentes aos usuários finais para simplificar a gestão de incidentes da DLP.
- Treine seus funcionários por meio de modelos de e-mail personalizados e notificações que são enviadas para cada incidente, bem como na forma de um resumo.
- Escale os incidentes atrasados da DLP dos usuários finais para os gerentes.
- Exiba relatórios resumidos de incidentes em aberto por política, gravidade, principais infratores e assim por diante.
- Rastreie tendências de incidentes da DLP, tendências de falsos positivos e tendências de correção.

Use esta seção para saber mais sobre os principais recursos e várias funções envolvidas no trabalho com incidentes do DLP.

Visão geral da resposta a incidentes da DLP

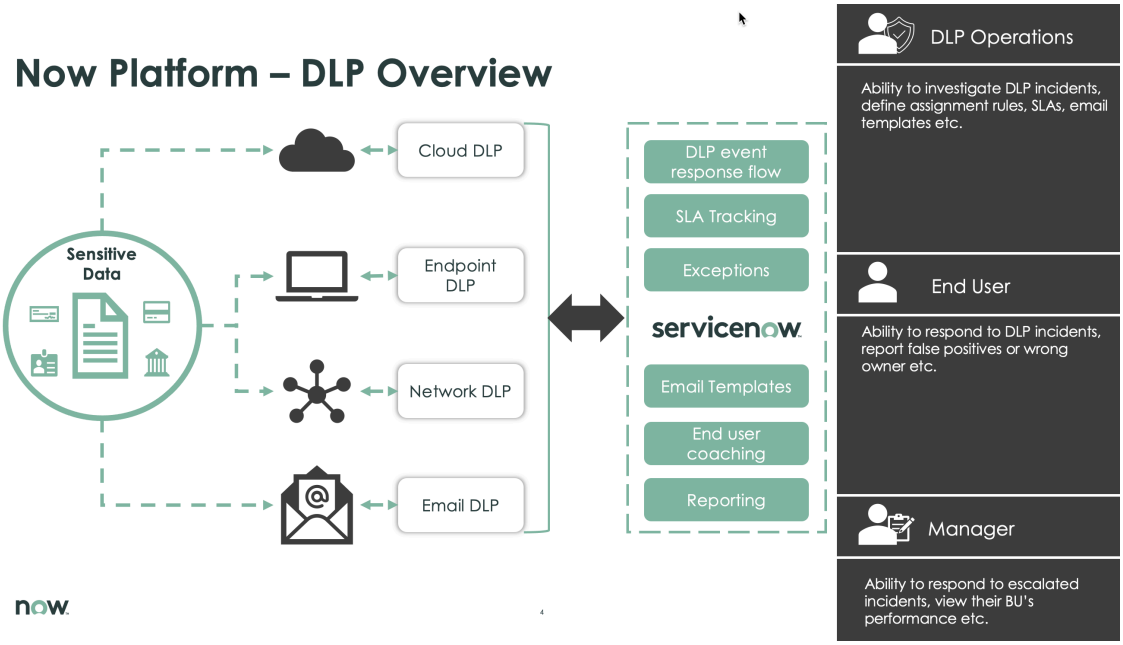
Saiba como você pode usar a aplicação Now Platform e Data Loss Prevention Incident Response (DLP IR). Gerencie informações confidenciais de seus clientes, como dados financeiros e proprietários, registros de saúde ou números de previdência social. Automatize os fluxos de trabalho de correção com a aplicação DLP Incident Response.

Data Loss Prevention Incident Response e o Now Platform



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



1. Esta é uma imagem clicável, então você pode tentar clicar nas diferentes seções para saber mais sobre a DLP
2. Tarefas de administrador da DLP - Esta é uma imagem clicável, portanto, você pode tentar clicar nas diferentes seções para saber mais sobre a DLP
3. Usando o portal do usuário final da DLP - Esta é uma imagem clicável, portanto, você pode tentar clicar nas diferentes seções para saber mais sobre a DLP
4. Como usar o Portal de operações da DLP: esta é uma imagem clicável, portanto, você pode tentar clicar nas diferentes seções para saber mais sobre a DLP
5. Usando o painel da DLP – Esta é uma imagem clicável, portanto, você pode tentar clicar nas diferentes seções para saber mais sobre a DLP

A aplicação Data Loss Prevention Incident Response inclui os seguintes recursos:

- Um espaço do usuário final em que os usuários finais ou funcionários podem revisar e responder aos incidentes atribuídos ao DLP.
- Um espaço para gerentes em que um gerente pode revisar os incidentes escalonados da DLP e agir adequadamente.
- Um espaço unificado onde sua equipe de operações da DLP pode rastrear as tendências nos incidentes em aberto, principais infratores, incidentes por origem de verificação e pode exibir, editar, atribuir e fechar os incidentes da DLP em várias origens (endpoints, redes e e-mail).
- Controles administrativos que definem os modelos de e-mail para coaching e comunicação do usuário final, regras de atribuição para atribuição automática de incidentes, regras de escalação automática e delegação para respostas a incidentes.

Introdução ao Incident Response da DLP

Revise as informações a seguir antes de começar a configurar sua aplicação Data Loss Prevention Incident Response (DLP IR).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e DLP necessárias.	A resposta a incidentes da DLP é compatível com as seguintes funções: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui o administrador da DLP (sn_dlir.admin). • sn_dlir.admin • sn_dlir.analyst
Verifique se as ServiceNow aplicações principais que são necessárias para oferecer suporte à aplicação Data Loss Prevention Incident Response estão instaladas e ativadas.	O plug-in Data Loss Prevention Incident Response (com.snc.data_loss_incident) é necessário para oferecer suporte ao produto Data Loss Prevention Incident Response. Verifique se as Operações de segurança aplicações a seguir estão instaladas e ativadas a partir do ServiceNow Store. Se não estiver instalado, instale e ative uma aplicação de cada vez na seguinte ordem para garantir uma instalação sem problemas: • Data Loss Prevention Incident Response (com.snc.data_loss_incident) • Security Support Common Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito de um produto ou aplicação das Operações de segurança ou Ativar uma aplicação da ServiceNow Store.
Domain Separation	Verifique o tópico Separação de domínios e resposta a incidentes da DLP se você pretende separar dados, processos e tarefas administrativas.

Tradução automática

Instalando e configurando DLP IR Incident Response

Baixe a aplicação Data Loss Prevention Incident Response (DLP IR) de ServiceNow Store e instale-a em sua instância.

Antes de invocar os fluxos de trabalho para a integração, instale e configure a aplicação Data Loss Prevention Incident Response da ServiceNow Store em sua instância Now Platform.

Instalar e configurar a aplicação Incident Response da DLP

Gerencie informações confidenciais e automatize os fluxos de trabalho de correção usando a aplicação Data Loss Prevention Incident Response (DLP IR) em sua instância Now Platform.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Antes de concluir as etapas de configuração, você deve baixar a aplicação de ServiceNow Store e instalá-la em sua instância.

Funções necessárias: admin e sn_dlir.admin

Procedimento

1. Siga as instruções para baixar uma aplicação da ServiceNow Store.
2. Depois de baixar a aplicação **Resposta a incidentes da DLP** e todas as aplicações dependentes, navegue até **Todos** > **Administração da DLP** > **Configuração padrão** para concluir o restante da configuração da aplicação.

Separação de domínios e resposta a incidentes da DLP

Você pode usar o Domain Separation com a Resposta a incidentes da DLP para separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona com a Resposta a incidentes da DLP

- Crie um usuário com as funções sn_dlir.admin e sn_dlir.analyst necessárias no respectivo domínio.
- Execute as configurações de resposta a incidentes da DLP no domínio apropriado.

Administração de resposta a incidentes da DLP

Você pode configurar e atribuir regras, configurar regras de prazo, usar modelos de e-mail, configurar ações de resposta do usuário final e muito mais para gerenciar os Data Loss Prevention Incident Response (DLP IR) incidentes no Now Platform.

A aplicação Data Loss Prevention Incident Response permite que você execute as seguintes configurações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de configuração padrão da DLP

Defina as definições de configuração padrão para incidentes Data Loss Prevention Incident Response (DLP IR) para identificar e configurar a notificação de incidente e as preferências de atribuição de incidente para seus usuários finais.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

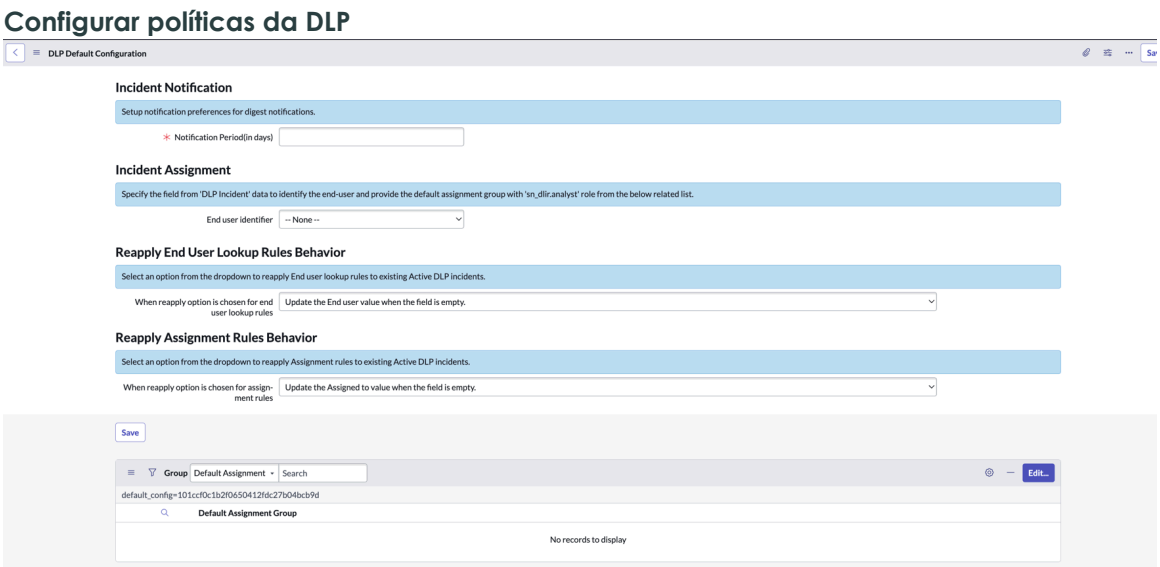
Você pode usar este módulo para definir as definições de configuração padrão quando as regras de atribuição principais e as regras de identificador estiverem esgotadas e não puderem corresponder a uma condição ou usuário. Você também pode definir e reaplicar regras de pesquisa de usuário final e regras de atribuição a incidentes ativos do DLP existentes.

A notificação de incidente do usuário final permite que você especifique a frequência com que as notificações por e-mail são enviadas para os usuários finais. Por exemplo, você pode configurar as preferências de notificação para acumular incidentes e enviar um resumo por e-mail uma vez por semana. Ao atribuir um incidente, você pode especificar a qual grupo você atribui inicialmente os incidentes da DLP. Você também pode especificar como os usuários finais são identificados pela equipe de operações da DLP.

Por exemplo, digamos que um usuário tenha armazenado informações de cartão de crédito em um arquivo em uma rede. Quando o produto de integração de DLP de terceiros cria um incidente para uma violação da política de dados confidenciais, os dados do incidente que a Now Platform DLP ingere contêm informações sobre o usuário final. Você poderá então atribuir o incidente ao usuário final correto.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Configuração padrão**.



2. No formulário, preencha os campos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de configuração padrão da DLP

Nome da configuração	Campo	Descrição
Notificação de incidente do usuário final	Período de notificação (dias)	Defina o número de dias após o qual uma notificação por e-mail deve ser enviada ao usuário final. O número de dias deve estar entre 1 e 60 dias.
	Atualizar automaticamente o estado primário com base em incidentes clonados/secundários	Opção para atualizar automaticamente o incidente de estado primário com base nos incidentes clonados ou secundários.
Atribuição de incidente	Identificador de usuário final	Especifique o campo a ser usado dos dados de incidente para identificar o usuário final. Os valores possíveis são os seguintes: ◦ **E-mail do responsável pelos dados** ◦ **Destino** ◦ **Arquivo criado por** ◦ **Arquivo modificado por** ◦ **Responsável pelo arquivo** ◦ **Nome de usuário de FTP** ◦ **Remetente**
Reaplicar comportamento das regras de pesquisa de usuário final	Quando a opção de reaplicação é escolhida para regras consulta de usuário final.	Opção para reaplicar regras de pesquisa de usuário final a incidentes ativos da DLP existentes. Você pode selecionar uma das seguintes opções para reaplicar: ◦ **Atualizar o valor do usuário final quando o campo estiver vazio**: atualiza o valor do usuário final dos incidentes ativos da DLP se o campo estiver vazio. ◦ **Atualizar o valor do usuário final**: atualiza o valor do usuário final dos incidentes ativos da DLP. ◦ **Atualizar os valores de Usuário final e Atribuído a quando ambos os campos estiverem vazios**: atualiza os valores de Usuário final e Atribuído a incidentes ativos da DLP existentes se ambos os campos estiverem vazios.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da configuração	Campo	Descrição
		Nota: Se esta opção for selecionada, a opção **Atualizar o valor Atribuído a quando o campo estiver vazio** será desabilitada automaticamente na seção Reaplicar comportamento das regras de atribuição, pois é aplicável a ambos. ◦ **Atualizar os valores de Usuário final e Atribuído a de todos os incidentes ativos da DLP**: atualiza os valores de Usuário final e Atribuído a de todos os incidentes ativos da DLP. **Nota:** Se esta opção for selecionada, a opção **Atualizar o valor Atribuído a para todos os incidentes ativos da DLP** será desabilitada automaticamente na seção Reaplicar comportamento das regras de atribuição, pois é aplicável a ambos.
Reaplicar comportamento das regras de atribuição	Quando a opção de reaplicação é escolhida para regras de atribuição.	Opção para reaplicar regras de atribuição a incidentes ativos do DLP existentes. Você pode selecionar uma das seguintes opções para reaplicar: ◦ **Atualize o valor de Atribuído a quando o campo estiver vazio.** ◦ **Atualize o valor Atribuído a para todos os incidentes ativos da DLP.**

3. Selecione o **Grupo de atribuição padrão** na seção da lista relacionada à qual todos os incidentes do DLP são atribuídos.
   Clique em **Editar** para adicionar o grupo de usuários. Quando você clica em **Editar** na seção de lista relacionada e seleciona um item nas colunas **Coleções** e, em seguida, adiciona o designado selecionado às colunas Grupo na página **Editar Membros** e salva a lista.

   Nota: Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dlir.analyst na lista relacionada. Você só pode selecionar um grupo.

4. Clique em **Salvar**.

Criar regras de pesquisa de usuário final

Você pode criar e configurar regras de pesquisa de usuário final e atribuir os incidentes da DLP aos respectivos usuários finais com base nessas regras.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

O administrador da DLP define essas regras de pesquisa de usuário final para atribuir automaticamente os usuários finais a incidentes da DLP usando somente o campo de usuário final. A regra de pesquisa de usuário final da DLP permite atribuir o usuário final em incidentes da DLP com base no identificador de usuário final, atributos personalizados ou script.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de pesquisa de usuário final da DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de pesquisa de usuário final da DLP

Campo	Descrição
Nome	Nome da regra de pesquisa de usuário final.
Ativo	Opção para indicar se a regra de pesquisa de usuário final está ativa.
Ordem de execução	A prioridade da regra de pesquisa de usuário final. Este campo indica a ordem na qual as regras de pesquisa de usuário final são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de pesquisa de usuário final com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de pesquisa de usuário final.
Condição	Condições no construtor de condições. Essas condições são baseadas na tabela de incidentes da DLP. Para criar uma condição para a regra de pesquisa de usuário final, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar mais condições, clique em **E** ou **OU**. ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode definir as condições para esta regra de pesquisa de usuário final selecionando a condição como **Origem da integração**, **contém**, **Symantec**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Pesquisar usuário final usando	Opção para pesquisar o usuário final usando o **campo Incidente** ou **Script**.
Identificador de usuário final	O identificador de usuário final do incidente da DLP. Este campo aparece quando o **campo Incidente** é selecionado no campo **Pesquisar usuário final usando**. Você pode selecionar um identificador de usuário final entre os seguintes: ◦ **E-mail do responsável pelos dados** ◦ **Destino** ◦ **Arquivo criado por** ◦ **Arquivo modificado por** ◦ **Responsável pelo arquivo** ◦ **Nome de usuário de FTP** ◦ **Remetente** **Nota:** Os identificadores de usuário final listados acima são configuráveis usando a propriedade do sistema `sn_dlir.assignment.fields`. Para obter mais informações, consulte Definir configurações avançadas. ◦ **Usuário personalizado do incidente**
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo

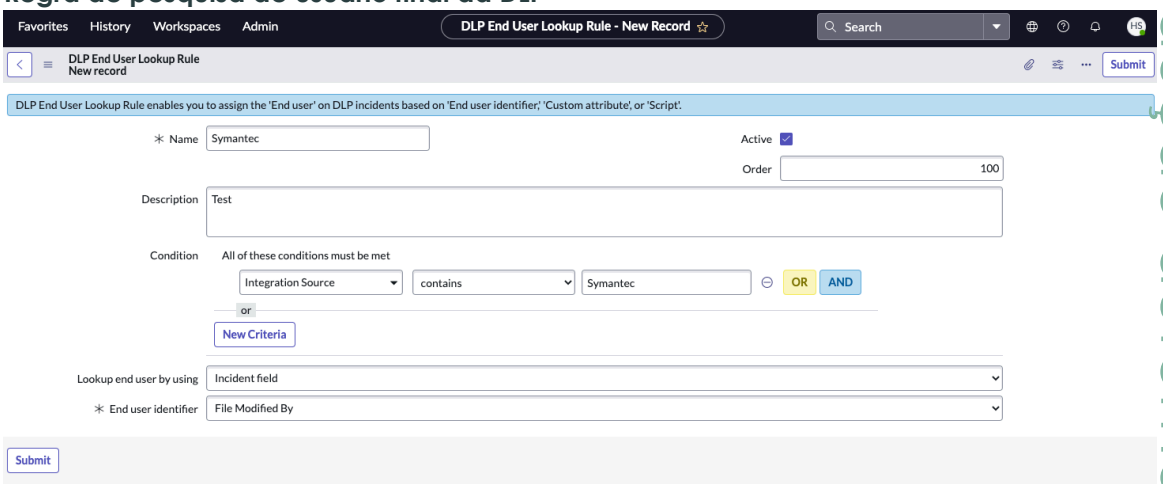
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	aparece somente quando **um** é selecionado no campo **Identificador do usuário final**.
Script	Você pode usar o editor de script para personalizar e formatar os valores de campo durante a criação da regra de pesquisa do usuário final. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário final.

Example
O exemplo a seguir mostra uma regra de pesquisa de usuário final com o nome "Symantec". O Construtor de condições requer que a "Origem da integração" seja "Symantec". A opção **Pesquisar usuário final usando** está definida como "Campo de incidente" e a opção **Identificador de usuário final** está definida como "Arquivo modificado por".

Regra de pesquisa de usuário final da DLP



4. Clique em **Enviar**.
   Você também tem a opção de selecionar uma ou mais regras de pesquisa de usuário final e reaplicá-las em todos os incidentes de DLP existentes.
5. Para reaplicar uma regra de pesquisa de usuário final em todos os incidentes da DLP existentes, clique em **Reaplicar**.

Criar regras de atribuição

Use esta seção para criar regras de atribuição. Em seguida, atribua os incidentes Data Loss Prevention Incident Response (DLP IR) a grupos de usuários, usuários finais, gerentes ou usuários do incidente.

Antes de Iniciar
Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar regras de atribuição para atribuir incidentes de IR da DLP a grupos de usuários, usuários finais ou gerentes. A atribuição dos incidentes do DLP ocorre quando as condições na regra de atribuição são atendidas.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de atribuição**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição da DLP

Campo	Descrição
Nome	Nome da regra de atribuição.
Ativo	Opção para indicar se a regra de atribuição está ativa.
Ordem de execução	A prioridade da regra de atribuição. Este campo indica a ordem na qual as regras de atribuição são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de atribuição com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva desta regra de atribuição.
Condição	Condições no construtor de condições. Essas condições são baseadas na tabela de incidentes da DLP. Para criar uma condição para a regra de atribuição, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por exemplo, suponha que você crie uma regra de atribuição de DLP para um endpoint. Você pode especificar que a origem da verificação de condição é um sistema de arquivos de endpoint que deve ser atendido antes de atribuir um incidente. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Atribuir a	Atribuição a um dos seguintes: ◦ Grupo de usuários ◦ Usuário final ◦ Gerente ◦ Usuário do incidente A atribuição ocorre quando as condições no Construtor de condições são atendidas.
Grupo de usuários	Opção para pesquisar e selecionar um grupo de usuários ao qual os incidentes da DLP serão atribuídos. Este campo aparece quando **o Grupo de usuários** é selecionado no campo **Atribuir a**. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dlir.analyst.
Usuário final	Opção para atribuir o incidente da DLP ao usuário final. A atribuição ocorre quando as condições no Construtor de condições são atendidas.
Atribuir usando campos de gerente	Gerente do usuário final. Este campo aparece quando **Gerente** é selecionado no campo **Atribuir a**. Você pode atribuir os incidentes da DLP a um gerente específico selecionando um dos campos de gerente, como Sobrenome, E-mail, Cidade, Número do funcionário.
Identificador de usuário	O identificador de usuário do incidente. Este campo aparece quando **Usuário do incidente** é selecionado no campo **Atribuir a**. Você pode selecionar um identificador de usuário entre as seguintes opções: ◦ **E-mail do responsável pelos dados** ◦ **Destino**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Arquivo criado por** ◦ **Arquivo modificado por** ◦ **Responsável pelo arquivo** ◦ **Nome de usuário de FTP** ◦ **Remetente** ◦ **Usuário personalizado do incidente**
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo aparece somente quando o **Usuário personalizado do incidente** é selecionado no campo **Identificador de usuário**.
Anexar avaliação	Opção para indicar se você deseja anexar uma avaliação ao incidente.
Estado da resposta pré-avaliação	Opção para selecionar em que estado o incidente deve estar antes que o usuário final responda. Também pode ser um estado personalizado. O valor padrão é Avaliação pendente.
Estado da resposta pós-avaliação	Opção para selecionar em que estado o incidente da DLP deve estar depois que o usuário responder. O valor padrão é Avaliação concluída.
Avançado	Opção avançada para identificar o usuário final. Este campo aparece somente quando o **Usuário personalizado do incidente** é selecionado no campo **Identificador de usuário**. Você pode usar o editor de script para personalizar e formatar os valores de campo durante a criação da regra de atribuição para identificar o usuário final. Em seguida, você escolhe a quem deseja atribuir o incidente da DLP, que pode ser um usuário final ou o gerente do usuário final. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário final.

Tradução automática

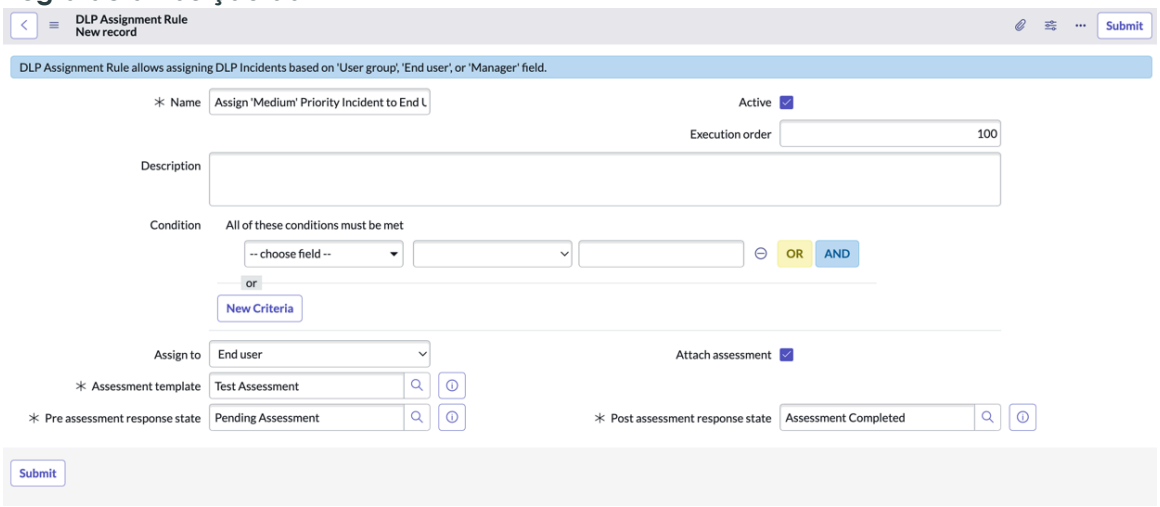
Example

O exemplo a seguir mostra uma regra de atribuição com o nome `Atribuir incidente de prioridade "média" ao usuário final`. O Construtor de condições requer que a origem da verificação seja `Atribuir incidente de prioridade "média" ao usuário`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

`final`e que o campo `Atribuir a` esteja definido como `Usuário final`. Em seguida, você pode pesquisar o "e-mail" do usuário final.

Regra de atribuição da DLP



4. Selecione o campo **Atribuir a** na seção da lista relacionada à qual todos os incidentes do DLP são atribuídos.
   Clique em **Editar** para adicionar o grupo de usuários. Quando você clica em **Editar** na seção de lista relacionada e seleciona um item nas colunas **Coleções** e, em seguida, adiciona o designado selecionado às colunas Grupo na página **Editar Membros** e salva a lista.

   Nota: Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dlir.analyst na lista relacionada. Você só pode selecionar um grupo.

5. Clique em **Enviar**.
   Você também tem a opção de selecionar uma ou mais regras de atribuição e reaplicá-las em todos os incidentes de DLP existentes.
6. Para reaplicar uma regra de atribuição em todos os incidentes de DLP existentes, clique em **Reaplicar**.

Criar regras de consolidação de incidentes

Crie uma regra de consolidação de incidentes para consolidar vários incidentes de natureza semelhante em um incidente primário.

Antes de Iniciar

Função necessária:

- sn_dlir.admin - Criar, editar e excluir
- sn_dlir.analyst e sn_dlir.analyst_read - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

O administrador da DLP define essas regras de consolidação de incidentes para consolidar automaticamente os incidentes da DLP da mesma natureza em um incidente primário.
A regra de consolidação de incidentes da DLP permite consolidar os incidentes da DLP com base na configuração fornecida para Duração da consolidação e Identificação da consolidação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de consolidação de incidentes da DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição da DLP

Campo	Descrição
Nome	Nome da regra de consolidação de incidentes.
Ativo	Opção para indicar se a regra de consolidação de incidentes está ativa.
Ordem de execução	A prioridade da regra de consolidação de incidentes. Este campo indica a ordem na qual as regras de consolidação de incidentes são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de consolidação de incidentes com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de consolidação de incidentes.
Condição	Condições no construtor de condições. Essas condições são baseadas na tabela de incidentes da DLP. Para criar uma condição para a regra de consolidação de incidentes, selecione qualquer um dos campos de incidentes. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por exemplo, você pode definir as condições para esta regra de consolidação de incidentes selecionando a condição como **Origem da integração**, **contém**, **Symantec**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Duração da consolidação	Opção para definir a duração da consolidação do incidente. Os incidentes neste período com os mesmos valores para os campos selecionados serão consolidados no primeiro incidente. O primeiro incidente correspondente a esta regra será o incidente primário e o restante dos incidentes serão incidentes secundários.
Consolidar incidentes por	Selecione o campo de incidente da DLP para consolidar os incidentes quando houver o mesmo valor no campo selecionado para diferentes incidentes. Selecione pelo menos um campo. Selecione pelo menos um campo.

O exemplo a seguir mostra uma regra de consolidação de incidentes com o nome Consolidar incidentes para integração da Symantec. O construtor de condições requer que a origem da integração seja Symantec. A opção **Duração da condição** está definida como 1 hora e a opção Nome da política está selecionada para **Consolidar incidente até**.

No momento da ingestão do incidente do Symantec DLP, esta regra será executada e, quando vários incidentes tiverem o mesmo nome de política, o incidente será consolidado no primeiro incidente ingerido correspondente a esta regra.

4. Clique em **Enviar**.
   Os incidentes consolidados com base na regra de consolidação estarão disponíveis na lista de incidentes secundários no Espaço do analista da DLP.

Criar regras de prazo de resposta

Configure as regras de prazo de resposta para determinar o tempo que você deseja dar aos usuários finais para responder aos incidentes atribuídos Data Loss Prevention Incident Response (DLP IR).

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar este módulo para definir as regras de data de vencimento da resposta para os diferentes tipos de incidentes do DLP e as regras para começar a contar a data de vencimento. Depois que a data de vencimento expirar, os usuários serão notificados sobre o incidente atrasado. Você também tem a opção de escalar o incidente atrasado para um dos seguintes:

- Gerente
- Usuário personalizado do incidente
- Grupo de usuários

Por exemplo, quando você escala o incidente atrasado para um gerente e especificou no máximo três níveis de escalação. O primeiro nível do gerente é notificado primeiro. Se o incidente estiver atrasado novamente, o gerente de segundo nível será notificado, seguido pelo terceiro nível se o incidente ainda estiver atrasado. Se o gerente tiver um delegado, ele terá a opção de atribuir a escalação ou o incidente atrasado ao delegado.

Você também tem a capacidade de criar regras de prazo de resposta múltipla.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de vencimento da resposta**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de prazo da resposta

Campo	Descrição
Nome	Nome da regra de prazo da resposta.
Ativo	Opção para indicar se a regra de prazo da resposta está ativa.
Vencimento em (dias)	Número de dias de vencimento.
Data de vencimento contada a partir de	Data de início usada para calcular a data de vencimento. A data de vencimento pode ser calculada a partir da primeira vez em que o usuário foi notificado sobre o incidente ou a partir da data de atribuição do incidente.
Notificar antes da data de vencimento	Opção para notificar o usuário final sobre o incidente da DLP antes da data de vencimento.
Notificar em (dias antes do prazo)	Número de dias antes da data de vencimento em que a regra aciona uma notificação para o usuário final.
Descrição	Descrição exclusiva para esta regra de prazo de resposta.
Condição	Condições no construtor de condições. Essas condições são baseadas na tabela de incidentes da DLP. Para criar uma condição para a regra de prazo de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	resposta, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Escalar	Opção para escalar o incidente do DLP para alguém se a data de vencimento da resposta tiver sido violada. Para obter mais informações, consulte Adicionar vários usuários para acessar incidentes da DLP.
Escalar incidente atrasado para	Opção para especificar se o incidente deve ser escalonado para um gerente, um usuário personalizado ou um grupo de usuários. Este campo aparece somente quando a opção **Escalar** está habilitada.
Atribuir usando	Especifique como um gerente deve ser identificado. Este campo aparece somente quando **Gerente** é selecionado no campo **Escalar incidente atrasado para**.
Níveis máximos de escalação	Opção para definir o número máximo de níveis de escalação para um gerente e um usuário personalizado. Como gerente ou usuário personalizado, você pode definir qualquer número de níveis de escalação. Por padrão, são fornecidos três níveis de escalação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

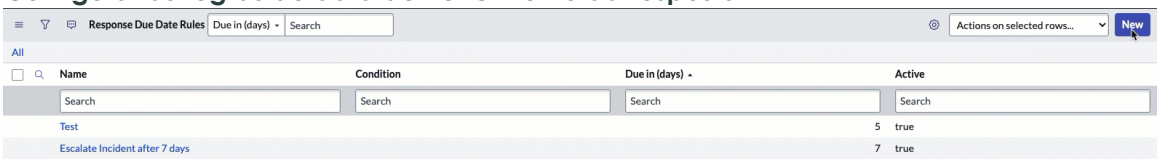
Campo	Descrição
	◦ Como gerente, você pode definir qualquer número de níveis de escalação atualizando o valor neste campo. ◦ Como usuário personalizado, você pode usar o ícone + para definir qualquer número de níveis de escalação.
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo aparece somente quando **Usuário personalizado do incidente** é selecionado no campo **Escalar incidente atrasado para**.
Grupo de usuários	Opção para pesquisar e selecionar um grupo de usuários para o qual escalar incidentes da DLP. Este campo aparece somente quando **o grupo de usuários** é selecionado no campo **Escalar incidente atrasado para**. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos com a função sn_dlir.analyst.

Example
O exemplo a seguir mostra a regra de prazo de resposta para determinar quanto tempo você deseja conceder aos usuários finais para responder aos incidentes Data Loss Prevention Incident Response (DLP) atribuídos. Depois que o usuário final é notificado pela primeira vez, o prazo da resposta é em dois dias. O construtor de condições mostra que a origem da verificação deve corresponder ao sistema de arquivos do endpoint para prosseguir com a criação da data de vencimento da resposta. A opção de escalação está selecionada. O incidente é escalonado para o gerente se a data de vencimento da resposta for violada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar as regras de data de vencimento da resposta



4. Clique em **Enviar**.

Adicionar vários usuários para acessar incidentes da DLP

Use o recurso de cadeia de escalação para permitir que todos os respectivos usuários envolvidos no incidente acessem os incidentes da DLP na exibição de lista, embora o incidente esteja atribuído a um usuário diferente.

Antes de Iniciar

Função necessária:

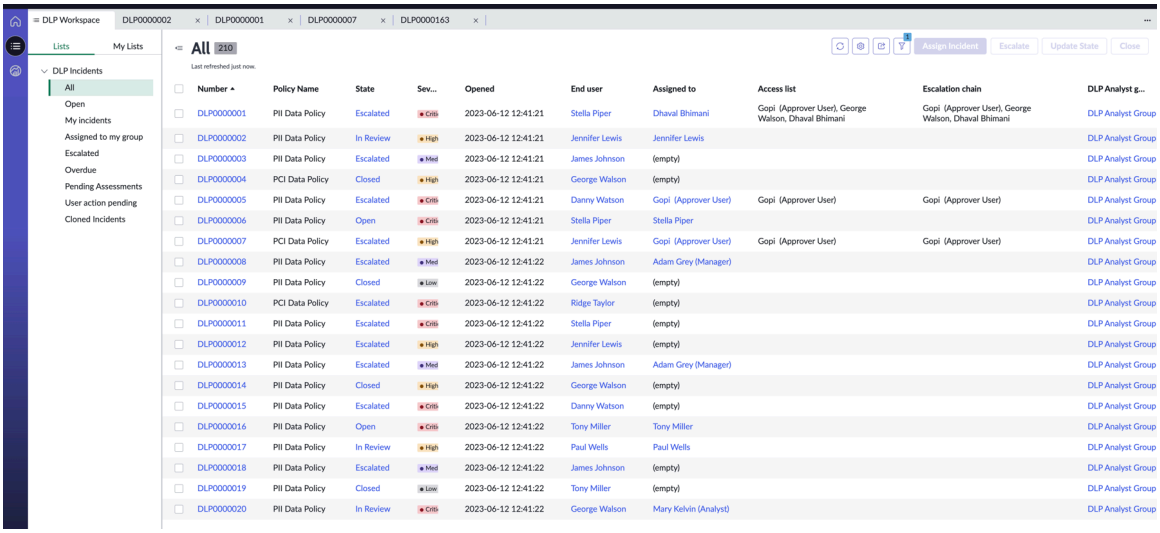
- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.read, sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Procedimento

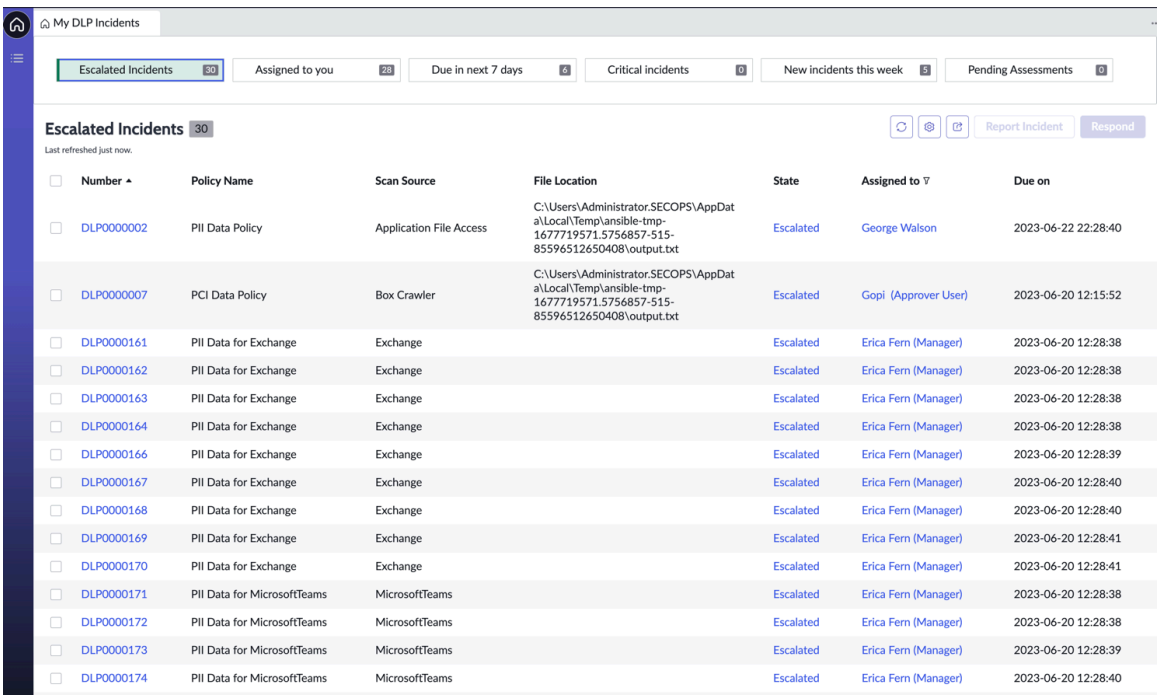
1. Navegar até **DLP** > **Espaço do analista da DLP**.
   Na exibição de lista, os usuários e seus delegados devem ser capazes de exibir o incidente da DLP na guia Incidentes **escalonados** no portal do usuário final.
2. Abra qualquer incidente.
3. Clique no botão **Escalar** para escalar um incidente.
4. Selecione o usuário ou o grupo de usuários na lista suspensa.
   Você pode adicionar vários usuários à cadeia de escalação. Todos os usuários que têm acesso são listados na seção Detalhes da exibição do formulário e também na guia **Todos os** incidentes. A cadeia de escalação é exibida com base nas definições de configuração. Para obter mais informações, consulte Definir configurações avançadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   Depois de enviar, o incidente será atribuído a um gerente. No entanto, o usuário final ainda poderá exibir o incidente.
6. Para verificar isso, navegue até o **Espaço do usuário da DLP** como um usuário final.
   Todos os incidentes atribuídos ao usuário final são exibidos.
7. Exiba a lista de incidentes **escalonados na seção Incidentes escalonados**.



Você também pode exibir a lista de acesso de usuários na coluna **Cadeia de escalação**na exibição de lista.

8. Abra qualquer incidente.
9. Clique no botão **Responder** para enviar a resposta do incidente.
10. Selecione a resposta na lista suspensa.
11. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar regras de aprovação

Crie regras de aprovação para obter aprovação de vários níveis de usuários aprovadores sempre que um tipo avançado de opção de resposta for selecionado.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

O administrador da DLP define essas regras de aprovação para conceder consentimento em solicitações geradas por usuários finais para a aprovação do tipo avançado de opção de resposta. O administrador da DLP também pode definir vários níveis de aprovação aqui.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de aprovação da DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição da DLP

Campo	Descrição
Nome	Nome da regra de aprovação.
Ativo	Opção para indicar se a regra de aprovação está ativa.
Ordem de execução	A prioridade da regra de aprovação. Este campo indica a ordem na qual as regras de aprovação são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de aprovação com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de aprovação.
Condição	Condições no construtor de condições. Essas condições são baseadas na tabela de incidentes da DLP. Para criar uma condição para a regra de aprovação, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar mais condições, clique em **E** ou **OU**. ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode definir as condições para esta regra de consolidação de incidentes selecionando a condição como **Origem da integração**, **contém**, **Microsoft**.
Aplicável para opções de resposta	Opção para selecionar a opção de resposta do tipo avançado. Você pode selecionar as opções de resposta múltipla.
Aprovador	Selecione o tipo de usuário do aprovador que você deseja definir. ◦ **Tabela de usuário**: selecione esta opção se quiser selecionar o usuário aprovador na tabela Usuários (sys_user). ◦ **Lista de aprovação personalizada**: selecione esta opção se quiser configurar vários níveis de aprovador personalizado para uma única solicitação
Identificador do aprovador	Este campo aparecerá quando a **Tabela de usuário** for selecionada para a opção **Aprovador**. Selecione o campo para identificar o aprovador da tabela Usuários (sys_user).
Número de níveis	Este campo aparecerá quando a **Tabela de usuário** for selecionada para a opção **Aprovador**. Número final neste campo para definir os níveis de aprovação. Por exemplo, se 3 for adicionado no campo Número de níveis e o Gerente for selecionado no campo Identificador do aprovador, a solicitação de aprovação passará para três níveis de aprovação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O exemplo a seguir mostra a regra de aprovação criada para uma das opções de resposta antecipada. A condição requer que o nome da origem da integração contenha a palavra-chave Microsoft que aciona esta configuração.

4. Para a opção **Aprovador**, selecione **Lista de aprovação personalizada**.
5. Clique em **Enviar**.
6. A lista relacionada de**Níveis de aprovação** será preenchida na exibição do formulário.
7. Na seção **Níveis de aprovação**, clique em **Novo**.
8. No formulário, preencha os campos.

Formulário Nível de aprovação

Campo	Descrição
Nome	Nome do nível de aprovação.
Ativo	Opção para indicar se o nível de aprovação está ativo.
nível	O nível da regra de aprovação. Este campo indica a ordem na qual os níveis de aprovação são executados quando dois ou mais níveis são configurados. O nível de aprovação com o número mais baixo tem a prioridade mais alta. Para definir o nível de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Regra de aprovação	Regra de aprovação para a qual você deseja definir esta configuração. Este será um campo somente leitura.
Descrição	Descrição exclusiva da regra de aprovação.
Aprovações obrigatórias	Selecione a opção para definir se a aprovação de todos os usuários/grupos configurados é necessária ou somente de um usuário.
Aprovadores	Opção para selecionar os aprovadores. **a.** Usuários e grupos: **i. Usuários**: clique no para adicionar um usuário específico da lista. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar a si mesmo como o usuário ao qual as condições da DLP são aplicáveis, clique no . ii. **Grupos**: clique no<add_icon> ícone para adicionar um grupo específico da lista. Você também pode adicionar um grupo usando a opção de pesquisa. b. **Localizar usando script**: você pode usar o editor de script para personalizar e formatar os valores de campo durante a criação do nível de aprovação. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário do aprovador.

9. Clique em **Enviar**.

Criar modelos de instruções do usuário

Crie e gerencie o modelo de instruções do usuário para incidentes do DLP para ajudar os usuários a entender as instruções envolvidas na resolução de incidentes e as próximas etapas envolvidas no processo de resolução.

Antes de Iniciar

O modelo de cartão de instruções do usuário exibe dois cabeçalhos diferentes que fornecem mais informações sobre um incidente específico na exibição do formulário.

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Quando um incidente é atribuído ao usuário final, pode ser necessário que o usuário saiba as instruções adicionais sobre como responder aos incidentes, apresentar aos usuários a terminologia e fornecer informações adicionais sobre o incidente. Esses modelos podem orientar os usuários a fornecer a resposta precisa aos incidentes do DLP.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Modelos de instruções do usuário**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Avaliação de incidentes da DLP

Campo	Descrição
Nome	Nome do modelo de instrução do usuário.
Descrição resumida	Descrição exclusiva deste modelo de instrução do usuário.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Opção para indicar se o modelo de instrução do usuário está ativo.
Ordem de Execução	Prioridade do modelo de instrução do usuário de incidente. Este campo indica a ordem na qual a ordem é executada para avaliar o modelo de instrução do usuário quando um incidente é criado. A opção com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O padrão é 100.
Condição de correspondência de incidentes	Os incidentes que corresponderem às condições definidas no Construtor de condições serão exibidos. Essas condições são baseadas nos dados de incidentes da DLP. Para criar uma condição para uma instrução do usuário, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em E ou OU: Se E for selecionado, todas as condições deverão ser atendidas. Se OU for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Aplica-se a	Selecione o usuário ou grupos de usuários aos quais o modelo se aplica. As outras opções disponíveis são: ◦ **Todos os usuários finais**: marque esta caixa de seleção se o modelo de instruções se aplicar a todos os usuários. ◦ **Todos os revisores de incidentes escalonados**: marque esta caixa de seleção se o modelo se aplicar a todos os revisores dos incidentes escalonados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Usuários específicos**: clique no ícone para adicionar um usuário específico da lista ao qual as condições de incidente da DLP são aplicáveis. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário ao qual as condições da DLP são aplicáveis, clique no ícone **Adicionar-me**. ◦ **Grupos de usuários específicos**: clique no ícone para adicionar um grupo específico da lista ao qual as condições de incidente da DLP são aplicáveis. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.
Modelo de instruções: instruções	Adicione instruções no editor de rich text com variáveis disponíveis no nível de incidente.

4. Expanda a seção **Modelo de instruções**, insira a instrução do modelo e adicione informações de nível de incidente nesta seção, se necessário.
5. Arraste e solte as variáveis necessárias para exibir determinados campos dinamicamente.
6. Clique em **Enviar**.
   Os modelos de instruções do usuário agora foram criados e você pode clicar em qualquer cabeçalho de instrução do usuário para saber os detalhes adicionais de um incidente do DLP.

   Para obter mais informações, consulte Data Loss Prevention Incident Response Espaço do usuário.

Configurar instruções do usuário de IU da DLP

Configure as mensagens de IU do sistema para adicionar cabeçalhos detalhados de instruções do usuário conforme necessário.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **IU do Sistema** > **Mensagens**.
2. Pesquise **user_instruction_card_heading**.

   Por padrão, user_instruction_card_heading e user_instruction_modal_window_heading são as duas configurações de mensagem de IU provisionadas para os usuários.

3. Clique em qualquer instrução do usuário para atualizar ou modificar.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar modelos de e-mail

Crie e gerencie os modelos de e-mail pré-configurados para enviar notificações aos usuários finais, grupos de usuários ou gerentes. Com esses modelos, você pode treinar e se comunicar com os usuários finais sobre os incidentes Data Loss Prevention Incident Response (DLP IR).

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

> **Importante:** Para que os analistas exibam as comunicações por e-mail de um incidente do DLP no fluxo de atividades, você deve adicionar ou acrescentar a função "sn_dlir.analyst" na propriedade do sistema global `glide.ui.activity.email_roles`.

Por Que e Quando Desempenhar Esta Tarefa

As notificações por e-mail são categorizadas pelas notificações de incidentes enviadas aos usuários finais, pelas notificações de escalação enviadas aos gerentes ou pelas notificações de data de vencimento. Você pode enviar notificações por e-mail sobre os prazos dos incidentes do DLP ou até mesmo orientar os usuários finais sobre o que fazer quando determinadas condições forem atendidas no filtro de condições de e-mail.
Os modelos de e-mail da DLP permitem que você envie a notificação por e-mail para usuários finais, gerentes e analistas. Você pode configurar os modelos a serem enviados por incidente ou como um resumo. O assunto e o corpo do e-mail podem conter variáveis para que você possa reutilizar o conteúdo existente.

A DLP fornece os seguintes modelos de e-mail pré-configurados com base nas categorias:

- **Modelo de e-mail da DLP - Notificação de aprovação por incidente: notifique** os usuários sobre a aprovação de suas solicitações.
- **Modelo de e-mail da DLP – Notificação de escalação:** envie notificações de escalação para gerentes na forma de resumos.
- **Modelo de e-mail da DLP - Notificação de aprovação pendente: notifique** os aprovadores sobre itens pendentes.
- **Modelo de e-mail da DLP - Notificação de cancelamento da solicitação de aprovação por incidente: notifique**os usuários sobre uma solicitação de aprovação que foi cancelada pela equipe de analistas da DLP.
- **Modelo de e-mail da DLP – Notificação de conclusão de resposta do usuário: notifique** a equipe de analistas da DLP sobre a resposta enviada pelos usuários.
- **Modelo de e-mail da DLP – Notificação de incidente do usuário:**este é um modelo padrão para notificação resumida do usuário. Envie notificações de incidentes aos usuários finais na forma de resumos a cada poucos dias, mesmo se não houver novos incidentes, para informar os usuários sobre o número total de incidentes no nome do usuário específico. Você também pode enviar notificações de resumo para notificar os usuários sobre as datas de vencimento mais próximas de incidentes do DLP com a gravidade crítica, alta, média ou baixa.
- **Modelo de e-mail da DLP - Notificação de aprovação pendente por incidente**: notifique os aprovadores sobre aprovações pendentes.
- **Modelo de e-mail da DLP - notificação de rejeição:** envie uma notificação de rejeição ao solicitante.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Modelo de e-mail da DLP - Notificação de data de vencimento:** envie uma notificação de data de vencimento do incidente. Se um incidente da DLP for atribuído ao usuário final e ele não tiver realizado nenhuma ação antes da data de vencimento, uma notificação por e-mail será enviada ao usuário final. Você também tem a opção de escalar o incidente da DLP para um gerente, um usuário personalizado ou um grupo de usuários se a data de vencimento da resposta tiver sido violada.

  Nota: As notificações de data de vencimento devem estar na forma de resumos.

- **Modelo de e-mail da DLP - Notificação de resposta do usuário por incidente: notifique** os analistas sobre a resposta enviada aos usuários por incidente.
- **Modelo de e-mail da DLP -** Notificação de escalação por incidente: notifique os gerentes sobre escalações por incidente.
- **Modelo de e-mail da DLP – Notificação de usuário por incidente: notifique** os usuários sobre a atribuição por incidente.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Modelos de E-mail**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Modelo de e-mail da DLP

Campo	Descrição
Nome	Nome do modelo de e-mail.
Ativo	Opção para indicar se o modelo de e-mail da DLP está ativo. Se esta opção não estiver habilitada, as notificações não serão enviadas para este modelo de e-mail.
Categoria	Categoria de notificação por e-mail. A DLP é compatível com as seguintes opções: ◦ **Notificação de incidentes para usuários finais**: enviada quando os incidentes são atribuídos aos usuários finais. ◦ **Notificação de escalação para gerentes**: enviada quando o prazo de resposta é violado ou atribuída manualmente ao gerente por meio do portal de operações da DLP. ◦ **Notificação de prazo**: enviada quando o prazo da resposta é violado. ◦ **Notificação de resposta do usuário para analistas**: enviada quando o usuário final realiza qualquer ação no incidente da DLP. ◦ **Notificação de aprovações pendentes**: notifique os aprovadores sobre itens pendentes. ◦ **Notificação de aprovação para o solicitante**: notifique os usuários sobre a aprovação de suas solicitações.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Rejeitar notificação ao solicitante**: notifique os usuários sobre a rejeição de suas solicitações. ◦ **Cancelar notificação ao solicitante**: notifique os usuários sobre o cancelamento de suas solicitações.
Tipo	Opção para indicar se o e-mail é enviado por incidente ou como um resumo. **Nota:** Se você selecionou **Notificação de data de vencimento** no campo **Categoria**, poderá usar somente resumos. Selecione esta opção.
Descrição	Descrição exclusiva deste modelo de e-mail.
Ordem de Execução	Prioridade do modelo de e-mail. Este campo indica a ordem na qual os modelos de e-mail são executados quando dois ou mais modelos de e-mail compartilham as condições de acionamento. O modelo de e-mail com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Condição do modelo	Opções nas condições do modelo que são baseadas na tabela de incidentes da DLP. Você pode selecionar qualquer um dos campos de incidente para criar a condição do gatilho do modelo de e-mail. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Usuários de Destino	Usuários de destino para o modelo quando as condições forem atendidas. Os usuários de destino podem ser um dos seguintes: ◦ **Todos os destinatários**: envie o e-mail para os usuários de destino. ◦ **Destinatários do grupo:** envie o e-mail somente para destinatários de um grupo específico usando a opção de filtro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Destinatários que correspondem aos critérios**: envie o e-mail para usuários de destino que correspondam aos critérios. Você pode usar o filtro para detalhar os usuários de destino com base nas condições. Por exemplo, cidade.

Modelo de e-mail	Modelo de e-mail que você pode selecionar. Você pode definir as variáveis para reutilizar o conteúdo existente para adicionar à notificação por e-mail.
	
	Os campos **Categoria** e **Tipo** determinam as variáveis que estão disponíveis para seleção. Por exemplo, digamos que a categoria de e-mail esteja definida como notificação de incidente e que o tipo de e-mail seja um resumo. As variáveis para seleção são campos de resumo para acomodar o acúmulo de vários incidentes do DLP.
	
	Aqui está um exemplo de HTML do corpo do e-mail de cada modelo de e-mail:
	◦ **Modelo padrão para notificação de aprovação por incidente**:
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	
	`- Date protection team`
	◦ **Notificação de cancelamento da solicitação de aprovação por incidente**
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	
	`- Data protection team`
	◦ **Modelo padrão para notificação de data de vencimento**:
	`Dear ${target_user.name},`
	
	`Following incidents require your response.`
	
	`${due_days_table}`
	
	`- Data protection team`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

	◦ **Modelo padrão para notificação de usuário Por incidente**:
	`Dear ${assigned_to.name},`
	
	`DLP Incident ${number} is assigned to you.`
	
	`Please review and submit your response.`
	
	`- Data protection team`
	
	◦ **Modelo padrão para notificação de incidente do usuário**:
	`Hello ${target_user.name},`
	
	`You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication.`
	
	`Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}.`
	
	`Please log in to the ${link_to_dlp_portal} and submit your response.`
	
	`- Data protection team`
	
	◦ **Modelo padrão para escalação - Resumo**:
	`Hi ${target_user.name},`
	
	`The following data security incidents have been escalated to you due to lack of response from the assignees.`
	
	`Please login to the incident response workspace to review the incidents and submit your response.`
	
	`${overdue_table}`
	
	`- Data protection team`
	
	◦ **Modelo padrão para escalação - por incidente**:
	`Dear ${assigned_to.name},`
	
	`Data security incident ${number} has been escalated to you.`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	``` Please review and submit your response or assign the incident back to the user. - Data protection team ``` ◦ **Modelo padrão para notificação de aprovação pendente**: ``` Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team ``` ◦ **Modelo padrão para notificação de aprovação pendente por incidente**: ``` Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team ``` ◦ **Modelo padrão para notificação de rejeição por incidente**: ``` Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team ``` ◦ **Modelo padrão para notificação de resposta do usuário por incidente**: ``` Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ```

Tradução automática

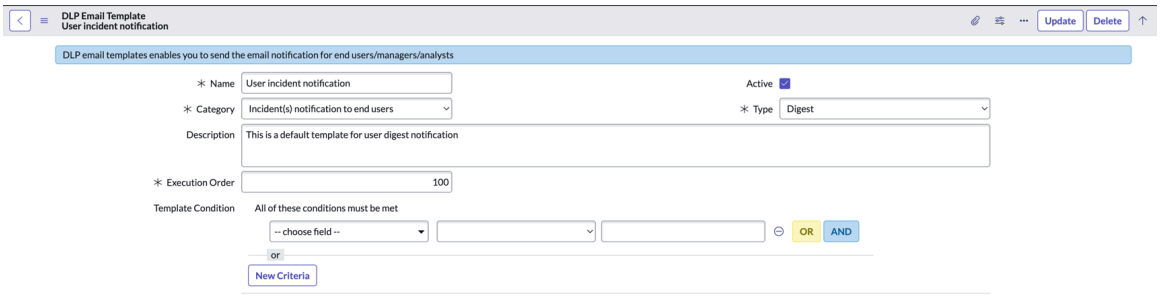
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

	◦ **Modelo padrão para notificação de conclusão de resposta do usuário**:
	`Hello ${target_user.name},`
	
	`This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication.`
	
	`Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.`

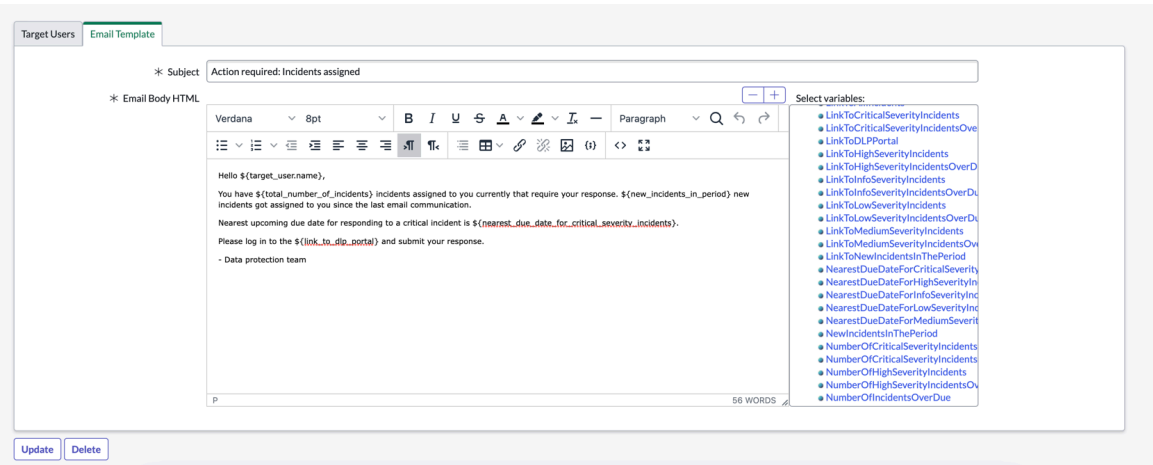
Example
O exemplo a seguir mostra o modelo de e-mail da DLP com os usuários de destino definidos como todos os destinatários.

Modelo de e-mail



O exemplo a seguir mostra um modelo de e-mail com o assunto "Notificação de incidente do usuário" e uma variável *new_incidents_in_period*. O corpo do e-mail contém várias variáveis que são adicionadas da coluna Selecionar variáveis.

Variáveis de modelo de e-mail



4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
O usuário final recebe um e-mail de notificação de resumo com todos os campos de variáveis selecionados no modelo.

Criar avaliações

Crie e gerencie avaliações para permitir que os usuários finais respondam a incidentes do DLP. Você pode usar as avaliações para coletar informações sobre os dados confidenciais expostos ou vazados dos incidentes do DLP.

Criar e gerenciar avaliações para incidentes do DLP

Antes de Iniciar
Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa
As avaliações de incidentes da DLP ajudam a identificar possíveis ameaças e vulnerabilidades aos seus dados com base na resposta do usuário final. Você pode usar essas informações para determinar as lacunas, preocupações e expectativas existentes dos usuários finais.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Avaliações**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Avaliação de incidentes da DLP

Campo	Descrição
Nome	Nome da avaliação de incidentes da DLP.
Ativo	Opção para indicar se a avaliação de incidentes da DLP está ativa.
Descrição	Descrição exclusiva desta avaliação de incidente da DLP.
Introdução da avaliação	Forneça uma introdução ou contexto para sua avaliação. Você também pode usar variáveis da seção Selecionar variáveis para exibir determinados campos dinamicamente.

4. Clique em **Enviar**.
5. Depois de criar uma avaliação, abra a avaliação e clique em **Designer de avaliação**.
6. Na seção Nova avaliação, selecione um tipo de pergunta de avaliação na seção Controles.
7. Arraste e solte o tipo de pergunta de avaliação necessária na seção Nova avaliação. Por exemplo, você pode arrastar e soltar o controle **Opção** na seção Nova avaliação ou Nova categoria.
8. Para adicionar mais categorias à avaliação, clique no .

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Para modificar uma categoria existente, clique no .
10. Depois de criar as diferentes perguntas de avaliação pela primeira vez, clique em **Salvar**e em **Publicar**.

Criar regras de opção de resposta a incidentes

Crie as regras de opção de resposta do incidente que o usuário final ou analista pode usar ao responder a um incidente.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode configurar o tipo de resposta que um usuário final deve executar com base no tipo de incidente do DLP. A aplicação DLP Incident Response do sistema base fornece as seguintes opções de resposta para os usuários:

- Avaliação concluída
- Conteúdo excluído
- Arquivo excluído
- Arquivo criptografado
- Conteúdo Mascarado
- Relatar falso-positivo
- Denunciar proprietário incorreto
- Necessário para processo de negócios
- Direitos revisados

Por exemplo, digamos que um usuário final relate um incidente do DLP como um falso-positivo. O estado deste incidente é marcado automaticamente como fechado porque o estado de destino configurado por você é fechado.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de opção de resposta do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regras de opção de resposta do incidente

Campo	Descrição
Nome	Nome da opção de resposta do incidente.
Ativo	Opção para indicar se a opção de resposta do incidente está ativa.
Ordem de execução	Prioridade da opção de resposta do incidente. Este campo indica a ordem na qual as opções de resposta do incidente são executadas quando

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	duas ou mais opções de resposta do incidente compartilham as condições de acionamento. A opção de resposta do incidente com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O padrão é 100.
Descrição	Descrição exclusiva para esta opção de resposta do incidente.
Estado de destino padrão	O estado de destino padrão que você configurou.
Condição	Condições no construtor de condições. Essas condições são baseadas na tabela de incidentes da DLP. Para criar uma condição para as opções de resposta do incidente, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.

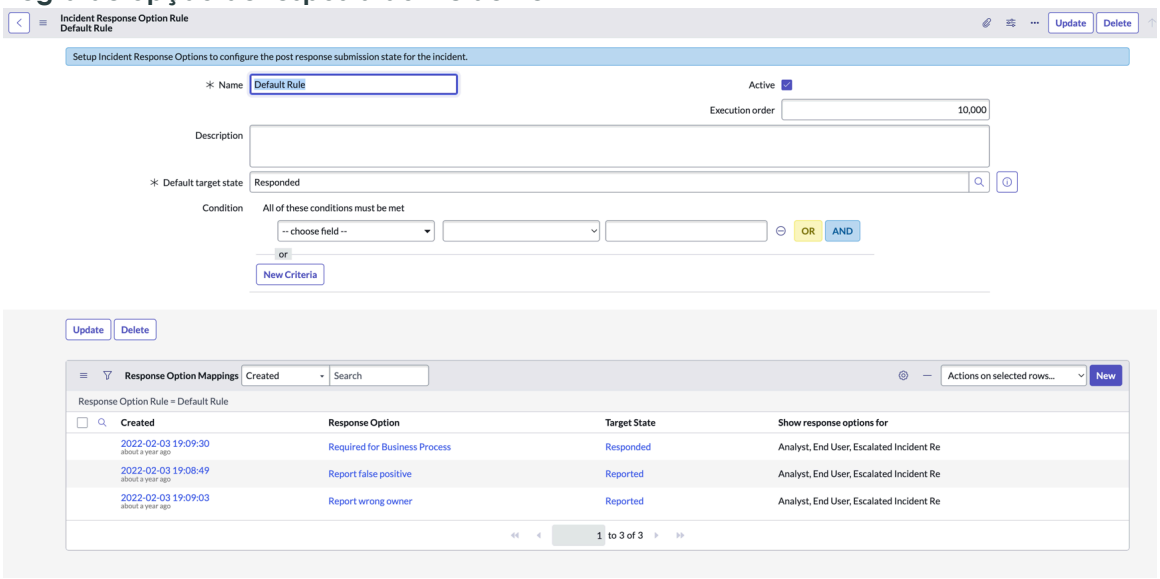
Example

O exemplo a seguir mostra a configuração de ação do usuário final para um endpoint. A condição requer que a origem da verificação seja um sistema de arquivos de endpoint que aciona esta configuração de ação do usuário final. O mapeamento mostra que o relatório de proprietário incorreto, o relatório de falso-positivo e o arquivo excluído são as opções de resposta disponíveis para o usuário final.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regra de opção de resposta do incidente



4. Na seção **Mapeamentos de opção de resposta**, clique em **Novo**.
5. No formulário, preencha os campos.

Formulário Mapeamento de opção de resposta

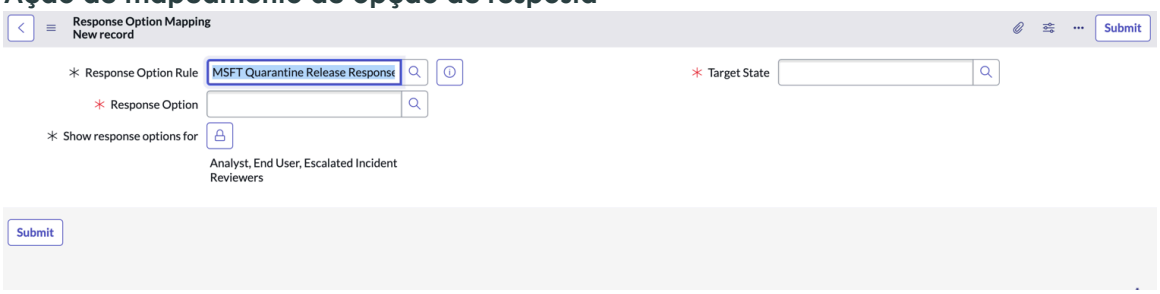
Regra de opção de resposta	Nome da regra de opção de resposta do incidente. Por exemplo, `SharePoint` implica que a origem da verificação é o SharePoint. Você pode inserir o nome da resposta do incidente ou pesquisar usando a pesquisa.
Opção de resposta	Opção para selecionar a opção de resposta. Você pode inserir a opção de resposta ou pesquisar usando a pesquisa.
Estado de destino	O estado de destino do incidente da DLP depois que o usuário final seleciona a ação apropriada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Nota: **a.** O campo **Estado de destino** aparecerá somente quando você selecionar a **Opção de resposta** que é do **Tipo: Básica**. Para obter mais informações sobre como os tipos de estado de destino são configurados, consulte Configurar opção de resposta para seus incidentes da DLP. **b.** Quando uma opção de resposta do **tipo: avançada** for selecionada, você não poderá definir o estado de destino e ele ficará oculto. O Estado de destino será atribuído com base no estado personalizado configurado no subfluxo do Flow Designer.
Mostrar opções de resposta para	Opção para determinar as funções do usuário para mostrar as opções de resposta. Você pode escolher entre **RevisoresAnalista**, **Usuário final** e Analista escalado usando a opção de desbloqueio. Você tem permissão para escolher uma ou todas as funções.

Ação de mapeamento de opção de resposta



6. Clique em **Enviar**.

Configurar opção de resposta para seus incidentes da DLP

Use este recurso para configurar o tipo de resposta que um usuário final ou analista deve executar.

Antes de Iniciar

A aplicação Incident Response do DLP do sistema de base fornece as seguintes opções de resposta:

1. Avaliação concluída

2. Conteúdo excluído

3. Arquivo excluído

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Arquivo criptografado
5. Conteúdo Mascarado
6. Relatar falso-positivo
7. Denunciar proprietário incorreto
8. Solicitar liberação de e-mail da quarentena

   Nota: Esta opção está disponível para os registros do Microsoft Exchange da DLP.

9. Necessário para processo de negócios
10. Direitos revisados

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Opções de resposta**.

   Por padrão, o sistema de base fornece dois tipos de opção de resposta:

   a. **Básica**: uma opção de resposta manual enviada pelo usuário.

   b. **Avançado**: uma opção de resposta automatizada aciona um subfluxo do Flow Designer quando o usuário envia a opção de resposta.

2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Opção de resposta do tipo: básica

Campo	Descrição
Nome	Insira o nome da opção de resposta do incidente.
Tipo	Opção para selecionar o tipo de opção de resposta.

Formulário Opção de resposta do tipo: Avançado

Campo	Descrição
Nome	Insira o nome da opção de resposta do incidente.
Tipo	Opção para selecionar a opção de resposta. Por padrão, este campo exibe os dois tipos de opções a seguir: ◦ **Básico**: ao selecionar esta opção ao criar uma nova opção de resposta, talvez seja necessário adicionar um nome de opção de resposta e o tipo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Avançado**: ao selecionar esta opção, os seguintes campos estarão disponíveis para seleção: ▪ **Fluxo**: selecione o subfluxo do Flow Designer. ▪ **Requer MID Server**: marque esta caixa de seleção se o fluxo selecionado usar o MID Server.
Fluxo	Selecione o fluxo do Flow Designer necessário para ativar a aplicação MID e a capacidade MID. Ao criar um subfluxo para a opção de resposta, adicione as seguintes entradas de subfluxo: **a. Nome**: ▪ dlp_incidente ▪ mid_server_capability ▪ mid_server_application **b. Tipo**: ▪ Referência (para a tabela de incidentes da DLP) ▪ SYS ID para a aplicação do MID Server e a capacidade do MID Server
Requer MID Server	Opção para determinar essa configuração do MID Server. Ao habilitar os campos **Aplicação** do **MIDServer e Capacidade** do MID Server, você pode configurar a Aplicação e a Capacidade do MID. **Nota:** Com base na configuração da aplicação do MID Server e da capacidade do MID Server, se algum MID estiver instalado e em execução, somente a opção de resposta ficará visível no espaço.
Aplicação do MID Server	Selecione a aplicação do MID Server necessária na lista suspensa.
Capacidade do MID Server	Selecione a capacidade do MID Server necessária na lista suspensa.

Nota: Se não houver nenhum MID Server disponível para a capacidade do MID Server selecionada, a opção de resposta não ficará visível. Se você quiser um MID Server específico da lista, será necessário configurar o app MID e torná-lo visível na lista. Em seguida, pelo menos um MID Server configurado deve estar ativo e em execução nas aplicações MID selecionadas e deve ter o Capacidade do MID Server selecionada.

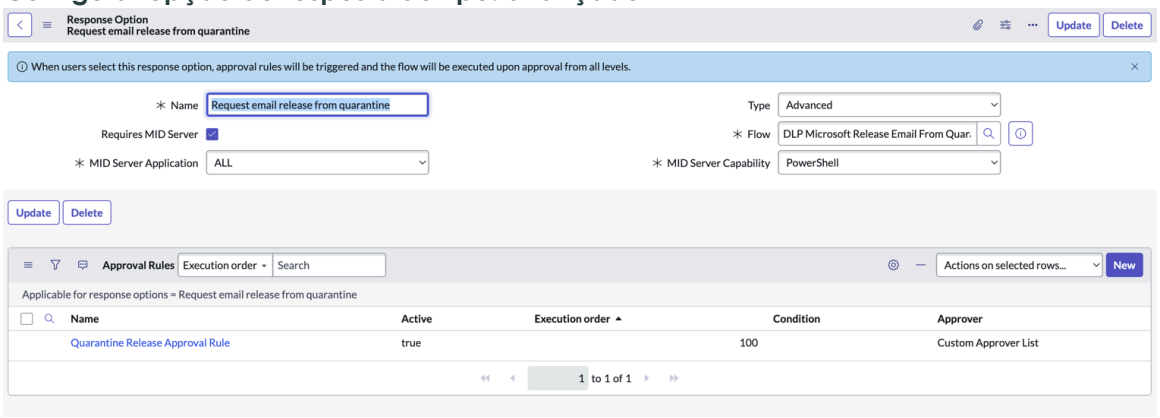
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.

> **Nota:** Se você estiver criando um tipo **Avançado** de opção de resposta, a lista relacionada **Regras de aprovação** será preenchida para você configurar a regra de aprovação para essa nova opção de resposta. Para obter mais informações, consulte Criar regras de aprovação.

Configurar opção de resposta do tipo: avançado



Criar configurações de gráfico de idade

Configure o gráfico de idade que aparece no Data Loss Prevention Incident Response (DLP IR) Portal de operações. Este gráfico mostra a contagem de incidentes em aberto pelo número de dias.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Configuração de gráfico de idade**.
2. Revise as entradas do gráfico de idade na tabela a seguir e personalize as entradas para seu ambiente.

Formulário Configurações da tabela etária da DLP

Nome	Condição
0 a 30 dias	Idade do incidente em aberto que está entre 0 e 30 dias.
31 a 60 dias	Idade do incidente em aberto que está entre 31 e 60 dias.
61 a 90 dias	Idade do incidente aberto que está entre 61 e 90 dias.
Mais de 90 dias	Idade do incidente em aberto que é superior a 90 dias.

3. Adicione uma nova configuração de gráfico de idade clicando em **Novo**.
4. No campo Nome, insira um **Nome** para a configuração do gráfico de idade da DLP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Defina as condições para a configuração do gráfico de idade da DLP.

   a. Para adicionar condições, clique em **E** ou **OU**.
      - Se **E** for selecionado, todas as condições deverão ser atendidas.
      - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

      Nota: As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.

   b. Para definir uma segunda condição de filtro, clique em **Novos critérios**.

6. Clique em **Enviar**.

Criar configurações de delegado de usuário

Impeça que determinados executivos da organização recebam notificações sobre os incidentes atribuídos ou escalonados para eles.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Considere um cenário em que o executivo é um usuário que pertence a um grupo executivo ou de liderança. O executivo não deve receber e-mails sobre atribuição ou escalação de incidentes. Um usuário delegado pode executar a ação necessária em nome do executivo.

Depois que um usuário tiver atribuído uma pessoa específica, Henry, como delegado, outro usuário não poderá atribuir Henry como delegado novamente. Da mesma forma, um delegado não pode atribuir outro usuário como delegado.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Delegar configuração**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Delegar formulário de configuração

Campo	Descrição
Usuário	Nome do usuário que precisa de um delegado para incidentes do DLP.
Delegado	Nome do usuário que pode responder ao incidente da DLP em nome do usuário final original.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar regras de identificação de infratores reincidentes

Crie regras de identificação de infratores reincidentes para identificar usuários que repetem o mesmo problema várias vezes.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode identificar infratores reincidentes usando determinadas regras ou critérios. Data Loss Prevention Incident Response fornece campos que você pode usar para identificar infratores reincidentes.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Regras de identificação de infrator reincidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regras de identificação de infrator reincidente

Campo	Descrição
Nome	Nome da regra de identificação de infrator reincidente.
Ordem de execução	Prioridade das regras de identificação de infratores reincidentes. Este campo indica a ordem na qual as regras de identificação de infratores reincidentes são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de identificação de infrator reincidente com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Descrição resumida	Descrição exclusiva desta regra de identificação de infrator reincidente.
Condição	Condições no construtor de condições que se baseiam na tabela de incidentes da DLP. Você pode selecionar qualquer um dos campos de incidente para criar a condição do gatilho para a regra de identificação de infrator reincidente.

Tradução automática

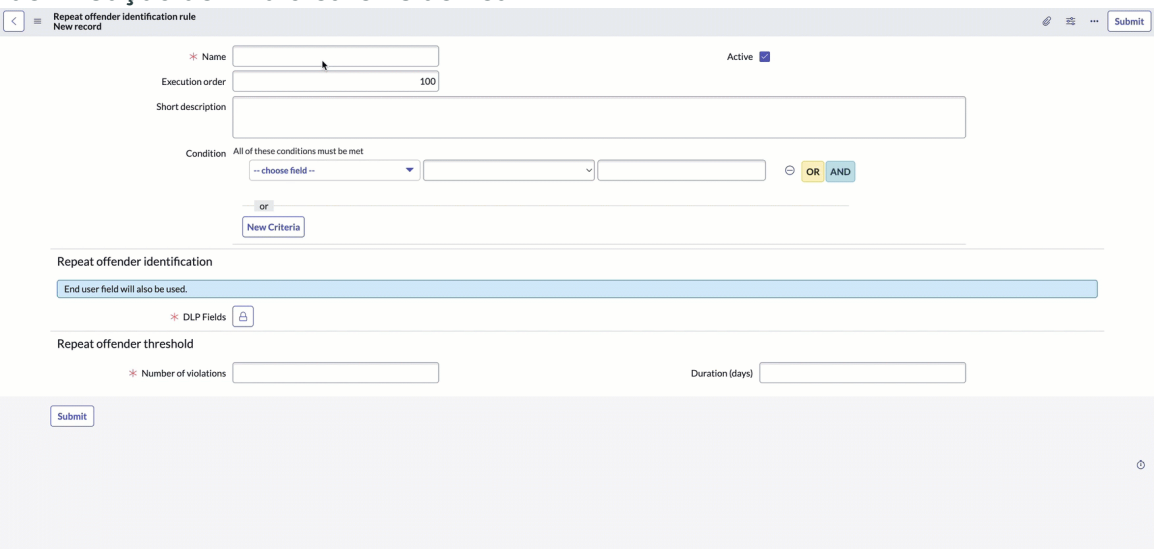
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Campos da DLP	Identifique os infratores reincidentes com base nos campos obrigatórios da DLP. Clique no ao lado dos Campos da DLP para exibir a lista de campos da DLP disponíveis. Selecione os campos da DLP que você deseja usar na coluna Disponível e mova-os para a coluna Selecionado. Por exemplo, você pode selecionar os campos**Nome do arquivo** e **Proprietário** do arquivo na coluna Disponível e movê-los para a coluna Selecionado. Em seguida, você pode identificar os infratores reincidentes com base nos campos **Nome do arquivo** e **Proprietário do arquivo**. Portanto, se um usuário violar o limite de infrator reincidente (número de violações e duração) e se o mesmo usuário corresponder aos campos da DLP, esse usuário específico será identificado como reincidente.
Número de violações	Defina o valor limite do infrator reincidente. Depois que o usuário repete as mesmas ações e viola o número especificado de violações, o usuário é identificado como um infrator reincidente.
Duração (em dias)	Defina o limite do infrator reincidente na forma de dias. Depois que o usuário repete as mesmas ações e viola o limite de duração, o usuário é identificado como um infrator reincidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificação de infratores reincidentes



4. Clique em **Enviar**.

Criar campos personalizados

Crie seus campos personalizados para os incidentes da DLP. Você pode criar diferentes tipos de campos personalizados, como cadeia de caracteres, número, caixa de seleção, opção, data e hora, e usá-los nos formulários de incidentes da DLP.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Importante: Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior.

Por Que e Quando Desempenhar Esta Tarefa

Os campos personalizados são associados a restrições de nível de campo. Portanto, se houver restrições de nível de campo, elas se aplicarão aos campos personalizados no portal de operações da DLP e no portal do usuário final.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Campos personalizados**.
2. Crie um campo personalizado clicando em **Novo**.
3. No formulário, preencha os campos.

Formulário Campo personalizado da DLP

Campo	Descrição
Nome	Nome do campo personalizado.
Tipo	Opção para selecionar o tipo de campo personalizado. Você pode escolher um dos seguintes tipos:

Tradução automática

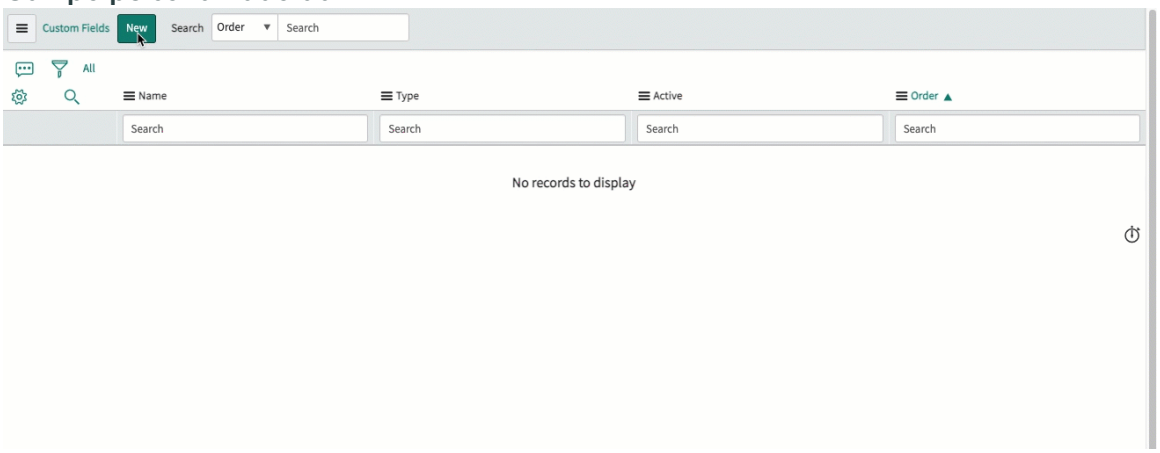
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Cadeia de caracteres** ◦ **Número** ◦ **Caixa de seleção** ◦ **Opção** Se você selecionar o tipo de campo personalizado como **Opção**, depois de criar o campo personalizado, poderá definir as opções de escolha do campo personalizado. Para criar uma opção de escolha de campo personalizado: **a.** Abra o campo personalizado necessário. **b.** Na seção Opções do campo de seleção personalizado, clique em **Novo**. **c.** No campo Nome da opção, defina o nome da opção necessária. **d.** Clique em **Enviar**. ◦ **Data** ◦ **Data/Hora** **Nota:** Depois de selecionar um tipo para o novo campo personalizado, você não terá permissão para modificá-lo. Se você quiser modificar o tipo, precisará criar um novo campo personalizado novamente com o tipo necessário.
Ordem	Opção para escolher a ordem em que os campos personalizados devem ser exibidos. Você pode definir o valor da ordem para cada campo personalizado. Os campos personalizados são classificados com base nos valores de ordem que você define. Por padrão, os campos personalizados são classificados em ordem crescente. Você pode classificar os campos personalizados em ordem decrescente clicando na coluna **Ordem**.
Ativo	Opção para indicar se o campo personalizado está ativo.
Descrição	Descrição do campo personalizado que você criou.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo personalizado da DLP



4. Clique em **Enviar**.

Definir configurações avançadas

Defina as configurações avançadas para que você possa determinar os campos no Incidente para identificar os usuários finais, entre outras capacidades.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Definir configurações avançadas no Data Loss Prevention Incident Response é opcional. Algumas configurações avançadas incluem o seguinte:

- Defina o número máximo de incidentes que podem ser enviados em um e-mail de resumo.
- Habilite o modo rápido para enviar e-mails mais rapidamente.
- Determine o detalhamento do log da aplicação.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Configurações Avançadas**.
2. No formulário, preencha os campos.

Formulário Configurações avançadas

Campo	Descrição
Os dados confidenciais que causaram a violação devem ser exibidos no incidente?	Opção para escolher se você deseja exibir os dados confidenciais que causaram a violação no incidente da DLP. Por padrão, esta opção está habilitada.
Os dados confidenciais que causaram a violação também devem ser exibidos nos incidentes secundários?	Opção para escolher se você também deseja exibir os dados confidenciais

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	que causaram a violação no incidente secundário da DLP. Por padrão, esta opção está desativada.
Lista de campos no incidente que são usados para identificar o usuário final	A lista de campos no incidente do módulo Regra de atribuição que são usados para identificar o usuário final. Você também pode especificar seus próprios atributos personalizados para identificar o usuário final.
Número máximo de incidentes em um e-mail de resumo	O número máximo de incidentes que podem ser enviados em um e-mail de resumo. Por padrão, o valor é 100.
Duração máxima da infração reincidente (em dias)	A duração máxima para identificar um infrator reincidente. Por padrão, o valor é 90 dias.
Modo rápido para enviar e-mails	Opção para validar e-mails e identificar problemas. Você pode executar a validação habilitando a opção **Sim**. Por padrão, esta opção está habilitada.
Esta propriedade é usada para definir o detalhamento do log da aplicação	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ◦ **error** ◦ **aviso** ◦ **informações** ◦ **depurar** Por padrão, o valor é **info**.
Excluir incidentes secundários e clonados de relatórios	Opção para excluir os incidentes clonados e secundários dos relatórios. Por padrão, esta opção é **Sim**.
Dia(s) de espera pela exclusão do conteúdo de correspondência no armazenamento em nuvem após o incidente ser encerrado	Opção para escolher o número de dias de espera para limpar o conteúdo de correspondência dos incidentes que estão inativos por um período de tempo específico. Por padrão, o valor é 90. Após 90 dias, se o incidente da DLP estiver inativo, o conteúdo de correspondência será limpo do armazenamento em nuvem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuir incidente ao grupo de analistas de DLP após o último nível de escalação	Marque esta caixa de seleção para atribuir o incidente ao analista após o último nível de escalação.
Permitir que os usuários acessem os incidentes após a escalação	Marque esta caixa de seleção para permitir que os usuários atribuídos acessem o(s) incidente(s) após a escalação. Quando você seleciona esta opção, todos os usuários que foram adicionados à lista da cadeia de escalação poderão acessar o(s) incidente(s).
Permitir que o analista edite a avaliação concluída	Marque esta caixa de seleção para permitir que o analista edite a avaliação concluída. Quando você seleciona esta opção, os analistas podem editar as Avaliações. Quando ela está desmarcada, você pode exibir as avaliações no modo Somente leitura.

3. Clique em **Salvar**.

Monitorar o processo de execução da integração da DLP

Rastreie e monitore a ingestão contínua ou o processo de execução da integração. Os processos de execução de integração contêm as estatísticas sobre a quantidade de dados que foi processada e o status da integração.

Função necessária: sn_dlir.admin.

O processo de execução da integração lista os detalhes sobre quantos registros foram ingeridos. Por exemplo:

1. Na integração da Symantec, o processo contém execuções de integração primária e secundária. O registro primário indica os dados de ingestão e o registro secundário indica as chamadas de aprimoramento e os registros de atributo personalizado.
2. Na integração da Microsoft, há apenas o processo de ingestão de registro primário a ser executado.

Processos de execução de integração da DLP: exibe as entradas da fila, o status das entradas da fila e os registros obtidos.

A execução de integração contém a Origem para a qual o perfil de integração e o registro de execução de integração são criados, intervalos de pesquisa de perfil, estados e subestados de ingestão, contagem de incidentes que indica o número de registros que são ingeridos.

1. Navegar até **Administração da DLP** > **Execuções de Integração**.
2. Selecione a execução de integração na lista.
3. Navegue até a **Integração da DLP Executar processo**.
4. Exibir o status de entrada da fila do registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrições de acesso a incidentes da DLP

Gerencie a visibilidade de um incidente específico do DLP que contém informações confidenciais. Você pode usar restrições de acesso a incidentes para definir quem pode acessar um incidente específico do DLP e restringir o acesso de usuários ou grupos específicos a esse incidente.

Criar restrições de nível de campo

Defina restrições de nível de campo em incidentes do DLP para proteger informações confidenciais contra exposição. Você pode usar restrições de nível de campo para controlar os usuários ou grupos que podem acessar campos específicos nos incidentes do DLP.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As restrições de nível de campo permitem que você exiba somente determinados campos para usuários ou grupos específicos, fornecendo uma maneira mais granular de controlar os dados que um usuário pode acessar. Você pode criar uma restrição de nível de campo definindo as condições de correspondência de incidentes da DLP, selecionando os usuários ou grupos aos quais essas condições se aplicam e escolhendo os campos da DLP que esses usuários ou grupos podem exibir.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Restrições de acesso a incidentes** > **Restrições de nível de campo**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de restrição de nível de campo da DLP

Campo	Descrição
Nome	Nome da restrição de nível de campo.
Ativo	Opção para indicar se a restrição de nível de campo está ativa.
Ordem de execução	Prioridade das restrições de nível de campo. Este campo indica a ordem na qual as restrições de nível de campo são executadas quando duas ou mais restrições de nível de campo compartilham as condições de acionamento. A restrição de nível de campo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Descrição resumida	Descrição exclusiva desta restrição de nível de campo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição de correspondência de incidente	Opções no incidente que correspondem às condições definidas. Você pode selecionar qualquer um dos campos de incidente para definir a condição do gatilho para as restrições de nível de campo. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode selecionar o campo como `Nome da política`e definir a condição como `em`e `Nome da política`. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas.
Aplica-se a	Opção para aplicar as condições de correspondência de incidente a usuários ou grupos específicos. Você pode aplicar as condições ao seguinte: ◦ **Todos os usuários finais**: opção para selecionar todos os usuários finais aos quais as condições de incidente da DLP são aplicáveis. ◦ **Todos os revisores de incidentes escalonados**: opção para selecionar todos os revisores de incidentes escalonados aos quais as condições de incidente da DLP são aplicáveis. Isso se refere a todos os incidentes do DLP escalados para o gerente. ◦ **Usuários**: clique no para adicionar um usuário específico da lista ao qual as condições de incidente da DLP são aplicáveis. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário ao qual as condições da DLP são aplicáveis, clique no ◦ **Grupos**: clique no ícone de para adicionar um grupo específico da lista ao qual as condições de incidente da DLP são aplicáveis. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.

Tradução automática

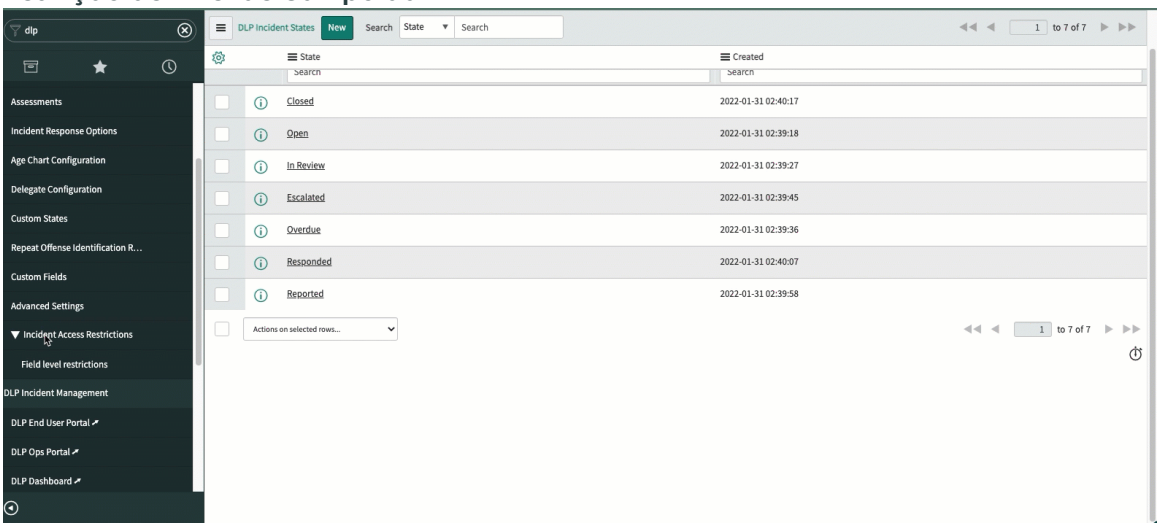
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Permitir acesso somente aos seguintes campos	◦ **Campos da DLP**: opção para definir os campos da DLP que você deseja permitir o acesso aos usuários ou grupos selecionados. Selecione os campos da DLP aos quais você deseja permitir o acesso na coluna Disponível e mova-os para a coluna Selecionado. **Nota:** Os usuários ou grupos selecionados poderão acessar somente os campos da DLP selecionados. Por exemplo, você pode selecionar os campos**Atribuído a** e **Aberto** na coluna Disponível e movê-los para a coluna Selecionado. Em seguida, os usuários ou grupos selecionados têm acesso somente aos campos Atribuído a e Aberto. ◦ **Carregar anexos**: opção para indicar se você deseja permitir que os usuários ou grupos selecionados carreguem anexos. ◦ **Campos personalizados**: opção para definir os campos personalizados que você deseja permitir o acesso aos usuários ou grupos selecionados. Você pode exibir os campos personalizados que criou na coluna Disponível. Selecione os campos personalizados que você deseja permitir o acesso na coluna Disponível e mova-os para a coluna Selecionado. **Importante:** ▪ Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior. ▪ Os usuários ou grupos selecionados poderão acessar somente os campos personalizados selecionados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrição de nível de campo da DLP



4. Clique em **Enviar**.

Criar restrições de nível de registro

Defina restrições de nível de registro em incidentes do DLP para proteger registros confidenciais contra exposição. Você pode usar restrições de nível de registro para controlar os usuários ou grupos que podem acessar registros específicos nos incidentes da DLP.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibição (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As restrições de nível de registro permitem que você forneça acesso a registros somente para usuários ou grupos específicos, fornecendo uma maneira mais granular de controlar os registros que um usuário pode acessar. Você pode criar uma restrição de nível de registro definindo as condições de correspondência de incidentes da DLP, selecionando os usuários ou grupos aos quais essas condições se aplicam e escolhendo os registros da DLP que esses usuários ou grupos podem exibir.

Procedimento

1. Navegar até **Todos** > **Administração da DLP** > **Restrições de acesso a incidentes** > **Restrições de nível de registro**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de restrição de nível de registro da DLP

Campo	Descrição
Nome	Nome da restrição de nível de registro.
Descrição resumida	Descrição exclusiva desta restrição de nível de registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

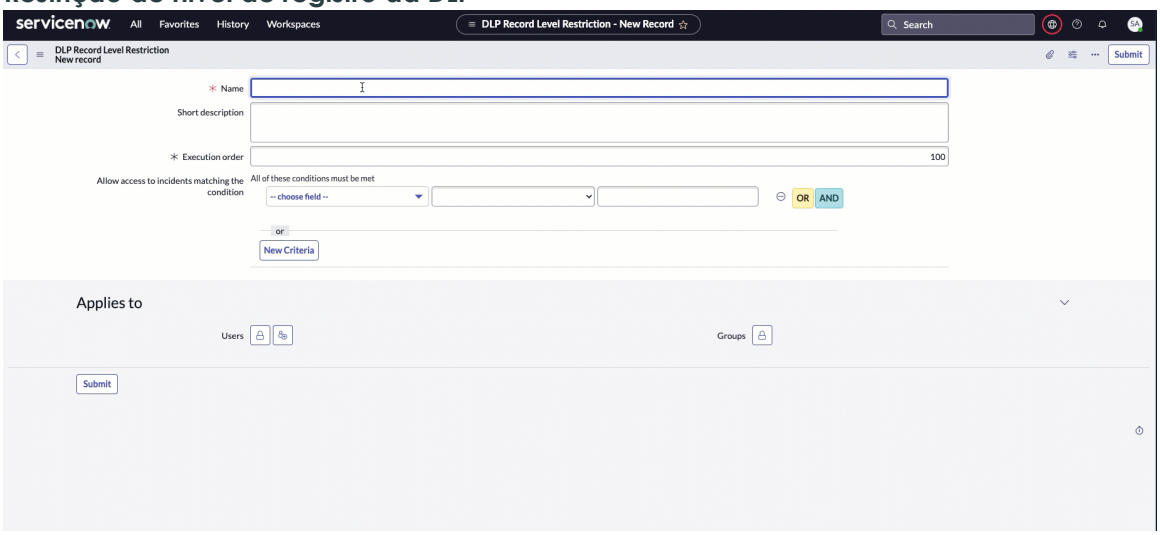
Campo	Descrição
Ordem de execução	Prioridade das restrições de nível de registro. Este campo indica a ordem na qual as restrições de nível de registro são executadas quando duas ou mais restrições de nível de registro compartilham as condições de acionamento. A restrição de nível de registro com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Permitir acesso a incidentes que correspondem à condição	As opções permitem o acesso aos incidentes que correspondem às condições definidas. Você pode selecionar qualquer um dos campos de incidente para definir a condição do gatilho para as restrições de nível de registro. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ◦ Se **E** for selecionado, todas as condições deverão ser atendidas. ◦ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no Construtor de condições fazem distinção entre maiúsculas e minúsculas. Por exemplo, você pode selecionar o campo como `Ativo`e definir a condição como `é`e `verdadeira`.
Aplica-se a	Opção para aplicar restrições de nível de registro a usuários ou grupos específicos. Você pode aplicar as condições da seguinte forma: ◦ **Usuários**: clique no para adicionar um usuário específico da lista ao qual o registro selecionado se aplica. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário ao qual o registro se aplica, clique no . Por exemplo, administrador do sistema. ◦ **Grupos**: clique no para adicionar um grupo específico da lista ao qual o registro selecionado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	se aplica. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.

Restrição de nível de registro da DLP



4. Clique em **Enviar**.

Arquivamento de incidentes da DLP

O Data Loss Prevention Incident Response é provisionado com uma regra de arquivamento no sistema de base para a tabela de incidentes do DLP. Os registros relacionados também são adicionados no sistema de base à regra de arquivamento de incidentes da DLP.

Antes de Iniciar

Função necessária: administrador

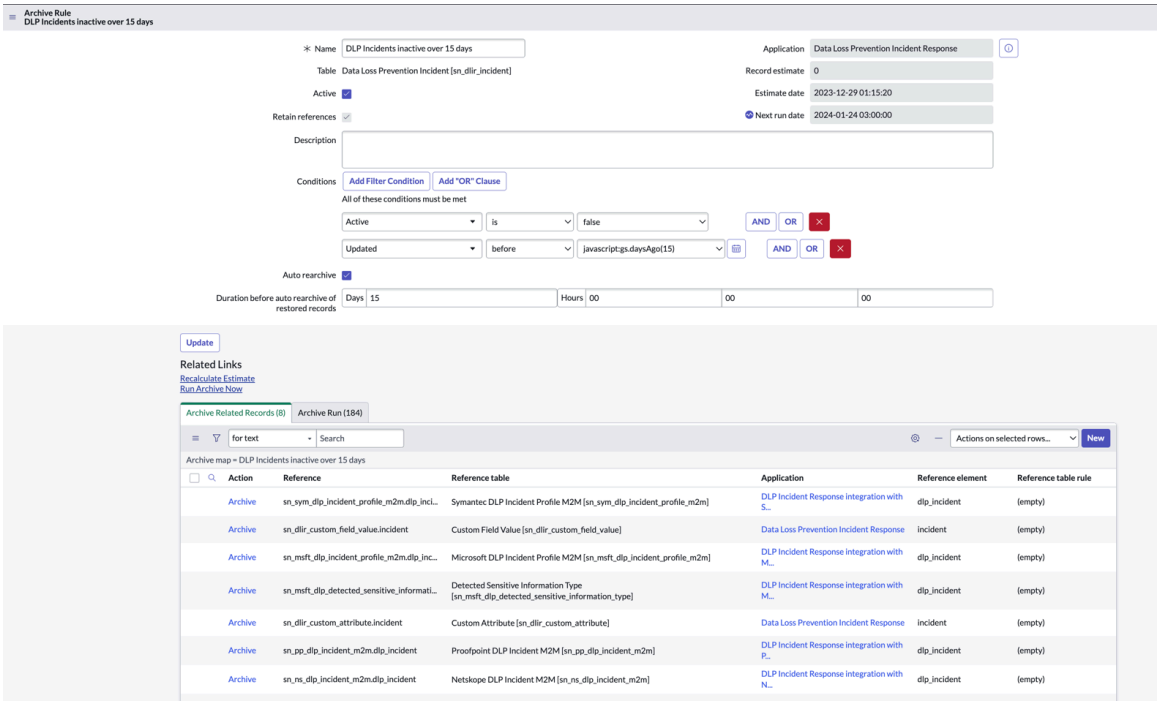
Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
   As regras de arquivamento do sistema que estão no sistema de base são exibidas.
2. Exiba a regra de arquivamento da DLP.

> **Nota:** **Incidentes da DLP inativos por mais de 15 dias** são a regra de arquivamento do sistema de base padrão para incidentes da DLP. Você pode modificar a regra de arquivamento se necessário. Esta regra significa que os incidentes que estão inativos acima de 15 dias serão arquivados automaticamente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Para obter informações sobre como as regras de arquivamento são criadas, consulte Criação de uma regra de arquivamento .

3. **Atualize** a regra, se necessário.

Arquivar registros relacionados à DLP

Use a lista relacionada Arquivar registros relacionados para incidentes da DLP para adicionar os registros relacionados à regra de arquivamento.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
2. Selecione a regra de arquivamento **de incidentes da DLP inativos por mais de 15 dias**.
3. Acesse a lista relacionada **Arquivar registros** relacionados.
4. Exibir os registros relacionados ao DLP.

Aplicação	Tabela de Referência
Integração de Resposta a incidentes do PPD com Symantec	Perfil de incidentes do Symantec DLP M2M [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	Valor do campo personalizado [sn_dlir_custom_field_value]
Integração de Resposta a incidentes do PPD com Microsoft	Perfil de incidentes do Microsoft DLP M2M [sn_msft_dlp_incident_profile_m2m]

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Tabela de Referência
Integração de Resposta a incidentes do PPD com Microsoft	Tipo de informação confidencial detectada [sn_msft_dlp_detected_sensitive_information_type]
Data Loss Prevention Incident Response	Atributo personalizado [sn_dlir_custom_attribute]
Integração de Resposta a incidentes do PPD com Proofpoint	Incidente do Proofpoint do DLP M2M [sn_pp_dlp_incident_m2m]
DLP Incident Response integration with Netskope	Incidente do Netskope DLP M2M [sn_ns_dlp_incident_m2m]
Integração de Resposta a incidentes do PPD com Symantec	Tipo de informação confidencial detectada [sn_sym_dlp_detected_sensitive_information_type]

Nota: Todas as tabelas do sistema, como e-mails, avaliações e anexos, serão direcionadas automaticamente para o registro arquivado da DLP.

5. Selecione a regra de registro relacionado ao arquivamento que você deseja arquivar.

Nota: Para obter mais informações sobre como adicionar mais registros relacionados, consulte Arquivar registros relacionados ao DLP em Now Platform.

Data Loss Prevention Incident Response Gestão de incidentes

Use a Data Loss Prevention Incident Response Gestão de incidentes para atualizar e gerenciar incidentes aproveitando o Espaço do usuário da DLP, o Espaço do analista da DLP e o Painel da DLP.

Data Loss Prevention Incident Response Espaço do usuário

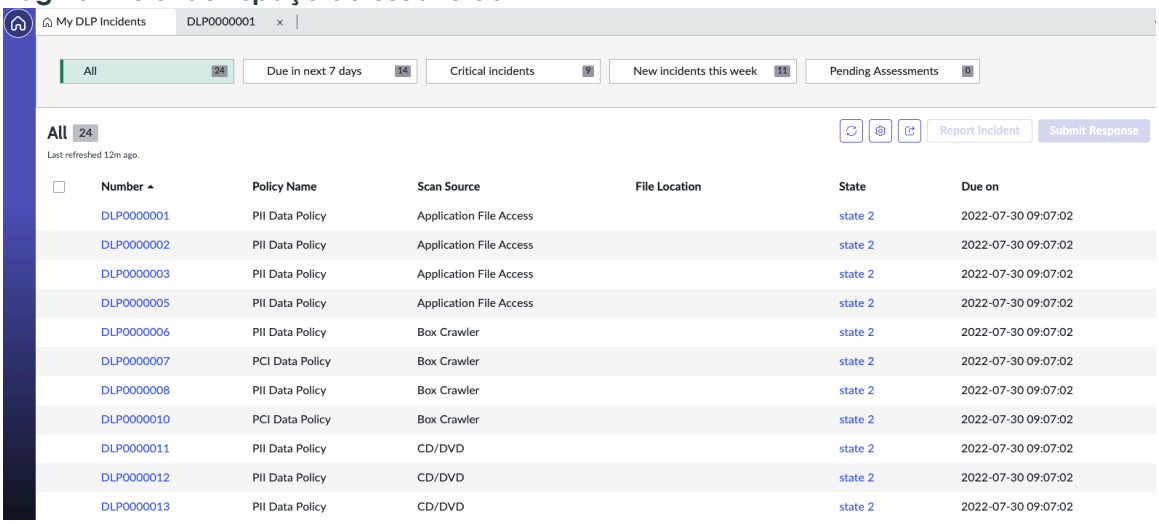
O espaço do usuário Data Loss Prevention Incident Response (DLP IR) é um espaço onde usuários finais, gerentes e aprovadores podem responder aos incidentes atribuídos ao DLP. Os usuários finais, gerentes e aprovadores podem responder aos incidentes especificando as ações corretas.

Você também pode criar e gerenciar avaliações para permitir que os usuários finais respondam a incidentes do DLP. O espaço consiste em uma página principal e exibições de lista que permitem que você veja os incidentes atribuídos ao DLP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página inicial do Espaço do usuário da DLP



Relatar ou responder a incidentes da DLP

Acesse o espaço do usuário Data Loss Prevention Incident Response (DLP), revise os incidentes atribuídos ao DLP e relate ou responda aos incidentes.

Antes de Iniciar

Função necessária:

- Qualquer usuário/funcionário válido

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do usuário da DLP**.
   A página Meus incidentes da DLP é aberta em uma nova guia.
2. Clique em uma exibição de lista para revisar os incidentes atribuídos a você.

Exibição em lista	Descrição
Todos	Exibir todos os incidentes atribuídos.
Vencimento nos próximos 7 dias	Exibir todos os incidentes que vencem nos próximos 7 dias.
Incidentes críticos	Exiba todos os incidentes com o rótulo de gravidade crítica.
Novos incidentes esta semana	Exibir todos os incidentes atribuídos esta semana.
Avaliações pendentes	Exibir todas as avaliações que ainda estão pendentes.

3. Você pode revisar os incidentes da DLP de duas maneiras:

   a. A primeira maneira é localizar e selecionar um ou mais incidentes do DLP que você deseja revisar e clicar na caixa de seleção ao lado dos incidentes.

   b. Escolha a opção apropriada para você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

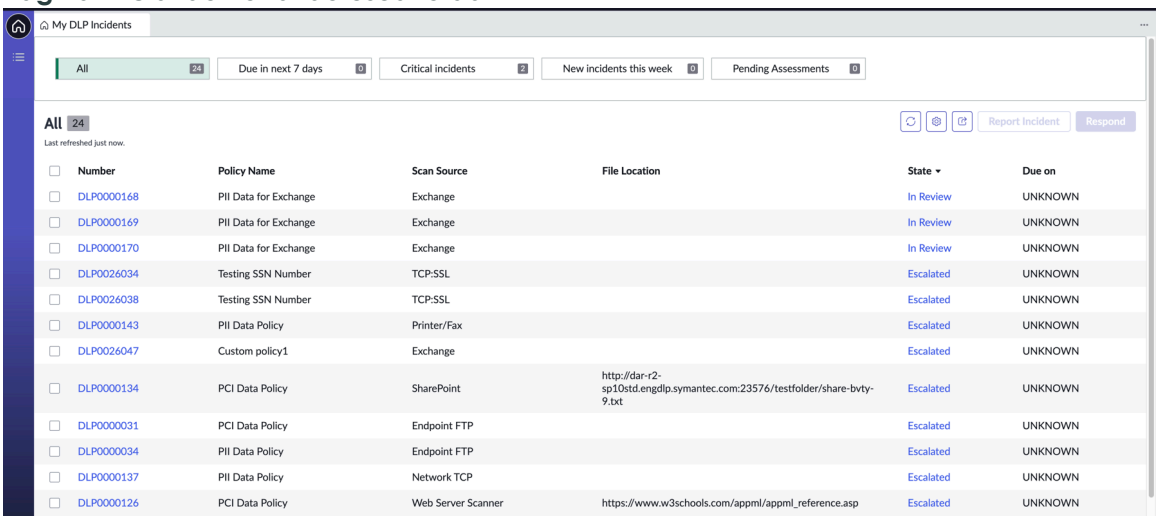
Página inicial do portal do usuário final da DLP

Opção	Descrição
Atualizar lista	Opção para atualizar a lista de incidentes do DLP se você tiver feito uma atualização.
Ações da lista	Lista de ações que você pode executar. Estas são as opções: ▪ **Salvar como** ▪ **Editar colunas** ▪ **Redefinir larguras** **Nota:** Quando você tiver sua própria lista personalizada, criada na seção **Minhas listas** configurada para o seu espaço, também poderá executar as ações de lista adicionais abaixo: ▪ **Renomear** ▪ **Salvar** ▪ **Excluir**
Copiar URL para todos	Opção para copiar os URLs de todos os incidentes do DLP.
Relatar incidente	Ação para relatar o incidente como falso-positivo ou responsável incorreto. Por exemplo, você pode denunciar um proprietário incorreto e sugerir outro proprietário ou relatar o incidente como um falso-positivo.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política da DLP, o usuário poderá escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários. A partir daqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página inicial do Portal do usuário da DLP



c. A segunda maneira é clicar em um incidente do DLP específico para abri-lo. A guia **Detalhes** exibe as seguintes seções:

- Detalhes: você pode exibir os detalhes do incidente do DLP, como número do incidente, gravidade e nome do arquivo.
- Compor: para adicionar comentários sobre o incidente do DLP que estão visíveis para todos, insira os comentários na guia Comentários. Para adicionar comentários que ficam visíveis para determinadas pessoas, insira os comentários na guia Anotações de trabalho (privado).
- Atividade: você pode exibir os detalhes das diferentes atividades no incidente da DLP.
- Anexos: se você tiver anexos relacionados ao incidente do DLP, clique em **Procurar** e selecione o anexo na sua unidade local.

  A guia **Detalhes adicionais** exibe todas as informações adicionais sobre o incidente do DLP, incluindo campos personalizados.

Importante:

- Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior.
- Se houver dados de campos personalizados disponíveis para um incidente do DLP específico, você poderá exibi-los na guia **Detalhes adicionais**. Se não houver campos personalizados para o incidente da DLP, você verá uma página em branco.

- **Tipo de**informação confidencial detectada: exibe as informações confidenciais detectadas do incidente.

Nota: Esta lista relacionada está visível somente para os incidentes do DLP criados para integrações da Microsoft ou da Symantec. No registro de incidentes da Microsoft ou da Symantec, sempre que o usuário acessa o registro de tipo de informação confidencial detectado, o conteúdo de correspondência realçado em relação a essa integração é exibido.

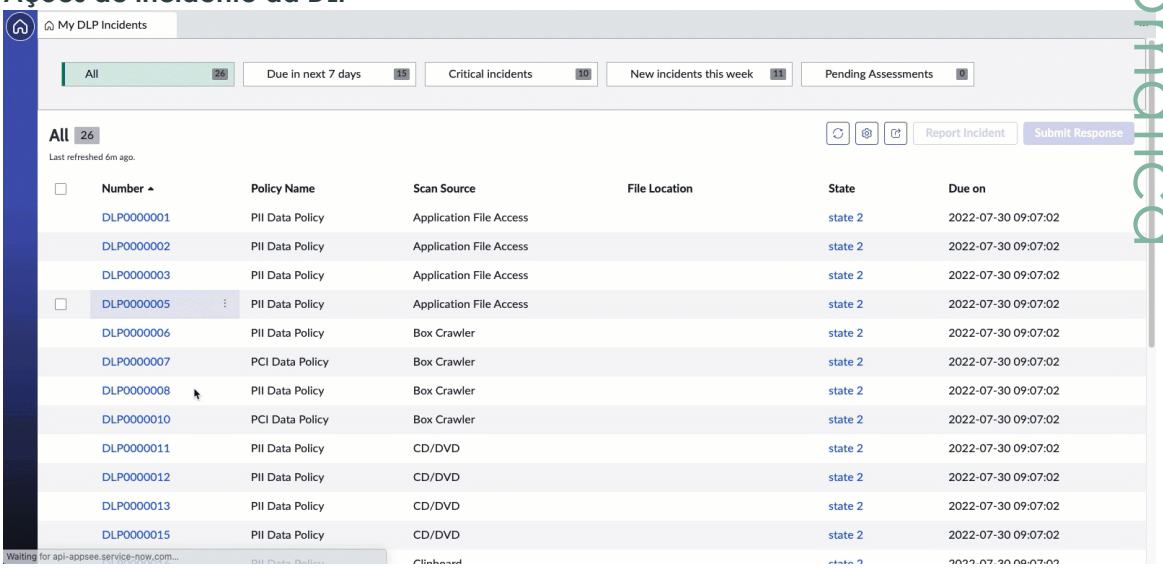
d. Escolha a opção apropriada para você.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Relatar falso-positivo	Ação para relatar que o incidente da DLP foi acionado ou criado incorretamente. Você pode mencionar os detalhes do motivo pelo qual marcou o incidente como falso-positivo no campo Comentários.
Relatar responsável incorreto	Ação para relatar que o incidente do DLP foi atribuído ao usuário incorreto. Se você souber o proprietário correto do incidente, poderá selecionar o nome do proprietário no campo Proprietário sugerido. Para adicionar detalhes adicionais, use o campo Comentários.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política da DLP, o usuário poderá escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários. A partir daqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena**.

Ações de incidente da DLP



4. Para fazer avaliações, selecione a exibição de lista **Avaliações pendentes**.

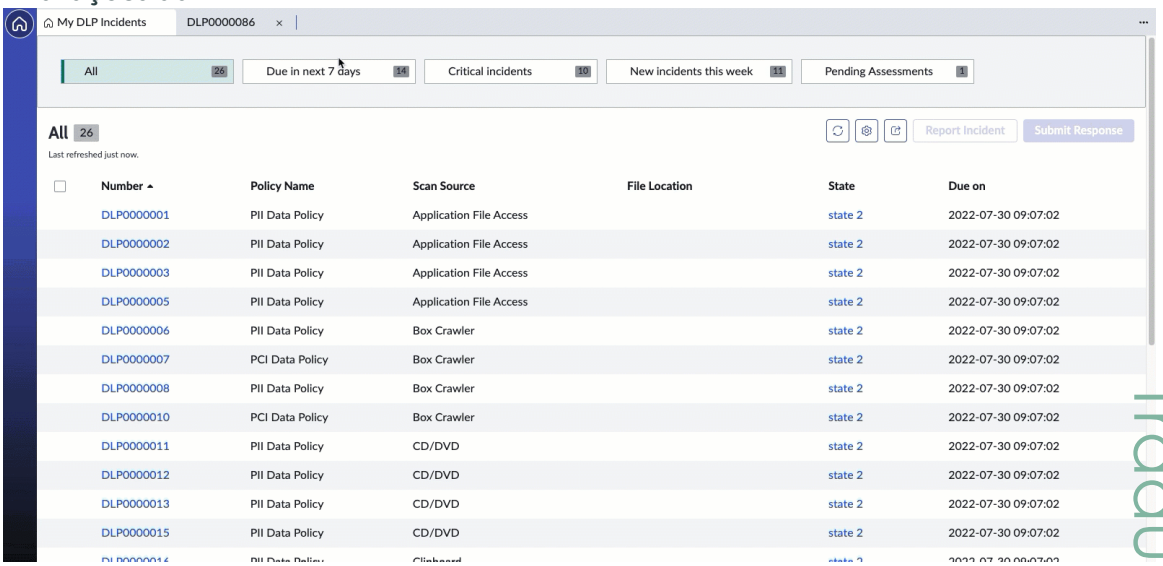
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em um número de avaliação específico para abri-lo.

b. Responda às perguntas de avaliação e clique em **Salvar** ou **Enviar** com base em seus requisitos.

Avaliações da DLP



5. Clique na seção do cartão **Instruções** que é exibida na parte superior de todos os campos na exibição do formulário de incidente da DLP para exibir as informações adicionais sobre um incidente específico.

Nota: Esta seção no espaço orienta os usuários sobre as informações do incidente, o que ajuda a entender as próximas etapas da resolução do incidente.

O cartão de instruções do usuário exibe dois cabeçalhos diferentes que fornecem mais informações sobre um incidente específico na exibição do formulário. Clique em qualquer cabeçalho de instrução do usuário para saber os detalhes adicionais.

Para obter mais informações, consulte Criar modelos de instruções do usuário e Configurar instruções do usuário de IU da DLP.

Como trabalhar com o módulo Minhas aprovações

O módulo Minhas aprovações estará disponível no Espaço de usuários da DLP para os usuários conectados. Os usuários podem aprovar ou rejeitar as solicitações de aprovação de atribuição aqui.

Antes de Iniciar

Função necessária:

- Usuário final
- Gerente
- Aprovador

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do usuário da DLP**.
A página **Meus incidentes da DLP** será exibida em uma nova guia.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Clique no módulo **Minhas aprovações** presente no módulo **Meus incidentes da DLP**. A exibição da lista Minhas aprovações será exibida.

   O aprovador pode aprovar ou rejeitar as solicitações na exibição de lista da página **Minhas aprovações**. É possível aprovar ou rejeitar as várias solicitações na exibição de lista.

   O aprovador pode exibir os detalhes da solicitação atribuída na exibição do formulário. Ao clicar na ação **Aprovar** ou **Rejeitar** na exibição do formulário, é possível aprovar ou rejeitar a solicitação individual.

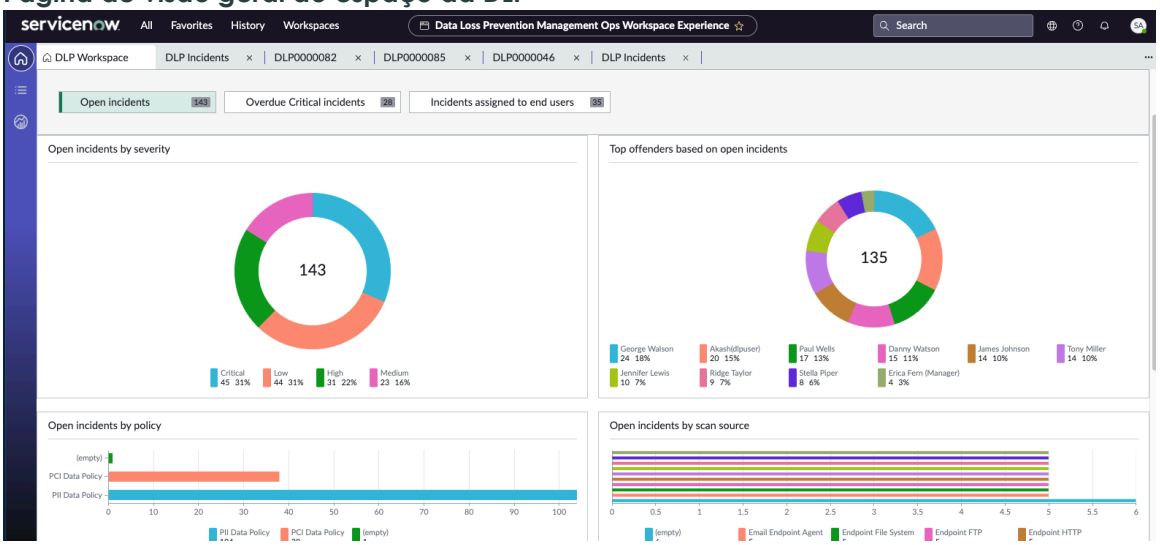
   Nota: Para exibir os detalhes do incidente da DLP, clique no disponível no campo **Aprovar**.

Data Loss Prevention Incident Response Espaço do analista

Use o espaço do analista Data Loss Prevention Incident Response (DLP IR) para exibir os incidentes da DLP. Atribua os incidentes a usuários finais para resolução e muito mais.

O espaço da DLP consiste em uma página inicial com painéis, exibições de lista e exibições de formulário que permitem monitorar incidentes da DLP.

Página de visão geral do espaço da DLP



Revisar e atribuir seus incidentes da DLP

Acesse o espaço do analista Data Loss Prevention Incident Response (DLP IR) para que você possa revisar os incidentes da DLP e atribuí-los ou resolvê-los. Você pode rastrear tendências em incidentes por gravidade, principais infratores, incidentes por origem de verificação e incidentes por política.

Página inicial do espaço da da DLP

Visão geral do espaço da Visão geral do espaço da DLP

Antes de Iniciar

Função necessária:

- sn_dlir.analyst — Editar e exibir incidentes da DLP.
- sn_dlir.analyst_read e sn_dlir.read — Exibir incidentes da DLP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do analista da DLP**.
   A página da lista de operações Meus incidentes do espaço da DLP é aberta em uma nova guia.
2. Clique no ícone da página inicial do espaço da **DLP** para exibir a exibição da página inicial do espaço.
3. Revise os widgets do painel para identificar tendências por incidentes por gravidade, principais infratores, incidentes por origem de verificação e incidentes por política.
4. Clique nos filtros apropriados na página inicial para exibir os widgets por suas várias categorias.

Filtros	Descrição
Incidentes abertos	Exibir todos os incidentes em aberto.
Incidentes críticos atrasados	Exiba os incidentes que têm o rótulo de gravidade crítica e que estão atrasados.
Incidentes atribuídos a usuários finais	Exibir os incidentes atribuídos a usuários finais.

5. Você pode revisar e atribuir os incidentes da DLP de duas maneiras:

   a. A primeira maneira é localizar e selecionar um ou mais incidentes do DLP que você deseja revisar e clicar na caixa de seleção ao lado dos incidentes.

   b. Escolha a opção apropriada para você.

Opção	Descrição
Atualizar lista	Opção para atualizar a lista de incidentes do DLP ao fazer uma atualização.
Ações da lista	Lista de ações que você pode executar. Estas são as opções: ▪ **Salvar como** ▪ **Editar colunas** ▪ **Redefinir larguras** **Nota:** Quando você tiver sua própria lista personalizada, criada na seção **Minhas listas** configurada para o seu espaço, também poderá executar as ações de lista adicionais abaixo: ▪ **Renomear** ▪ **Salvar** ▪ **Excluir**
Copiar URL para todos	Opção para copiar os URLs de todos os incidentes do DLP.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Exibir painel do filtro	Opção para detalhar os incidentes necessários usando a opção de filtro. **i.** Clique no filtro no canto superior esquerdo da página e selecione **Exibição avançada**. **ii.** Use um filtro existente ou crie o seu próprio adicionando condições que contenham um campo, operador e valores. **iii.** Para adicionar mais condições, clique em **E** ou **OU**: ▪ Se **E** for selecionado, todas as condições deverão ser atendidas. ▪ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. **iv.** Clique em **Atualizar**.
Atribuir Incidente	Ação para determinar a quem atribuir o incidente da DLP. Estas são as opções: ▪ **Atribuir incidente a**: opção para atribuir o incidente a um analista, usuário final ou outra pessoa. ▪ **Usuário**: opção para determinar a qual usuário o incidente deve ser atribuído. ▪ **Pré-resposta do usuário do**estado do incidente: opção para determinar em que estado o incidente deve estar antes que o usuário responda. Também pode ser um estado personalizado. ▪ **Anexar avaliação**: opção para indicar se você deseja anexar uma avaliação ao incidente. Se habilitada, as opções abaixo estarão disponíveis: ▪ **Modelo de avaliação**: opção para selecionar um modelo de avaliação para o incidente da DLP. ▪ **Pós-resposta do usuário do estado do incidente** Opção para selecionar em qual estado o incidente da DLP deve estar depois que o usuário responder.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política da DLP, o usuário poderá escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	A partir daqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena**.
Escalar	Ação para escalar o incidente. Você pode escalar o incidente selecionando o usuário para o qual deseja escaloná-lo. Você também pode obter informações adicionais no campo Comentários.
Atualizar Estado	Ação para atualizar o estado do incidente. Você pode atualizar o estado do incidente selecionando um dos estados nas opções suspensas. Também pode ser um estado personalizado.
Fechar	Ação para fechar os incidentes. Selecione o **Código de fechamento** correspondente na lista suspensa e adicione comentários de fechamento. O recurso **Fechar** em Data Loss Prevention Incident Response é feito de forma assíncrona e síncrona na exibição de lista. **i.** Fechamento síncrono: ao fechar incidentes de forma síncrona, isso significa que a ação de fechamento é executada imediatamente. Quando você seleciona vários incidentes para fechamento e se a contagem de incidentes for menor ou igual a 100, os incidentes serão fechados em primeiro plano na exibição de lista de incidentes da DLP. Aqui, 100 é o valor padrão. **ii.** Fechamento assíncrono: isso significa que a solicitação de fechamento é enviada e a aplicação executa a solicitação em segundo plano se a contagem de incidentes selecionados for maior que 100.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Você precisa atualizar a exibição de lista de incidentes da DLP para ver o status atualizado dos incidentes. **Nota:** ▪ A contagem de incidentes selecionados para fechamento assíncrono ou síncrono é configurada usando a propriedade do sistema *sn_dlir.closure_sync_count_limit*. ▪ Por padrão, a contagem de incidentes é definida como 100.

c. A segunda maneira é clicar em um incidente do DLP específico para abri-lo.

- Guia**Detalhes** : exibe as seguintes seções:
  - **Detalhes**: você pode exibir os detalhes do incidente da DLP, como número do incidente, gravidade, nome do arquivo e assim por diante. Você também tem a capacidade de modificar os campos Gravidade, Estado, Usuário final e Grupo de analistas da DLP, respectivamente, e salvá-los.
  - **Compor**: para adicionar comentários sobre o incidente do DLP que estão visíveis para todos, insira os comentários na guia Comentários. Para adicionar comentários que ficam visíveis para determinadas pessoas, insira os comentários na guia Anotações de trabalho (privado).
  - **Atividade**: você pode exibir os detalhes das diferentes atividades no incidente da DLP.
  - **Anexos**: se você tiver anexos relacionados ao incidente do DLP, clique em **Procurar** e selecione o anexo na sua unidade local.
- Guia**Detalhes adicionais** : exibe todas as informações adicionais sobre o incidente da DLP, incluindo campos personalizados.

Importante:

- Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior.
- Você pode usar a guia **Detalhes adicionais** para ver se algum campo personalizado foi criado para um incidente específico da DLP ou não.

- Guia**Atributos personalizados** : exibe a lista de atributos personalizados relacionados ao incidente da DLP.
- **Outros incidentes do usuário final**: exibe o incidente do mesmo usuário final. É possível consolidar incidentes executando a ação **Adicionar como incidente** secundário a partir desta lista relacionada.
- **Tipo de**informação confidencial detectada: exibe as informações confidenciais detectadas do incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esta lista relacionada está visível somente para os incidentes do DLP criados para integrações da Microsoft ou da Symantec. No registro de incidentes da Microsoft ou da Symantec, sempre que o usuário acessa o registro de tipo de informação confidencial detectado, o conteúdo de correspondência realçado em relação a essa integração é exibido.

- **Incidentes secundários**: exibe os incidentes secundários criados manualmente (executando a ação "Adicionar como incidente secundário") ou a partir das regras de consolidação da DLP. É possível desvincular o incidente secundário executando "Desvincular incidente secundário" nesta lista relacionada.
- **Incidentes clonados**: exibe os incidentes clonados do incidente primário. Ao clicar na ação **Clonar incidente** da exibição do formulário, você pode criar um novo incidente clonado.
- Guia**Avaliações** : exibe a lista de avaliações atribuídas ao incidente da DLP.

d. Escolha a opção apropriada para você.

Opção	Descrição
Atribuir Incidente	Ação para determinar a quem atribuir o incidente da DLP. Estas são as opções: ▪ **Atribuir incidente a**: opção para atribuir o incidente a um analista, usuário final ou outra pessoa. ▪ **Usuário**: opção para selecionar o usuário ao qual o incidente deve ser atribuído. ▪ **Pré-resposta do usuário do**estado do incidente: opção para selecionar em qual estado o incidente deve estar antes que o usuário responda. Também pode ser um estado personalizado. ▪ **Anexar avaliação**: opção para indicar se você deseja anexar uma avaliação ao incidente. Se habilitada, as opções abaixo estarão disponíveis: ▪ **Modelo de avaliação**: opção para selecionar um modelo de avaliação para o incidente da DLP. ▪ **Pós-resposta do usuário do estado do incidente**: opção para selecionar em qual estado o incidente da DLP deve estar depois que o usuário responder.
Cancelar aprovação	Ação para cancelar a solicitação de aprovação. Esta ação ficará visível para os analistas na exibição do formulário somente quando o incidente da DLP estiver no estado **Aprovação pendente**. As opções disponíveis são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ **Atribuir incidente a**: opção para atribuir o incidente a ninguém, a um analista ou a outra pessoa. ▪ **Usuário**: opção para selecionar o usuário ao qual o incidente deve ser atribuído. ▪ **Estado pós-cancelamento do incidente**: opção para selecionar em qual estado o incidente deve estar após o cancelamento da solicitação. ▪ **Comentários**: para fornecer detalhes adicionais para o cancelamento.
Atribuir Avaliação	Ação para anexar uma avaliação ao atribuir o incidente. As opções são as seguintes: ▪ **Modelo de avaliação**: opção para selecionar um modelo de avaliação para o incidente da DLP. ▪ **Pós-resposta do usuário do estado do incidente**: opção para selecionar em qual estado o incidente da DLP deve estar depois que o usuário responder.
Baixar arquivo	Ação para baixar o arquivo ou e-mail que tem o conteúdo violado. Esta ação pode ser realizada para incidentes criados para o Microsoft OneDrive, SharePoint Online ou Exchange Online.
Salvar	Ação para salvar as mudanças feitas. Você tem a opção de modificar os campos Gravidade, Estado e Usuário final do incidente da DLP e salvá-los.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política da DLP, o usuário poderá escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários. A partir daqui, você também pode selecionar as opções de resposta avançadas. **Por exemplo: Solicitar liberação de e-mail da quarentena**.
Escalar	Ação para escalar o incidente. Você pode escalar o incidente selecionando o usuário para o qual deseja escaloná-lo. Você também pode obter informações adicionais no campo Comentários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

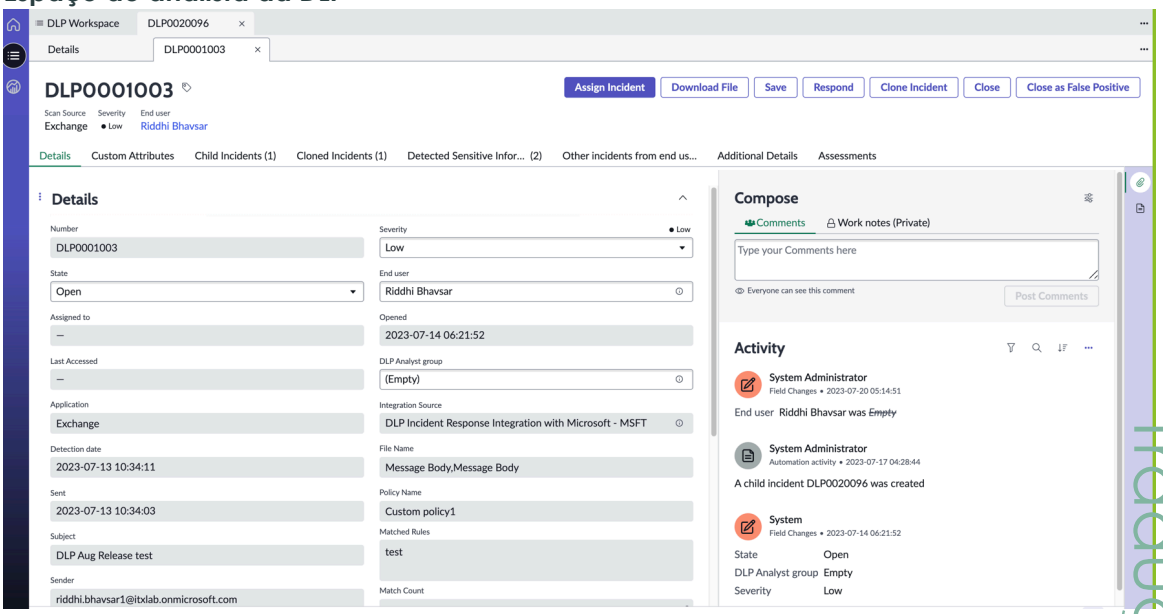
Opção	Descrição
Clonar incidente	Ação para criar um incidente de clone se o registro do incidente afetar vários usuários. Você pode atribuir os incidentes clonados a várias partes interessadas, como jurídico/TI. Depois de criar um registro de incidente de clone, uma nova guia **Incidentes clonados** é criada no incidente primário da DLP e todos os incidentes clonados são listados nesta exibição. **Nota:** ▪ Se o registro de incidente da DLP primária for encerrado, todos os registros de incidentes clonados serão encerrados automaticamente. ▪ Se um registro de incidente da DLP contiver um incidente clonado, ele não poderá ser atribuído a usuários finais. Os registros de incidentes da DLP primária podem ser gerenciados somente por usuários com a função de analista. ▪ Você também tem a opção de atualizar automaticamente o estado primário com base no estado dos incidentes clonados no módulo Configuração padrão. Por exemplo, se todos os incidentes clonados forem movidos para o estado Escalado, o incidente primário também será movido para o estado Escalado.
Fechar	Ação para fechar o incidente. Você deve selecionar o **Código de fechamento** correspondente na lista suspensa e adicionar comentários de fechamento, se necessário.
Fechar como falso-positivo	Ação para fechar o incidente como falso-positivo. Você também pode adicionar

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	comentários adicionais antes de fechar o incidente.

Espaço do analista da DLP



6. Você pode ver a exibição de lista na página inicial, acessando o canto superior esquerdo da página e clicando na guia **Listas**.
   A categoria Listas consiste nas páginas de lista padrão e personalizadas para incidentes do DLP.
   - Guia **Listas**: listas padrão para incidentes da DLP. Estas são as listas padrão:
     - Todos
     - Aberto
     - Meus Incidentes
     - Atribuído ao meu grupo
     - Escalado
     - Atrasado
     - Avaliações pendentes
     - Ação do usuário pendente
     - Incidentes clonados
     - Incidentes arquivados
   - Guia **Minhas listas**: exibe todas as listas que você renomeou e todas as que criou.

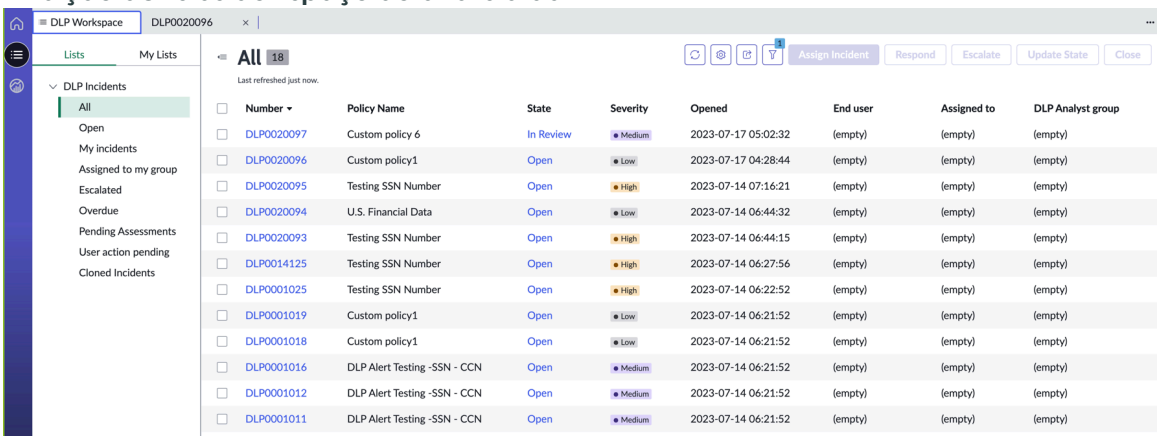
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example

O exemplo a seguir mostra o espaço da DLP com as categorias de exibição de lista. A opção **Todas** as exibições de lista está selecionada.

Exibição de listas do Espaço do analista da DLP



Exibir incidentes arquivados da DLP

Use o espaço do analista da DLP para exibir os incidentes arquivados da DLP

Antes de Iniciar

Função necessária:

- sn_dlir.analyst — Editar e exibir incidentes da DLP.
- sn_dlir.analyst_read e sn_dlir.read — Exibir incidentes da DLP.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do analista da DLP**.
   Por padrão, a seção Meus incidentes é exibida.
2. Clique **em Incidentes arquivados**.
   A lista de incidentes arquivados da DLP é exibida.
3. Clique no botão **Mostrar contagem de incidentes** para exibir a contagem de incidentes arquivados.

   Nota:

   - Por padrão, a contagem de incidentes arquivados está oculta para melhorar o tempo de carregamento da lista. Você deve clicar no botão **Mostrar contagem de incidentes** para exibir a contagem de incidentes. Além disso, uma mensagem informativa é exibida mostrando a contagem de incidentes.
   - A propriedade do sistema glide.ui.list.seismic.omit.count está habilitada no sistema de base para os incidentes arquivados para ocultar a contagem da lista de incidentes.

4. Selecione um ou mais incidentes do DLP que você deseja exibir.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O incidente da DLP exibe a seção de detalhes do incidente.

Nota:

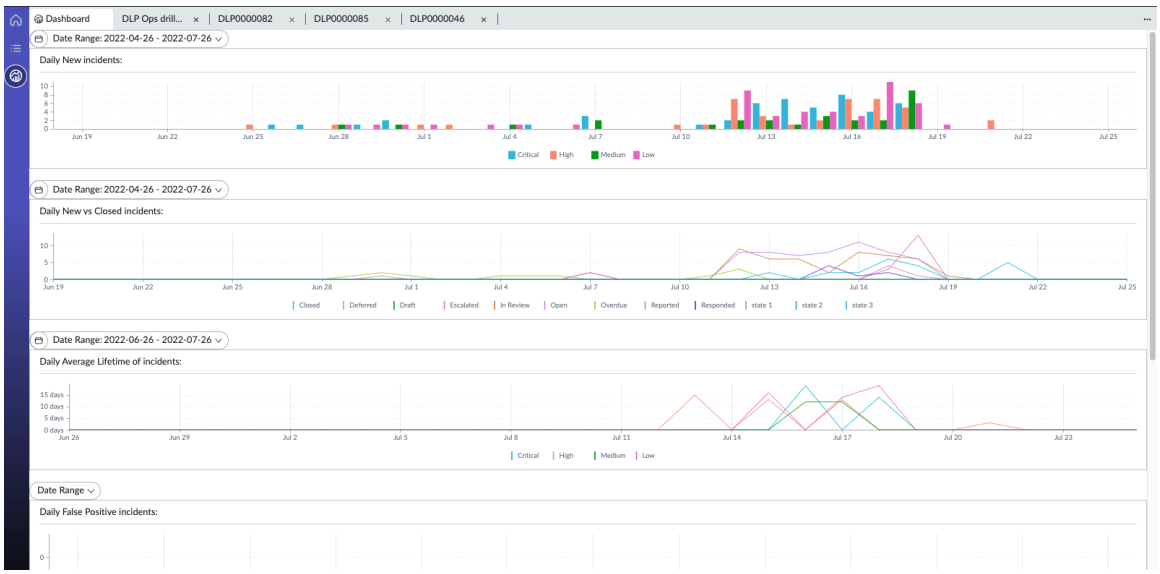
- A guia **Outros incidentes de usuários finais** também incluirá os incidentes arquivados.
- **A opção Corresponder conteúdo** é compatível com todos os incidentes arquivados (que também serão compatíveis com todas as integrações), mas **o download do arquivo** é compatível somente com integrações da Microsoft.

Painel da Data Loss Prevention Incident Response

O painel Data Loss Prevention Incident Response (DLP IR) fornece uma visão geral de alto nível de seus incidentes de DLP e tendências de incidentes diários em sua instância na forma de gráficos gráficos. Esses gráficos ajudam a exibir, gerenciar e corrigir com eficácia os incidentes do DLP.

O painel Data Loss Prevention Incident Response fornece informações importantes sobre seus incidentes do DLP diariamente. Você pode configurar indicadores e coletar regularmente snapshots de dados dos incidentes que correspondem às condições nas propriedades do indicador. Os dados coletados são visualizados usando widgets no painel. Para analisar os incidentes da DLP em diferentes intervalos de tempo, você pode aplicar diferentes intervalos de datas.

Painel da DLP



Analise as tendências diárias de incidentes em seus incidentes da DLP

Acesse o painel Data Loss Prevention Incident Response (DLP IR) para analisar as tendências diárias em seus incidentes da DLP e corrigi-los com eficácia.

Antes de Iniciar

Função necessária:

- sn_dlir.analyst — Editar e exibir incidentes da DLP.
- sn_dlir.analyst_read e sn_dlir.read — Exibir incidentes da DLP.

Por Que e Quando Desempenhar Esta Tarefa

Você pode visualizar as tendências diárias usando widgets no painel da DLP. Os dados ou estatísticas das tendências diárias dos incidentes do DLP são coletados das propriedades do indicador de incidentes diários que são definidas pela sua organização. Você pode

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

obter informações importantes aplicando diferentes intervalos de dados para analisar os incidentes do DLP em diferentes intervalos de tempo para os seguintes gráficos:

- **Novos incidentes diários**: dados dos incidentes gerais do DLP criados diariamente, independentemente do estado dos incidentes. Os incidentes do DLP são categorizados com base nas gravidades, incluindo Médio, Crítico, Alto e Baixo. Cada gravidade de incidente da DLP é representada por uma cor específica no gráfico.
- **Incidentes diários novos x incidentes encerrados**: os diferentes estados dos incidentes da DLP e uma comparação entre os novos incidentes diários e os incidentes encerrados diariamente. A categoria Novo diário inclui todos os incidentes do DLP nos estados Aberto, Rascunho, Escalado, Em revisão, Atrasado, Relatado, Respondido ou Personalizado (se houver). A categoria Incidente encerrado inclui os incidentes encerrados da DLP. Cada estado de incidente da DLP é representado por uma cor específica no gráfico.
- **Vida útil média diária dos incidentes**: a vida útil de um incidente é o período entre a abertura e o fechamento de um incidente específico da DLP. O tempo de vida médio diário é calculado somente para os incidentes encerrados da DLP.
- **Incidentes falso-positivos diários**: dados de todos os incidentes do DLP relatados como falso-positivos diários. Os incidentes falso-positivos diários são categorizados com base nas gravidades, incluindo Médio, Crítico, Alto e Baixo. Cada gravidade de incidente falso-positivo diário é representada por uma cor específica no gráfico.
- **Idade x gravidade dos incidentes**: comparação de dados de todos os incidentes do DLP, categorizados pela idade e configurados com a gravidade dos incidentes do DLP. A categoria Idade inclui todos os incidentes da DLP abaixo da idade definida pela sua organização. Para obter mais informações sobre Gráficos de idade, consulte Criar configurações de gráfico de idade. A gravidade de incidentes inclui todos os incidentes do DLP na categoria Alta ou Baixa. Cada gravidade é representada por uma cor específica no gráfico.
- **Incidentes escalonados diariamente**: dados de todos os incidentes escalonados da DLP diariamente. Os incidentes escalonados diariamente são categorizados com base nas gravidades, incluindo Médio, Crítico, Alto e Baixo. Cada gravidade de incidente escalonada diariamente é representada por uma cor específica no gráfico.

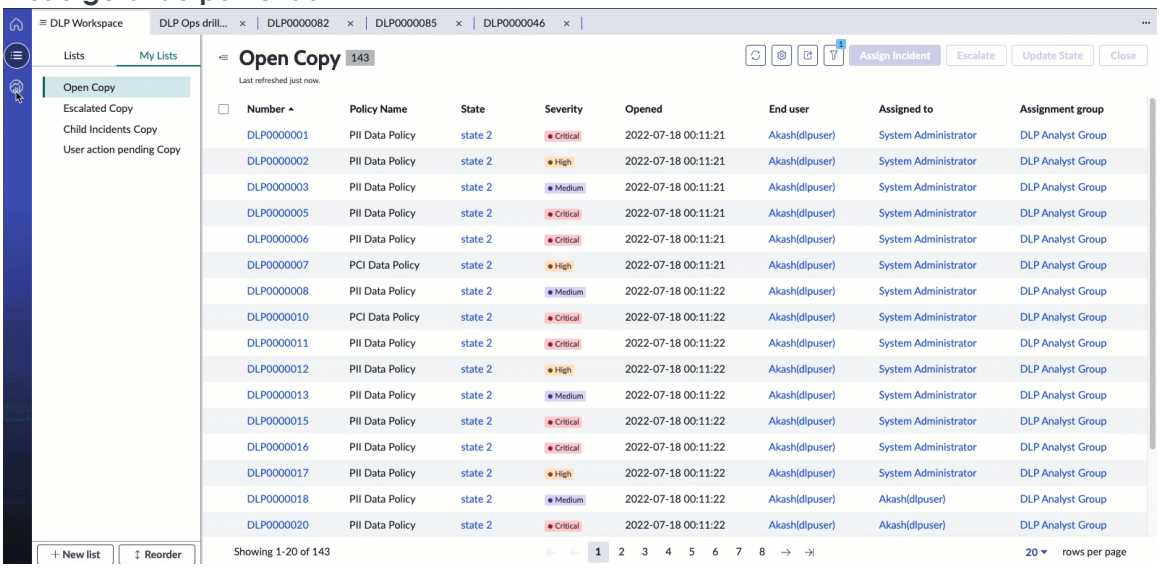
Procedimento

1. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Painel da DLP**.
   A página Meu painel da DLP é exibida em uma nova guia do navegador.
2. Selecione um widget de painel para o qual você deseja executar uma análise de tendências diária.
   Por exemplo, o gráfico de Novos incidentes diários.
3. Revise os widgets do painel para identificar tendências.
4. Clique **em Intervalo de datas**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral do painel da DLP



5. Selecione um intervalo de datas no calendário e clique em **Aplicar**.

   Example
   Por exemplo, o gráfico de Novos incidentes diários é atualizado para o intervalo de dados selecionado.

6. Use os filtros abaixo do gráfico para fazer uma busca detalhada e realizar uma análise mais aprofundada.

Integração de entrada para Data Loss Prevention Incident Response

Crie um ou vários incidentes do DLP usando a REST API de entrada.

Criar um único incidente da DLP

Função necessária: sn_dlir.api_integration_user.

Para criar um único incidente da DLP, defina os seguintes parâmetros conforme necessário:

Campo	Descrição
Método HTTP	*POST*
URL	`https://{instance}/api/now/import/sn_dlir_incident_import`
Cabeçalho de solicitação	Aceitar: *application/json* Tipo de conteúdo: *application/json*
Carga de amostra	`{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>",`

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	"data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"", "user_justification":"" }

Exemplo de resposta	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id":
	"7cda322297c2411056a43d1e6253af1f"
	}

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

	``
	    ]
	}
	``

Criar vários incidentes da DLP

Função necessária: sn_dlir.api_integration_user.

Para criar vários incidentes do DLP a partir da mesma solicitação, defina os seguintes parâmetros conforme necessário:

Campo	Descrição
Método HTTP	*POST*
URL	`https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple`
Cabeçalho de solicitação	Aceitar: *application/json* Tipo de conteúdo: *application/json*

Carga de amostra	```
	{
	    "records": [
	        {
	            "file_name": "<value>",
	            "file_modified_by": "<value>",
	            "work_notes": "<value>",
	            "url": "<value>",
	            "scan_source": "<value>",
	            "data_owner_email": "<value>",
	            "file_created_by": "<value>",
	            "file_owner": "<value>",
	            "policy_name": "<value>"
	        },
	        {
	            "dest_ip": "<value>",
	            "dest_ip_port": "<value>",
	            "detection_date": "<value>",
	            "endpoint_on_corporate_net":
	 "<value>",
	            "files": "<value>",
	            "file_created": "<value>",
	            "file_created_by": "<value>",
	            "file_location": "<value>",
	            "file_modified_by": "<value>",
	            "file_name": "<value>",
	            "file_owner": "<value>",
	        }
	    ]
	}
	``

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

Exemplo de resposta	{
	"import_set_id":
	"a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}

Nota: Por padrão, a transformação é assíncrona. Para definir a transformação síncrona, crie um novo registro na tabela Inserir Múltiplos REST [sys_rest_insert_multiple], selecione a tabela de origem como **sn_dlir_incident_import**e defina a transformação como **síncrona**.

Integrações da DLP

O sistema base Data Loss Prevention Incident Response inclui integrações com pacotes de software de prevenção de perda de dados de terceiros.

Esta seção fornece instruções para ativar os plug-ins e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.

Configurações de Integração

O sistema base inclui uma série de cartões para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que tenham dependências de Operações de segurança plug-ins. Os cartões de integração podem ser exibidos selecionando **Operações de segurança** > **Configurações de Integração**.

Data Loss Prevention Incident Response O é compatível com os seguintes pacotes de software de prevenção de perda de dados de terceiros:

Symantec Integração para Data Loss Prevention Incident Response

A Symantec integração de DLP oferece suporte à ingestão de Data Loss Prevention Incident Response incidentes criados na implantação Symantec Data Loss Prevention Incident Response. Após a ingestão, você pode usar as funcionalidades de gestão de incidentes para corrigir os incidentes da DLP.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

A Symantec integração de DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Esta integração inclui os seguintes recursos principais:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Capacidade de criar vários perfis de integração para diferentes Symantec endpoints de API.
- Ingestão programada de incidentes do DLP de Symantec para sua instância ServiceNow.
- Capacidade de aplicar filtros de API para recuperar os incidentes que correspondem aos critérios de filtro e também especificar o filtro para Symantec incidentes da DLP que precisam ser importados.
- Mapeamento dos estados de incidentes da DLP em sua instância ServiceNow para estados de incidentes da DLP em Symantec.
- Atualize automaticamente o status do incidente em Symantec quando o estado mudar em sua instância ServiceNow.
- Capacidade de personalizar e definir o mapeamento de gravidade entre incidentes do Symantec DLP com incidentes da ServiceNow.

Para saber mais sobre a integração, consulte a documentação do produto Symantec .

Primeiros passos com Symantec integração de DLP para prevenção de perda de dados

Antes de poder usar a integração, você deve baixá-la do ServiceNow® Store.

Check-list

Revise as informações a seguir antes de começar a configurar sua Symantec integração DLP para prevenção de perda de dados.

Check-list

Campo	Descrição
Verifique se você atribuiu as funções da aplicação Now Platform, Aplicação de prevenção de perda de dados, MID necessárias.	As funções a seguir são usadas na integração Symantec da DLP na Now Platform: • O administrador (admin) instala as aplicações do ServiceNow® Store e atribui o administrador de prevenção de perda de dados (sn_dlir.admin). • O usuário com a função sn_dlir.admin pode configurar a integração e configurar os perfis de incidentes. • Os usuários com a função sn_dlir.analyst terão funções de leitura na integração.
Atribua as Symantec funções de usuário da DLP necessárias.	Revise as Symantec funções e permissões de integração da DLP.
Verifique se você está usando Symantec DLP 15.8	A Symantec integração de DLP para prevenção de perda de dados foi testada com a versão 15.8 da Symantec prevenção de perda de dados. **Nota:** Verifique se você está usando Symantec DLP 15.8

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Campo	Descrição
Verifique se a ServiceNow® aplicação principal necessária para oferecer suporte à integração Symantec do DLP está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Instalar e configurar a Symantec integração DLP para prevenção de perda de dados

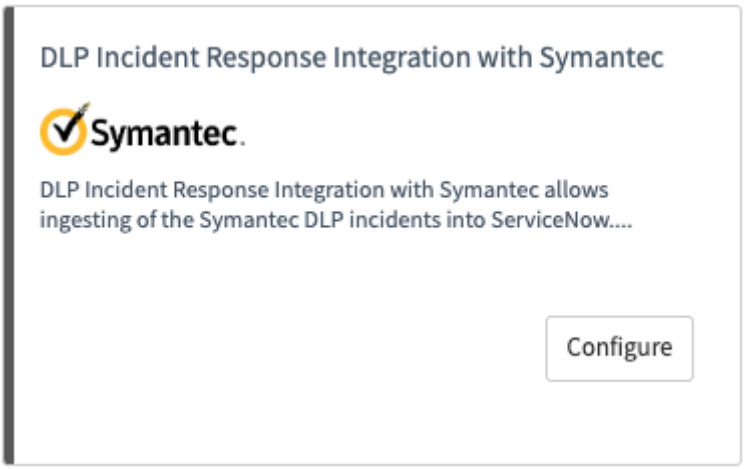
Instale e configure a Symantec integração DLP do ServiceNow® Store em sua instância Now Platform. Comece a investigar incidentes da DLP usando os Symantec dados de incidentes da DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Baixe a Symantec integração de DLP do ServiceNow® Store e instale-a.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco Integração de resposta a incidentes da DLP com Symantec e clique em **Configurar**.



4. No formulário, preencha os campos.

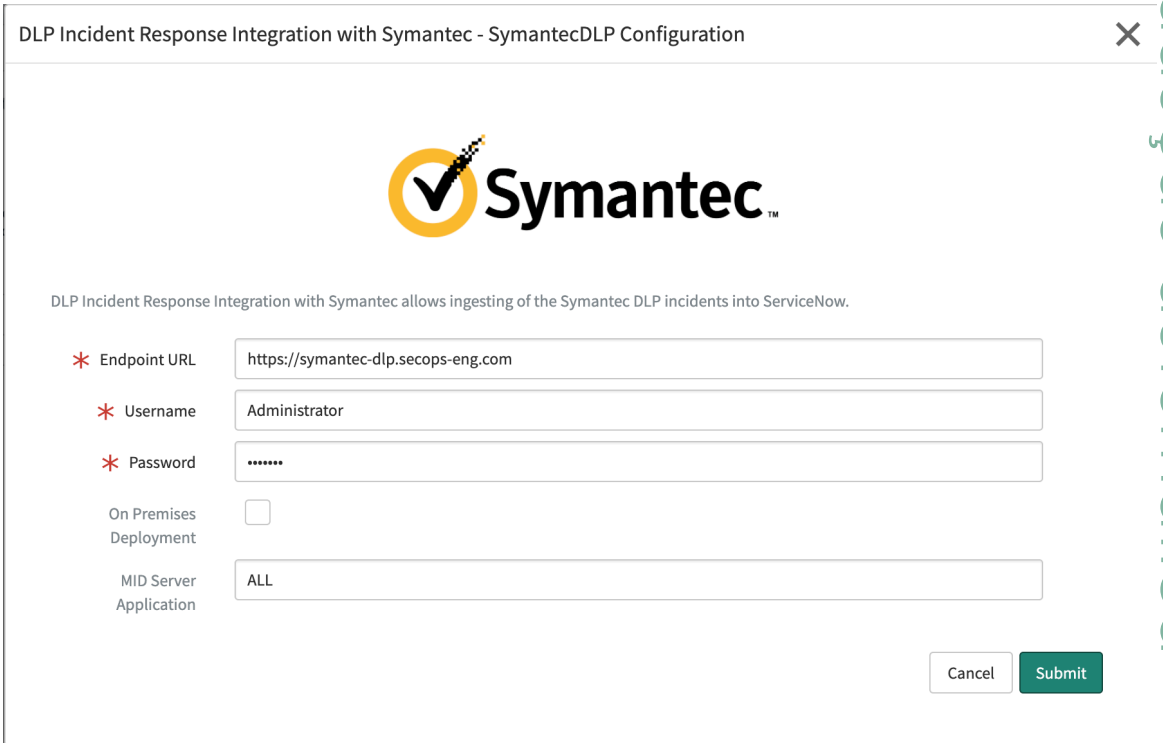
Formulário de configuração de integração do Symantec DLP

Campo	Descrição
Nome	Nome da Symantec configuração de integração da DLP.
URL de endpoint	Symantec Endpoint de REST API.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de usuário	Symantec nome da conta. Para obter informações sobre as funções e permissões necessárias, consulte Funções e permissões .
Senha	Symantec senha da conta.
Implantação no local	Opção que você pode selecionar se o Symantec for implantado em uma instância no local. Ao selecionar esta opção, você deve usar o MID Server para se conectar à Symantec.
Aplicação do MID Server	O nome da aplicação MID que é usado para se comunicar com Symantec. Este campo é necessário quando você seleciona a opção **Implantação no** local.



Tradução automática

5. Clique em **Enviar**.

Resultados
Depois de validar e enviar a configuração com sucesso, a Symantec integração de DLP é salva na página Integrações de segurança como um bloco.

Criar um perfil para Symantec integração de DLP

Crie um perfil de incidente em sua instância Now Platform. Determine os Symantec incidentes do DLP que são adequados para criar incidentes do DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Configure o Now Platform® para buscar os incidentes do DLP do endpoint Symantec. Armazene esses incidentes em sua instância ServiceNow® como incidentes da DLP.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção Nome.

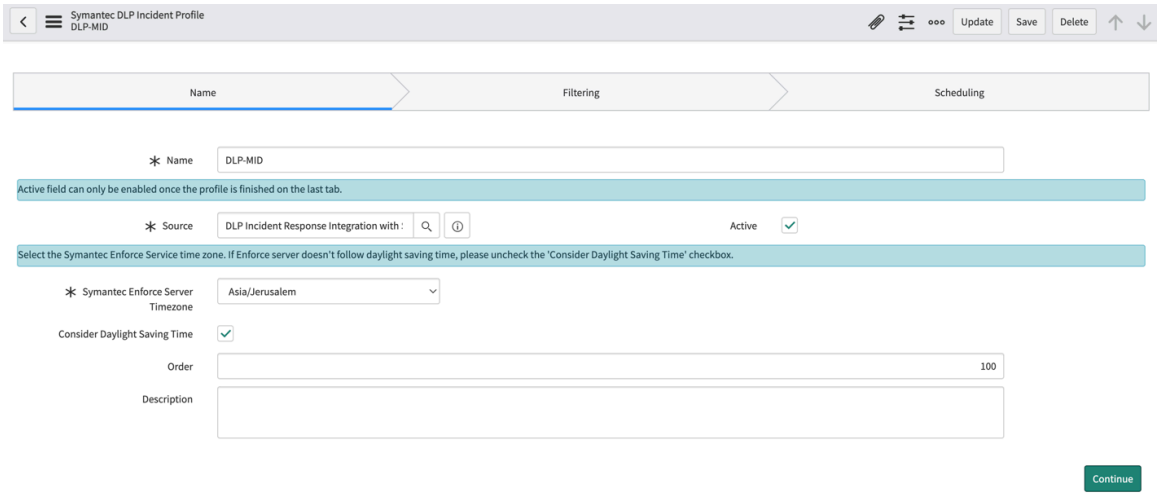
Criar um perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	Symantec Instância da DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidentes que você planeja ingerir para o perfil.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois que você clica em **Concluir** na seção Programação. Quando o perfil está ativo, isso indica que Now Platform está pesquisando ativamente Symantec incidentes da DLP. Os incidentes correspondentes do DLP são criados no DLP quando as condições de filtragem são correspondidas com base nos parâmetros de programação que você forneceu.
Fuso horário do servidor do Symantec Enforce	Selecione o fuso horário do servidor do Symantec Imforce no perfil para que os incidentes não sejam perdidos devido a problemas de fuso horário.
Considerar o horário de verão	Marque esta caixa de seleção se o servidor de imposição seguir o horário de verão.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa é considerado como a prioridade mais alta. Por padrão, o valor é 100.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição exclusiva deste perfil.



O que Fazer Depois

Para passar para a seção Filtragem, clique em **Continuar**.

Definir filtros a serem aplicados na criação do incidente

Defina e defina as condições do filtro para detalhar os Symantec incidentes de DLP de entrada. Determine os incidentes que devem ser criados como incidentes do DLP em ServiceNow®.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

A filtragem ajuda a isolar incidentes do DLP e limitar o número de incidentes do DLP que você cria. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento

1. Marque a caixa de seleção **Filtro baseado em API para ingestão de incidentes** para aplicar os filtros de API e recuperar os incidentes que correspondem aos critérios de filtro.
2. Adicione os filtros de API.
   A seguir está um exemplo que mostra os filtros de API.

```
{
                "operandOne": {
                    "name": "incidentStatusName"
                },
                "filterType": "string",
                "operator": "EQ",
                "operandTwoValues": [
                    "incident.status.New"
                ]
            }
```

Nota: Para obter mais informações sobre os filtros de API na integração da Symantec, consulte Listas de incidentes: parâmetros - Detalhes do objeto de solicitação .

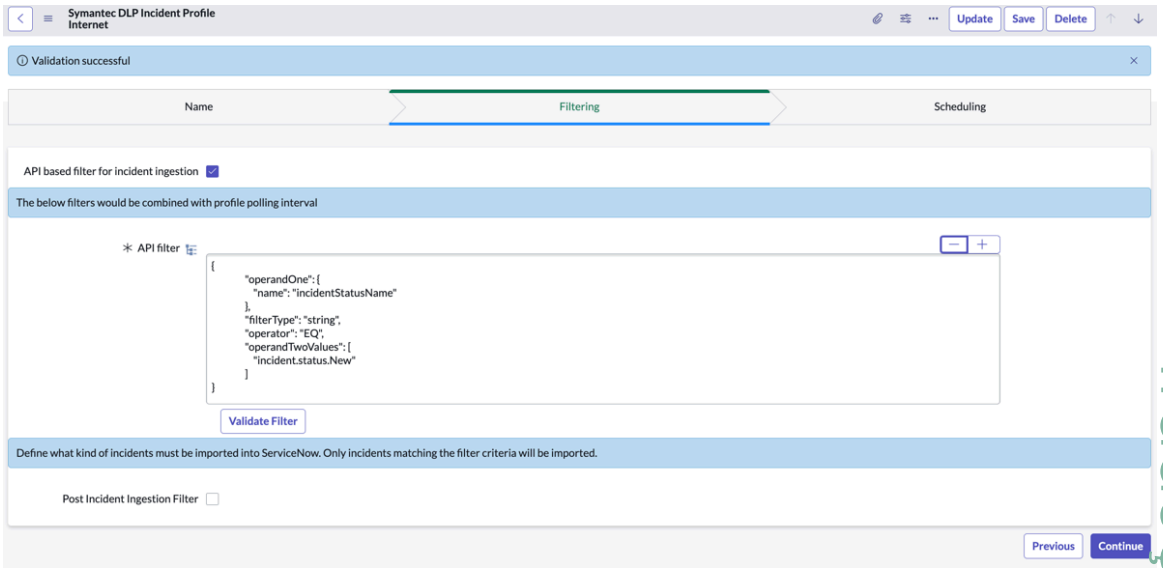
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

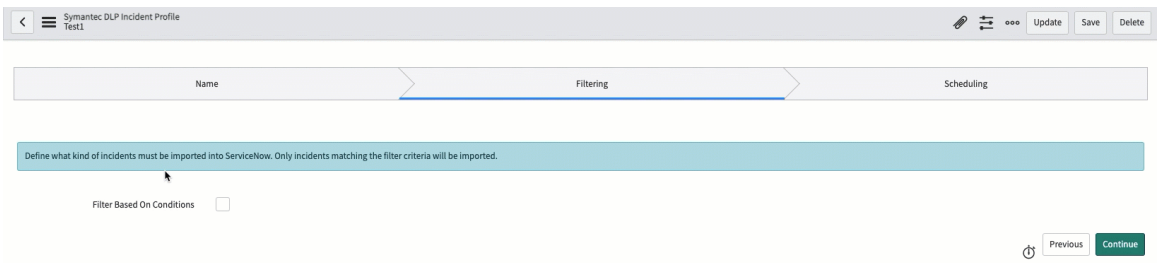
3. Clique em **Validar filtro** depois de aplicar os filtros de API.

Nota: Se a validação não for bem-sucedida, será exibida uma mensagem de erro informando que a validação falhou e isso acontece quando os filtros não são inseridos corretamente de acordo com as APIs da Symantec.

Como adicionar filtros de API



4. Marque a caixa de seleção **Filtro de ingestão pós-incidente** para definir os critérios que um incidente do Symantec DLP de entrada deve satisfazer para que um incidente do DLP seja criado.
   As opções no primeiro campo nas Condições do filtro correspondem aos campos que estão disponíveis no incidente da DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.
5. No construtor de condições, defina os filtros no campo **Condições do filtro**.



6. Para adicionar mais condições, clique em **E**ou **OU**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se **E**for selecionado, todas as condições deverão ser atendidas.
- Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.

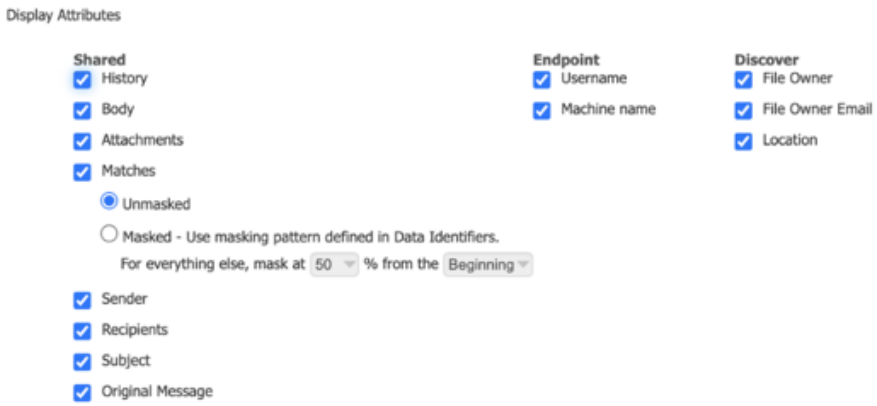
O que Fazer Depois
Para configurar a programação, clique em **Continuar**.

Configurar armazenamento de arquivo de evidências

Configure o armazenamento de arquivos de evidências para armazenar com segurança o arquivo de evidências dos incidentes da DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Verifique se o usuário da Symantec que você está configurando para a integração do Symantec DLP da ServiceNow deve ter as opções Corpo, Anexos e Mensagem original habilitadas na página de configuração de funções no portal do Symantec DLP. Para obter mais informações, consulte a seção Exibir atributos disponível no documento Configuração de funções para obter mais informações.



Por Que e Quando Desempenhar Esta Tarefa
Você pode configurar o armazenamento de arquivos de evidências para armazenar arquivos com segurança. Isso fornece uma opção para armazenamento interno na instância da ServiceNow, garantindo que os arquivos sejam armazenados e criptografados usando a criptografia em nível de coluna da ServiceNow. Para obter mais informações, consulte Criptografia em nível de coluna na documentação da NowPlatform.

Quando um analista da DLP executa a ação Baixar arquivos de evidências para incidentes da DLP no espaço do analista, o arquivo será baixado do armazenamento selecionado se a opção de armazenamento de arquivo de evidências estiver habilitada. Caso contrário, o arquivo será baixado diretamente da origem da Symantec e não será persistente na instância da ServiceNow. Para obter mais informações, consulte Baixar arquivos de evidências.

Nota: Para oferecer suporte à origem de integração do ambiente local, a função mid_server conterá a função sn_dlir.secure_file_download para oferecer suporte ao armazenamento de arquivos de evidências no armazenamento interno usando o MID Server.

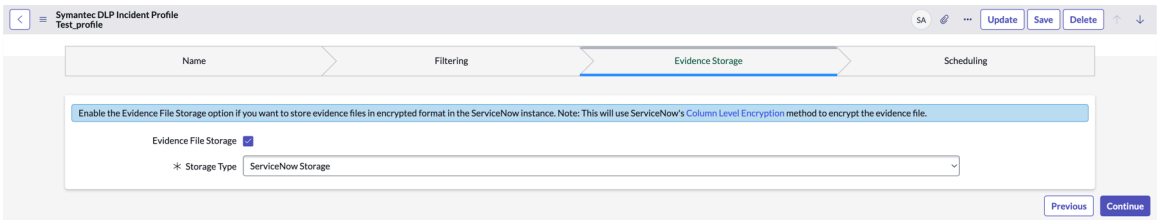
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração da DLP da Symantec** > **Perfil do incidente**.
2. Clique na seção **Armazenamento de evidências** no formulário Perfil de incidente.
3. Marque a caixa de seleção **Armazenamento de arquivo de evidências** para habilitar o armazenamento de arquivos.
4. Selecione o tipo de armazenamento preferencial.

Tipo	Descrição
Armazenamento de arquivo de evidências	Opção para habilitar o armazenamento de arquivos de evidências.
Tipo de armazenamento	Opção para selecionar o tipo de armazenamento preferencial. **Nota: Armazenamento da ServiceNow**: armazenará os arquivos de evidências na instância da ServiceNow em um formato criptografado.



5. Clique em **Continuar** e vá para a seção **Programação**.

Resultados
Os arquivos de evidências são armazenados de acordo com a configuração, após a conclusão da ingestão do incidente.

Programar Symantec Recuperação de incidentes da DLP

Defina uma programação para recuperar os dados do incidente e ingerir Symantec incidentes da DLP que correspondam aos critérios no perfil. Configure a programação para definir como e quando você extrai incidentes de Symantec.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer uma recuperação única usando a caixa de seleção **Recuperação única**. A data histórica pode ser até os últimos três meses a partir da data atual.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da Symantec integração de incidentes da DLP. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

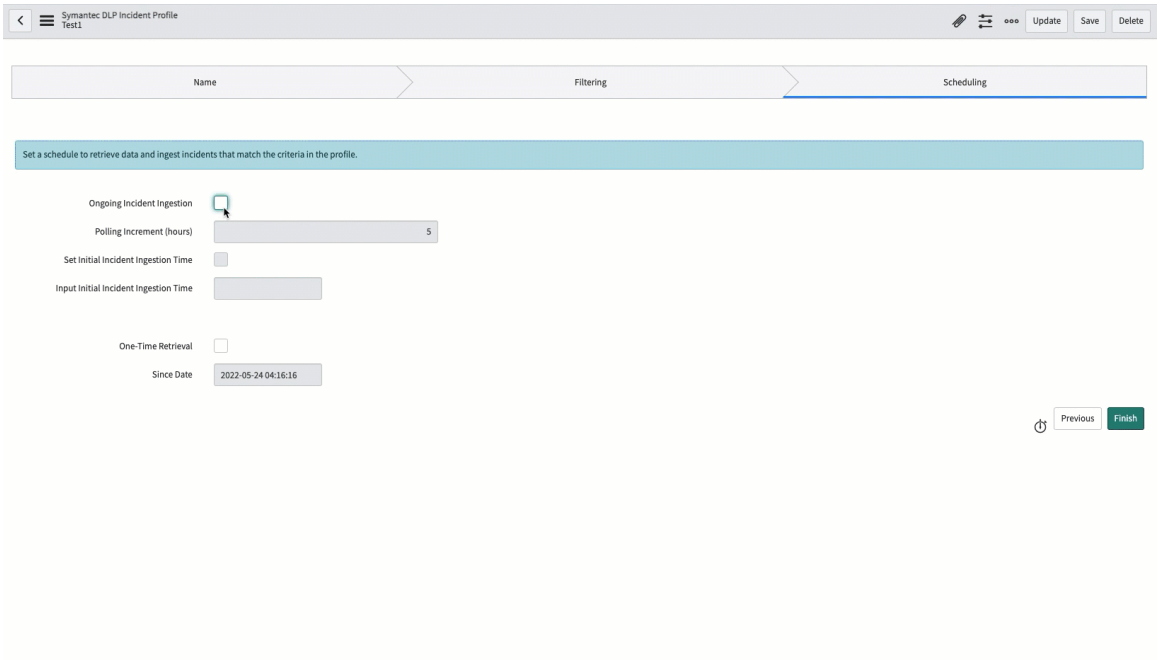
1. Defina uma programação para recuperar dados e incluir incidentes que correspondam aos critérios no perfil.
2. No formulário, preencha os campos.

Programação do incidente da DLP

Campo	Descrição
Adição de incidentes em andamento	A ingestão de incidentes em andamento que a instância Now Platform extrai da Symantec para novos incidentes. Os incidentes da DLP serão criados se forem encontrados incidentes acionados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	A frequência de pesquisa definida em minutos. Este campo é definido automaticamente para 300 minutos.
Definir horário de adição do incidente inicial	Opção para definir uma data e hora para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora que você especifica para a ingestão de incidentes.
Horário de adição do incidente inicial	Primeira vez em que os dados são ingeridos. Você pode ver que os valores começam a aparecer quando o tempo de ingestão do incidente inicial é definido.
Horário de adição do próximo incidente (estimado)	Próximo período para uma ingestão de incidente estimada.
Recuperação Única	Opção para habilitar a extração única de dados históricos. Se este campo for selecionado, os dados históricos serão extraídos do Symantec DLP de acordo com a data adicionada no campo **Desde a data**.
Desde a Data	Data a partir da qual os dados devem ser recuperados da Symantec. Este campo pode ser definido para no máximo três meses.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para salvar a configuração de perfil criada, clique em **Concluir** na janela pop-up.

4. Para ativar o perfil, abra o perfil criado.

5. Habilite a opção **Ativo**.

6. Clique em **Atualizar**.

Resultados
Após a criação e a ativação bem-sucedidas do perfil, os incidentes são recuperados periodicamente de acordo com a configuração definida no perfil e adicionados à tabela de incidentes da DLP.

Mapeamento de Symantec status de incidente da DLP com ServiceNow status de incidente

Sincronize o status dos incidentes do DLP ingeridos no ServiceNow com os incidentes do DLP do Symantec. Mapeie o campo Status do **incidente da ServiceNow com o campo Status** do **incidente da Symantec**.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
O status do incidente é recuperado dinamicamente da origem do endpoint Symantec, que é adicionada no mapeamento. Você precisa executar um mapeamento de status de incidente individual.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Mapeamento de status do incidente**.

2. Forneça um **Nome** para identificar o mapeamento.

3. Selecione a Integração de **origem** de onde você deseja buscar o status.

4. Mapeie o status de **incidente da DLP com o status** de incidente da **Symantec**.

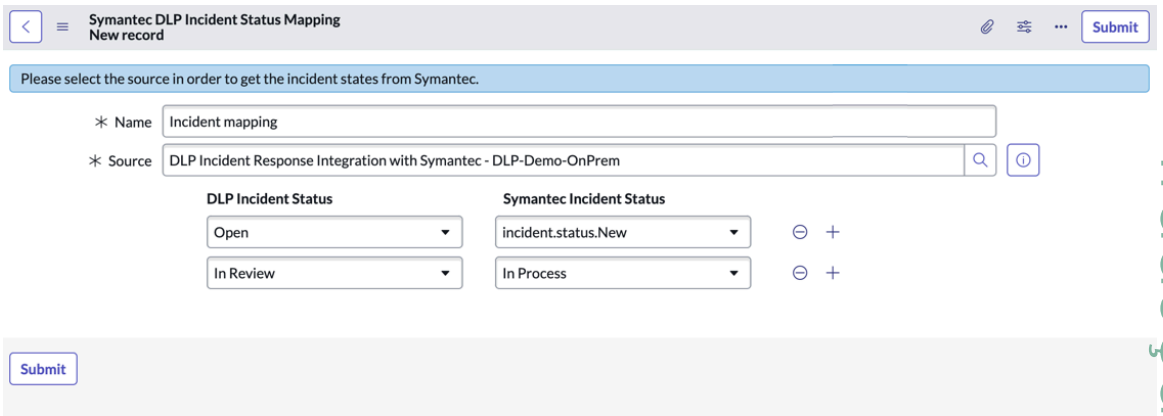
Nota: Não é necessário mapear todos os estados, você pode mapear somente os estados necessários.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de status de incidentes do Symantec DLP

Campo	Descrição
Nome	Nome do registro de mapeamento.
Origem	A origem do endpoint da Symantec configurado de onde você deseja obter o status do incidente.
Status do incidente da DLP	Lista de status de incidentes do DLP.
Status do incidente da Symantec DLP	Lista de status obtida da origem (endpoint da Symantec).



5. Clique em **Enviar**.

Resultados

Depois de criar com sucesso o registro para mapear status dos ServiceNow incidentes, o status dos incidentes ServiceNow será sincronizado com o status dos incidentes Symantec da DLP.

Se você alterar o status de qualquer incidente do DLP em sua instância ServiceNow, o status dos incidentes do DLP Symantec associados será alterado na plataforma de origem Symantec com base no mapeamento definido no registro.

Mapeamento de gravidade entre incidentes do Symantec DLP com incidentes da ServiceNow

Use o recurso de mapeamento de gravidade para configurar e sincronizar o mapeamento entre Symantec incidentes e Now Platform® incidentes.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

O mapeamento de gravidade da DLP permite mapear a gravidade de origem com a gravidade do incidente da DLP. Você pode personalizar e definir o valor de severidade de origem e mapeá-lo para o valor de severidade de incidente desejado da DLP.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Mapeamento do incidente de gravidade**.

2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No formulário, preencha os campos.

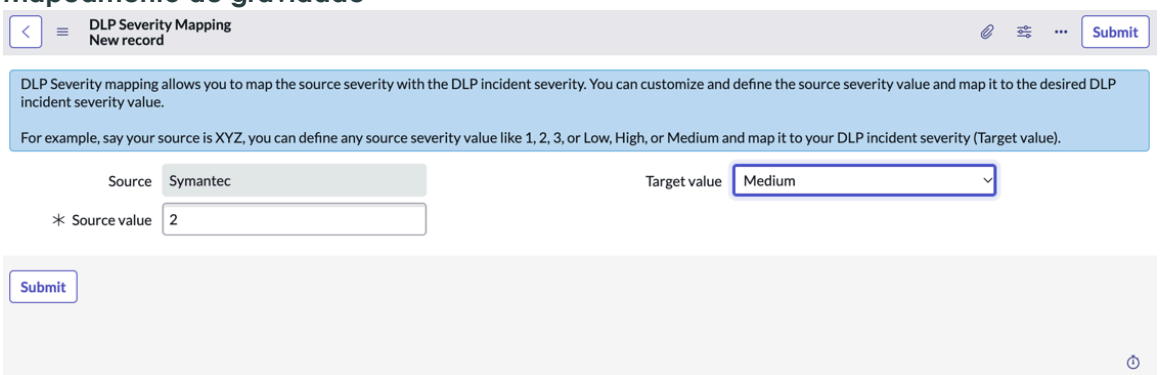
Mapeamento de gravidade da DLP

Campo	Descrição
Origem	A origem do endpoint da Symantec configurada de onde você deseja buscar o incidente.
Valor de Meta	O valor de destino é o ID de gravidade do incidente da DLP. Os valores disponíveis são Crítico, Alto, Médio, Baixo e Informativo (usado como a gravidade das informações no Symantec).
Valor de Origem	O valor de origem é a gravidade do incidente da Symantec.

Nota: No sistema de base, há quatro mapeamentos de gravidade que são enviados para os usuários da DLP.

4. Clique em **Enviar**.

Mapeamento de gravidade



Configurar regras de resposta inteligente

Configure as regras de resposta inteligente da Symantec para executar ações de resposta nos incidentes do DLP da Symantec ingeridos.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

Verifique se o usuário da Symantec que você está configurando para a integração do DLP do ServiceNow Symantec deve ter essas Regras de resposta inteligente selecionadas na página de **configuração de funções**. Para obter mais informações, consulte a seção **Ações** disponível no documento Configuração de funções .

Para as regras de resposta inteligente buscadas, o administrador da DLP pode criar as regras de opção de resposta do incidente e os mapeamentos de opção de resposta para configurar as ações de resposta a serem executadas em incidentes do Symantec DLP ingeridos.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração da DLP da Symantec** > **Regras de resposta inteligente**.
   Você verá todas as opções de resposta inteligente disponíveis para cada configuração de integração definida. Para obter mais informações, consulte Instalar e configurar a Symantec integração DLP para prevenção de perda de dados e siga o procedimento explicado sobre como configurar a integração da Symantec: origem de configuração caso não tenha sido configurada.
2. Clique em qualquer uma das Regras de resposta inteligente para abrir a exibição do formulário.

   Siga Criar regras de opção de resposta a incidentes para criar regras de opção de resposta a incidentes e mapeamentos de opção de resposta para exibir esta regra de resposta inteligente no modal de resposta do espaço da DLP.
3. Crie as regras de aprovação para a Regra de resposta inteligente usando a guia **Regras de aprovação** na lista relacionada ou seguindo o procedimento explicado na seção Configurar regras de aprovação.
   As regras de aprovação para cada regra de resposta inteligente ficarão visíveis na lista relacionada de regras de aprovação.
4. Depois de criar as regras de opção de resposta do incidente, você pode ver o registro na lista relacionada do registro de regra de resposta inteligente.
5. Use o botão **Atualizar regra de resposta inteligente** na exibição de lista para atualizar manualmente a origem.
   As regras de resposta inteligente adicionarão, atualizarão ou excluirão automaticamente todos os dias para todas as origens.

Executar regras de resposta inteligente

Use este recurso para executar Regras de resposta inteligente para os incidentes do Symantec DLP.

Antes de Iniciar

Você precisa configurar as Regras de resposta inteligente seguindo o procedimento explicado aqui nesta seção, Configurar regras de resposta inteligente.

Função necessária: sn_dlir.admin

Nota:

As opções de resposta no espaço estarão disponíveis para o usuário final, analista ou gerente com base na configuração mencionada na seção Configurar opção de resposta para seus incidentes da DLP.

Procedimento

1. Navegar até **Todos** > **DLP** > **Espaço do usuário da DLP**.
2. Abra qualquer incidente do Symantec DLP.
3. Clique **em Responder**.
4. Selecione a opção de resposta na lista suspensa Resposta.
   As opções de resposta ficarão visíveis com base na configuração da **Regra de opção de resposta do incidente** e nos **Mapeamentos de opção**de resposta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.

> **Nota:** Você também pode configurar as regras de aprovação para as opções de resposta seguindo o procedimento explicado na seção Criar regras de aprovação. Quando uma regra de aprovação for configurada para a Regra de resposta inteligente, o fluxo de aprovação será acionado primeiro e, depois de receber todas as aprovações, o fluxo de Opção de resposta inteligente será acionado. O estado do incidente da DLP será atualizado de acordo com o estado de destino do mapeamento da opção de resposta após a execução bem-sucedida da opção de resposta.

Baixar arquivos de evidências

Baixe arquivos de evidências de incidentes da DLP que violam a política da DLP na Symantec.

Antes de Iniciar

Baixe este arquivo para sua máquina local a partir do espaço do analista de IR da DLP e do espaço do usuário final de IR da DLP. A ação Baixar arquivos estará disponível somente para os aprovadores no espaço do usuário final de IR da DLP.

Função necessária:

- sn_dlir.analyst
- sn_dlir.secure_file_download (qualquer aprovador com esta função)

Procedimento

1. Navegar até **Todos** > **Integração da DLP da Symantec** > **Configuração**.
2. Habilite a propriedade **Deve o download do arquivo violador do incidente relatado ser permitido**.
   Depois de habilitar esta propriedade, você poderá ver a ação **Baixar arquivo** no Espaço do analista da DLP para qualquer incidente do Symantec DLP.
3. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do analista da DLP**.
4. Abra um registro de incidente do DLP que é ingerido da origem da Symantec.
5. Clique **em Baixar arquivo**.

> **Nota:** O arquivo que violou a política DLP na Symantec será baixado na máquina local do usuário.

Para que o aprovador exiba a ação Baixar arquivo, siga as etapas mencionadas abaixo:

6. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do usuário da DLP**.
   A página Meus incidentes da DLP será exibida em uma nova guia.
7. Selecione o módulo **Minhas aprovações** disponível no módulo Meus incidentes da DLP.
   A exibição da lista Minhas aprovações será exibida.
8. Abra um registro de solicitação de aprovação gerado para o incidente do Symantec DLP.
9. Clique no ícone de informações (i) disponível no campo Incidente da DLP na exibição do formulário.
10. Clique **em Baixar arquivo**.

Resultados

Depois de executar esta ação, o arquivo de evidências no formato ZIP (se o incidente tiver violações em vários componentes e/ou os dados da mensagem original também estiverem

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

disponíveis) ou um único arquivo (se o incidente tiver violações em um único componente ou somente os dados da mensagem original serão disponível) será baixado para a máquina local do usuário.

Nota: Como administrador da DLP, você pode controlar o acesso da ação **Baixar arquivo** desabilitando a opção **Caso o download do arquivo violador do incidente relatado seja permitido** na página **Configurações avançadas**. Para obter mais informações, consulte Definição das configurações avançadas do Data Loss Prevention Incident Response .

Definir as Symantec configurações de integração da DLP

Modifique as Symantec propriedades do sistema padrão de integração da DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Navegar até **Integração da DLP da Symantec** > **Configurações**.
2. Modifique as seguintes configurações conforme necessário.

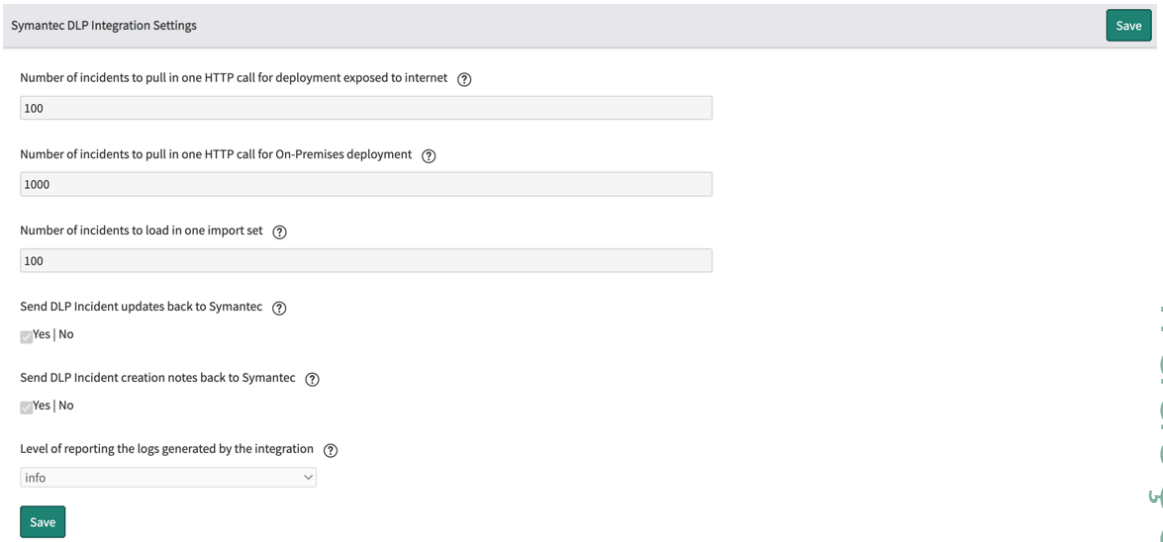
Configurações

Campo	Descrição
Impor um limite no número de incidentes para extrair uma chamada HTTP para implantação no local sn_sym_dlp.page_size_on_prem	Número máximo de incidentes a serem obtidos em uma chamada HTTP para implantação no local de Symantec. ◦ Tipo: inteiro ◦ Valor padrão: 1000
Impor um limite no número de incidentes para extrair uma chamada HTTP para implantação exposta à internet sn_sym_dlp.page_size_on_internet	Número máximo de incidentes a serem obtidos em uma chamada HTTP para implantação Symantec exposta à Internet. ◦ Tipo: inteiro ◦ Valor padrão: 100
Número de incidentes a serem carregados em um conjunto de importação sn_sym_dlp.incidents_per_attachment	Número de registros a serem armazenados em um arquivo de anexo para processamento. ◦ Tipo: inteiro ◦ Valor padrão: 100
Enviar atualizações de incidentes da DLP de volta para a Symantec sn_sym_dlp.incident_update	Esta propriedade permite restringir qualquer sincronização de estado entre ServiceNow e Symantec incidentes da DLP. ◦ Tipo: booleano ◦ Valor padrão: **verdadeiro**
Enviar anotações de criação de incidentes da DLP de volta para a Symantec sn_sym_dlp.incident_creation_notes	Esta propriedade permite que você envie uma anotação de volta para a Symantec assim que um incidente for criado em ServiceNow.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Tipo: booleano ◦ Valor padrão: **verdadeiro**
Nível de emissão de relatórios dos logs gerados pela integração sn_sym_dlp.logging.verbosity	Propriedade que define a emissão de relatórios dos logs gerados pela integração.



3. Clique em **Salvar**.

Separação de domínios na integração Symantec da DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico.

Como o Domain Separation funciona com Symantec integração de DLP

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração da DLP Symantec no domínio apropriado.

Data Loss Prevention Incident Response Integration with Proofpoint

A Proofpoint integração de DLP oferece suporte à ingestão de incidentes de prevenção de perda de dados criados na implantação Proofpoint de prevenção de perda de dados. Após a ingestão, você pode usar as funcionalidades de gestão de incidentes para corrigir os incidentes da DLP.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

A Proofpoint integração de DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Esta integração inclui os seguintes recursos principais:

- Criação de vários perfis para diferentes Proofpoint endpoints.
- Automatizar a criação de incidentes da DLP.
- Mapeamento do campo de estado de incidente da DLP Proofpoint para o campo de estado de incidente da DLP.
- Filtragem de Proofpoint incidentes da DLP.
- Ingestão de incidentes em sua instância ServiceNow assim que os incidentes são criados no locatário Proofpoint da DLP.
- Proofpoint A integração da DLP é compatível com endpoints e tipos de e-mail de incidentes.
- Atualizações automáticas para o Proofpoint status de incidente da DLP e comentários para a criação de incidentes da DLP e para mudança de estado e fechamento no lado ServiceNow.

Conheça esta integração

Identificador do documento	Título do documento
Proofpoint site de documentação do produto	Documentação do produto Proofpoint
ServiceNow® site de documentação do produto	Site de documentação do produto da ServiceNow

Introdução à integração Proofpoint para Prevenção de perda de dados

A Proofpoint integração de DLP oferece suporte à ingestão de incidentes de prevenção de perda de dados criados no locatário Proofpoint de prevenção de perda de dados. Após a ingestão, as funcionalidades de gestão de incidentes que corrigem os incidentes do DLP serão usadas.

Check-list

Revise as informações a seguir antes de começar a configurar sua Proofpoint integração DLP para prevenção de perda de dados.

Check-list

Campo	Descrição
Verifique se você atribuiu as funções de aplicativo Now Platform e Data Loss Prevention Incident Response.	As funções a seguir são usadas na Proofpoint integração de DLP na Now Platform:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Campo	Descrição
	• O administrador (admin) instala as aplicações do ServiceNow® Store e atribui o administrador de prevenção de perda de dados (sn_dlir.admin). • O usuário com a função sn_dlir.admin pode configurar a integração e configurar os perfis de incidentes. • Os usuários com a função sn_dlir.analyst têm funções de leitura na integração.
Atribua as Proofpoint funções de usuário da DLP necessárias.	Revise as Proofpoint funções e permissões de integração da DLP.
Verifique se você está usando Proofpoint DLP 1.0.1 ou posterior.	A Proofpoint integração de DLP para prevenção de perda de dados foi testada com Proofpoint Data Loss Prevention, versão 1.0.1 ou posterior.
Verifique se a aplicação principal do usuário final necessária para oferecer suporte à Proofpoint integração do DLP está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Instalar e configurar a integração Proofpoint para prevenção de perda de dados

Instale e configure a Proofpoint integração DLP do ServiceNow® Store em sua instância Now Platform. Comece a investigar incidentes da DLP usando os Proofpoint dados de incidentes da DLP.

Antes de Iniciar

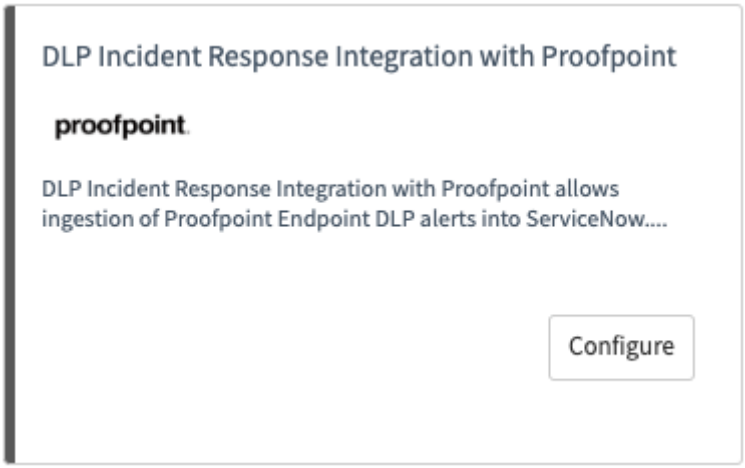
Função necessária: sn_dlir.admin

Procedimento

1. Baixe a Proofpoint integração de DLP do ServiceNow® Store e instale-a.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco `Integração de resposta a incidentes da DLP com Proofpoint` e clique em **Configurar**.

Tradução automática

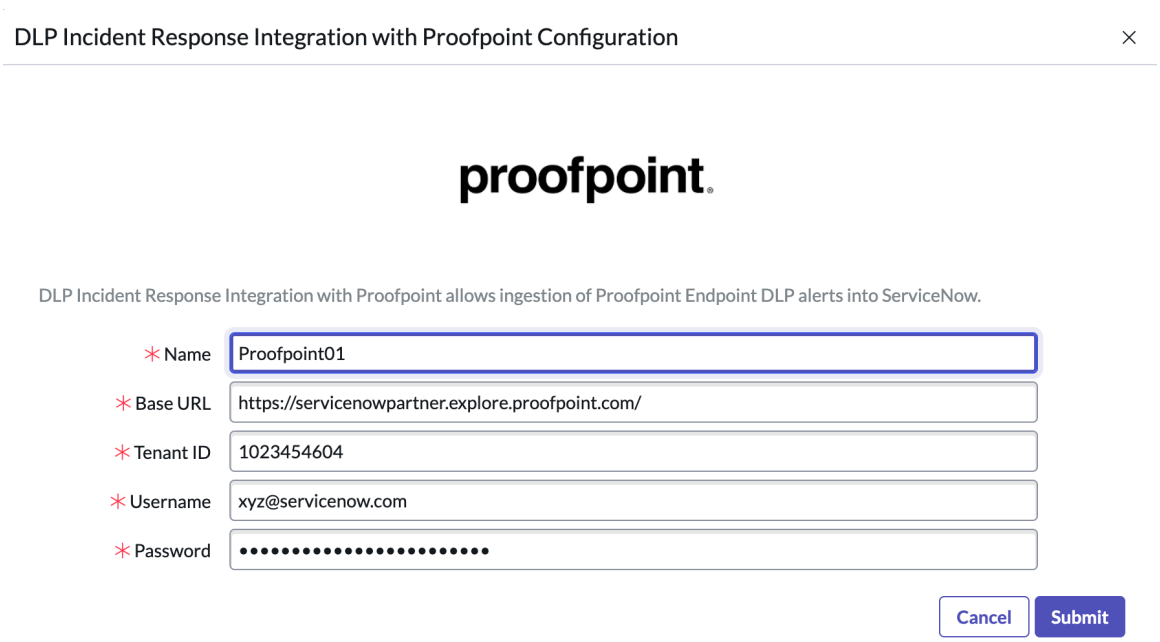
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos.

Proofpoint Formulário de configuração de integração da DLP

Campo	Descrição
Nome	Nome da Proofpoint configuração de integração da DLP.
URL base	URL para o Proofpoint que serve como endpoint REST.
ID de locatário	O ID do locatário Proofpoint a ser usado.
Nome de usuário	Nome de usuário configurado para sua conta de usuário em Proofpoint.
Senha	Senha configurada para sua conta de usuário em Proofpoint.



5. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
Depois de validar e enviar a configuração com sucesso, a Proofpoint integração de DLP é salva na página Integrações de segurança como um bloco.

Configure o Webhook no locatário Proofpoint da DLP para notificações de alerta para ServiceNow

Configure um webhook em Proofpoint usando o endpoint de REST API para começar a receber os alertas do locatário da DLP Proofpoint. Sua instância ServiceNow cria incidentes da DLP a partir desses alertas. A Proofpoint integração de DLP fornece um endpoint de REST API para que os usuários finais configurem o webhook.

Antes de Iniciar
Função necessária: sn_pp_dlp.api_integration_user

Procedimento
1. Faça login no **Proofpoint**.
2. Navegar até **Locatário do Proofpoint** > **Aplicação de administração** > **Integração** > **Políticas de notificação**.
3. Crie uma política de notificação com um nome apropriado.
4. Clique na **política de notificação** e gerencie os webhooks configurados na política de notificação.
5. Crie uma nova configuração de webhook clicando em **Adicionar webhooks**.
6. Selecione o tipo de webhook como **Genérico**.
7. Em Entrada de URL, insira uma URL usando o formato: `https://`<Instance_Name> .service-now.com/api/sn_pp_dlp/provpointalertapi/getalerts .
8. Mantenha o método como **POST**.
9. Adicione os seguintes cabeçalhos ao webhook:
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow
      instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. Não altere os outros valores.
11. Clique em **Salvar**.
12. Navegar até **Locatário do Proofpoint** > **Aplicação de administração** > **Políticas** > **Regras**.
13. Na seção Ações, selecione as regras para as quais a notificação do webhook deve ser gerada.
14. Adicione as políticas de notificação recém-criadas que têm um webhook configurado.
15. Clique em **Salvar**.

Criar um perfil para Proofpoint integração de DLP

Crie um perfil de incidente em sua instância Now Platform. Determine os Proofpoint incidentes do DLP que são adequados para criar incidentes do DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

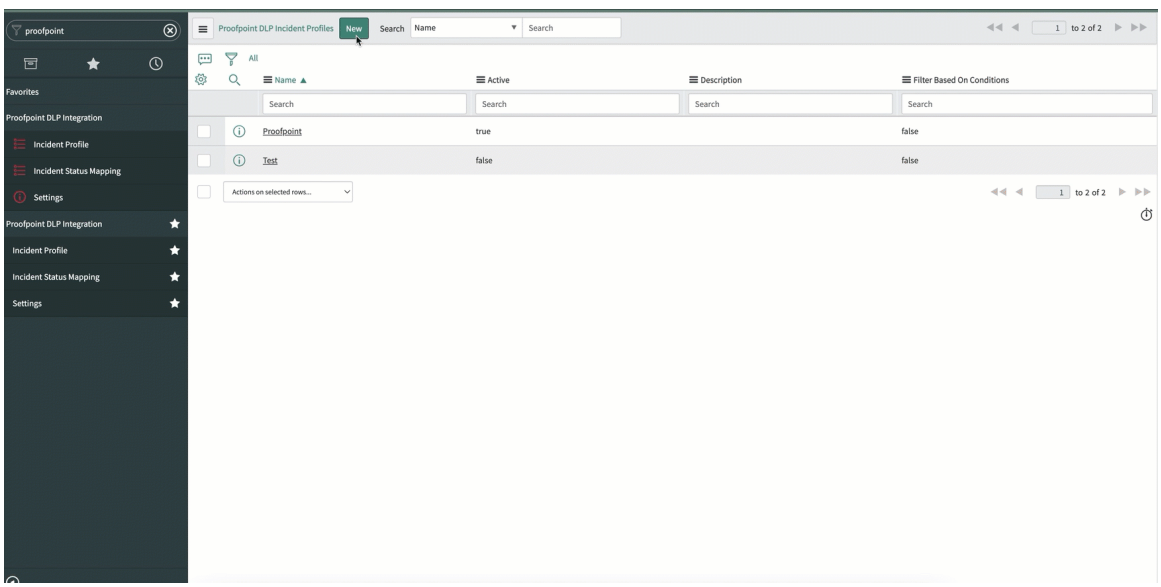
Configure o Now Platform para preencher alertas da DLP de Proofpoint. Armazene os alertas como incidentes do DLP em sua instância ServiceNow.

Procedimento

1. Navegar até **Integração com o Proofpoint do DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção **Nome**.

Criar um perfil para Proofpoint formulário de integração de DLP

Campo	Descrição
Nome	Nome do perfil. Este nome ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	A Proofpoint instância da DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidentes que você planeja ingerir para o perfil.
Ativo	Opção para tornar o perfil ativo. Quando o perfil está ativo, sua instância Now Platform está pronta para receber os incidentes de Proofpoint.
Descrição	Descrição para ajudar a distinguir este perfil de outros perfis.



4. Clique em **Continuar** e vá para a seção Filtragem.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir filtros a serem aplicados na criação de incidentes

Defina e defina as condições de filtro para filtrar os Proofpoint incidentes de DLP de entrada. Controle quais incidentes do DLP devem ser criados em ServiceNow®.

Antes de Iniciar

Função necessária: sn_dlir.admin

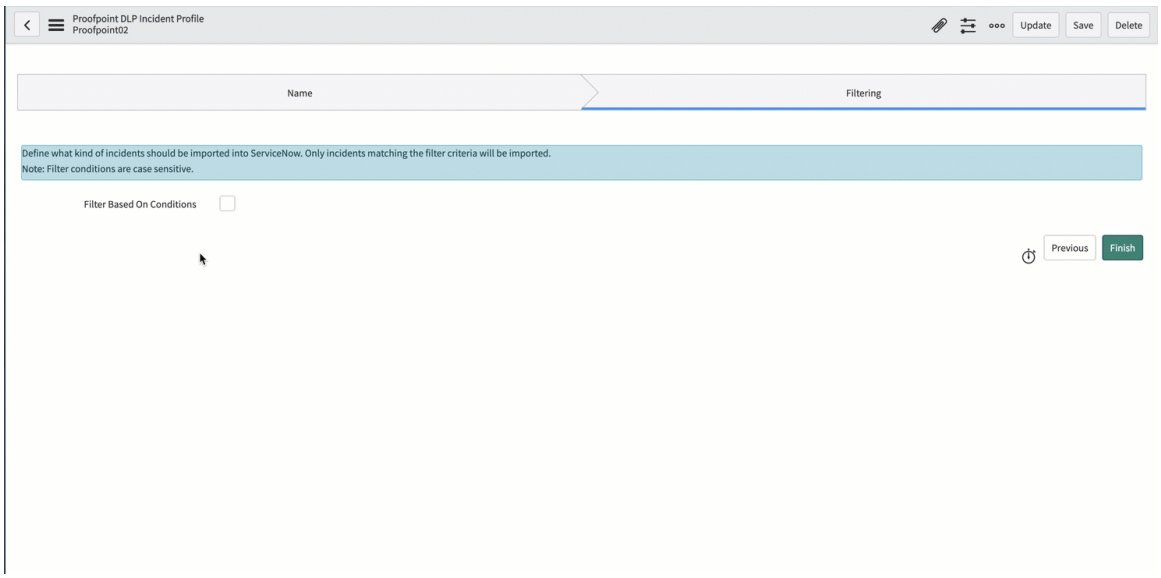
Por Que e Quando Desempenhar Esta Tarefa

Esse tipo de filtragem ajuda a isolar incidentes do DLP e limitar o número de incidentes do DLP que você cria. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento

1. Selecione a opção **Filtrar com base nas condições** e defina os critérios que um Proofpoint incidente de DLP de entrada deve satisfazer para que um incidente de segurança seja criado.
2. Usando as listas e os campos do construtor de condições, defina os filtros no campo **Condições do filtro**.

   As opções no primeiro campo nas **Condições do filtro** correspondem aos campos que estão disponíveis no incidente da DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.



3. Adicione mais condições clicando em **E**ou **OU**.
   - Se **E**for selecionado, todas as condições deverão ser atendidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Clique em **Concluir**.

Mapear Proofpoint status de incidentes da DLP com ServiceNow status de incidente

Sincronize o status dos incidentes de DLP ingeridos em sua instância ServiceNow e os incidentes de DLP de Proofpoint. Mapeie o status de incidente ServiceNow com o status de incidente Proofpoint.

Antes de Iniciar

Função necessária: sn_dlir.admin

Tradução automática

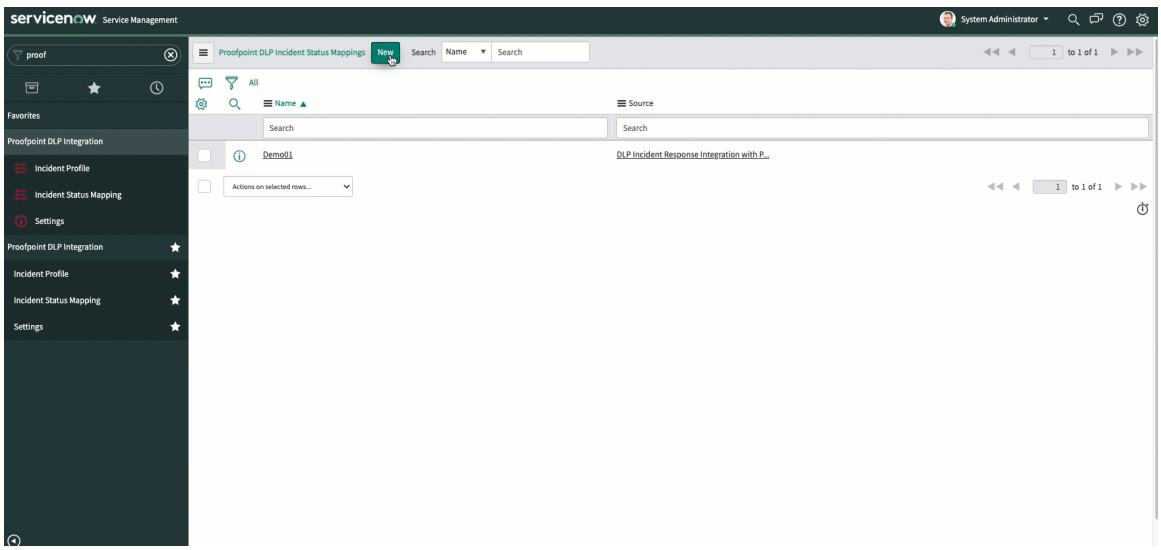
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Integração com o Proofpoint do DLP** > **Incidente** > **Mapeamento do status do incidente**.
2. Forneça um **Nome** para identificar o mapeamento.
3. Selecione o bloco **Origem** (configuração de integração) para o qual o Mapeamento de status deve ser aplicado.
4. Mapeie o status do **incidente da DLP da ServiceNow com o status** do incidente do **Proofpoint**.

Mapear o status de incidentes do Proofpoint do DLP com o formulário de status de incidente da ServiceNow

Campo	Descrição
Nome	Espaço reservado para o registro de mapeamento.
Origem	Origem do endpoint configurado Proofpoint de onde você deseja buscar o status do incidente.
Status do incidente da ServiceNow	Lista de status de incidentes do DLP.
Status do incidente do ponto de prova	Valores mapeados padrão para estados padrão disponíveis em incidentes do DLP. Para estados personalizados, o status Proofpoint padrão é **Novo**. Você pode modificar e adicionar o status Proofpoint necessário no campo de entrada.



5. Clique em **Enviar**.

Resultados

Um registro para mapeamento foi criado com sucesso. Os status dos ServiceNow incidentes serão sincronizados com os Proofpoint incidentes da DLP.

Quando você altera o status de qualquer incidente do DLP em sua instância ServiceNow, o status do incidente do DLP Proofpoint associado será alterado na plataforma de origem Proofpoint, de acordo com o mapeamento definido no registro.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir Proofpoint configurações de integração da DLP

Modifique as Proofpoint propriedades do sistema padrão de integração da DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Procedimento

1. Navegar até **Integração com o Proofpoint da DLP** > **Configurações**.
2. Modifique as seguintes configurações conforme necessário.

Campo	Descrição
Tempo limite máximo para chamadas HTTP sn_pp_dlp.maximum_http_time_out	Tempo limite máximo para chamadas HTTP (em segundos). ◦ Tipo: inteiro ◦ Valor padrão: 30
Enviar atualizações de incidentes da DLP de volta para o Proofpoint sn_pp_dlp.incident_update	Esta propriedade permite restringir qualquer sincronização da sua instância [ServiceNow para Proofpoint incidentes da DLP. ◦ Tipo: booleano ◦ Valor padrão: verdadeiro
Nível de emissão de relatórios dos logs gerados pela integração sn_pp_dlp.logging.verbosity	O nível de logs de emissão de relatórios gerados pela integração.

3. Clique em **Salvar**.

Resultados
Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Domain Separation in Proofpoint Integração com DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico.

Como o Domain Separation funciona com Proofpoint integração de DLP

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração da DLP Proofpoint no domínio apropriado.

Data Loss Prevention Incident Response Integration with Netskope

A Netskope integração de DLP oferece suporte à ingestão de incidentes de prevenção de perda de dados criados na implantação Netskope de prevenção de perda de

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

dados. Netskope A DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Após a ingestão, você pode usar as funcionalidades de gestão de incidentes para corrigir os incidentes da DLP.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Criação de vários perfis para diferentes Netskope locatários.
- Automatizando a criação de incidentes da DLP da ServiceNow a partir de Netskope incidentes da DLP.
- Filtragem de Netskope incidentes da DLP.
- Ingestão programada de Netskope incidentes de DLP que criam incidentes de DLP na ServiceNow.
- Atualize automaticamente o status do objeto em Netskope quando o estado da DLP mudar em sua instância da ServiceNow.
- Exiba os detalhes forenses (violação de conteúdo) do incidente da DLP no espaço do analista de IR da DLP e no espaço do usuário final da DLP.

  Nota: O conteúdo violador não persiste na ServiceNow. O conteúdo é extraído quando o incidente é aberto no espaço.

- Baixando arquivo de evidências diretamente de Netskope sob demanda.

  Nota: O arquivo de evidências não persiste na ServiceNow. O arquivo de evidências é extraído quando o analista clica em **Baixar arquivo** no espaço.

- Notificação por e-mail para usuários administradores da DLP sobre a expiração do token Netskope.
- A notificação por e-mail será enviada aos usuários administradores da DLP se ela exceder o limite de novas tentativas definido para falhas de chamada de API de incidente.
- Netskope também oferece suporte ao processo de execução de integração. Para obter mais informações, consulte Monitorar o processo de execução da integração da DLP.

Primeiros passos com Netskope integração de DLP para prevenção de perda de dados

Revise as informações a seguir antes de começar a configurar sua Netskope integração DLP para prevenção de perda de dados.

Tarefa de configuração	Descrição
Verifique se você atribuiu a Now Platform, aplicação de prevenção de perda de dados necessária.	As funções a seguir são usadas na Netskope integração de DLP na Now Platform: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui o administrador de prevenção de perda de dados (sn_dlir.admin).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de configuração	Descrição
	• O usuário com a função sn_dlir.admin pode configurar a integração e configurar os perfis de incidentes. • Os usuários com a função sn_dlir.analyst terão funções de leitura na integração.
Atribua os privilégios necessários para o Netskope token da API v2.	Os seguintes privilégios de endpoint são usados na tokenização da Netskope API v2. • Leitura: /api/v2/incidents/dlpincidents • Leitura: /api/v2/events/dataexport/events/incident • Leitura + gravação: /api/v2/incidents/update
Verifique se a aplicação principal do usuário final necessária para oferecer suporte à Netskope integração do DLP está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Instalar e configurar a Netskope integração DLP para prevenção de perda de dados

Instale e configure a integração Netskope de DLP da instância ServiceNow StoreNow Platform. Você pode começar a investigar incidentes da DLP usando os Netskope dados de incidentes da DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Baixe a Netskope integração de DLP do ServiceNow Store e instale-a.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**
3. Pesquise o bloco `Integração de resposta a incidentes da DLP com Netskope` e clique em **Configurar**.
4. No formulário, preencha os campos.

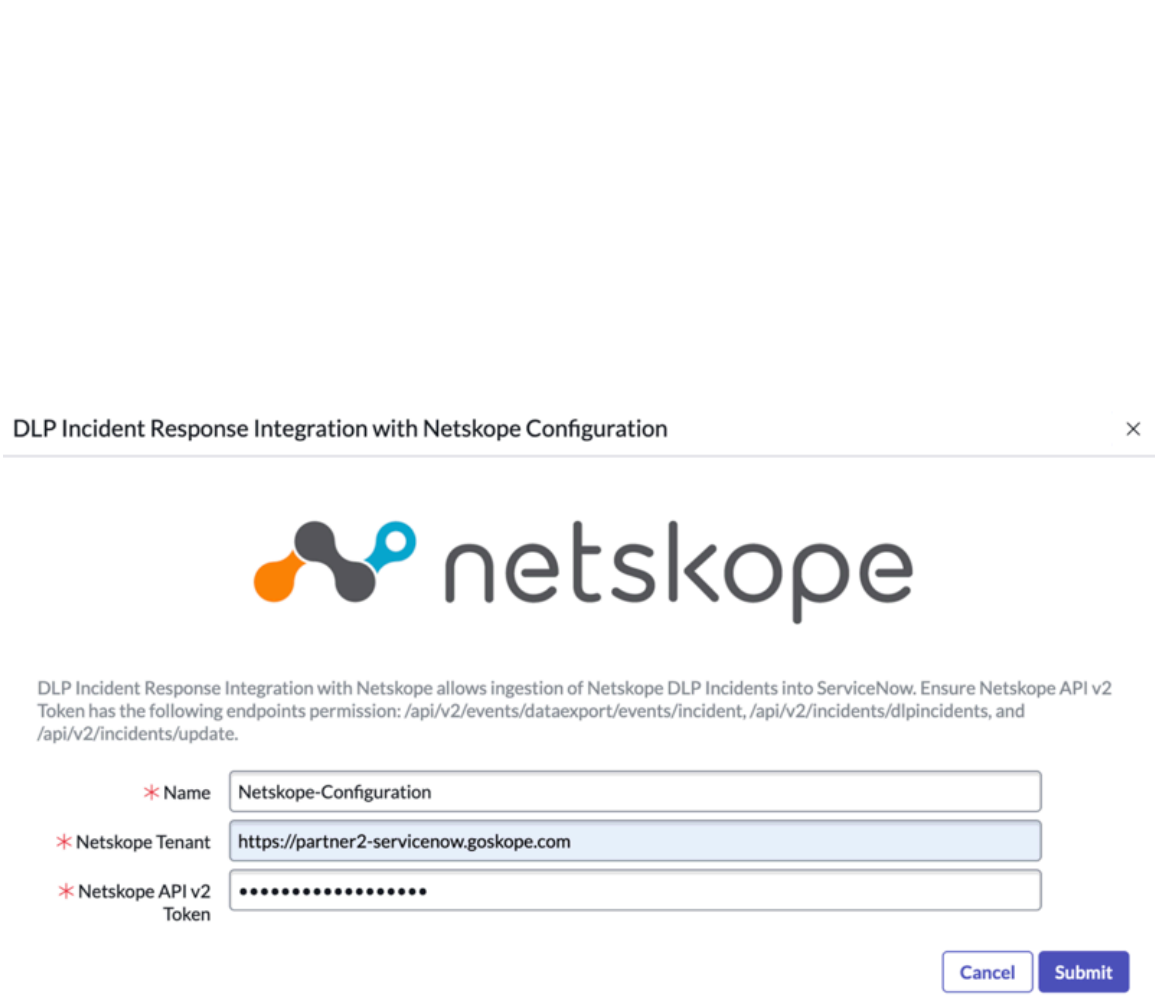
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Certifique-se de que o Token Netskope API v2 tenha os privilégios de endpoint abaixo:

- Leitura: /api/v2/incidents/dlpincidents
- Leitura: /api/v2/events/dataexport/events/incident
- Leitura + gravação: /api/v2/incidents/update

Criar



Campo	Descrição
Nome	Nome da Netskope configuração de integração da DLP.
Locatário do Netskope	A URL base NetskopeNetskope do locatário [].
Token da API do Netskope v2	Token configurado para REST API v2 em sua conta de usuário em Netskope.

5. Clique em **Enviar**.

Resultados
Depois de validar e enviar a configuração com sucesso, a Netskope integração de DLP é salva na página Integrações de segurança como um bloco.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um perfil para Netskope integração de DLP

Crie um perfil de incidente em sua instância Now Platform.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Configure Now Platform para recuperar os incidentes do DLP do endpoint Netskope. Armazene os incidentes em sua instância ServiceNow como incidentes da DLP.

Procedimento

1. Navegar até **Integração do Netskope DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Criar um perfil

Campo	Descrição
Nome	Nome do perfil. O nome deve ser exclusivo para cada perfil. Este nome ajuda a identificar o perfil.
Origem	Netskope Instância da DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidentes que você planeja ingerir para o perfil. **Nota:** Somente um perfil ativo é permitido por origem.
Ativo	Indicador de que o perfil está ativo. **Nota:** Este campo está disponível somente depois que você clica em **Concluir** na última seção Programação. Quando o perfil está ativo, sua instância Now Platform está pesquisando ativamente Netskope incidentes da DLP. Incidentes de DLP correspondentes são criados como incidentes de DLP da ServiceNow quando as condições de filtragem são correspondidas com base nos parâmetros de programação que você forneceu.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa é considerado como a prioridade mais alta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por padrão, o valor é 100.
Descrição	Descrição para ajudá-lo a distinguir este perfil de outros perfis.

4. Clique em **Continuar** e vá para a seção Filtragem.

Definir filtros a serem aplicados na criação do incidente

Defina e defina as condições de filtro para filtrar os Netskope incidentes de DLP de entrada. Controle quais desses incidentes devem ser criados como incidentes do DLP em sua instância ServiceNow.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Esse tipo de filtragem ajuda a isolar incidentes do DLP e limitar o número de incidentes do DLP que você cria. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento
1. Selecione a opção **Filtrar com base nas condições** e defina os critérios que um incidente do Netskope DLP de entrada deve satisfazer para que um incidente do DLP seja criado.
2. Usando as listas e os campos do construtor de condições, defina os filtros no campo **Condições do filtro**.

   As opções no primeiro campo nas **Condições do filtro** correspondem aos campos que estão disponíveis na tabela de **importação de incidentes do Netskope DLP**. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.
3. Adicione mais condições clicando em **E**ou **OU**.
   - Se **E**for selecionado, todas as condições deverão ser atendidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Clique em **Continuar** e vá para a seção Programação.

Programar Netskope recuperação de incidentes da DLP

Defina uma programação para recuperar Netskope incidentes da DLP que correspondam aos critérios no perfil.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode planejar a frequência com que pesquisará novos Netskope incidentes que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer uma recuperação única usando a caixa de seleção **Recuperação única**. A data histórica pode ser até um mês a partir do passado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Configure a programação para definir como e quando você extrai incidentes de Netskope.
2. No formulário, preencha os campos.

Programar os Netskope incidentes da DLP

Campo	Descrição
Adição de incidentes em andamento	Ingestão contínua de incidentes que sua instância Now Platform extrai de Netskope para novos incidentes. Se forem encontrados incidentes acionados que correspondam aos critérios de filtragem de incidentes, os incidentes da DLP serão criados.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos. Este valor padrão é definido como **5**.
Definir horário de adição do incidente inicial	Opção para definir a ingestão de incidentes inicial com base na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora que você especifica para a ingestão de incidentes.
Horário de adição do incidente inicial	A primeira vez em que os dados são ingeridos. **Nota:** O valor ficará visível somente se a opção **Definir tempo de ingestão do incidente inicial** estiver selecionada.
Horário de adição do próximo incidente (estimado)	O próximo tempo estimado de ingestão de incidentes.
Recuperação Única	Opção para habilitar a extração única de dados históricos. **Nota:** Se selecionado, os dados históricos serão extraídos da Netskope DLP de acordo com a data adicionada em **Desde a data**.
Desde a Data	Data a partir da qual os dados são obtidos de Netskope.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: No máximo, os últimos 30 dias de dados podem ser obtidos de Netskope.

3. Clique em **Concluir**.
4. No pop-up, salve a configuração de perfil criada clicando em **Concluir**.
5. Ative o perfil.
   a. Abra o perfil criado.
   b. Defina **Ativo** como **verdadeiro**.
   c. Clique em **Atualizar**.

Resultados
Após a ativação bem-sucedida da criação do perfil, os incidentes serão obtidos periodicamente de acordo com a configuração definida no perfil. Os incidentes serão adicionados à tabela de incidentes da DLP.

Como mapear o status do incidente da DLP com Netskope

A seção de mapeamento de status do incidente permite que os usuários forneçam os mapeamentos entre o status do incidente da DLP na ServiceNow e o status do objeto Netskope.

Antes de Iniciar
O mapeamento será usado ao ingerir qualquer incidente DLP de Netskope para a ServiceNow, bem como sincronizar qualquer mudança de estado do incidente DLP na ServiceNow de volta para Netskope.

Sincronize o status dos incidentes de DLP ingeridos na ServiceNow com o incidente de DLP de Netskope. Mapeie o campo Status do incidente da ServiceNow com o campo Status do objeto Netskope.

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Você precisa criar um mapeamento de status de incidente one-to-one de Netskope e o status da ServiceNow.

Procedimento
1. Navegar até **Integração do Netskope DLP** > **Mapeamento de status de incidente**.
2. Forneça um Nome para identificar o mapeamento.
3. Selecione a Integração de origem.
4. Mapeie o status de incidente da DLP com o status de objeto Netskope (o estado duplicado Netskope também pode ser mapeado).
   A sincronização de status da ServiceNow para Netskope será desabilitada se você não criar um registro de mapeamento.

Importante: Você precisa mapear todos os status de objeto Netskope para todos os status da ServiceNow. Selecione a origem para sincronizar o status do incidente da DLP novamente com o objeto Netskope.

Tradução automática

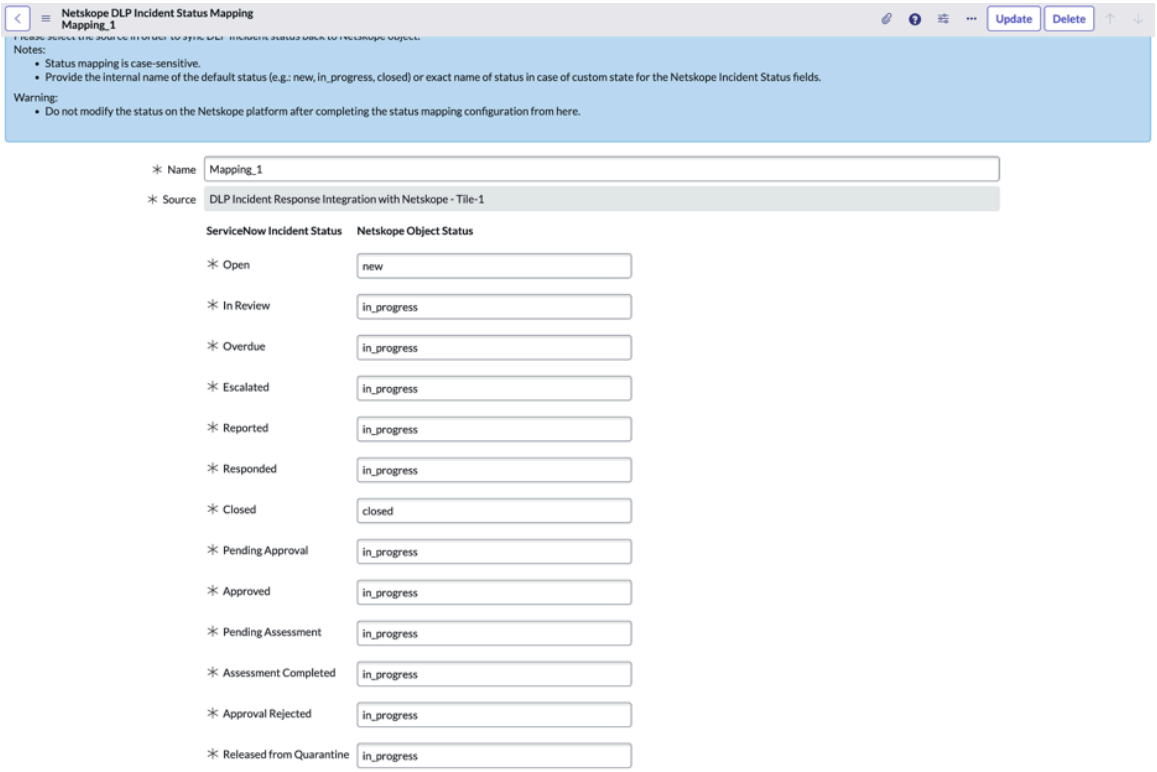
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As seguintes informações e mensagens de alerta são exibidas quando você mapeia o status do incidente, revisa as mensagens e prossegue.

Nota:

- O mapeamento de status faz distinção entre maiúsculas e minúsculas.
- Forneça o nome interno do status padrão (por exemplo: novo, in_progress, fechado) ou o nome exato do status em caso de estado personalizado para os campos de status do objeto Netskope.

Aviso: Não modifique o status na plataforma Netskope depois de concluir a configuração do mapeamento de status aqui.



Netskope Mapeamento de status de incidente da DLP

Campo	Descrição
Nome	Nome do registro de mapeamento.
Origem	A origem do endpoint configurada Netskope de onde você deseja sincronizar o status do incidente.
Status do incidente da DLP	Indica a lista de status de incidentes do DLP.
Netskope Status do objeto	Indica a lista de status de objeto Netskope.

5. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
Depois de criar com sucesso o registro para mapeamento de status, sempre que houver uma atualização no estado do incidente da DLP da ServiceNow, ele será refletido automaticamente no lado Netskope de acordo com o mapeamento.

Nota: Se você alterar o status de qualquer incidente do DLP no locatário Netskope diretamente, a sincronização de status do SN para Netskope não funcionará, considerando as limitações da API. Certifique-se de mapear todos os status de incidente da DLP com o status de objeto Netskope com cuidado.

Definir Netskope configurações de integração da DLP

Modifique as Netskope propriedades do sistema padrão de integração da DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Procedimento
1. Navegar até **Integração do Netskope DLP** > **Configurações**.
2. Modifique as seguintes configurações conforme necessário.

Definir Netskope configurações de integração da DLP

Campo	Descrição
O download do arquivo de violação do incidente relatado deve ser permitido sn_ns_dlp.enable_file_download.	Opção para escolher se você deseja habilitar o download do arquivo. Por padrão, esta opção está habilitada.
Tempo limite máximo para chamadas HTTP, em segundos sn_ns_dlp.maximum_http_time_out.	Tempo limite máximo para chamadas HTTP, em segundos. Este campo é definido automaticamente como 30.
Número máximo de novas tentativas a serem realizadas para falhas de API. sn_ns_dlp.maximum_retry.	Número máximo de novas tentativas a serem realizadas para falhas de API. O valor padrão é definido como 3.
Nível de emissão de relatórios dos logs gerados pela integração sn_ns_dlp.logging.verbosity.	Defina o nível de logs de emissão de relatórios gerados pela integração. Este campo é definido automaticamente como **info**.

3. Clique em **Salvar**.

Resultados
Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Baixar arquivos de evidências

Baixe arquivos que violam a política DLP em Netskope. Baixe este arquivo para sua máquina local a partir do espaço do analista de IR da DLP e do espaço do usuário final de IR da DLP para aprovadores.

Antes de Iniciar
Função necessária:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_dlir.analyst
- sn_dlir.secure_file_download (qualquer aprovador com esta função)

Por Que e Quando Desempenhar Esta Tarefa
Você precisa habilitar o download de arquivo para Netskope antes de prosseguir.

Procedimento
1. Navegar até **Todos** > **Integração do Netskope DLP** > **Configurações**.
2. Habilite a propriedade **Deve ser permitido baixar o arquivo de violação do incidente relatado**.
   Você poderá ver o botão **Baixar arquivo** no espaço do analista de IR da DLP e no espaço do usuário final de IR da DLP.
3. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do analista da DLP**.
4. Abre um registro de incidente da DLP que é ingerido da origem Netskope.
5. Clique **em Baixar arquivo**.
   O arquivo que viola a política DLP no Netskope será baixado para a máquina local do usuário.

> **Nota:** O administrador da DLP pode controlar o acesso à ação **Baixar arquivo** para todas as integrações, desabilitando a opção **Caso o download do arquivo violador do incidente relatado seja permitido** na página **Configurações avançadas** da Administração da DLP. Para obter mais informações, consulte Definir configurações avançadas.

Notificações para usuários no mecanismo de nova tentativa

Netskope A integração tentará novamente o número configurado de vezes em caso de falhas de API durante a ingestão de incidentes da DLP.

Depois que o limite máximo de novas tentativas é excedido, a integração Netskope envia uma notificação por e-mail para usuários que têm a função de administrador da DLP (sn_dlir.admin).

Depois de concluir a instalação e a configuração da integração, forneça a função de administrador da DLP (sn_dlir.admin) aos usuários que devem ser notificados quando o limite máximo de novas tentativas for excedido.

Quando o limite máximo de novas tentativas for excedido, o perfil ignorará a ingestão por até uma hora. O número máximo de novas tentativas é configurado usando a propriedade: `Número máximo de novas tentativas a serem executadas para falhas de API`. Para obter mais informações, consulteDefinir Netskope configurações de integração da DLP.

Notificações por e-mail sobre a expiração da credencial

Quando o token usado na instância ServiceNow expira, a integração Netskope envia uma notificação por e-mail para usuários com a função de administrador da DLP (sn_dlir.admin).

Depois que a configuração da integração for concluída, forneça a função de administrador da DLP (sn_dlir.admin) aos usuários que devem ser notificados se o token expirar.

Se o token expirar, a ingestão de dados para perfis associados ficará em espera até que a configuração de integração do Netskope seja atualizada com um token válido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você deve criar um token ou renovar o antigo em Netskopee atualizar o token na instância ServiceNow. Se você renovar o token estendendo o tempo de expiração, a aplicação Netskope detectará automaticamente a renovação e continuará com a coleta de dados. Se você criar um token, deverá atualizar o token na configuração.

Domain Separation in Netskope Integração com DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico.

Como o Domain Separation funciona com Netskope integração de DLP

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração da DLP Netskope no domínio apropriado.

Data Loss Prevention Incident Response com Microsoft

O Data Loss Prevention Incident Response com Microsoft fornece uma estrutura principal para importar incidentes de prevenção de perda de dados (DLP) de várias origens, como Microsoft aplicações de escopo (Microsoft Teams, Exchange Online, SharePoint Online, OneDrive for Business). Os dispositivos de endpoint permitem o fluxo de trabalho de correção que envolve usuários finais, gerentes e a equipe de operações da DLP com atribuições e escalações automatizadas de incidentes.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Use os principais recursos desta integração para realizar as seguintes ações:

- Crie vários perfis para contas diferentes.
- Automatize a criação de DLP IR incidentes.
- Mapeie os campos de evento [Microsoft DLP IR para campos de incidente DLP IR.
- Filtrar Microsoft DLP IR eventos.
- Programe a ingestão de DLP IR eventos que criam DLP IR incidentes periodicamente.
- Armazene o conteúdo correspondente de cada evento do Microsoft DLP no armazenamento em nuvem externa.
- Exclua o conteúdo correspondente no armazenamento em nuvem externa após a exclusão do incidente [DLP IR em ServiceNow.
- Baixe arquivos para DLP IR incidentes do tipo Exchange, OneDrive e SharePoint.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça esta integração

Identificador do documento	Título do documento
Microsoft site de documentação do produto	Site de documentação de produtos da Microsoft
ServiceNow site de documentação do produto	Site de documentação do produto da ServiceNow

Introdução à integração do Microsoft DLP IR para prevenção de perda de dados

Revise as informações a seguir antes de começar a configurar sua integração Microsoft DLP IR para prevenção de perda de dados.

Check-list

Configuração de tarefa	Descrição
Obtenha as credenciais do Microsoft Purview para buscar os dados do evento e as credenciais da conta de armazenamento do AWS/Azure para armazenar o conteúdo de correspondência Registrar uma aplicação com a plataforma de identidade da Microsoft	Registre uma aplicação na plataforma Microsoft Azure aqui para obter o ID do cliente, o segredo do cliente e o ID do locatário. Para obter informações sobre as funções necessárias para criar uma aplicação, consulte Pré -requisitos. Para obter informações sobre as permissões/ funções de API necessárias em uma aplicação do Microsoft Azure para configurá-la na integração ServiceNow do Microsoft DLP, consulte a tabela a seguir.
Permissões necessárias para que o usuário do Azure obtenha o acesso de leitura/gravação/exclusão de blob no armazenamento do Azure	O usuário do Azure deve ter a função **de colaborador de dados de blob de armazenamento** para ler, gravar e excluir blobs no armazenamento do Azure.
Permissões necessárias para que o usuário da AWS obtenha o acesso de leitura/gravação/exclusão de objeto no armazenamento da AWS	Deve ser criada uma política que conceda acesso de lista, leitura, gravação e exclusão para o objeto no armazenamento S3 da AWS.
Atribua e verifique se você tem as funções necessárias para Now Platform e as funções de Administração de perda de dados.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_dlir.admin. • A função sn_dlir.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Configura os perfis de incidentes.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração do Microsoft DLP IR estão	Verifique se as seguintes DLP IR aplicações e aplicações comuns de suporte à segurança estão instaladas e ativadas na ServiceNow

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
instaladas e ativadas antes de configurar esta integração.	Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Permissões/funções de API necessárias em uma aplicação do Microsoft Azure

Você precisa das seguintes permissões/funções de API em uma aplicação do Microsoft Azure para configurá-la na **ServiceNow** *integração do Microsoft DLP.*

API	Nome da permissão	Tipo	Descrição	Necessário para qual funcionalidade da ServiceNow?	O consentimento do administrador é necessário?
API de gestão do Office 365	FeedDeAtividade.Ler	Aplicação	Leia eventos de política da DLP, incluindo dados confidenciais detectados	Para ingerir os eventos do DLP do escopo do MSFT para ServiceNow. **Nota:** Esta permissão é obrigatória para obter os dados do MSFT em ServiceNow.	Sim
API do Microsoft Graph	Files.Read.All	Aplicação	Leia arquivos em todos os conjuntos de sites que você pode acessar.	Baixar arquivo: para baixar o anexo na instância da ServiceNow que causou o evento da DLP do OneDrive ou do SharePoint **Nota:** Isso é opcional. Você pode ignorar esta permissão de API se não quiser permitir que os analistas baixem o anexo que causou o evento da DLP.	Sim

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Permissões/funções de API necessárias em uma aplicação do Microsoft Azure
Você precisa das seguintes permissões/funções de API em uma aplicação do Microsoft Azure para configurá-la na **ServiceNow** *integração do Microsoft DLP.*

API	Nome da permissão	Tipo	Descrição	Necessário para qual funcionalidade da ServiceNow?	O consentimento do administrador é necessário?
	E-mail.Lido	Aplicação	Leia e-mails em todas as caixas de correio.	Baixar arquivo: para baixar o conteúdo do e-mail (corpo e anexo) na instância da ServiceNow que causou o evento DLP do Exchange. **Nota:** Isso é opcional. Você pode ignorar esta permissão de API se não quiser permitir que os analistas baixem o conteúdo de e-mail (corpo, anexo) que causou o evento da DLP.	Sim
	User.Read	Delegado	Entre e leia o perfil do usuário.	Esta é a permissão padrão que estará disponível para todas as novas aplicações.	Não

Tradução automática

Informações confidenciais detectadas (opcional)

O conteúdo de correspondência é armazenado externamente no armazenamento de blob do Azure ou no bucket do Amazon S3 e será extraído do armazenamento externo quando o usuário exibir um incidente.

Qualquer uma das permissões a seguir será necessária se os usuários quiserem exibir a correspondência de conteúdo/informações confidenciais detectadas na aplicação DLP Core:

1. Se você for um usuário Microsoft Azure, deverá ter a função de Colaborador de Dados de Blob de Armazenamento para ler, gravar e excluir blobs no Armazenamento do Azure.
2. Se você for um usuário do Amazon S3, deverá criar uma política que forneça acesso de lista, leitura, gravação e exclusão para o objeto no armazenamento do Amazon S3.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar a integração do Microsoft DLP

Instale e configure a integração do DLP Incident Response com Microsoft DLP do ServiceNow® Store em sua instância Now Platform. Comece a investigar incidentes da DLP usando os Microsoft dados de eventos da DLP.

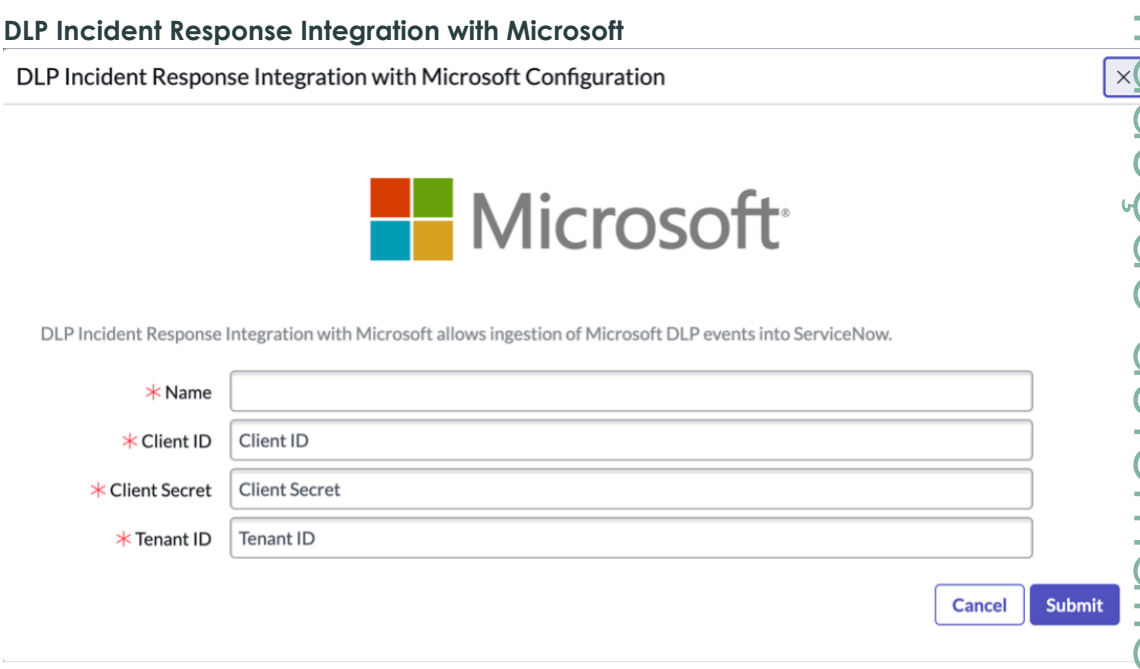
Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Baixe a Microsoft integração de DLP do ServiceNow® Store e instale-a.
2. Navegar até **Operações de segurança** > **Integrações** > **Configurações de Integração**.
3. Configure a Microsoft integração da DLP.

   a. Pesquise o bloco **DLP Incident Response Integration with Microsoft** e clique em **Configurar**.



   b. No formulário, preencha os campos.

Formulário de configuração de integração do DLP da Microsoft

Campo	Descrição
Nome	Nome da Microsoft configuração de integração da DLP.
ID de cliente	ID de cliente da aplicação criada no portal do Microsoft Azure.
Segredo do cliente	Segredo do cliente do app criado no portal do Microsoft Azure.
ID de locatário	ID do locatário do usuário.

   c. Clique em **Enviar**.

Tradução automática

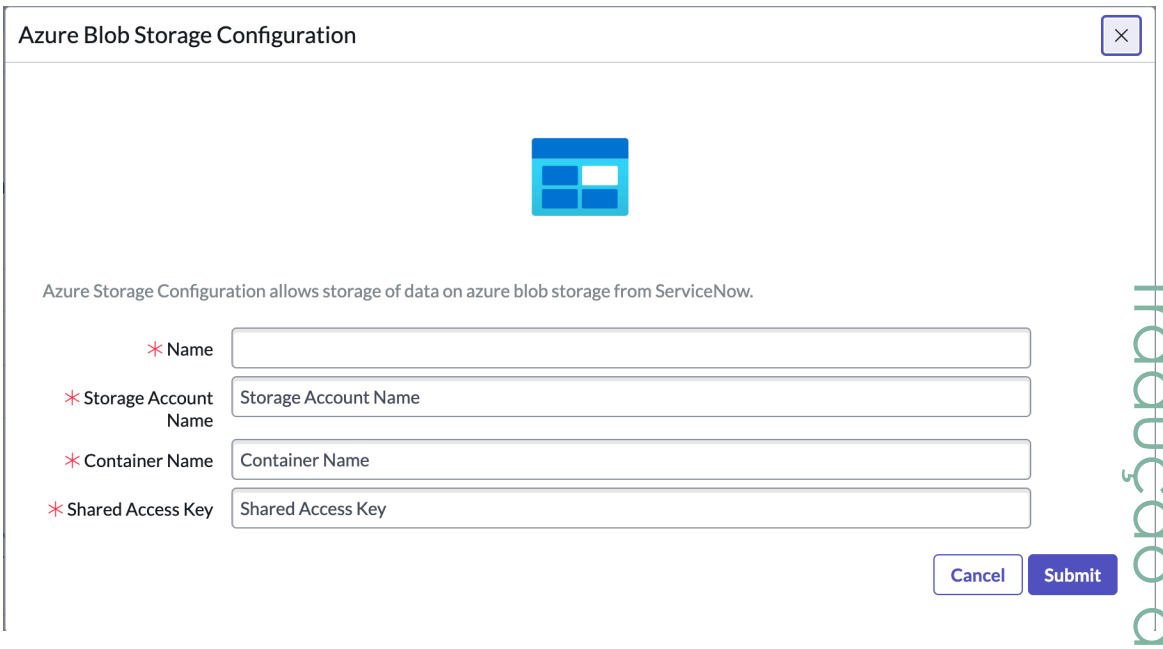
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de validar e enviar a configuração com sucesso, a Microsoft integração de DLP é salva na página Integrações de segurança como um bloco.

4. Atualize a configuração de armazenamento do Azure.

   a. Na página Integrações de segurança, pesquise o bloco **Configuração de armazenamento do Azure**.

   b. No bloco Configuração de armazenamento do Azure, clique em **Atualizar**.



   c. No formulário, preencha os campos.

Formulário de configuração de armazenamento do Azure

Campo	Descrição
Nome	Nome da configuração de armazenamento do Azure.
Nome da conta de armazenamento	Nome da conta de armazenamento criada no portal do Azure
Nome do contêiner	Nome do contêiner criado na conta de armazenamento no portal do Azure.
Chave de acesso compartilhada	Chave de acesso compartilhada para a conta de armazenamento.

   d. Clique em **Enviar**.

   Depois de validar e enviar a configuração com sucesso, a configuração de armazenamento do Azure será salva na página Integrações de segurança como um bloco.

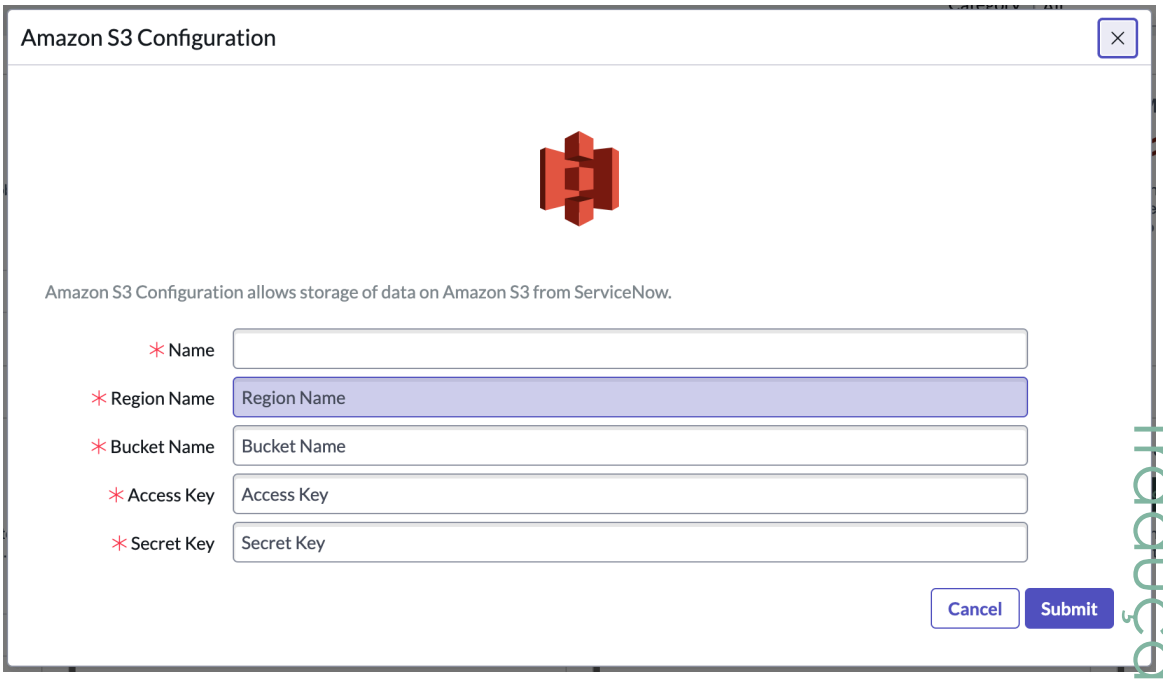
5. Atualize a configuração de armazenamento da AWS.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na página Integrações de segurança, pesquise o bloco **Configuração de armazenamento da AWS**.

b. No bloco Configuração de armazenamento da AWS, clique em **Atualizar**.



c. No formulário, preencha os campos.

Formulário de configuração de armazenamento da AWS

Campo	Descrição
Nome	Nome da configuração de armazenamento da AWS.
Nome da região	Nome da região da conta de armazenamento da AWS.
Nome do Bucket	Nome do bucket criado no portal da AWS.
Chave de acesso	Chave de acesso com acesso de leitura, gravação e exclusão.
Chave Secreta	Chave compartilhada com acesso para leitura, gravação e exclusão

d. Clique em **Enviar**.

Resultados
Depois de validar e enviar a configuração com sucesso, a configuração do AWS S3 será salva na página Integrações de segurança como um bloco.

Criar um novo perfil de incidente para Microsoft integração de DLP

Crie um perfil de incidente em sua instância Now Platform para recuperar os dados do Microsoft Purview e adicionar os dados à tabela de incidentes ServiceNow DLP IR.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_dlir.admin (Criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa
Configure o Now Platform® para recuperar os eventos do escopo Microsoft. Armazene esses eventos na tabela Incidente DLP IR em sua instância ServiceNow®.

Procedimento
1. Navegar até **Integração do Microsoft DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção Nome.

Criar um formulário de perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	A instância Microsoft DLP IR que você configurou para ingerir incidentes. Se você tiver várias configurações de integração, selecione o registro de configuração de integração apropriado para os tipos de incidentes que você planeja ingerir para o perfil.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois que você clica no campo **Concluir** na seção Programação. Quando o perfil está ativo, isso indica que o Now Platform está pesquisando ativamente Microsoft DLP IR eventos com base na configuração definida no perfil.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa é considerado como a prioridade mais alta. Por padrão, o valor é 100.
Descrição	Descrição exclusiva do perfil.

O que Fazer Depois
Para passar para a seção Filtragem, clique em **Continuar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir filtros a serem aplicados na criação do incidente

Defina e defina as condições de filtro para filtrar os eventos de entrada do Microsoft DLP. Controle quais desses eventos devem ser criados como incidentes DLP IR em sua instância ServiceNow.

Antes de Iniciar

Função necessária: sn_dlir.admin (Criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

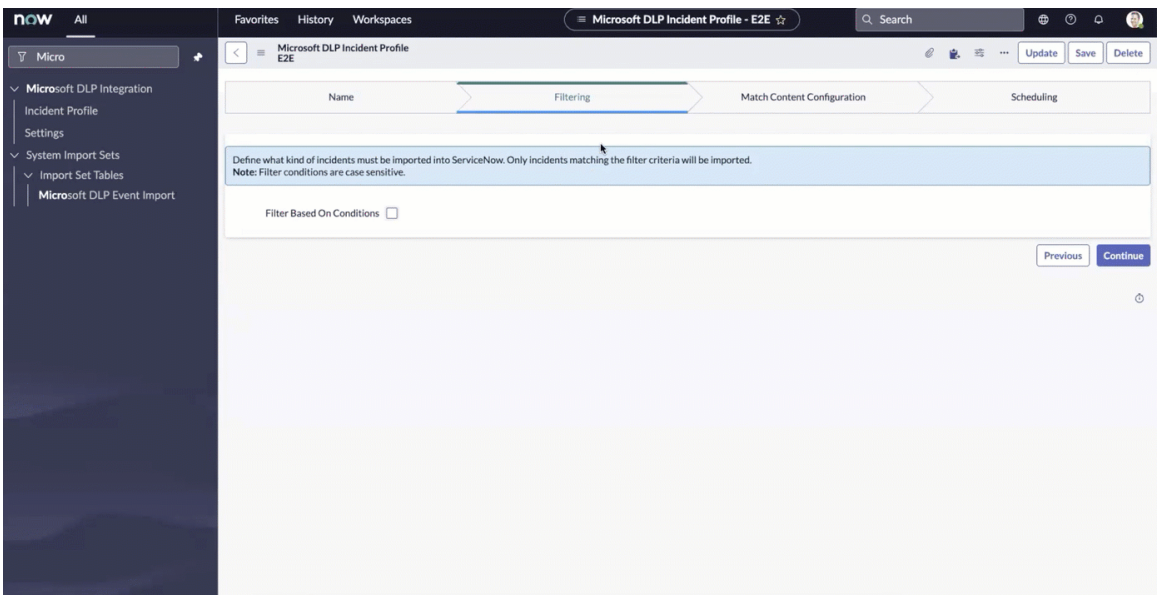
Esse tipo de filtragem ajuda a isolar eventos do Microsoft DLP para limitar o número de DLP IR incidentes que você cria. Se os critérios de filtragem estiverem definidos, somente os eventos que corresponderem às condições serão criados como incidentes da DLP.

Procedimento

1. Selecione a opção **Filtrar com base nas condições**.
2. Usando as listas e os campos do construtor de condições, defina os filtros no campo **Condições do filtro**.

   Defina os critérios que um evento de DLP de entrada Microsoft deve satisfazer para que um incidente de DLP seja criado.

   As opções no primeiro campo nas **Condições do filtro** correspondem aos campos que estão disponíveis no evento do Microsoft DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do evento.



3. Adicione mais condições clicando em **E**ou **OU**.
   - Se **E**for selecionado, todas as condições deverão ser atendidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Clique em **Continuar** e vá para a seção Corresponder configuração de conteúdo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar a correspondência de conteúdo para o incidente

Forneça a configuração para armazenar as informações confidenciais no armazenamento em nuvem externa, como o armazenamento do Azure ou o bucket S3 da AWS, para recuperar esse conteúdo em um carregamento ao acessar o incidente de IR da DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin (Criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Procedimento

1. Na barra de andamento, clique na etapa **Corresponder configuração de conteúdo**.
2. No formulário, preencha os campos.

Corresponder configuração de conteúdo

Campo	Descrição
Armazenar conteúdo de correspondência	Opção para armazenar o conteúdo correspondente no armazenamento em nuvem. **Importante:** Se esta opção não estiver selecionada, o conteúdo de correspondência de política para incidentes da DLP não poderá ser visto no espaço da DLP. A habilitação desta opção garante que o conteúdo de correspondência retornado nos incidentes do DLP seja armazenado no armazenamento em nuvem externa (por exemplo, Azure, AWS). Você também pode recuperar e exibir o conteúdo de correspondência sempre que um incidente da DLP for aberto no espaço. Para obter informações sobre a configuração do Armazenamento em nuvem externa, consulte Instalar e configurar a integração do Microsoft DLP.
Excluir conteúdo de correspondência na exclusão de incidente	Opção para excluir o conteúdo de correspondência do incidente do armazenamento em nuvem externa. Esta opção está visível somente quando o campo **Armazenar conteúdo de correspondência** está selecionado.
Credenciais de acesso à nuvem externas	O armazenamento em nuvem externo em que o conteúdo de correspondência é armazenado. Você pode consultar as credenciais de nuvem externa adicionadas para a configuração de armazenamento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Esta opção está visível somente quando o campo **Armazenar conteúdo de correspondência** está selecionado.

3. Clique em **Continuar** e vá para a seção Programação.

Programar a DLP IR recuperação de incidentes da Microsoft

Defina uma programação para recuperar os dados do incidente e ingerir Microsoft DLP IR incidentes que correspondam aos critérios no perfil. Configure a programação para definir como e quando você extrai incidentes de Microsoft.

Antes de Iniciar

Função necessária: sn_dlir.admin (Criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer uma recuperação única usando a caixa de seleção **Recuperação única**. A data histórica pode ser até os últimos três meses a partir da data atual.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da integração de incidentes Microsoft DLP IR. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Procedimento

1. Defina uma programação para recuperar dados e incluir incidentes que correspondam aos critérios no perfil.
2. No formulário, preencha os campos.

Programação do formulário de incidente da DLP

Campo	Descrição
Adição de incidentes em andamento	A ingestão de incidentes em andamento que a instância Now Platform extrai da Microsoft para novos incidentes. DLP IR incidentes serão criados se incidentes acionados forem encontrados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	A frequência de pesquisa do Microsoft. Este campo é definido automaticamente para 300 minutos.
Definir horário de adição do incidente inicial	Opção para definir uma data e hora para a ingestão inicial. As ingestões subsequentes são baseadas no período de intervalo de pesquisa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Esta opção fica visível somente quando o campo **Ingestão de incidentes contínuos** está selecionado.
Horário de entrada de adição do incidente inicial	Data e hora que você especifica para a ingestão de incidentes. ◦ Se o valor estiver definido, a recuperação de dados da Microsoft será iniciada a partir da data futura adicionada. ◦ Este campo fica visível somente quando **Definir tempo de ingestão inicial** está selecionado.
Horário de adição do incidente inicial	Primeira vez em que os dados são ingeridos. Você pode ver que os valores começam a aparecer quando o tempo de ingestão do incidente inicial é definido.
Horário de adição do próximo incidente (estimado)	O próximo período para uma ingestão de incidente estimada.
Recuperação Única	Opção para habilitar extrações únicas de dados históricos. Se este campo for selecionado, os dados históricos serão extraídos do Microsoft DLP IR de acordo com a data adicionada no campo **Desde a data**.
Desde a Data	Data a partir da qual os dados devem ser recuperados da Microsoft. Este campo pode ser definido para um máximo de 7 dias.

Tradução automática

3. Salve a configuração de perfil criada clicando em **Concluir** na janela pop-up.
4. Ative o perfil.
   a. Abra o perfil criado.
   b. Habilite a opção **Ativo**.
   c. Clique em **Atualizar**.

Resultados

Após a criação e a ativação bem-sucedidas do perfil, os incidentes são recuperados periodicamente de acordo com a configuração definida no perfil e adicionados à tabela de incidentes da DLP.

Definir as configurações de integração do Microsoft DLP IR

Modifique as propriedades do sistema padrão de integração Microsoft DLP IR.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_dlir.admin

Procedimento
1. Navegar até **Integração Microsoft com DLP** > **Configurações**.
2. Modifique as seguintes propriedades conforme necessário.

Configurações de integração do DLP da Microsoft

Campo	Descrição
Tempo limite máximo para chamadas HTTP (sn_pp_dlp.maximum_http_time_out)	Tempo limite máximo para chamadas HTTP (em segundos). ◦ Tipo: inteiro ◦ Valor padrão: 30
Nível de emissão de relatórios dos logs gerados pela integração (sn_pp_dlp.logging.verbosity)	O nível de logs de emissão de relatórios gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ◦ **error** ◦ **aviso** ◦ **informações** ◦ **depurar** ◦ **desativado** Por padrão, o valor é **info**.
Destino do relatório dos logs gerados pela integração (sn_pp_dlp.logging.destination)	O destino dos logs que são gerados pela integração. Você também pode atualizar o valor para as seguintes opções: ◦ **banco de dados** ◦ **arquivo** ◦ **nenhum** Por padrão, o valor é **db**.

3. Clique em **Salvar**.

Resultados
Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Solicitar e-mail de liberação da quarentena

Use este recurso para liberar o e-mail em quarentena do portal de conformidade do Microsoft Purview.

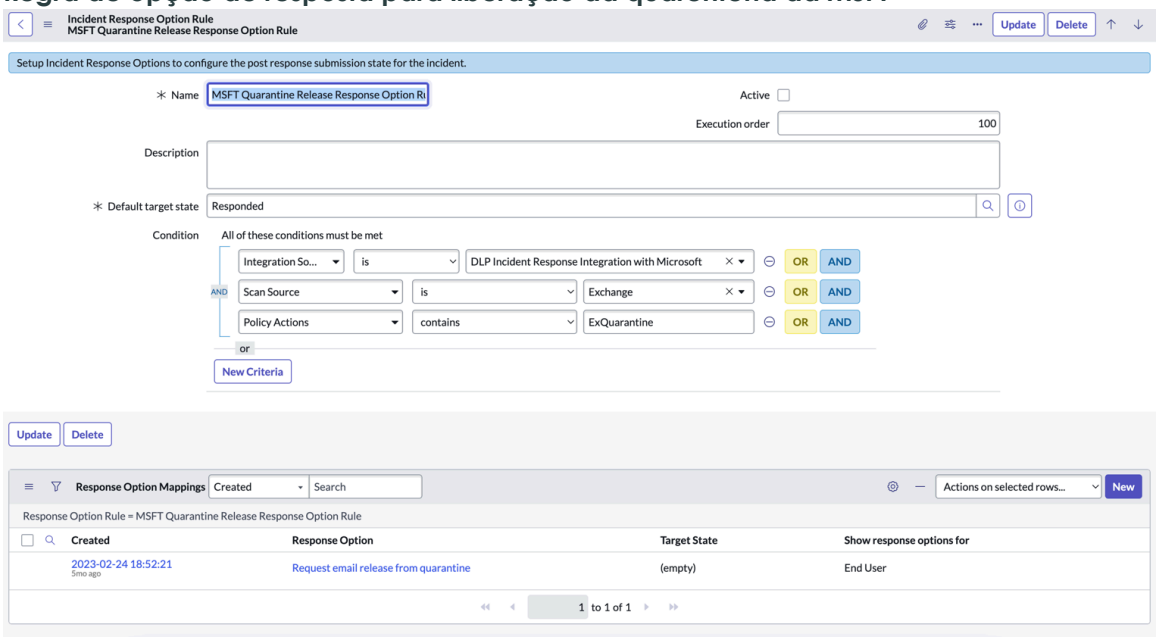
Antes de Iniciar
Por padrão, o sistema de base fornece a opção **Solicitar liberação de e-mail da quarentena** e a **Regra de opção de resposta de liberação da quarentena da MSFT** para liberar o e-mail

Tradução automática

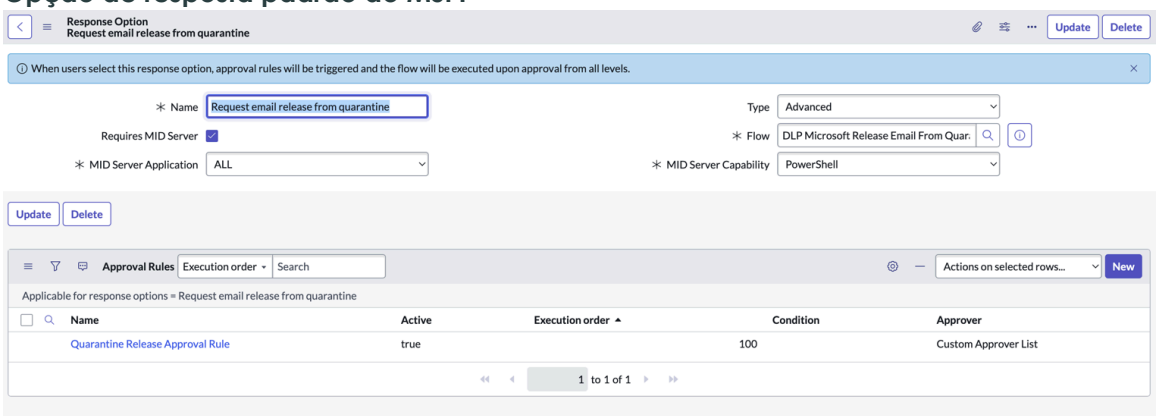
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

da quarentena. Este registro padrão também tem a **Regra de aprovação da liberação da quarentena** configurada com ele para aproveitar a funcionalidade de aprovação para esta ação. Para obter mais informações, consulte Criar regras de opção de resposta a incidentes, Configurar opção de resposta para seus incidentes da DLP e Criar regras de aprovação.

Regra de opção de resposta para liberação da quarentena da MSFT



Opção de resposta padrão do MSFT



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você estiver usando esta opção de resposta, certifique-se de que o MID Server esteja funcionando com o recurso PowerShell. Se um MID Server não estiver funcionando e não tiver o recurso PowerShell, o usuário final não poderá selecionar **Solicitar liberação de e-mail da ação de quarentena** no espaço Usuários da DLP. Para obter mais informações, consulte Criar regras de opção de resposta a incidentes e Configurar opção de resposta para seus incidentes da DLP.

- Se você quiser um MID Server específico da lista, será necessário configurar o app MID e torná-lo visível na lista. Em seguida, pelo menos um MID Server configurado deve estar ativo e em execução nas aplicações MID selecionadas e deve ter o Capacidade do Power Shell.
- Para usar a opção Liberar da quarentena, você precisa de permissões de API. Na página Permissões de API da Microsoft, verifique **Office 365 Exchange Online** > **Câmbio.GerenciarComoApp** está listado e contém os seguintes valores:
  - ▪ **Tipo**: **aplicação**.
  - ▪ **Consentimento do administrador necessário**: **Sim**.
  - ▪ **Status**: o valor incorreto atual é **Não concedido para** <Organization> para a entrada **Office 365 Exchange Online** > **Exchange.ManageAsApp** e altere o valor do status. Para obter mais etapas sobre as permissões de API, consulte Atribuir permissões de API à aplicação no site de documentação da Microsoft.

    Nota: Esta etapa é necessária para se conectar ao Exchange Online usando o princípio de serviço.
- Você também deve precisar da função de **administrador de segurança** no princípio de serviço,
  - Pesquise **funções e administradores do Microsoft Entra ID** no portal do Microsoft Azure, adicione a atribuição ao app registrado (Princípio do serviço) e siga o procedimento explicado na Documentação da Microsoft sobre como atribuir uma função .
- Esta opção se aplica somente a incidentes do Microsoft Exchange que têm a opção **Ação de política** como **ExQuarentena** na exibição do formulário de incidente.

Função necessária: usuário final

O procedimento a seguir explica como enviar esta ação do Espaço do usuário da DLP.

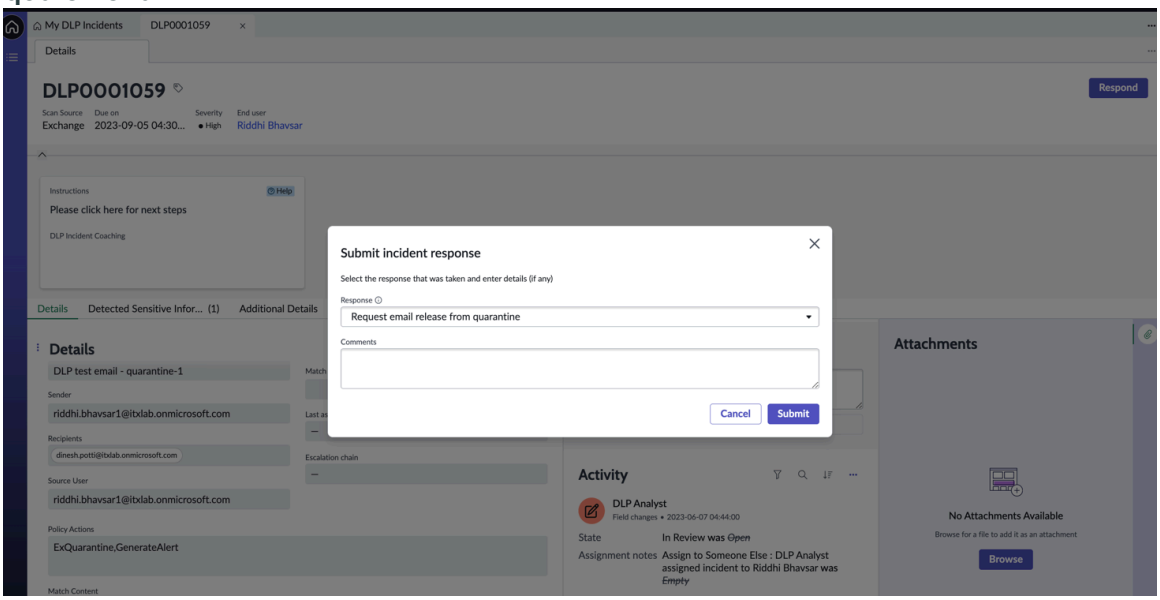
Procedimento

1. Navegar até **DLP** > **Espaço do usuário da DLP**.
2. Abra qualquer incidente do Microsoft Exchange DLP.
   Verifique se a **ação de política** do incidente está definida como ExQuarantine.
3. Clique **em Responder**.
4. Selecione a opção **Solicitar e-mail de liberação da quarentena** na lista suspensa Resposta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enviar resposta do incidente - Solicitar liberação de e-mail da opção de quarentena



5. Clique em **Enviar**.

> **Nota:** Quando uma regra de aprovação for configurada para esta ação, o fluxo de aprovação será acionado primeiro e, depois de receber todas as aprovações, o e-mail de solicitação de liberação da quarentena será acionado e o e-mail será liberado da quarentena. O estado do incidente da DLP será atualizado para **Liberado da quarentena** após a liberação bem-sucedida.

Baixar arquivos para incidentes do DLP do tipo Exchange Online, OneDrive e SharePoint

Baixe arquivos ou e-mail que violem a política DLP no Microsoft Purview. Baixe este arquivo ou envie-o por e-mail para sua máquina local a partir da DLP IR exibição Incidente. Você pode baixar os arquivos para DLP IR incidentes do tipo Origem de verificação Exchange Online, OneDrive e SharePoint.

Antes de Iniciar

Função necessária:

- sn_dlir.admin, sn_dlir.analyst
- Qualquer aprovador válido

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes da DLP** > **Espaço do analista da DLP**.
2. Abra um registro de incidente DLP do tipo Verificar origem Exchange Online, OneDrive ou SharePoint que é ingerido da origem da Microsoft.
3. Clique **em Baixar arquivo**.
   O arquivo ou e-mail que violou a política DLP no lado do Microsoft Purview será baixado para a máquina local do usuário.

> **Nota:** O administrador da DLP pode controlar o acesso da ação **Baixar arquivo** desabilitando a configuração **Deve ser permitido baixar o arquivo violador do incidente relatado** na página Configurações avançadas. Para obter mais informações, consulte Definir configurações avançadas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Separação de domínios em Microsoft integração de DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: básico.

Como o Domain Separation funciona com Microsoft integração de DLP

Siga estas etapas para obter o Domain Separation:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração da DLP Microsoft no domínio apropriado.

Operações de segurança funcionalidade comum

Sempre que qualquer um dos plug-ins das aplicações [Operações de segurança principais (Security Incident Response, Resposta a vulnerabilidades, Inteligência contra ameaçasou Conformidade de configurações) for ativado, o plug-in Security Support Common será ativado. Este plug-in carrega vários módulos que fornecem funcionalidade comum em todas as aplicações Operações de segurança.

Nota: Somente usuários com [sn_sec_cmn.admin] podem exibir e usar o módulo Operações de segurança. Esta função é herdada quando você recebe uma função administrativa em qualquer uma das aplicações Operações de segurança.

Módulos das Operações de segurança

Recurso	Descrição
Referência do Security Operations Integrations, Integrações do Inteligência contra ameaças, Integrações do Resposta a vulnerabilidades	Várias integrações estão incluídas com as aplicações [Operações de segurança (Security Incident Response, Inteligência contra ameaçase Resposta a vulnerabilidades). Esta seção fornece instruções para ativar os plug-ins e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema de base.
Operações de segurança processamento de e-mail	Você pode configurar a integração de informações de sistemas de detecção externos, fornecer granularidade no processamento de registros de operações de segurança, lidar com e-mails incompatíveis e impedir a duplicação de registros usando Processamento de E-mails.
Grupos	• **Grupos de Filtros** Crie e use grupos de filtros para localizar registros de qualquer tabela em sua instância. Por exemplo, você pode criar um grupo de todos os computadores do mesmo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
	fabricante. Você também pode filtrar itens de configuração (ICs) que tenham vulnerabilidades semelhantes ou que se enquadrem em um intervalo de endereços IP de sub-rede específico. • **Escalações** Você pode criar um caminho de escalação para incidentes de segurança em caso de problemas que exigem mais atenção ou experiência. Depois que um grupo de escalação existir, um botão aparecerá em qualquer incidente de segurança nesse grupo.
Marcadores de Segurança	**Marcadores**: as regras de marcador de segurança fornecem filtragem para acesso a marcadores de segurança.
Fluxos de trabalho	• **Exibir Fluxos de Trabalho de Segurança** Você pode exibir os vários fluxos de trabalho incluídos nas aplicações Operações de segurança. Você pode criar fluxos de trabalho a partir de modelos e no Editor de fluxo de trabalho. • **Gatilhos de Fluxo de Trabalho** Operações de segurança Os gatilhos de fluxo de trabalho contêm uma condição em uma tabela. Todos os fluxos de trabalho anexados ao registro do gatilho de fluxo de trabalho são executados quando a condição é atendida.
Utilitários	• **Mapeamento de Dados de Aprimoramento** Mapeamento de Dados de Aprimoramento transforma dados de arquivos XML, JSON ou Propriedades em registros ServiceNow. Operações de segurança fluxos de trabalho usam mapas de dados de aprimoramento e fornecem dados de saída para incidentes de segurança. • **Transformações de Valores de campos** Transforma valores de campo de cliente exclusivos em valores de campo reconhecidos por Operações de segurança análise de e-mail, enriquecimento de dados ou tabelas usando mapas de campo. Oferece suporte a campos de opção, faz referência e alinha

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
	dados externos na terminologia e formato padrão para o novo registro. • **Mapeamento de Campos** As tabelasOperações de segurança podem ser mapeadas de e para outras tabelas, vinculando um incidente de segurança a um caso de atendimento ao cliente ou um problema a outras partes do sistema Operações de segurança. Por exemplo, você pode integrar um plug-in a uma tarefa Security Incident Response. • **Orquestração sob Demanda** Durante a Security Incident Response análise, um analista de segurança pode executar uma tarefa que é orientada por um fluxo de trabalho de incidente de segurança. Por exemplo, execute um despejo de processo em um IC específico. Isso pode ser realizado com a orquestração sob demanda. • **Grupos de sistemas operacionais** N/D. • **Registro da aplicação SecOps** N/D.
CMDB	**Regras de**identificador de IC: identificadores de IC são regras usadas para pesquisar um item de configuração (IC) no CMDB que contém informações correspondentes de uma integração de terceiros. Essas regras definem os campos que contêm dados correspondentes e a ordem de precedência pela qual eles são avaliados. O menor valor de **Ordem** é avaliado primeiro.

Tradução automática

Criar e definir grupos de filtros nas Operações de segurança

Crie e use grupos de filtros para localizar registros de qualquer tabela em sua instância. Por exemplo, você pode criar um grupo de todos os computadores do mesmo fabricante. Você também pode filtrar itens de configuração (ICs) que tenham vulnerabilidades semelhantes ou que se enquadrem em um intervalo de endereços IP de sub-rede específico.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Os grupos de filtros podem conter registros atualizados dinamicamente, uma série de registros estáticos que não são filtrados usando condições ou uma combinação de registros estáticos e atualizados dinamicamente. Alguns grupos de filtros estão incluídos no sistema de base, por exemplo, exclusões de IC.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Grupos** > **Grupos de Filtros**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome do grupo de filtros.
Ativo	Caixa para ativar o grupo.
Descrição	Descrição do grupo de filtros.
Endereço IP da Rede	O endereço IP da rede que contém os endereços IP dos ICs que você deseja adicionar ao grupo. Este campo aparece somente se você selecionou Item de configuração [cmdb_ci] ou uma tabela que estende o item de configuração no campo **Tabela**.
Máscara de sub-rede	A sub-rede que contém os endereços IP dos ICs que você deseja adicionar ao grupo,por exemplo, 255.255.255.0. Este campo aparece somente se você selecionou Item de configuração [cmdb_ci] ou uma tabela que estende o item de configuração no campo **Tabela**.
Tabela	A tabela a ser filtrada.
Condição	Use o Construtor de condições para definir os critérios a serem filtrados.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   Uma guia **Condições avançadas** é exibida.

   Mais guias aparecem dependendo do tipo de tabela que você especificou no campo **Tabela**, da seguinte forma:

Tabela	Guias exibidas
Item de configuração [cmdb_ci] ou uma tabela que estende a tabela de itens de configuração	**ICs adicionados manualmente** e **ICs correspondentes**
Tarefa [task] ou uma tabela que estende a tabela de tarefas	**Tarefas adicionadas manualmente** e **tarefas correspondentes**
Uma tabela não relacionada a um IC ou tarefa	**Registro Adicionado Manualmente**

5. Para definir mais condições para o seu grupo de filtros:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique **em Condições avançadas**.

b. Insira uma nova linha na lista incorporada **Condições do grupo de filtros adicionais** para selecionar outros grupos de filtros pré-criados que você deseja combinar com o grupo de filtros que está sendo atualizado.
Se você quiser que o grupo de filtros selecionado filtre registros com base em um campo de referência, um campo mapeado será selecionado automaticamente quando o registro atual for salvo.

> **Nota:** O valor do **campo Mapeado** não pode ser editado na lista incorporada **Condições do grupo de filtros adicionais**. Para mudar o campo, clique no ícone de informações para abrir o registro.

c. Clique em **Atualizar**.

6. Para adicionar manualmente mais ICs ou tarefas ao grupo de filtros:
   a. Clique na guia **ICs adicionadosmanualmente ou Tarefas adicionadas manualmente**.
   b. Clique em **Editar**.
   c. Selecione os ICs ou tarefas que você deseja adicionar.
   d. Clique em **Salvar**.
7. Para exibir os ICs ou tarefas que correspondem aos seus critérios de seleção:
   a. Clique na guia **ICs** correspondentes ou **Tarefas correspondentes**.
   b. Se você alterou os critérios, atualize a lista clicando com o botão direito do mouse no cabeçalho do formulário e selecionando **Atualizar lista**.

Transformação de dados compartilhados

Os plug-ins Security Incident Response, Resposta a vulnerabilidadese Inteligência contra ameaças compartilham recursos comuns para dados de relacionamento e regras de duplicação, usados para importar informações externas e internas para Operações de segurança.

Análise de E-mails, Regras de Duplicaçãoe Mapeamento de Campos usam dados de entrada (um e-mail, arquivo JSON ou XML ou um registro) e transformam esses dados no formato correto para criar um novo registro. Cada um desses recursos extrai dados de sua própria maneira, mas eles são transformados no novo registro usando muitos dos mesmos processos.

Dados de relacionamento

Ao adicionar informações a uma lista relacionada (como um observável associado em um incidente de segurança), você pode criar um registro de relacionamento que consiste em uma tabela m2m. Às vezes, há dados adicionais nesse registro de relacionamento a serem definidos. Por exemplo, um observável sendo um IP de origem (em oposição a um IP de destino). Essas informações vão para o campo **Dados de relacionamento** no formulário de **transformação** de campo usado pela **Análise de e-mail** ou para uma lista relacionada **Campos de mapeamento** de **campo no formulário de mapeamento** de campo.

O campo **Dados de relacionamento** geralmente está vazio. É mais comumente usado para endereços IP em observáveis na **Análise de e-mail**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode transformar dados de qualquer registro ServiceNow em qualquer outro registro ServiceNow usando **Campos de mapeamento** de campo no recurso **Mapeamento** de campo. Por exemplo, para transformar dados de um incidente em um incidente de segurança ou um incidente de segurança em um PRB.

Regras de duplicação das Operações de segurança

Use Regras de Duplicação para lidar com registros duplicados de segurança, vulnerabilidade, IoCs e assim por diante.

As regras de duplicação têm duas finalidades. Eles evitam que muitos registros duplicados sejam criados e, quando uma duplicata é detectada, eles especificam quais campos no registro são atualizados. Somente duplicatas ativas são procuradas. Se o registro não estiver ativo, por exemplo, se o incidente for encerrado, qualquer novo problema idêntico se tornará um novo incidente.

Regras de duplicação são usadas por **Análise de e-mail**, Mapeamento de **campo**e **Mapeamento de dados de aprimoramento**.

Informações relacionadas

- Criar analisadores de e-mail em Operações de segurança
- Mapear tabelas para tabelas com mapeamento de campo das Operações de segurança

Criar regras de duplicação no Operações de segurança

Você pode usar Regras de Duplicação para identificar novos e-mails, dados de aprimoramento ou mapas de campo com registros duplicados ativos e processá-los adequadamente.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Regras de Duplicação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado:

Regra de duplicação

Campo	Descrição
Nome	O nome da regra de duplicação.
Tabela	Tabela em que os registros são criados e usados para determinar duplicação.
Campos de identificação	Selecione um conjunto de campos que indicam um incidente de segurança duplicado, observável, vulnerabilidade e assim por diante, quando os valores nesses campos forem idênticos.
Ação duplicada	Controla como lidar com e-mails duplicados. As opções são: Criar como secundário Cria um registro como secundário do original. O campo que vincula o secundário ao primário é o campo **Primário**. Não criar nem atualizar registros

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	(padrão) Não faz nada. Ignora duplicatas. Atualizar registro duplicado Atualiza os campos no registro existente conforme especificado em **Ações de duplicação.** **Nota:** Se você escolher **Atualizar registro duplicado**, a lista relacionada **Ações** de duplicação será exibida.
Ativo	Marque esta caixa de seleção para ativar a regra.
Descrição	Descreve a finalidade e a aplicação desta regra de duplicação; quando ela deve ser usada, por exemplo, uma regra projetada para observável baseado em IP ou incidentes de segurança do firewall.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar** ou clique em **Atualizar**.
5. Para definir ações de duplicação, se você escolheu **Atualizar registro duplicado**, clique em **Novo** para criar ações de duplicação para cada campo que deseja atualizar no incidente.
6. Preencha ou edite os campos no formulário para descrever como atualizar o campo:

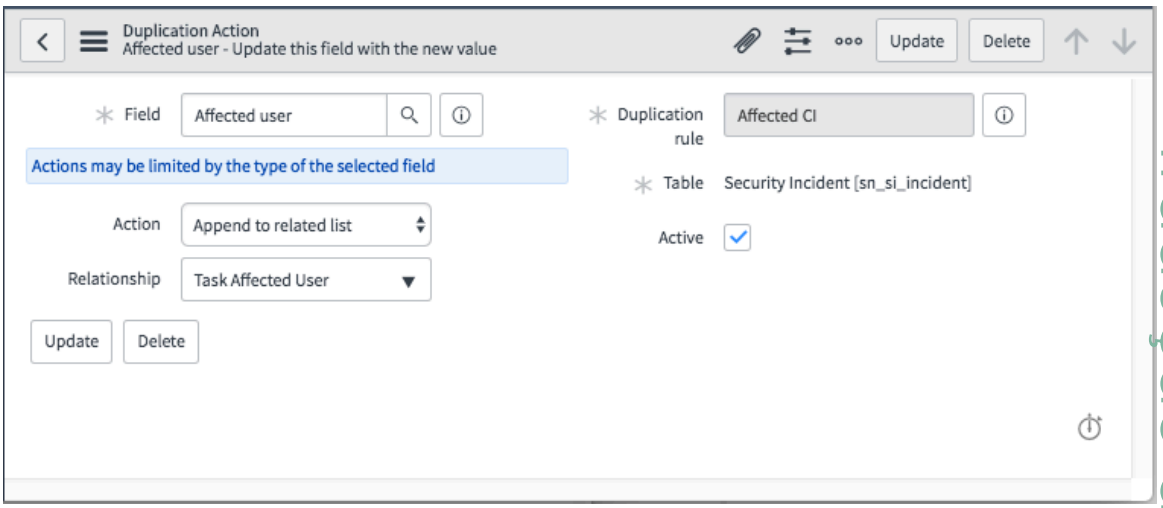
Ações de duplicação

Campo	Descrição
Campo	O nome do campo a ser usado para a ação de duplicação.
Ação	As ações compatíveis variam de acordo com o tipo de campo. As opções são: Atualizar este campo com o novo valor Substitui o valor anterior no registro existente por este valor. Anexar o novo valor a uma lista separada por vírgulas, se exclusivo Trata o valor como uma entrada em uma lista separada por vírgulas e adiciona os novos dados (se houver) como uma nova entrada nessa lista. Se os dados já estiverem na lista, eles não serão adicionados duas vezes. Anexar o novo valor a este campo Anexa o novo valor ao final do texto existente no campo. Adicionar um a um campo de contador Adiciona um ao campo numérico. Definir o campo como hoje Define o campo para a data e hora atuais. Anexar à lista relacionada Adiciona o registro relacionado com este valor à lista relacionada do registro atual. Aparece quando há uma tabela de muitos para muitos, com uma coluna do mesmo tipo, vinculada à tabela que está sendo atualizada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

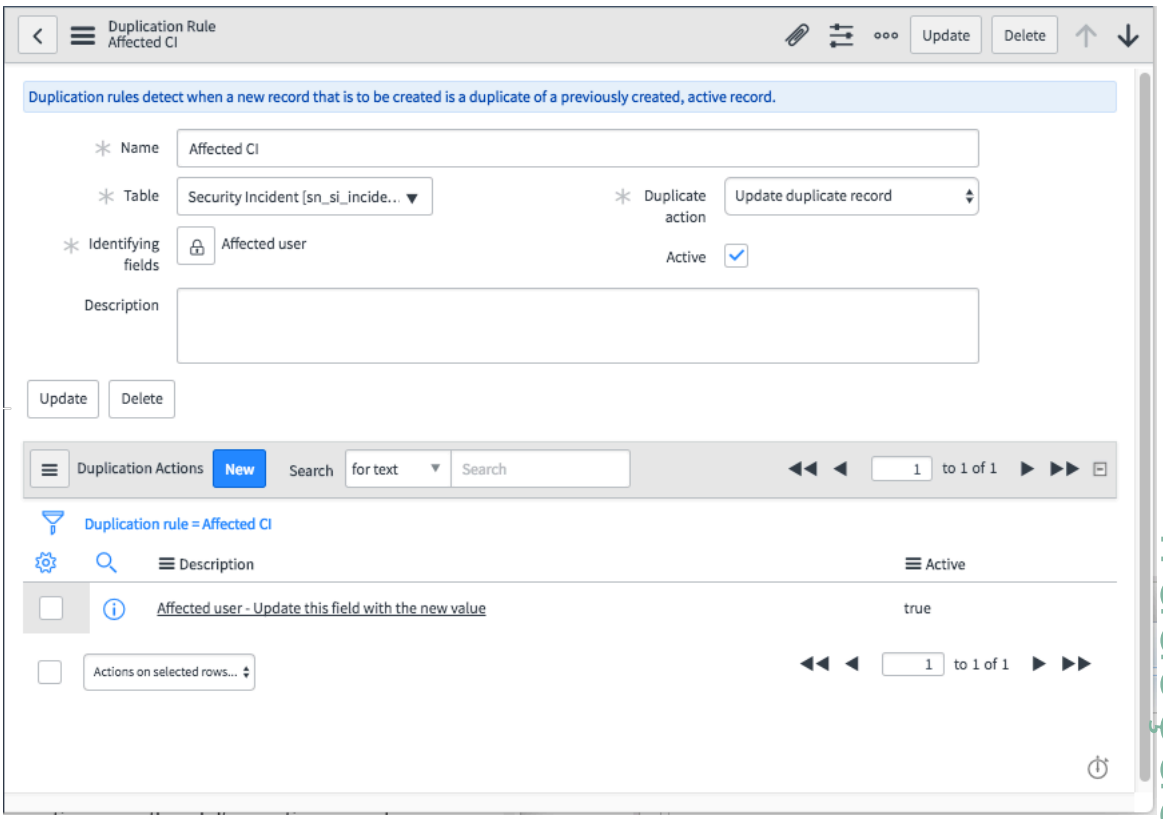
Campo	Descrição
	Por exemplo, **IC** afetado ou **Usuário afetado**.
Relacionamento	[Opcional] Este campo aparece somente quando a ação **Anexar à lista relacionada** é escolhida. É o nome da lista relacionada que você deseja associar a esta regra.
Regra de duplicação	Regra da qual esta ação faz parte.
Tabela	Tabela em que os registros são criados. Exibe somente como informações.
Ativo	Marque esta caixa de seleção para ativar a ação.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.



Operações de segurança processamento de e-mail

Você pode configurar a integração de informações de sistemas de detecção externos, fornecer granularidade no processamento de registros de operações de segurança, lidar com e-mails incompatíveis e impedir a duplicação de registros usando Processamento de E-mails.

Processamento de E-mails consiste nestes recursos:

Recurso	Descrição
Análise de E-mails	Gere novos registros Operações de segurança a partir de e-mails do sistema externo.
Regras de Duplicação	Identifica novos e-mails com incidentes conhecidos e os processa adequadamente.
Propriedades	Especifica contas usadas como entrada em Análise de E-mails para segurança, vulnerabilidade e IoCs. Fornece granularidade no processamento de registros Operações de segurança.
E-mails Incompatíveis	Lista os e-mails que não correspondem a nenhum registro Operações de segurança.

Operações de segurança propriedades de e-mail

E-mail Propriedades especifica quais caixas de entrada são usadas como entrada em Análise de E-mails para importar informações de sistemas de detecção externos para criar registros de segurança, vulnerabilidade e IoCs. Você pode configurar uma conta geral

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para todos os sistemas de detecção externos usarem ou contas de e-mail individuais para Security Incident Response, Inteligência contra ameaçasou Resposta a vulnerabilidades.

Criar Operações de segurança propriedades de e-mail

Você pode especificar endereços de e-mail para relatórios e controlar comportamentos automáticos de e-mail usando e-mail Propriedades.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin
Configure ferramentas de detecção externas para enviar e-mails para sua caixa de entrada de análise de e-mail.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Processamento de E-mails** > **Propriedades**.
2. Insira as caixas de correio dos destinatários conforme apropriado:
   Estes são endereços de e-mail de entrada a serem processados pela **Análise de e-mail**, em vez de **Ações de entrada**.

Propriedades de análise de e-mail

Campo	Descrição
Caixa de entrada para Operações de segurança ferramentas	Endereço de e-mail completo para Operações de segurança. Por exemplo, secops_support@yourcompany.com.
Caixa de entrada para ferramentas de Incidente de segurança	Endereço de e-mail completo para Security Incident Response. Por exemplo, sir_support@your.company.com.
Caixa de entrada para Resposta a vulnerabilidades ferramentas	Endereço de e-mail completo para Resposta a vulnerabilidades. Por exemplo, vuln_resp@yourcompany.com.
Caixa de entrada para Inteligência contra ameaças ferramentas	Endereço de e-mail completo para Inteligência contra ameaças. Por exemplo, Threat_intel@yourcompany.com.

3. Clique em **Salvar**.

Operações de segurança análise de e-mail

Gere novos registros Operações de segurança de sistemas de detecção externos usando Análise de E-mails. Este recurso fornece um método para integrar informações de ferramentas externas, como detecção de malware, detecção de vulnerabilidades, firewalls, inteligência contra ameaças e muito mais.

Como os e-mails são analisados

Qualquer sistema que pode enviar um e-mail pode criar Operações de segurança registros, por exemplo, incidentes de segurança, solicitações, itens vulneráveis, vulnerabilidades, observáveis de incidentes de segurança, métodos de ataque e muito mais.

Todos os Operações de segurança plug-ins (Security Incident Response, Inteligência contra ameaçase Resposta a vulnerabilidades) têm uma propriedade (**email_to**) que define o endereço de e-mail para o qual as integrações externas devem enviar e-mails, a serem

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

analisados pelos analisadores de e-mail. Confira **Processamento de E-mails** > **Propriedades** para obter mais informações.

O e-mail enviado para qualquer um dos Operações de segurança endereços de e-mail é armazenado em uma tabela de eventos de e-mail. Esses e-mails são processados para determinar se correspondem a algum analisador de e-mail.

Os e-mails que têm uma correspondência são sinalizados e as regras de transformação e duplicação criam ou atualizam um registro Operações de segurança. O e-mail está vinculado a esse registro e sinalizado como `correspondente`.

E-mails que não correspondem são listados em E-mails Incompatíveis como um registro Operações de segurança. Eles podem ser revisados para ajudar a criar analisadores de e-mail para lidar com esses e-mails. Uma ação de reprocessamento permite que você execute novamente o e-mail incompatível por meio dos analisadores. O log de e-mail original está vinculado a esse registro.

As regras de duplicação para a transformação de e-mail gerenciam vários e-mails relacionados ao mesmo problema. Essas regras definem o que torna um registro duplicado e podem impedir que registros duplicados sejam criados. Quando uma duplicata é detectada, a regra especifica qual ação executar: nenhuma ação (não criar um novo registro), criar o novo registro como um registro secundário do registro existente ou atualizar o registro existente. Ao atualizar, a regra de duplicação especifica quais campos no registro existente são atualizados.

Nota: Um Operações de segurança analisador de e-mail funciona em conjunto com as ações de entrada da plataforma e não as substitui. Ele não oferece suporte à definição de valores em campos indiretos, por exemplo, entradas **sys_journal_field**.

Por padrão, os eventos de e-mail são excluídos após 30 dias.

Vários registros

Sistemas de detecção externos (detectores de malware, vulnerabilidade e assim por diante) podem enviar e-mails que relatam vários itens de uma só vez. O analisador de e-mail oferece suporte a separadores no e-mail.

Por exemplo, um detector de malware pode enviar a você um relatório por e-mail sobre todos os sistemas em sua rede infectados por um malware específico, com informações sobre o malware primeiro, seguido por uma lista dos sistemas afetados.

Exemplo de e-mail mal-intencionado

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==============================
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==============================
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==============================
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Neste exemplo, quando o **Separador de Registros** é definido em sua **Transformação de E-mail**como **==========**, ele divide o e-mail em quatro seções que são avaliadas separadamente. Isso cria um incidente de segurança para cada um dos três sistemas afetados.

Nota: A seção de cabeçalho é detectada, mas não tem nenhum sistema afetado, portanto, ela é usada em todos os três registros e não cria um quarto registro.

As transformações de campo extraem dados de cada seção. Se algo no cabeçalho ou rodapé do e-mail se aplicar a todos os registros, como Hash de Malware, Nome de Malware e Tipo neste exemplo, a transformação de campo para eles deverá definir **Pesquisar valor** como um valor que pesquisa no corpo do e-mail **Em o início de uma linha no corpo do e-mail** ou **em qualquer lugar no corpo do e-mail**.

As transformações de campodevem ser definidas para pesquisar **no início de uma linha na seção de registro ou na seçãode** dados definidos em cada seção, como sistema, endereço IP ou status. As opções de seção de registro só estão disponíveis quando há um separador de registro definido na transformação de e-mail.

Ao analisar um e-mail com um separador definido, os registros são criados somente para seções com pelo menos uma parte de dados específicos da seção.

Neste exemplo, três registros são criados, embora haja quatro seções definidas. A primeira seção é um cabeçalho e não tem nada específico para apenas um sistema. Se algum dos campos na primeira seção fosse preenchido (Sistema, IP ou Status), um registro também seria criado para essa seção.

Informações relacionadas

Criar analisadores de e-mail em Operações de segurança

Operações de segurança mapeamento de dados de aprimoramento

Operações de segurança mapeamento de campo

Criar analisadores de e-mail em Operações de segurança

Análise de E-mails cria Operações de segurança registros do seu e-mail para segurança, vulnerabilidade e observáveis para agilizar a resposta e a correção de ameaças.

Antes de Iniciar

- Configure ferramentas de detecção externas para enviar e-mails para um endereço de e-mail central.
- Defina o endereço de e-mail em Operações de segurança Propriedades. Para obter mais informações, consulte Criar Operações de segurança propriedades de e-mail.
- Atribua uma conta de usuário a este endereço de e-mail e forneça a esse usuário controles de segurança de acesso para criar e atualizar os registros de eventos de e-mail.
- Tenha uma cópia do e-mail relevante da sua ferramenta de detecção externa à sua frente.
- Decida que tipo de registro você deseja criar, um incidente de segurança, registro de vulnerabilidade, tarefa e assim por diante. Esta opção determina a tabela selecionada.

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Análise de E-mails**.
2. Clique em **Nova**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme o apropriado.

   Nota: Se mais de um campo for especificado, todos os campos deverão corresponder ao e-mail para criar um registro.

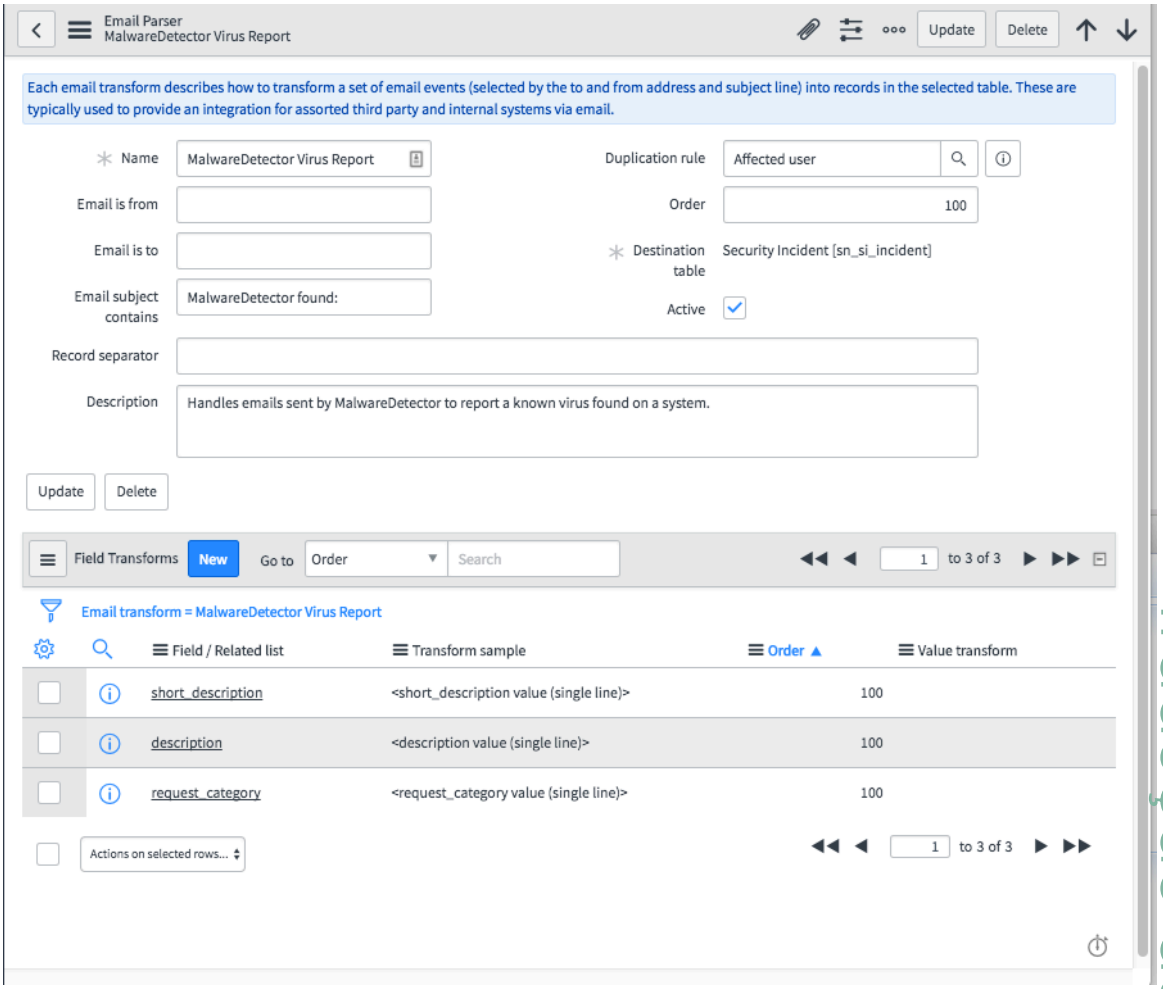
   Analisador de e-mail

Campo	Descrição
Nome	O nome do analisador de e-mail.
O e-mail é de	Se preenchido, somente e-mails deste endereço serão transformados por este analisador de e-mail.
O e-mail é para	Se preenchido, somente e-mails deste endereço serão transformados por este analisador de e-mail.
O assunto do e-mail contém	Se preenchido, somente os e-mails em que o assunto contém esta frase serão transformados por este analisador de e-mail.
Regra de duplicação	Controla como lidar com e-mails duplicados para qualquer e-mail que esta transformação manipule. Para obter mais informações, consulte Transformação de dados compartilhados.
Ordem	Em que ordem considerar as transformações. A primeira transformação de e-mail correspondente é usada. Normalmente, você deseja configurar os analisadores de e-mail mais específicos nos números mais baixos, com algum fallback. Forneça aos analisadores de e-mail catchall números de **pedido** mais altos para que eles sejam executados se nada mais corresponder. O padrão é 100. Quando tudo corresponde, o analisador de e-mail mais específico (corresponde **de**, **a**e **assunto**) é usado.
Tabela de destino	A tabela em que você deseja criar registros.
Ativo	Se esta transformação está ativa, em uso ou não. Se desmarcado, nenhum e-mail será transformado com este código.
Separador de registros	Quando os e-mails tratados por este analisador de e-mail criam vários registros, este campo contém o separador entre as informações desses registros. Para obter mais informações, consulte Operações de segurança análise de e-mail.
Descrição	Descrição deste analisador de e-mail, com qual ferramenta ele funciona, a finalidade e assim por diante.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar**.
   Uma guia **Transformações de campo** é exibida. Esta guia mostra como os campos individuais na tabela de destino são definidos com base no conteúdo do e-mail.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para adicionar **transformações de campo**, execute estas etapas.
   a. Na guia **Transformações de campo**, clique em **Novo**.
   b. Preencha os campos no formulário, conforme o apropriado.

Opção	Descrição
Campo	**Descrição**
Armazenar valor em um campo ou uma lista relacionada	Selecione onde encontrar o valor. As opções incluem: ◦ Armazene o valor em um campo no novo registro ◦ Vincular a este valor a uma lista relacionada ◦ Vincular a este valor, criando um novo registro se um registro correspondente não existir **Nota:** Se a tabela de destino não tiver listas relacionadas, este campo não será exibido.
Campo	Selecione o campo a ser preenchido com este valor.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Para campos de opção, as correspondências são feitas com as escolhas existentes usando o rótulo ou valor de escolha subjacente. Se nenhuma correspondência for encontrada, o campo será definido, mas nenhuma nova entrada será adicionada à lista de seleção. Para obter mais informações, consulte Listas de seleção . Para campos de referência, uma entrada é definida somente quando um valor correspondente ao nome de exibição do registro ou um `sys_id` válido é encontrado. Para obter mais informações, consulte Campos de referência .
Lista relacionada	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se não existir um registro correspondente**, este campo especificará a lista relacionada à qual informações serão adicionadas.
Campo de valor	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se não existir um registro correspondente**, este campo especifica o campo na tabela exibida no relacionado lista. É usado para pesquisar e localizar um registro existente. Por exemplo, se sua lista relacionada for **ICs afetados**, este campo poderá conter **Nome** ou Nome de **domínio totalmente qualificado**ou qualquer outro campo no registro de IC a ser usado para pesquisar o IC adicionado à lista de **ICs afetados**.
Dados de relacionamento	Quando **Armazenar valor em um campo ou lista relacionada** é definido como **Vincular a este valor em uma lista relacionada**, um registro é criado para vincular esse registro (como um incidente de segurança) ao valor (um IC, um Observável e assim por diante.). Este campo especifica todas as

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	informações adicionais (pares de campo e valor) que devem ser adicionadas ao registro de vinculação. Por exemplo, ao adicionar um Observável para um IP de origem, especifique que este IP é o IP de origem, em vez do IP de destino. Para vários valores, use um separador ^, por exemplo, type= Source IP^Active=true.
Novos dados de registro	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor, criar um novo registro se não existir um registro correspondente**, se nenhum registro relacionado correspondente ao valor analisado for encontrado, um registro será criado. Este campo especifica os dados estáticos a serem adicionados a esse registro. Para **ICs afetados**, se nenhum IC correspondente for encontrado, um registro de IC será criado). Quando isso acontece, o valor encontrado no e-mail é definido como o campo **Valor** no registro de IC. Você pode definir dados adicionais - uma anotação indicando o motivo pelo qual o IC foi criado, algumas informações sobre com que tipo de ICs você está trabalhando e assim por diante. Uma amostra seria: description=Created by Malware Scanner email parser^type=autodetect.
Pesquisar valor	Selecione o local no e-mail para pesquisar. As opções incluem: ◦ **No início de uma linha do corpo do e-mail** ◦ **Em qualquer parte do corpo do e-mail** ◦ **Na linha de assunto do e-mail** ◦ **Sempre o valor estático** Quando você define um **Separador de registros**, mais opções (**Em qualquer lugar na seção de registro** e **No início de uma linha na seção de registro)** permitem que você pesquise somente na seção atual em vez de em todo o corpo do e-mail (consulte Operações de segurança análise de e-mail para obter mais informações informações. As informações que estão em um cabeçalho ou rodapé, aplicando-se a todos os registros, são pesquisadas em todo o corpo do e-mail. As informações que diferem en-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	tre os registros são pesquisadas somente na seção.
Separador de valores	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se não existir um registro correspondente**, este campo especificará o separador a ser usado para listas de itens. por exemplo, uma vírgula ou ponto-e-vírgula quando os dados do e-mail são uma lista de endereços IP.
Prefixo de valor	O texto que sempre precede o valor colocado neste campo a ser extraído.
Final do valor	Selecione o que indica o fim do valor. As opções incluem: **Fim da linha**, **Fim do e-mail** (traz todo o texto restante no e-mail) ou **Até** (para quando encontra o texto especificado) ou **Até** (para quando encontra o texto especificado).
Sufixo de valor	Quando o **Fim do valor** é definido como **Até**, este campo especifica qual texto sempre segue o valor colocado neste campo. Por exemplo, procurar um valor que vem depois de "O computador afetado está" e antes de "". analisará "AB123" de "O vírus dementes foi encontrado. O computador afetado é o AB123. O tempo estimado de infecção foi 15h45" em um e-mail.
Transformação de valor	Escolha a entrada de transformação de campo a ser aplicada. Converte o valor encontrado no e-mail em um valor diferente, usado para preencher campos de opção, referência ocasional e outros campos.
Ordem	A ordem na qual o campo transforma a execução, da mais baixa para a mais alta. Uma transformação de campo com uma entrada de ordem de 100 é tentada primeiro. Somente se essa transformação de campo não conseguir encontrar um valor, uma transformação de campo com uma ordem superior (200) no mesmo campo será executada.
Transformação de e-mail	A transformação à qual esta transformação de campo pertence.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Tabela de destino	Tabela de destino da transformação de e-mail. Ele contém dados informativos da transformação de e-mail.
Ativo	O padrão é verificado. Quando marcada, a transformação do campo está ativada. Desmarque esta caixa para desativar a transformação do campo.

a. Clique em **Enviar**.
O novo registro é usado para analisar as informações no e-mail em um novo registro.

Informações relacionadas

Criar regras de duplicação no Operações de segurança

Criar transformações de valor de campo Operações de segurança

Definir Resposta a vulnerabilidades notificações por e-mail

Editar registros de e-mail no Operações de segurança

Adicione ou crie transformações em seus registros de eventos de e-mail existentes.

Antes de Iniciar

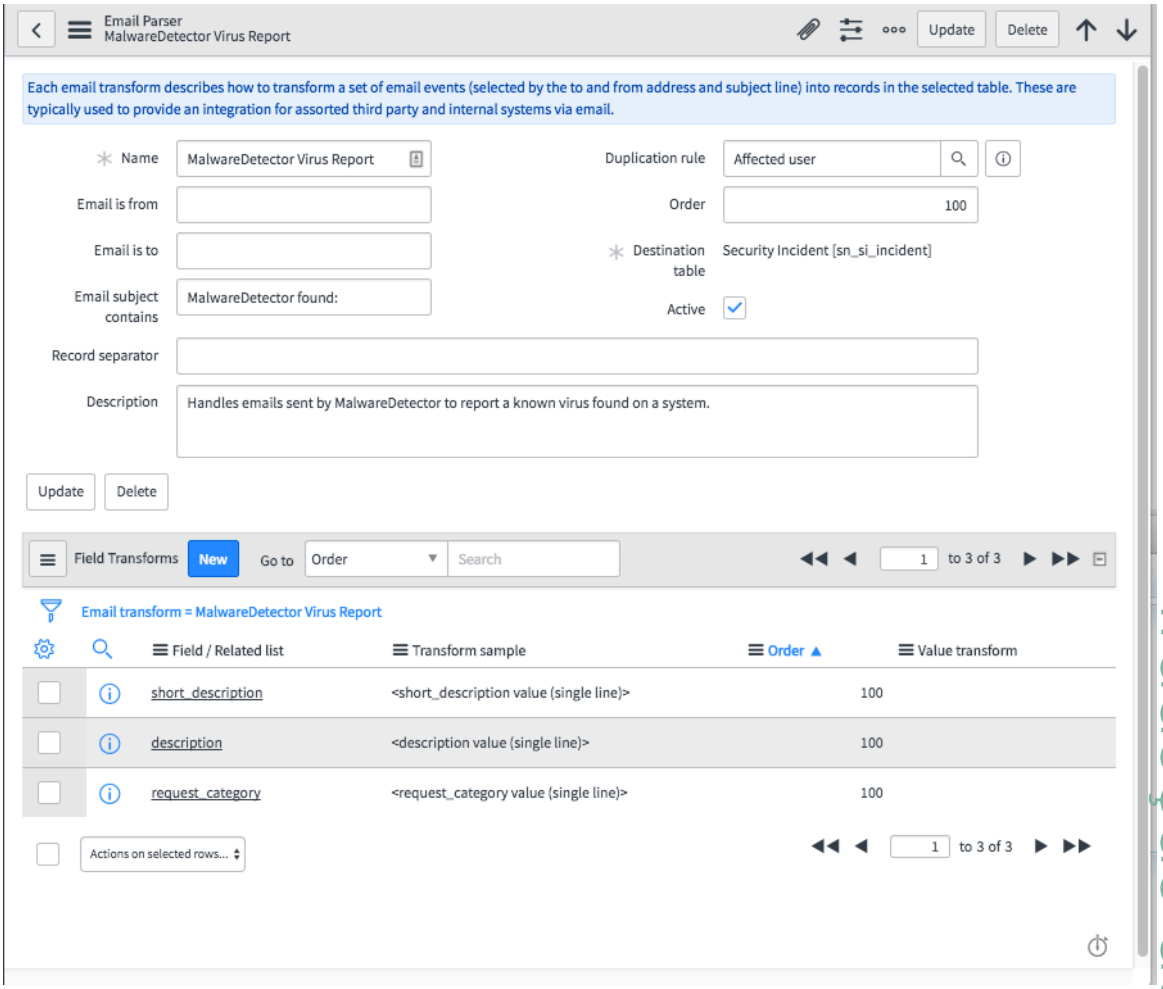
Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Análise de E-mails**.
2. Clique no analisador de e-mail para editar.
   Se o registro for somente leitura, clique no link aqui na mensagem do cabeçalho.
   Você será direcionado para o formulário editável da transformação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Edite os campos conforme apropriado.

4. Para editar **Transformações de campo**, clique no campo e altere conforme apropriado.

5. Clique em **Atualizar.**

Eventos de e-mail Operações de segurança incompatíveis

Os eventos de e-mail que não correspondem a um analisador de e-mail têm o sinalizador "correspondido" não definido. Você pode exibir esses registros de eventos de e-mail na lista E-mails Incompatíveis, para revelar sistemas de detecção externos cujos e-mails ainda não foram analisados.

Ao criar analisadores de e-mail, você pode tentar reprocessar o evento de e-mail (do formulário ou da lista) para validar um novo analisador de e-mail.

Exibir e reprocessar e-mails incompatíveis de Operações de segurança

Você pode revisar E-mails Incompatíveis para filtros descontinuados ou como candidatos a um novo filtro para manter ou melhorar a taxa na qual você detecta ameaças de e-mail.

Antes de Iniciar
Função necessária: sn_sec_cmn.read

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **E-mails Incompatíveis**.
   Se algum e-mail incompatível for encontrado, ele será listado.
2. Os campos do formulário são os seguintes:

Eventos de e-mail de segurança

Campo	Descrição
De	Endereço de e-mail do remetente.
Para	Endereço de e-mail dos destinatários.
Assunto	Linha de assunto no e-mail.
Corpo	Conteúdo do corpo do e-mail.
Correspondido	Indica se este evento de e-mail foi correspondido.

3. Para reprocessar este e-mail, crie um registro de e-mail ou edite um registro de e-mail existente para corresponder às informações neste e-mail.
   Consulte Criar analisadores de e-mail em Operações de segurança.
4. Navegar de volta para **Operações de segurança** > **E-mails Incompatíveis**.
5. Clique em **Reprocessar evento de e-mail** para tentar processar este e-mail.
   Ele retorna você para a lista principal E-mails Incompatíveis. Se o novo registro de e-mail corresponder, o evento de e-mail não estará mais na lista. Uma mensagem indica se foi correspondido ou não.

Operações de segurança mapeamento de campo

As tabelasOperações de segurança podem ser mapeadas de e para outras tabelas, vinculando um incidente de segurança a um caso de atendimento ao cliente ou um problema a outras partes do sistema Operações de segurança.

O mapeamento de campo define o mapeamento usado quando um registro da tabela de origem é usado para criar um novo registro na tabela de destino. Normalmente usados para criar um incidente de segurança a partir de outro registro, esses mapas definem quais campos em um incidente de segurança são inseridos em um novo problema ou quais campos de um incidente existente do cliente preenchem um novo incidente de segurança.

Mapear tabelas para tabelas com mapeamento de campo das Operações de segurança

Operações de segurança fornece granularidade de mapeamento de campo mais fina para que você possa mapear uma tabela Operações de segurança para qualquer outra tabela.

Antes de Iniciar
Função necessária: sec_cmn.write

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Mapeamento de Campos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

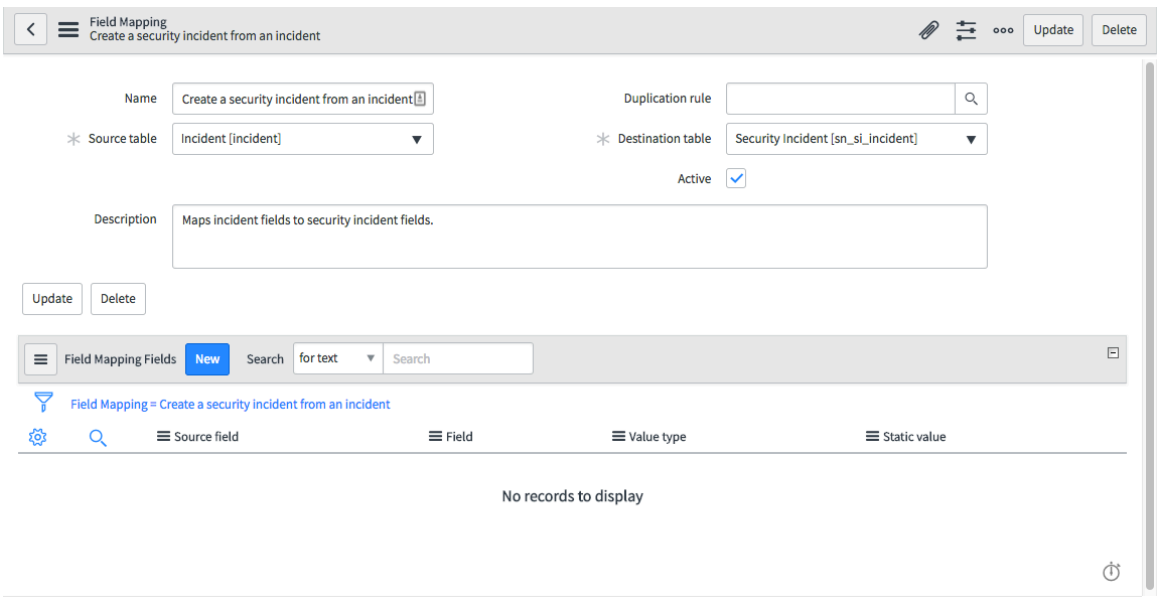
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de campo

Campo	Descrição
Nome	O nome do mapa de campo.
Tabela de origem	A tabela que fornece os dados a serem usados para criar um registro na tabela de destino.
Regra de duplicação	Controla como lidar com registros de origem que gerariam um registro duplicado. Para obter mais informações, consulte Transformação de dados compartilhados.
Tabela de destino	A tabela em que novos registros são criados.
Ativo	Marque esta caixa de seleção para ativar o mapeamento. **Nota:** Somente um mapeamento entre tabelas pode estar ativo por vez. Se dois mapas contiverem as mesmas tabelas, a versão mais antiga será desativada automaticamente.
Descrição	Descrição do mapa de campo.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar**.
   A guia**Campos de mapeamento de campo** é exibida. Este registro define quais dados são colocados no campo de destino, em registros criados por esta transformação de campo.



5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme o apropriado.

Opção	Descrição
Campo	**Descrição**
Armazenar valor em um campo ou uma lista relacionada	Selecione onde encontrar o valor. As opções incluem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	◦ Adicionar novo valor a um campo no registro ◦ Vincular a este valor a uma lista relacionada ◦ Link para este valor, criando um registro se não existir um registro correspondente **Nota:** Se a tabela de destino não tiver listas relacionadas, este campo não será exibido.
Campo	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Adicionar novo valor em um campo no registro**, este campo especifica o campo a ser preenchido. **Nota:** Para campos de opção, as correspondências são feitas com as escolhas existentes usando o rótulo ou valor de escolha subjacente. Se nenhuma correspondência for encontrada, o campo será definido, mas nenhuma nova entrada será adicionada à lista de seleção. Para obter mais informações, consulte Listas de seleção . Para campos de referência, uma entrada é definida somente quando um valor correspondente ao nome de exibição do registro ou `sys_id` válido é encontrado. Para obter mais informações, consulte Campos de referência .
Lista relacionada	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se não existir um registro correspondente**, este campo especificará a lista relacionada à qual informações serão adicionadas.
Campo de valor	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se não existir um registro correspondente**, este campo especifica o campo na tabela exibida no relacionado

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	lista, que é usada para pesquisar e encontrar um registro existente. Por exemplo, se sua lista relacionada for **ICs afetados**, este campo poderá conter **Nome** ou Nome de **domínio totalmente qualificado**ou qualquer outro campo no registro de IC que deva ser usado para pesquisar o IC adicionado à lista de **ICs afetados**.
Dados de relacionamento	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada**, um novo registro será criado para vincular esse registro (como um incidente de segurança) ao valor (um IC, um observável e assim por diante). Este campo especifica todas as informações adicionais (pares de campo e valor) que devem ser adicionadas a esse registro de vinculação. Por exemplo, ao adicionar um observável para um IP de origem, você pode especificar que este IP é a origem, em vez do IP de destino. Para vários valores, use um separador ^, por exemplo, type= Source IP^active=true.
Novos dados de registro	**Quando Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor, criar um novo registro se não existir**um registro correspondente, se um registro relacionado correspondente ao valor analisado não for encontrado, um novo registro será criado. Este campo especifica os dados estáticos a serem adicionados a esse registro. Por exemplo, para **ICs afetados**, se não pudermos encontrar o IC, essa configuração indicará que um novo IC foi criado). O valor encontrado no registro de origem é definido como o campo **Valor** no registro de IC. Você pode definir dados adicionais - uma nota indicando por que este IC foi criado, algumas informações sobre com que tipo de ICs você está trabalhando. Uma amostra seria: `description=Created by malware Incident report^type=autodetect`
Separador de valores	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se não existir um registro correspondente**, este campo especifica o se-

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	parador a ser usado para listas de itens, geralmente uma vírgula ou ponto e vírgula.
Tipo de valor	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Adicionar novo valor em um campo no registro**, este campo especifica o tipo de valor. As opções incluem: ◦ **Registro do campo de origem** ◦ **Anexar ao campo como uma nova linha** ◦ **Valor estático** ◦ **Valor estático mais o valor do campo de registro de origem**
Campo de origem	Escolha o campo de origem que contém o valor a ser colocado no campo de destino ou na lista relacionada selecionada.
Campo estático	Valor estático para o campo.
Transformação de valor	Escolha a entrada de transformação de valor de campo a ser aplicada. Ele é usado para mapear campos de opção entre registros, por exemplo, convertendo o conjunto de opções de **categoria** de um incidente de segurança no campo de **tipo** apropriado para uma solicitação de mudança.
Tabela de destino	Preenchido automaticamente com a tabela de destino.
Mapeamento de Campos	Preenchido automaticamente com o mapa de campo primário.
Tabela de origem	Preenchido automaticamente com a tabela de origem.

Tradução automática

7. Clique em **Enviar**.

Operações de segurança transformações de valor de campo

Transforma valores de campo de cliente exclusivos em valores de campo reconhecidos por Operações de segurança análise de e-mail, enriquecimento de dados ou tabelas usando mapas de campo. Oferece suporte a campos de opção, faz referência e alinha dados externos na terminologia e formato padrão para o novo registro.

Você pode mapear dados para campos como Categoria, Estado ou Grupo de atribuição nos valores usados na tabela Operações de segurança. Por exemplo, mapeie "Em análise" para "Trabalho em andamento".

Criar transformações de valor de campo Operações de segurança

As transformações de valor de campo definem uma transformação entre os dados de origem fornecidos e o valor de substituição a ser usado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_sec_cmn.basic ou sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa
Defina cada entrada de transformação a ser aplicada quando houver uma correspondência com o valor de pesquisa, quando o valor de pesquisa estiver contido nos dados de origem fornecidos ou quando nenhuma correspondência for encontrada. Defina um valor padrão para quando nenhuma correspondência for encontrada. Se nenhum valor padrão estiver definido e nenhuma correspondência for encontrada, os dados de origem originais serão usados.

Procedimento
1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Transformações de Valores de campos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Transformações de valor de campo

Campo	Descrição
Nome	O nome da transformação do valor do campo.
Descrição	Descrição do mapa de campo.
Entradas de Transformação de Valor de Campo	A lista de tabelas de entradas. **a.** Em **Substituir dados**, clique duas vezes em "Inserir uma nova linha". **b.** Escolha uma das seguintes opções: Quando a data deste campo corresponde Quando os dados para este campo contêm Quando nenhuma outra entrada de transformação corresponde aos dados (padrão) **c.** Clique na marca de seleção verde. **d.** Clique duas vezes em **Valor de pesquisa**, adicione o valor de pesquisa. **e.** Clique na marca de seleção verde. **f.** Clique duas vezes em Valor de **substituição para** adicionar o valor correspondente ServiceNow. **g.** Repita se necessário.
Ativo	Marque esta caixa de seleção para ativar a transformação.
Aplicação	Escopo da aplicação.

4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança mapeamento de dados de aprimoramento

Mapeamento de Dados de Aprimoramento transforma dados de arquivos XML, JSON ou Propriedades em registros ServiceNow. Operações de segurança fluxos de trabalho usam mapas de dados de aprimoramento e fornecem dados de saída para incidentes de segurança.

Operações de segurança inclui vários mapas de dados de aprimoramento, acionados por vários fluxos de trabalho, por exemplo, Integrações de operações de segurança - Fluxo de trabalho Obter estatísticas de rede e Integração de comandos do sistema de operações de segurança - Obter fluxo de trabalho de processos em execução. A saída do mapa de dados de aprimoramento de fluxos de trabalho Operações de segurança é exibida na guia **Dados** de aprimoramento no formulário de incidente de segurança.

Criar um Operações de segurança mapa de dados de aprimoramento

Transforme dados do formato de arquivo JSON, XML ou Propriedades em registros ServiceNow usando mapas de dados de aprimoramento.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Os mapas de dados de aprimoramento existentes são usados por fluxos de trabalho fornecidos em Operações de segurança. Você pode exibir a lista em **Mapeamento de dados de aprimoramento**. Para usar um mapa, você precisa de um gatilho, seja uma regra de negócio ou fluxo de trabalho.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Mapeamento de Dados de Aprimoramento**.
2. Clique em **Nova**.
3. Preencha os campos, se for o caso.

Como criar um mapa de dados de aprimoramento

Campo	Descrição
Nome	Nome deste mapa de dados de aprimoramento.
Formato de entrada	Escolha um formato na lista: JSON (padrão) XML Formato do arquivo de propriedades
Chave de prefixo	Use para limitar o conjunto de dados de entrada a uma chave especificada. A raiz do conjunto de dados de entrada está definida para esta chave. Neste exemplo, se você inserisse file_info, os valores de entrada seriam limitados aos valores em file_info.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	<?xml version="1.0" encoding="UTF-8"?> <malware> <version>2.0</version> <file_info> <malware>yes</malware> <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1> <filetype>PE</filetype> <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Aplicação	Escopo da aplicação.
Regra de duplicação	Regra que define quando um registro é considerado uma duplicata e quais ações tomar com registros duplicados.
Tabela de destino	Escolha uma tabela na lista.
Ativo	Marque esta caixa de seleção para ativar o mapa.
Descrição	Insira uma descrição do mapa de dados de aprimoramento.

4. Clique em **Enviar**.
   A guia Campos de mapeamento de dados de aprimoramento é exibida.
5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme o apropriado.

Campos de mapeamento de dados de aprimoramento

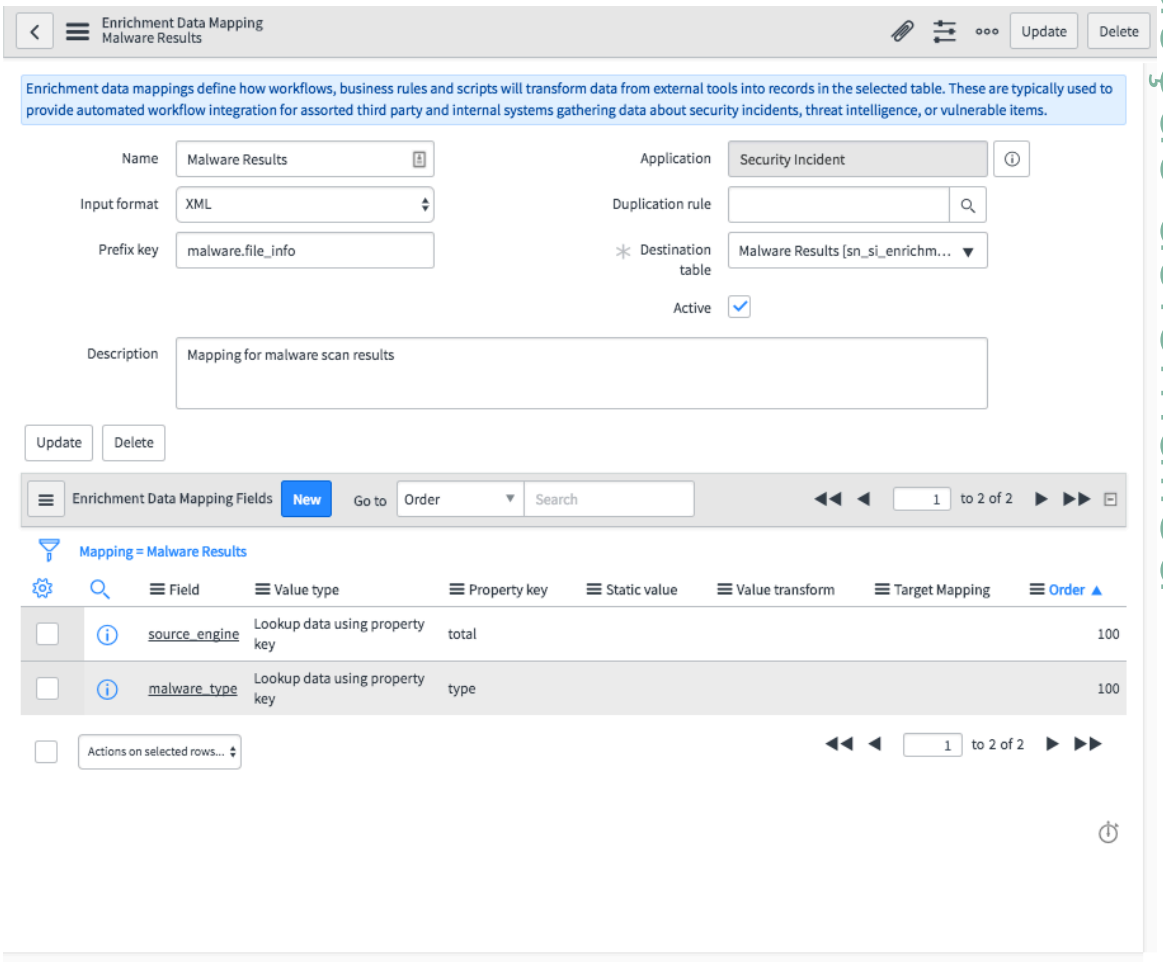
Campo	Descrição
Campo	Nome do mapa de dados de aprimoramento.
Tipo de valor	Escolha na lista: Pesquisar dados usando a chave de propriedade Valor estático Valor estático e dados da chave de propriedade O campo é uma matriz ou objeto (aninhamento de dados brutos)

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Cada opção tem entradas diferentes. Valores de campo e matrizes ou objetos exigem uma chave de propriedade.
Chave de propriedade	Determina a chave para a pesquisa de dados de entrada e o valor gravado no campo de destino.
Transformação de valor	A transformação do valor do campo que mapeia um valor para outro.
Aplicação	Escopo da aplicação.
Ordem	Em que ordem considerar o mapeamento. A primeira correspondência é usada. O padrão é 100.
Mapeamento	Nome do mapa de dados de aprimoramento.
Tabela de destino	A tabela para a qual os campos a serem mapeados estão indo.

7. Clique em **Enviar**.
   A seguir está um exemplo de um mapa de dados de aprimoramento.



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operações de segurança escalação definida pelo usuário

Você pode criar um caminho de escalação para incidentes de segurança em caso de problemas que exigem mais atenção ou experiência. Depois que um grupo de escalação existir, um botão aparecerá em qualquer incidente de segurança nesse grupo.

Criar um Operações de segurança grupo de escalação definido pelo usuário

Escale um incidente de segurança para qualquer grupo associado ao incidente usando Escalações.

Antes de Iniciar

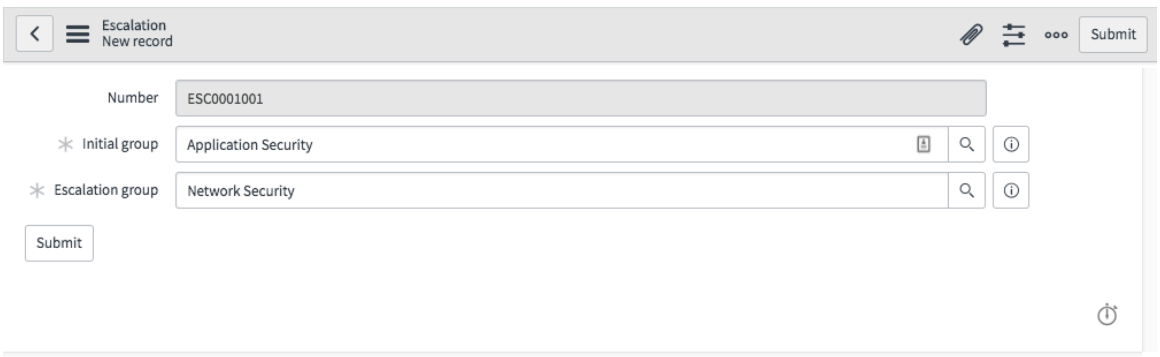
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Grupos** > **Escalações**.
2. Clique em **Novo**.
3. Preencha os campos no formulário, conforme o apropriado.

Escalações

Campo	Descrição
Número	Número do incidente de escalação (o campo é gerado automaticamente).
Grupo inicial	Selecione o grupo ao qual este incidente de segurança pertence.
Grupo de escalação	Selecione o grupo para o qual o incidente de segurança será escalonado.

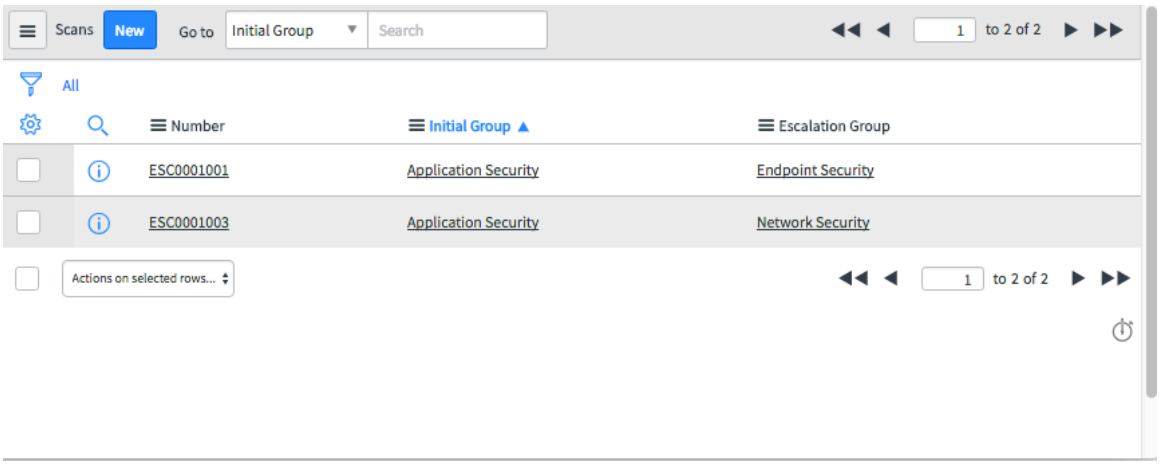


4. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um grupo de escalação está disponível para todos os incidentes de segurança no grupo inicial. Você pode criar vários grupos.



Criar substituições de propriedade separadas por domínio

Ao usar o Domain Separation, você pode criar substituições nas propriedades existentes das Operações de segurança que permitem personalizar as funções das aplicações em cada um dos seus domínios.

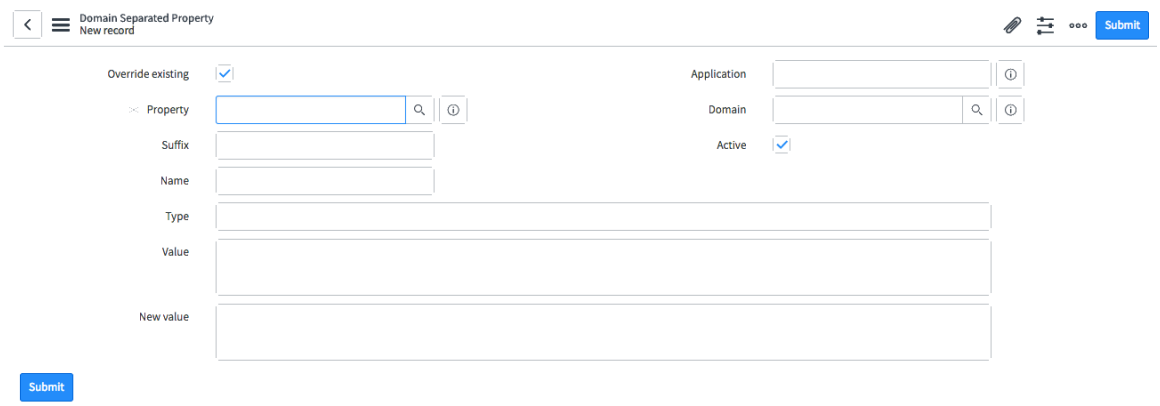
Antes de Iniciar

Requer que Domain Support - Domain Extensions esteja ativado. Você também pode aprender sobre o Visualizador de substituição de domínio .

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Propriedades Separadas de Domínio**.
2. Clique em **Nova**.



3. No formulário, preencha os campos.

Formulário de propriedade da Separação de domínios

Campo	Descrição
Substituir existente	Marque esta caixa de seleção para criar um valor específico de domínio para uma propriedade existente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	Selecione a aplicação que contém a propriedade que você deseja substituir.
Propriedade	Selecione a propriedade da aplicação selecionada para a qual você deseja criar uma substituição específica de domínio.
Domínio	Selecione o domínio para o qual você está criando esta substituição de propriedade.
Ativo	Ative ou desative a substituição.
Sufixo	Exibe o sufixo da propriedade.
Nome	Exibe o nome da propriedade.
Tipo	Exibe o tipo de propriedade.
Valor	Exibe o valor atual definido para a propriedade.
Novo valor	Insira um novo valor para a propriedade a ser aplicada a este domínio.

4. Clique em **Enviar**.
   A substituição da propriedade é aplicada à propriedade selecionada no domínio especificado. Quando a lógica desta propriedade é acionada, o sistema verifica se há substituições de propriedade separadas por domínio. Se uma substituição do domínio for encontrada, o novo valor será usado. Caso contrário, o valor do domínio padrão será usado.

Informações relacionadas

Noções básicas sobre o Domain Separation

Criar um grupo de sistemas operacionais

Grupos de sistemas operacionais são usados para mapear um sistema operacional para tipos de processo e scripts específicos em Security Incident Response fluxos de trabalho. Os scripts definem como os processos em execução dos grupos de sistemas operacionais definidos são recuperados. Novos sistemas operacionais podem ser adicionados conforme necessário.

Antes de Iniciar

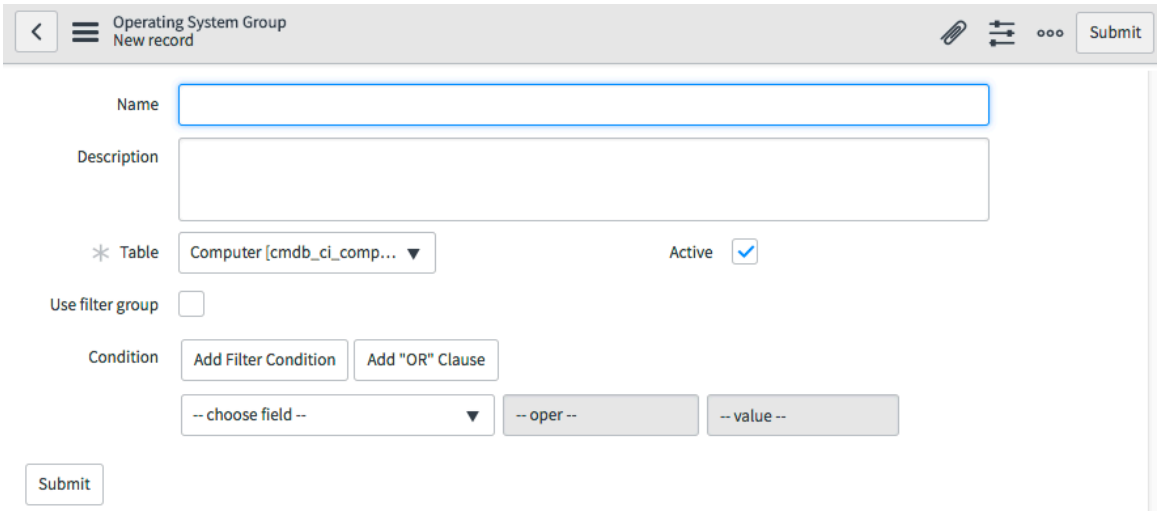
Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Grupos de Sistemas Operacionais**.
   O sistema base inclui scripts para três sistemas operacionais:
   - SO baseado em BSD
   - SO baseado em POSIX
   - SO Windows
2. Clique em **Nova**.

Tradução automática

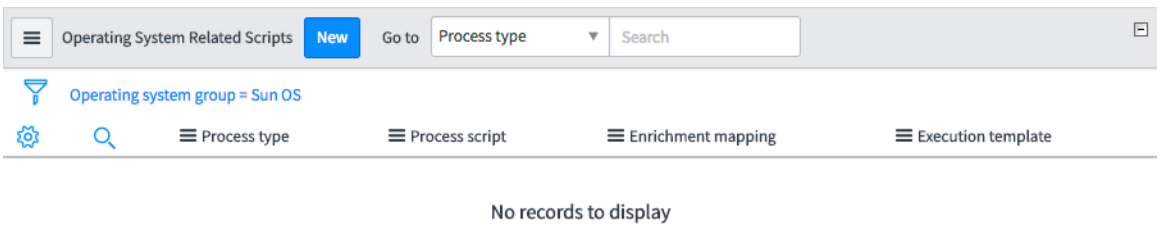
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Preencha os campos conforme necessário.

Campo	Descrição
Nome	O nome do grupo do sistema operacional.
Descrição	Uma descrição para o grupo de sistemas operacionais.
Tabela	A tabela afetada.
Ativo	Marque esta caixa de seleção para ativar o grupo de sistemas operacionais.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros para localizar registros correspondentes na tabela selecionada.
Grupo de filtros	Selecione o grupo de filtros para localizar registros correspondentes na tabela selecionada. Este campo será exibido somente se você marcar a caixa de seleção **Usar grupo de filtros**.
Condição	O Os campos doconstrutor de condições serão exibidos somente se você não marcar a caixa de seleção **Usar grupo de filtros**.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
A lista relacionada Scripts relacionados ao sistema operacional é aberta.



5. Clique em **Nova**.

6. Selecione scripts que correspondam aos fluxos de trabalho que você está usando para obter processos em execução, serviços e/ou estatísticas de rede.

7. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Anexar um arquivo de script a um MID Server sincronizado

Configurar grupos de marcadores de segurança e marcadores

Você pode atribuir marcadores a incidentes de segurança, tarefas de resposta, itens vulneráveis, observáveis, IoCs e casos de segurança para criar metadados no registro de resposta e definir quem deve ter acesso a tipos específicos de conteúdo de segurança. Os marcadores podem ser adicionados a grupos de segurança para organizá-los.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Marcadores de Segurança** > **Grupos**.
   Três grupos de classificação padrão estão incluídos no sistema de base.
   - **Lista de permissões/listas de proibições de aprimoramento**: este grupo define se um registro deve ser tratado como um registro de lista de permissões ou de proibições. Os registros da lista de permissões geralmente são menos significativos, portanto, podem ser ignorados. Os registros da lista de proibições geralmente são de maior interesse.
   - **Metatag**: este grupo é fornecido como dados de demonstração. Você pode usá-lo para criar marcadores de classificação personalizados que são usados por aplicações de operações de segurança.
   - **Protocolo de semáforo**: este grupo é usado para garantir que informações confidenciais sejam compartilhadas com o público correto. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade. Para cada cor, você pode atribuir as funções de acesso de leitura/gravação apropriadas. Ao compartilhar observáveis com um círculo de segurança confiável, o marcador atribuído ao perfil do círculo de segurança confiável determina quais observáveis marcados com TLP podem ser compartilhados com o círculo, da seguinte forma:
     - **TLP: WHITE:** somente observáveis com TLP: WHITE podem ser compartilhados com um perfil TLP: WHITE.
     - **TLP: VERDE:** observáveis com TLP: VERDE e TLP: BRANCO podem ser compartilhados com um perfil TLP: VERDE.
     - **TLP: ÂMBAR:** observáveis com TLP: ÂMBAR, TLP: VERDE e TLP: BRANCO podem ser compartilhados com um perfil TLP: AMBER.
     - **TLP: RED:**todos os observáveis, independentemente do marcador TLP, podem ser compartilhados com um perfil TLP: RED, já que TLP: RED é o marcador TLP com classificação mais alta.

     Nota: Você pode adicionar outras cores TLP, mas qualquer uma além das quatro cores incluídas é considerada inválida pelo Fórum de Equipes de segurança e resposta a incidentes (FIRST).
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	Insira o nome do grupo de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Permitir várias seleções	Marque esta caixa se quiser atribuir vários marcadores de segurança a um registro que compartilha um grupo.
Ativo	Ativar ou desativar o grupo.
Descrição	Insira uma descrição deste grupo.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A lista relacionada Marcadores de segurança é exibida.
5. Na lista relacionada Marcadores de segurança, clique em **Novo**.
6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome do marcador de classificação.
Grupo de marcadores de segurança	Se o marcador foi criado usando o botão **Novo** na lista relacionada ao grupo, este campo será padronizado para o grupo atual. Se necessário, você pode adicionar o marcador a um grupo diferente, mas isso é opcional.
Ordem	Especifique a ordem em que o marcador aparece em formulários ou em uma lista.
Cor	Selecione a cor deste marcador.
Impor acesso restrito	Marque esta caixa de seleção para atribuir funções de leitura e/ou gravação necessárias para os usuários lerem ou gravarem em registros que têm este marcador de segurança.
Ativo	Ative ou desative o marcador.
Descrição	Uma descrição deste marcador.
Função (acesso de leitura)	Para atribuir acesso de leitura a um marcador de segurança, clique no ícone de cadeado, selecione as funções de acesso apropriadas e clique no ícone de cadeado novamente. Este campo aparecerá somente se você marcar a caixa de seleção **Impor acesso restrito**.
Funções (acesso de gravação)	Para atribuir acesso de gravação a um marcador de segurança, clique no ícone de cadeado, selecione as funções de acesso apropriadas e clique no ícone de cadeado novamente. Este campo aparecerá somente se você marcar a caixa de seleção **Impor acesso restrito**.

7. Repita conforme necessário para criar mais marcadores de segurança.
8. Clique em **Atualizar**.

Nota: Você também pode criar novos marcadores navegando até **Operações de segurança** > **Marcadores de Segurança** > **Marcadores**. O procedimento é o mesmo.

Criar regras de marcador de segurança

As regras de marcador de segurança fornecem filtragem para acesso a marcadores de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Marcadores de Segurança** > **Marcadores**.
2. Escolha ou crie um marcador de segurança.
3. Na guia relacionada **Regras de marcador de segurança**, clique em **Novo**.
4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da regra de marcador de segurança.
Marcador de segurança	O marcador de segurança a ser anexado à regra.
Ativo	Ative ou desative o marcador de segurança.
Descrição	Uma descrição desta regra.

5. Determinar **filtragem de registro.**
6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Usar grupo de filtros	Associa o grupo de filtros à regra.
Tabela	A tabela que contém a regra.
Condição	Adicione uma ou mais condições de filtro.

7. Clique em **Enviar**

Importar regras de marcador de segurança

Você pode importar regras de marcador de segurança de outras tabelas em sua implantação.

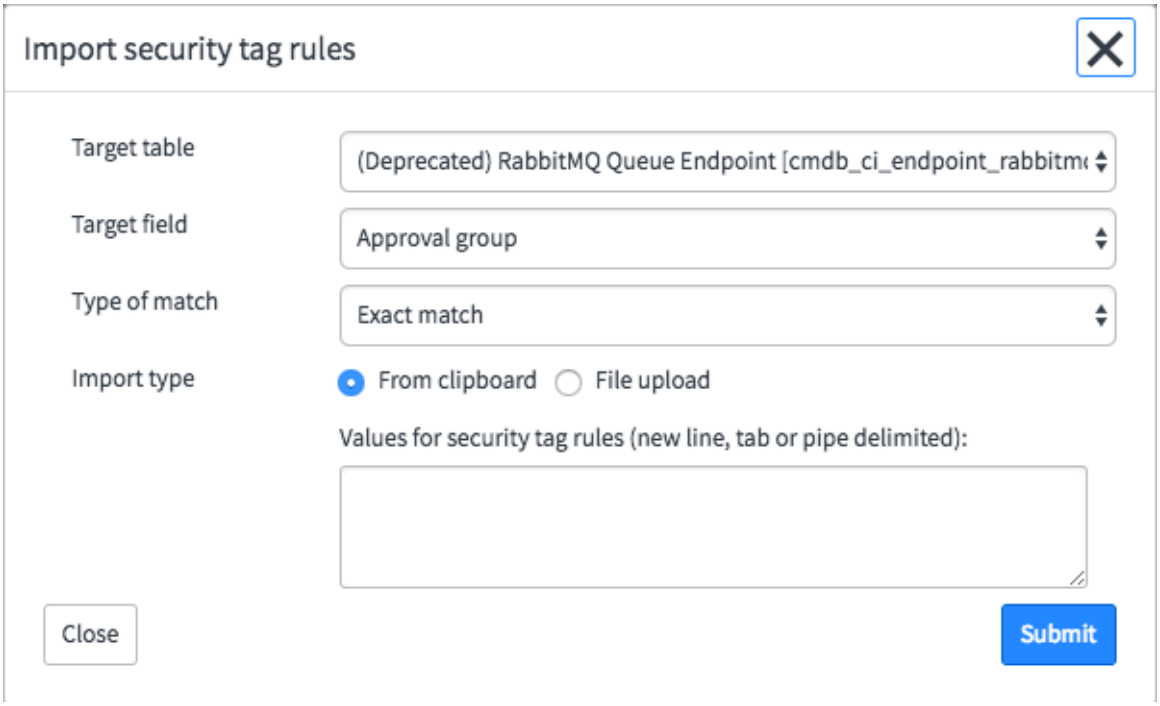
Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Marcadores de Segurança** > **Marcadores**.
2. Escolha ou crie um marcador de segurança.
3. Clique no link relacionado **Importar regras de marcador de segurança**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Tabela de destino	Escolha a tabela a ser usada para importar regras.
Campo de destino	Escolha o campo a ser usado para importar regras.
Tipo de correspondência	Escolha como corresponder as regras importadas aos marcadores de **segurança** de: Correspondência exata (padrão) Contém Começa com Termina com Expressão regular
Tipo de importação	Escolha: Da área de transferência Copie uma lista de valores delimitados para a área de texto. Os valores são analisados em marcadores de segurança. Do carregamento do arquivo Carregue um arquivo com valores delimitados. Os valores são analisados em marcadores de segurança. Adicione valores para as regras de marcador de segurança usando novos delimitadores de linha ou pipe.

5. Clique em **Enviar**

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anotações de segurança

Uma anotação de segurança é uma nota de explicação ou comentários adicionados a um item de configuração, observável ou uso em um incidente de segurança.

Várias anotações de segurança estão disponíveis para usuários e observáveis (requer o plug-in Inteligência contra ameaças). Relatórios sobre anotações de segurança também estão disponíveis.

Criar anotações de segurança para ICs

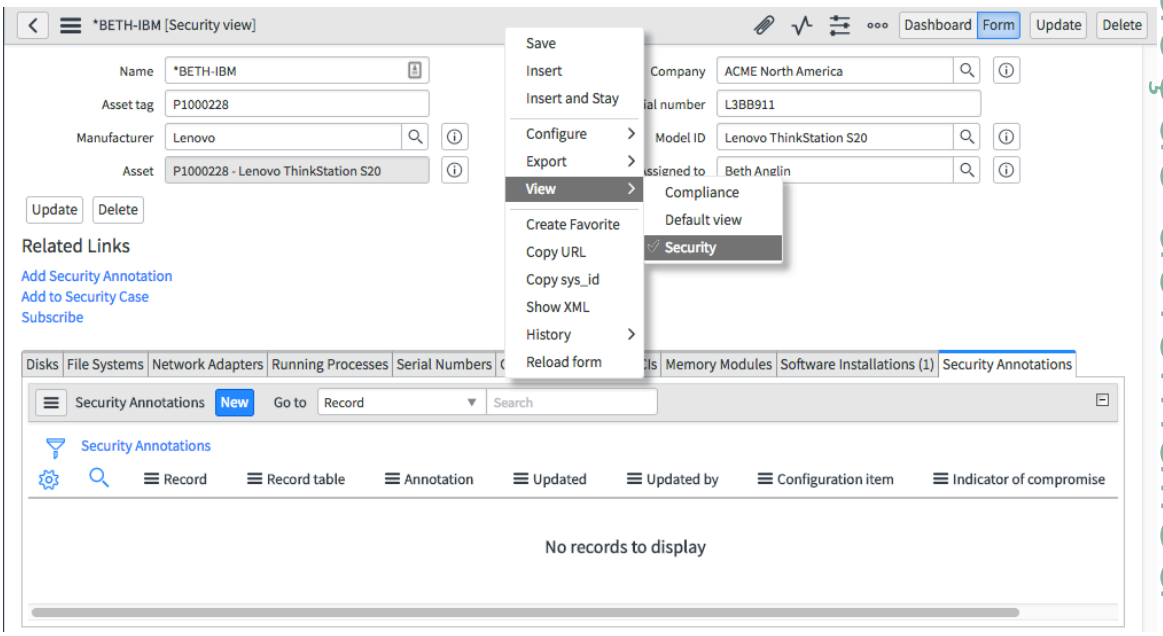
As anotações em ICs permitem que você rastreie a atividade entre incidentes. Você pode adicionar anotações a um único ou a vários ICs.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Em um incidente de segurança ou na tabela Item de configuração, abra um IC.
2. Clique com o botão direito do mouse no cabeçalho e escolha **Exibição** > **Segurança**.



3. Na guia da lista relacionada **Anotações de segurança**, clique em **Novo**.
4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

> **Nota:** Você pode adicionar a mesma anotação a vários ICs selecionando ICs na lista, escolhendo **Adicionar anotação de segurança**, inserindo uma anotação em qualquer formato de texto e clicando em **Enviar**.

Criar anotações de segurança para observáveis

Você pode selecionar um ou vários observáveis e aplicar anotações de segurança a eles usando o menu de seleção **Ações nas linhas selecionadas**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

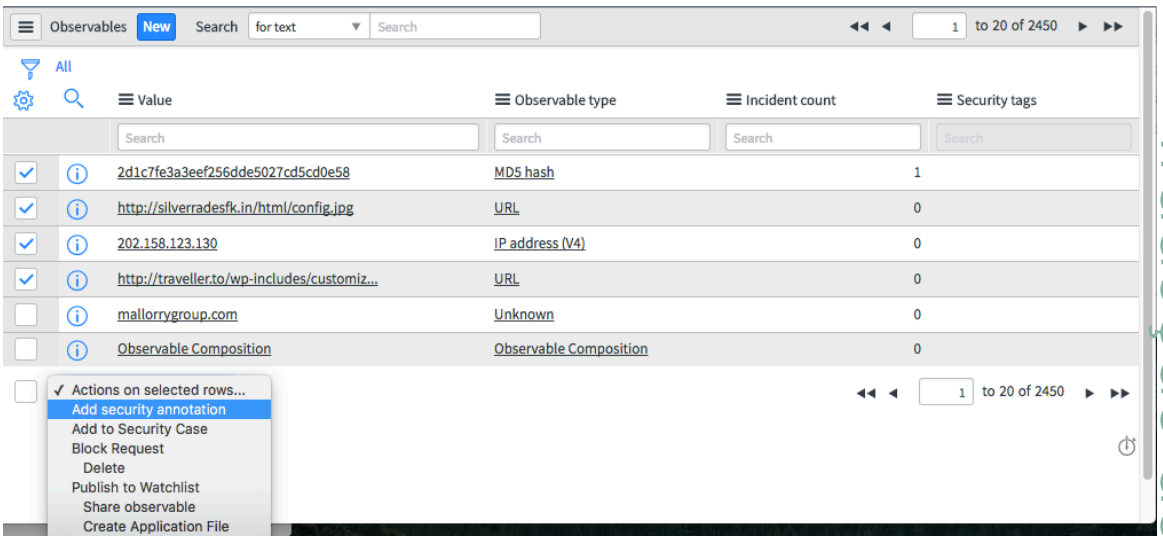
Antes de Iniciar

- Requer o plug-in Inteligência contra ameaças e a ativação. O plug-in Inteligência contra ameaças está disponível como uma assinatura separada.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Observáveis**
2. Selecione um ou mais observáveis na lista.
3. No menu suspenso **Ações em linhas selecionadas**, escolha **Adicionar anotação de segurança**.



4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

Criar anotações de segurança para usuários

Você pode selecionar um ou vários usuários e aplicar anotações de segurança a eles usando o menu de seleção **Ações nas linhas selecionadas**.

Antes de Iniciar

Requer o plug-in Inteligência contra ameaças e a ativação. O plug-in Inteligência contra ameaças está disponível como uma assinatura separada.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Usuários**
2. Selecione um ou mais usuários na lista.
3. No menu suspenso **Ações em linhas selecionadas**, escolha **Adicionar anotação de segurança**.
4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

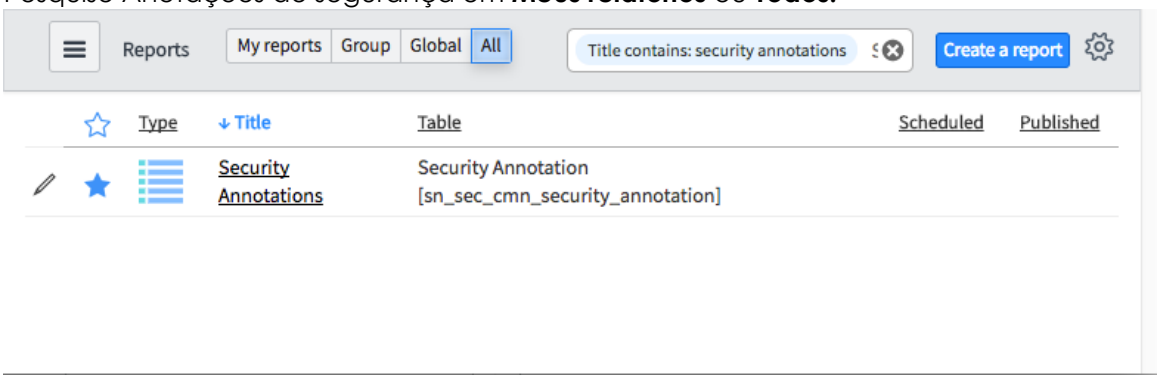
Exibir relatórios de anotações de segurança

O relatório Anotações de segurança apresenta detalhes armazenados na tabela Anotações de segurança [sn_sec_cmn_security_annotations]. Você pode personalizar as colunas no relatório e agrupar os dados da maneira que for mais adequada para você.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Relatórios** > **Exibir/Executar**.
2. Pesquise Anotações de segurança em **Meus relatórios** ou **Todos.**



Informações relacionadas

Exibir a lista de Relatórios

Componentes instalados com Security Support Common

Vários tipos de componentes são instalados com Security Support Common. Eles fornecem funcionalidade comum para uso em várias aplicações de segurança, como Security Incident Response.

Localizando e exibindo componentes instalados

Consulte Exibir componentes instalados com Security Support Common mais informações sobre como localizar e exibir componentes instalados.

Exibir componentes instalados com Security Support Common

Vários tipos de componentes são instalados quando você ativa o plug-in Security Support Common, incluindo, entre outros, tabelas, funções de usuário e módulos.

Localizando componentes

Nota: A tabela Arquivos de aplicações lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Se você quiser limitar a lista de componentes instalados a funções, trabalhos agendados e tabelas para a aplicação Comum de suporte de segurança, siga estas etapas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos agendados e as tabelas instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condições (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação.
3. No Construtor de condições, para adicionar um segundo filtro, clique em **E**e selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, Trabalho **agendado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Pesquisar Operações de segurança

Você pode encontrar informações rapidamente em qualquer aplicação Operações de segurança usando o ícone de pesquisa no cabeçalho da tela. O Zing é o mecanismo de indexação e pesquisa de texto que executa todas as pesquisas de texto em sua instância.

Antes de Iniciar

Função necessária: sn_si.read ou superior

Procedimento

1. Clique no ícone de pesquisa ( ) no canto superior direito da tela.
2. Digite os critérios pelos quais você deseja pesquisar e pressione **Enter**.
   Se você tiver o plug-in Security Incident Response ativado, os critérios de pesquisa inseridos apresentarão qualquer texto de descrição resumida, ICs, endereços IP ou URLs correspondentes em seus incidentes de segurança, tarefas Security Incident Response ou solicitações de segurança. Se você tiver os plug-ins Resposta a vulnerabilidades ou Inteligência contra ameaças ativados, os resultados da pesquisa incluirão vulnerabilidades, itens vulneráveis, entradas vulneráveis, observáveis, IoCs e modo/métodos de ataque.

Informações relacionadas

Introdução à pesquisa

Pesquisa de texto do Zing

Referência do Security Operations Integrations

Os desenvolvedores e parceiros da ServiceNow podem usar as informações nesta seção para entender a funcionalidade oculta das integrações de terceiros, incluindo diretrizes de desenvolvimento, capacidades de integração e fluxos de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ServiceNow Operações de segurança diretrizes de desenvolvimento de integração

A plataforma ServiceNow fornece vários mecanismos para desenvolver integrações com sistemas externos. O pacote de produtos ServiceNow Operações de segurança adiciona capacidades de integração destinadas a simplificar o processo de integração com sistemas externos voltados para a segurança.

A maioria dos conceitos neste guia pressupõe alguma familiaridade com a funcionalidade ServiceNow padrão. Para integrar com o pacote Operações de segurança], é necessário ter conhecimento dos seguintes conceitos ServiceNow :

- Inclusões de script
- Serviços web de entrada/saída
- Fontes de dados
- Conjuntos para importação
- Mapas de transformação

Programa de parceiro de tecnologia

Todos os requisitos para certificação de aplicação ou diretrizes fornecidas na documentação do Programa de parceiros de tecnologia substituem todas as informações neste guia. Este guia não substitui a documentação do programa de parceiros de tecnologia e serve apenas como um suplemento à documentação existente.

Para obter mais informações, consulte a publicação no blog do curso de treinamento do Programa de parceiros de tecnologia .

Tipos de ServiceNow integrações fornecidas

As aplicações [Operações de segurança (Security Incident Response, Inteligência contra ameaçase Resposta a vulnerabilidades) podem ser integradas perfeitamente a outras aplicações ServiceNow para aprimorar sua funcionalidade.

As seguintes integrações são fornecidas no sistema de base Operações de segurança.

Security Incident Response – Integração com Gestão de eventos

Os recursos da aplicação Gestão de eventos foram expandidos para oferecer suporte a Security Incident Response. O plug-in de suporte Security Incident Response Gestão de eventos analisa automaticamente o conteúdo de eventos em Gestão de eventos para preencher campos em incidentes de segurança.

Caso de uso coberto:

Criação de eventos de segurança no sistema Gestão de eventos a partir das ferramentas Security Information and Gestão de eventos (SIEM)

Capacidades úteis fornecidas:

- Funcionalidade de gestão de eventos - correlação de eventos, regras de evento e regras de alerta
- Mapeamento automático de valores de additional_information para o incidente de segurança resultante

Recursos:

Documentação de suporte à gestão de eventos de incidentes de segurança

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação da Gestão de eventos

Security Incident Response - Integração de API do conjunto de importação

Além de usar Gestão de eventos para enviar eventos relacionados à segurança, a aplicação Security Incident Response fornece uma API de Conjunto para importação que permite a criação direta de incidentes de segurança. O endpoint REST do Conjunto para importação de incidentes de segurança é http://localhost:8080/api/now/import/sn_si_incident_import.

Esta técnica de integração é útil quando a) Gestão de eventos não está instalado ou b) se deseja simplesmente criar incidentes de segurança sem passar pelo evento > alerta > fluxo de incidente de segurança que é necessário ao usar Gestão de eventos.

Caso de uso coberto:

Criação de incidentes de segurança diretamente das ferramentas SIEM.

Capacidades úteis fornecidas:

Correspondência automática de IC na criação de incidentes de segurança com base em IP, NetBIOS ou nome de domínio totalmente qualificado.

Recursos:

Documentação da API do conjunto de importação da plataforma

Documentação do Conjunto para importação de serviço web de incidente de segurança

Inteligência contra ameaças - integração de pesquisa de origem

As origens de pesquisa fornecem a capacidade de enviar dados para origens de pesquisa externas para determinar se esses dados são mal-intencionados. Geralmente, esses dados são um endereço IP, URL, arquivo ou hash de arquivo.

Caso de uso coberto:

Pesquise um endereço IP, URL, arquivo ou hash com um serviço de pesquisa externo.

Capacidades úteis fornecidas:

- Maneira consistente de solicitar pesquisas de itens do catálogo e incidentes de segurança.
- Capacidades de limitação e limitação de taxa fornecidas com pouca/nenhuma codificação.
- Criação automática de entradas observáveis de Indicadores de compromisso (IoC) para todos os problemas encontrados por fontes de pesquisa.

Inteligência contra ameaças - integração da origem da ameaça

As origens de ameaças fornecem a capacidade de extrair dados de repositórios externos de inteligência contra ameaças. Esses dados são importados para as várias tabelas de Indicadores de Compromisso que existem no sistema. As coleções TAXII e as listas de bloqueio simples são compatíveis nativamente. Para adicionar novas coleções TAXII (ou perfis com base em um serviço de gestão de descoberta ou coleta), basta adicionar uma entrada. Da mesma forma, adicionar uma nova lista de bloqueios simples de coluna única é uma questão de inserir um novo registro e fornecer o URL da lista de bloqueios. Para conjuntos de dados mais complicados, uma integração personalizada pode ser fornecida para fazer uma chamada para um URL e analisar a resposta.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso de uso coberto:

Recupere dados de uma origem de inteligência contra ameaças para carregar em tabelas de IoC.

Capacidades úteis fornecidas:

- Suporte para listas de bloqueio simples e coleções TAXII sem codificação.
- Mecanismo simples para executar mensagens REST para recuperar dados.
- Recuperação/processamento de dados desacoplados para reutilização do componente de integração.
- Suporte nativo para processamento de dados de passagem retornados para fontes de dados (e conjuntos para importação/mapas de transformação).
- Oferece suporte a várias solicitações de dados por integração (para chamadas paginadas) com a capacidade de passar contexto para chamadas subsequentes

Recursos:

Definir uma origem de ameaça

Resposta a vulnerabilidades - Integração de invocação de scanner

A Invocação do Verificador de vulnerabilidades é um ponto de entrada de integração leve que oferece suporte à invocação de verificações de vulnerabilidade da instância. Um scanner de vulnerabilidade de terceiros é chamado de forma assíncrona para programar uma verificação de itens de configuração ou endereços IP.

Caso de uso coberto:

Faça uma solicitação ao scanner de terceiros para verificar um IC (usando informações de host derivadas do IC) ou endereço IP/endereços IP.

Capacidades úteis fornecidas:

- Estrutura simples para definir implementações de scanner.
- Maneira consistente de solicitar verificações de itens do catálogo, incidentes de segurança e itens vulneráveis.
- Atualização automática de tarefas com o resultado da invocação de verificação.

Resposta a vulnerabilidades - integração de dados

As integrações de dados de vulnerabilidade têm como objetivo recuperar dados de vulnerabilidade de sistemas de vulnerabilidade de terceiros. As saídas esperadas dessas integrações são entradas de vulnerabilidade e itens vulneráveis. Essa integração permite que os verificadores de vulnerabilidade de terceiros funcionem de forma independente, com a expectativa de que as vulnerabilidades possam ser trabalhadas e rastreadas na instância.

Casos de uso cobertos:

- Recuperar bibliotecas de vulnerabilidades
- Recuperar emparelhamentos de vulnerabilidade/IC
- Sincronizar ICs com o sistema de gestão de vulnerabilidades

Capacidades úteis fornecidas:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Recuperação/processamento de dados desacoplados para reutilização do componente de integração.
- Suporte nativo para processamento de dados de passagem retornados para fontes de dados (e conjuntos para importação/mapas de transformação).
- Oferece suporte a várias solicitações de dados por integração (para chamadas paginadas) com a capacidade de passar contexto para chamadas subsequentes.

Recursos:

Documentação de integração de dados de vulnerabilidade

Operações de segurança Configurações de integração

Muitas das integrações incluídas no sistema de base exigem pouca ou nenhuma configuração e operam da mesma maneira. Certas integrações, como Qualys Cloud Platform, no entanto, exigem etapas separadas para configurar a integração. Outros oferecem suporte a diferentes conjuntos de tipos de verificação e pesquisa e a diferentes limites de taxa.

Esta seção descreve as diferenças entre as integrações compatíveis e aponta para mais documentação, conforme necessário.

- Integração do Carbon Black: permite que você investigue e responda a incidentes de segurança usando as APIs Carbon Black para consultar e interagir com endpoints associados a incidentes de segurança.
- Antibot Check Point - Integração do analisador de e-mails: usa um analisador de e-mail que consome notificações por e-mail do Antibot do Check Point para criar incidentes de segurança.
- Integração de enriquecimento de incidentes do Elasticsearch: pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.
- Integração de Have I been pwned?: permite que a lista de contas violadas (endereços de e-mail e nomes de usuário) seja pesquisada rapidamente por meio de um serviço RESTful.
- HPE Security ArcSight ESM - Integração do analisador de e-mail: usa um analisador de e-mail que consome notificações por e-mail do HPE ArcSight ESM para criar incidentes de segurança.
- HPE ArcSight Logger - Integração de enriquecimento de incidentes: pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.
- IBM QRadar - Incident Enrichment Integration: pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.
- McAfee ESM - Integração do analisador de e-mail: usa um analisador de e-mail que consome notificações por e-mail do McAfee ESM para criar incidentes de segurança.
- McAfee ESM - Incident Enrichment Integration: pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.
- OPSWAT Metadefender visão geral da integração: permite que os dados de ameaças, detectados pelo scanner Metadefender de terceiros, sejam baixados para a aplicação Inteligência contra ameaças para acompanhamento, priorização e resolução.
- Integração de Palo Alto Networks - AutoFocus: o AutoFocus da Palo Alto Networks, um serviço em nuvem de inteligência contra ameaças, permite pesquisar informações de sessão relacionadas a observáveis de incidentes de segurança.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração de Palo Alto Networks - Firewall: o firewall da Palo Alto Networks permite configurar e manter firewalls para evitar ameaças conhecidas e desconhecidas na rede, na nuvem e nos endpoints.
- Integração de Palo Alto Networks - WildFire: a integração do WildFire permite consultar trabalhos de análise de forma programática no WildFire e recuperar resultados históricos por meio de uma interface de API XML simples.
- Noções básicas sobre Qualys Vulnerability Integration: Qualys Cloud Platform é usado em Resposta a vulnerabilidades.
- Splunk - Integração de aprimoramento de incidentes: pesquisa seus logs e adiciona informações de detecção relevantes aos seus incidentes de segurança.
- Integração do VirusTotal: usado em Inteligência contra ameaças. Para usar esta origem de pesquisa, você deve ativar o plug-in VirusTotal Integration.
- Configuração da integração da API WhoisXML: fornece dados consistentes e bem estruturados de uma pesquisa Whois. Mantém dados precisos do Whois acessíveis 24 horas por dia, 7 dias por semana.

Ativar e configurar integrações de terceiros

Você pode ativar os plug-ins para integrações de terceiros e configurá-los para uso na mesma tela.

Antes de Iniciar

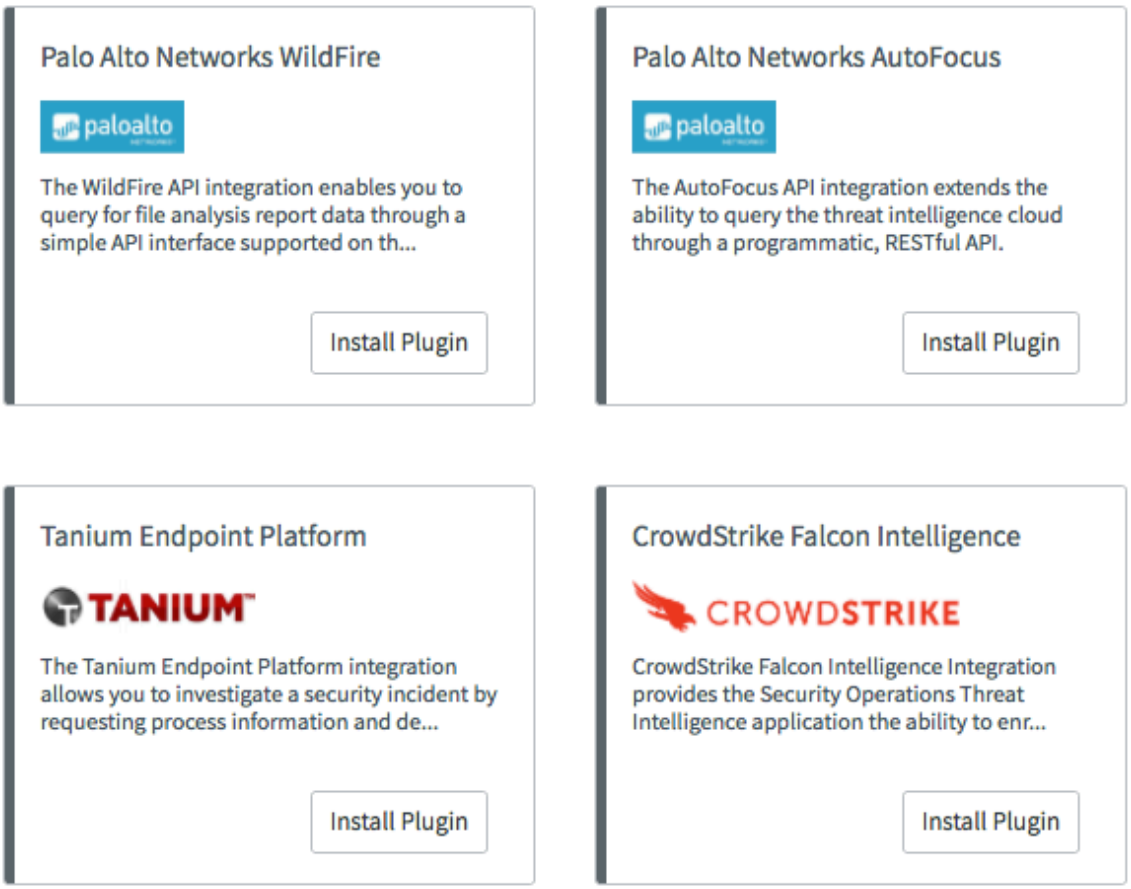
Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões, semelhante ao grupo de cartões a seguir. Você pode apontar para qualquer cartão para obter uma descrição da integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Para instalar o plug-in de uma determinada integração, clique em **Instalar plug**-in .

a. No formulário Plug-in do sistema, revise os detalhes do plug-in e clique no link relacionado **Ativar/Fazer upgrade**.

b. Clique em **Ativar**.
Quando a ativação estiver concluída, a tela de integração de segurança será reaberta e o botão da integração que você ativou será rotulado como **Configurar**.

3. Clique em **Configurar**.

Nota: Se você estiver configurando o Qualys Vulnerability Integration, consulte Instalação de Resposta a vulnerabilidades e aplicações compatíveis.

4. Insira a **chave de API**.

5. Clique em **Enviar**.

Criar uma integração

Você pode criar uma integração e adicionar o cartão de integração associado à tela Integrações de segurança. Este procedimento se destina a parceiros que criam integrações de terceiros.

Antes de Iniciar
Função necessária: sn_sec_cmn.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Público:parceiros que criam integrações de terceiros.

Procedimento

1. No filtro de navegação, digite sn_sec_core_integration_item.list e pressione a tecla **Enter**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Nome	O nome da integração.
ID do plug-in	O plug-in que deve ser ativado para usar a integração.
Ordem	Indica a ordem em que este cartão de integração aparece.
Texto da faixa	Clique no link, selecione uma imagem ou logotipo para aparecer no cartão de integração e clique em **OK**.
Instalado	Campo somente leitura que indica se o plug-in já foi instalado.
Configurável	Indica se você pode configurar a integração.
Categorias	Usado para filtrar os cartões de integração.
Descrição resumida	Uma descrição da integração que aparece na dica de dica da ferramenta do cartão.
Descrição	Uma descrição mais longa da integração.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A lista relacionada **Integração e configurações** é exibida. Você pode usar esta lista relacionada para definir opções de configuração para a integração. Essas opções aparecem quando você clica no botão **Configuração** no cartão de integração associado.
5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme o apropriado.

Campo	Descrição
Rótulo	O nome do item de integração.
Nome	O plug-in que deve ser ativado para usar a integração.
Integração	Exibe a integração para a qual você está definindo itens de integração
Ordem	Indica a ordem em que este item de integração aparece.
Tipo	Na lista, selecione o tipo de campo: ◦ Cadeia de caracteres ◦ Inteiro ◦ Decimal ◦ Data ◦ Booliano ◦ Senha

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ IPv4 ◦ IPv6 ◦ URL
Valor	Insira o valor associado ao **Tipo** selecionado. Se um valor inválido para o **tipo** selecionado for inserido, nenhum registro será recuperado quando a integração for executada. Por exemplo, se você selecionar o tipo de URL e inserir um valor de 12.32.23.10, nenhum registro será recuperado.

7. Clique em **Enviar**.

Dicas para escrever integrações

Evite algumas das dificuldades que você pode encontrar ao escrever suas próprias integrações seguindo estas diretrizes.

Use a funcionalidade da plataforma ServiceNow sempre que possível

Em geral, os recursos de integração incorporados às aplicações [Operações de segurança (Security Incident Response, Inteligência contra ameaçase Resposta a vulnerabilidades) têm como objetivo aprimorar ou simplificar a funcionalidade de integração da plataforma ServiceNow existente. Ao escrever integrações, certifique-se sempre de usar a funcionalidade da plataforma quando ela existir. Aqui estão algumas funcionalidades ServiceNow comuns que podem ser usadas em vez de "rodar por conta própria".

- Serviços web de saída - para a maioria das interações com sistemas de terceiros, a comunicação é por meio de serviços web. Nesses casos, utilize os serviços web de saída da plataforma (REST e SOAP são compatíveis).
- Fontes de dados/conjuntos para importação/mapa de transformação – para processar dados e inserir em tabelas ServiceNow, o mecanismo preferencial é usar fontes de dados e componentes associados.

Use estruturas de integração de Operações de segurança sempre que possível

Como Operações de segurança os mecanismos de integração resolveram muitos problemas comuns, não é necessário reimplementar as funcionalidades básicas para cada integração. Por exemplo, os dados de vulnerabilidade e as estruturas de origem da ameaça oferecem suporte à manipulação de várias páginas e à transmissão desses dados para fontes de dados/transformações/conjuntos para importação. Da mesma forma, a estrutura de origem de verificação ou pesquisa fornece a funcionalidade de limitação de taxa configurável. Como regra, ao implementar um recurso ou conjunto de recursos, verifique se a estrutura de integração Operações de segurança existente cobre seu caso de uso. Em caso afirmativo, use essa estrutura.

Estenda as estruturas de integração de Operações de segurança existentes conforme necessário

A maioria das tabelas e scripts usados pelas estruturas de integração Operações de segurança foram estendidas para atender às necessidades futuras. Se um caso de uso for encontrado enquanto você estiver gravando uma integração, estenda uma tabela de integração ou script para se adequar melhor a esse caso de uso.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fornecer feedback à ServiceNow sobre problemas encontrados durante a integração

Como uma integração está sendo desenvolvida ou testada, certifique-se de fornecer feedback quando forem encontrados problemas. Mesmo que uma solução alternativa seja necessária, a equipe Suporte e atendimento ao cliente pode fornecer uma melhoria em versões futuras que podem aliviar o problema em integrações futuras.

Teste com carga razoável

Um problema comum com integrações é que elas não estão equipadas para lidar com cargas realistas. Como cada integração é uma aplicação com escopo, há mais limitações impostas pela plataforma para garantir a estabilidade do sistema. Essas limitações podem resultar no encerramento de trabalhos de longa execução ou chamadas de API. Você pode garantir que processos de longa execução ou processos que processam muitos dados sejam tratados normalmente, reduzindo o tempo que cada chamada ou processo leva (geralmente fornecendo um meio de paginar solicitações de API ou agrupar grandes conjuntos de dados).

Solução de problemas de integração

Essas sugestões de solução de problemas podem ajudar a resolver problemas comuns que você pode encontrar ao configurar ou executar integrações.

Substitua um certificado SSL de terceiros não confiável ou expirado

Quando uma conexão SSL é necessária em uma integração, há circunstâncias em que o certificado fornecido pelo fornecedor de terceiros ainda não é confiável em ServiceNow ou expirou. Você pode substituí-lo ou adicionar um novo certificado.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira a URL do endpoint na barra de endereço do navegador.
      Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM no sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
      Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou na área de transferência anteriormente.
5. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Estrutura de capacidades de integrações 2.0

A nova Estrutura de capacidades de integração 2.0 foi redesenhada para permitir a implementação de integrações de maneira simples e consistente. Isso garante uma experiência consistente para tipos semelhantes de integrações (por exemplo: pesquisa de reputação de observável).

A nova estrutura tem capacidades implementadas usando fluxos .

Os benefícios da implementação da estrutura aprimorada incluem:

- Os fluxos de capacidade que incluem somente componentes de nível de negócios sem qualquer lógica específica de implementação.
- Os fluxos de capacidade agora aceitam uma ampla matriz de entradas e formatos para máxima flexibilidade (por exemplo, referências observáveis, referências de IC, tarefas, qualquer tabela ou combinações de sys_id).
- A limitação ou limitação de taxa nas execuções de integração agora é fácil de configurar (removendo a necessidade de fazer isso usando código personalizado ou mudanças nos fluxos de trabalho de implementação).
- As capacidades aprimoradas de auditoria e acompanhamento de execução agora permitem melhores relatórios e uma solução de problemas mais fácil.
- Funções robustas de manipulação de erros são integradas aos fluxos de capacidade para evitar a duplicação de rotinas de implementação.
- Capacidade de configurar o gatilho condicional das capacidades ou das integrações. Isso fornece flexibilidade para iniciar automaticamente automações com base na categoria de incidente.
- Uma condição de filtro padrão foi introduzida em todas as capacidades para filtrar observáveis permitidos listados antes que as entradas sejam fornecidas para as integrações.

Nota: Esta nova estrutura de capacidades não atualiza a estrutura de capacidades atual. Ambas as estruturas podem funcionar em paralelo. Para obter instruções sobre como aproveitar a nova estrutura de capacidades, consulte Como usar o novo Capability Framework com uma integração instalada e Como usar o novo Framework de capacidade com um fluxo.

Integrações e componentes compatíveis

O plug-in Security Incident Response inclui todos os fluxos de capacidade listados no Integration Capabilities Framework 2.0 e filtros padrão de alto nível que você pode habilitar ou desabilitar dependendo dos seus requisitos.

Nota: Se você quiser usar o novo Capability Integration Framework com a versão New York, deverá instalar o plug-in ServiceNow IntegrationHub Starter Pack Installer. Entre em contato com o Suporte ao cliente para obter assistência com a instalação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões da aplicação compatíveis

A partir do Security Incident Response 10.0, as seguintes integrações são compatíveis:

Aplicação	Versão mínima necessária
Integração de análise híbrida de Operações de segurança	10.0.0
Security Operations PhishTank Integration	10.0.0
Security Operations ThreatCrowd Integration	10.0.0
Integração do CrowdStrike Intelligence com as Operações de segurança	10.0.0
Operações de segurança "Have I Been Pwned?" Integração	10.0.0
Integração do Metadefender das Operações de segurança	10.0.0
Integração futura registrada de Operações de segurança	10.0.0
Security Operations VirusTotal Integration	10.0.0
Integração com Reverse Whols das Operações de segurança	10.0.0

A partir do Security Incident Response 10.4, as seguintes integrações são compatíveis:

Aplicação	Versão mínima necessária
Security Operations RiskIQ Integration	10.0.0
Integração com o Shodan das Operações de segurança	10.0.0
Integração de Whols das Operações de segurança	10.0.0
Security Operations Carbon Black Integration	10.3.1
Integração de pesquisa do Splunk de Operações de segurança	10.3.0
Security Operations ArcSight Logger Integration	10.3.0
Security Operations McAfee ESM Integration	10.3.0
Security Operations Elasticsearch Integration	10.3.0
Security Operations IBM QRadar Integration	10.3.1
Host do CrowdStrike Falcon das Operações de segurança	10.3.0

Componentes incluídos

O novo Capability Integration Framework inclui os seguintes componentes:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Capacidades**: todas as seguintes capacidades que existem no produto hoje como fluxos de trabalho foram reprojetadas usando Fluxos :
  - **Solicitação de bloqueio**: fornece uma maneira de bloquear observáveis associados a um incidente de segurança em um firewall, proxy da web ou algum outro ponto de controle. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.
  - **Pesquisa e exclusão de e-mail**: fornece uma maneira de pesquisar um servidor de e-mail durante uma investigação de segurança e, se necessário, excluir e-mails do servidor.
  - **Aprimorar item de configuração**: fornece uma maneira geral de aprimorar itens de configuração com informações adicionais de várias fontes. Essa capacidade é usada durante as investigações de resposta do incidente para aprimorar os dados associados a um incidente de segurança.
  - **Aprimorar observável**: fornece uma maneira geral de aprimorar observáveis com informações adicionais de várias fontes. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.
  - **Ingestão de eventos**: fornece uma maneira geral de criar um incidente de segurança mapeando eventos de uma origem de integração para um incidente de segurança.
  - **Obter estatísticas de rede**: recupera uma lista de conexões de rede ativas de um endpoint ou host. Essa capacidade é usada para aprimoramento de incidentes durante as investigações.
  - **Obter processos em execução**: recupera uma lista de processos em execução de um endpoint ou host. Essa capacidade é usada para aprimoramento de incidentes durante as investigações.
  - **Isolar host**: fornece uma maneira de isolar um endpoint ou um host associado a um incidente de segurança. O isolamento de host é executado em um item de configuração (IC).
  - **Publicar na lista**de observação: fornece uma maneira de adicionar observáveis associados a um incidente de segurança a uma lista de observação que monitora eventos de segurança e gera alertas. Essa capacidade é usada como parte da resposta do incidente durante as investigações.
  - Pesquisa de detecções: pesquisa vários**SIEMs**ou outros armazenamentos de log para instâncias de observáveis. Esta capacidade é usada para determinar a presença de IoCs mal-intencionados em seu ambiente.
  - **Pesquisa de ameaças**: executa pesquisas de inteligência contra ameaças para determinar se um determinado observável está associado a uma ameaça à segurança conhecida. Essa capacidade é usada como parte da resposta do incidente durante as investigações.
- **Novas tabelas**:
  - sn_sec_cmn_capability: capacidade e fluxo que implementa a capacidade.
  - sn_sec_cmn_capability_implementation: o fluxo de implementação real que fornece os serviços da capacidade.
  - sn_sec_cmn_capability_execution: o registro de execução de uma capacidade no tempo de execução.
  - sn_sec_cmn_capability_implementation_execution: o registro de execução de uma implementação de capacidade no tempo de execução.
  - sn_sec_cmn_filter_condition: as condições de filtro que podem ser aplicadas no tempo de execução à capacidade ou a uma implementação de capacidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Incluir script**: CapabilityProcessor: lida com todo o código de processamento da estrutura.
- **Limite de taxa**: capacidade máxima de solicitações simultâneas por período: define quantas integrações podem ser executadas em paralelo.
- **Implementação da capacidade do processo de trabalho programado**: é executada a cada 15 segundos e pode ser desabilitada na página Propriedades de administração de segurança (**Incidente de segurança** > **Administração** > **Propriedades**.
  - Habilita ou desabilita o trabalho agendado, implementações de capacidade de processo: este trabalho programa e gerencia automaticamente os fluxos de execução de implementação de capacidade.
  - Habilita ou desabilita pesquisas ou aprimoramentos automatizados: configuração que ativa ou desativa o trabalho agendado que executa a pesquisa automatizada de ameaças ou o aprimoramento de observáveis quando observáveis são adicionados a incidentes de segurança na estrutura de capacidades atual.
  - Habilita ou desabilita o trabalho agendado, Pesquisar observáveis de incidentes de segurança: este trabalho programa automaticamente uma pesquisa de ameaças ou um trabalho de aprimoramento de observáveis quando observáveis são adicionados a um incidente de segurança.

Configurações no novo Framework de capacidade

Esta seção descreve as configurações disponíveis na nova estrutura.

Antes de Iniciar

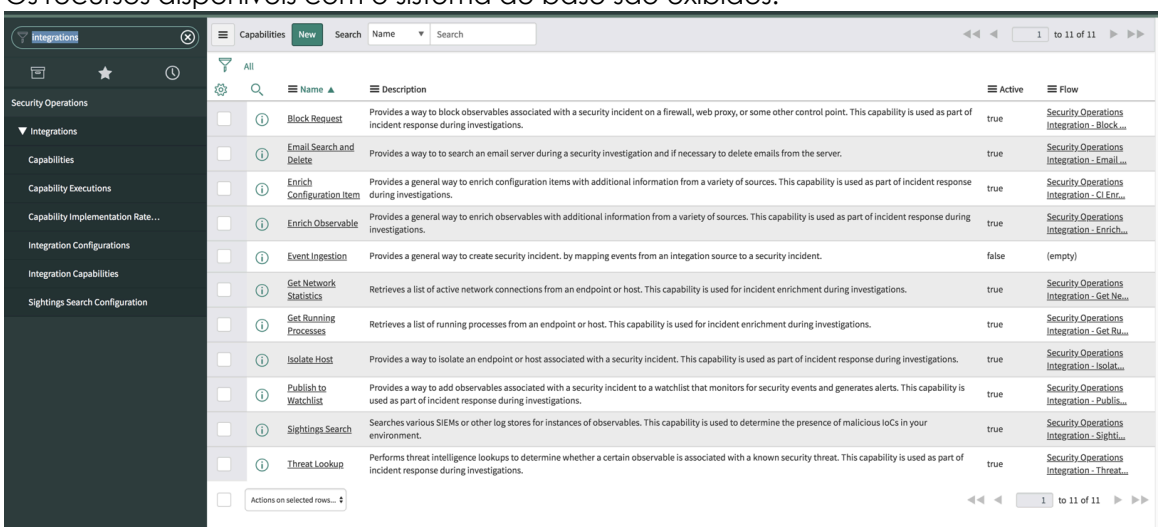
Função necessária: sn_si.admin, flow_designer, action_designer

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Integrações** > **Capacidades**.

   Nota: Versão 10.4: a partir do Security Incident Response 10.4, o nome do menu **Capacidades** foi alterado para **Capacidades de integração (Fluxos)**.

2. Os recursos disponíveis com o sistema de base são exibidos.



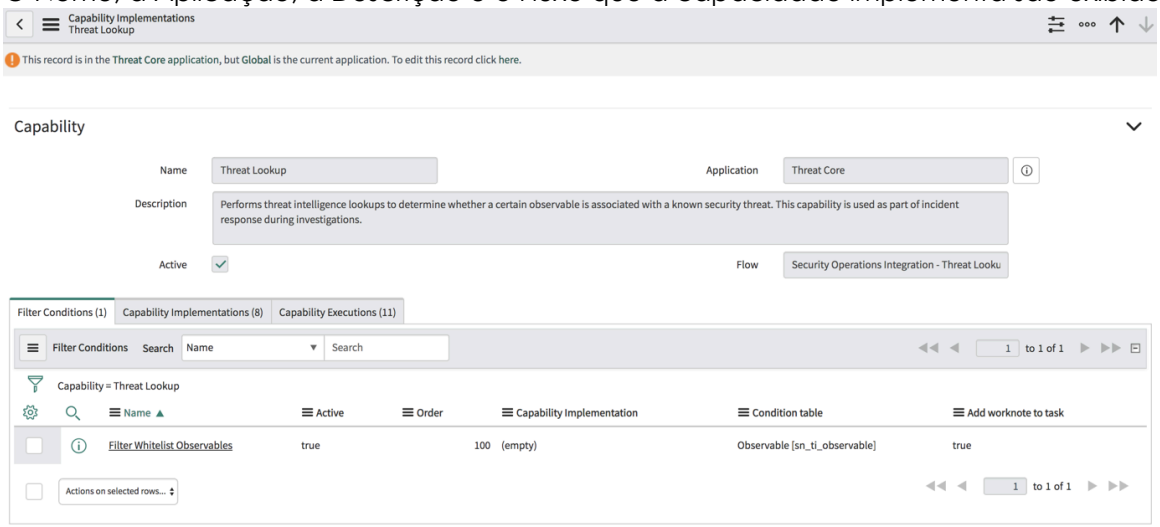
Nota:

Esses são os recursos fornecidos com o sistema de base. Você pode usar os recursos ou personalizá-los conforme necessário. As etapas a seguir descrevem como configurar uma capacidade e as integrações implementadas para a capacidade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

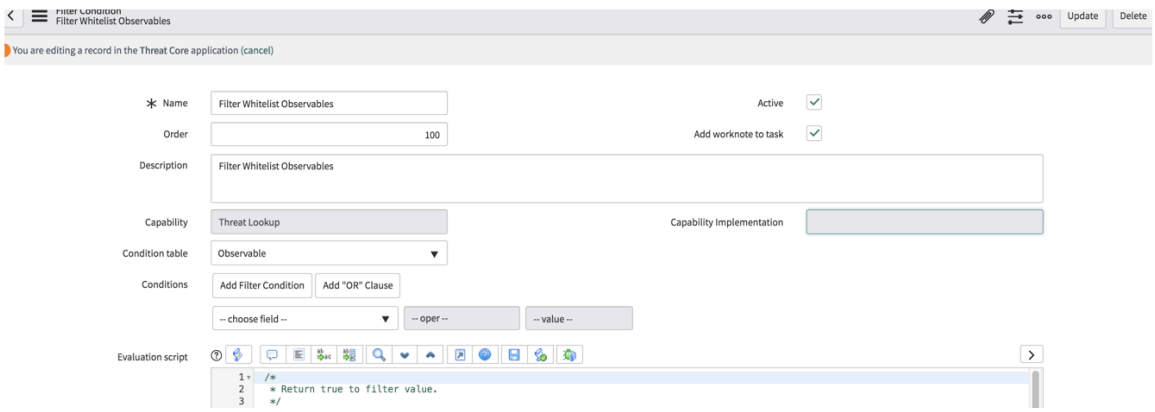
3. Clique no link na coluna Nome para configurar uma capacidade.
   O Nome, a Aplicação, a Descrição e o Fluxo que a capacidade implementa são exibidos.



4. Marque a caixa de seleção **Ativo** para ativar a capacidade.

   - **Condições de filtro no nível de capacidade**: quando uma capacidade de integração implementa um fluxo, as condições de filtro associadas ao fluxo são executadas antes que o fluxo de capacidade seja iniciado. Por exemplo, a capacidade Pesquisa de ameaças inclui a condição Filtrar observáveis na lista de permissões, conforme mostrado acima. Clique no link Nome para editar a condição do filtro.

     Nota: Marque a caixa de seleção **Adicionar anotação de trabalho à tarefa** para adicionar anotações de trabalho e incluir informações sobre as condições de filtro usadas.



   Você pode definir condições de filtro, um script ou uma combinação de ambos. No exemplo acima, um script é usado para definir as condições do filtro. Quando o fluxo de capacidade é executado, o script pesquisa observáveis da lista de permissões e os remove da tabela.

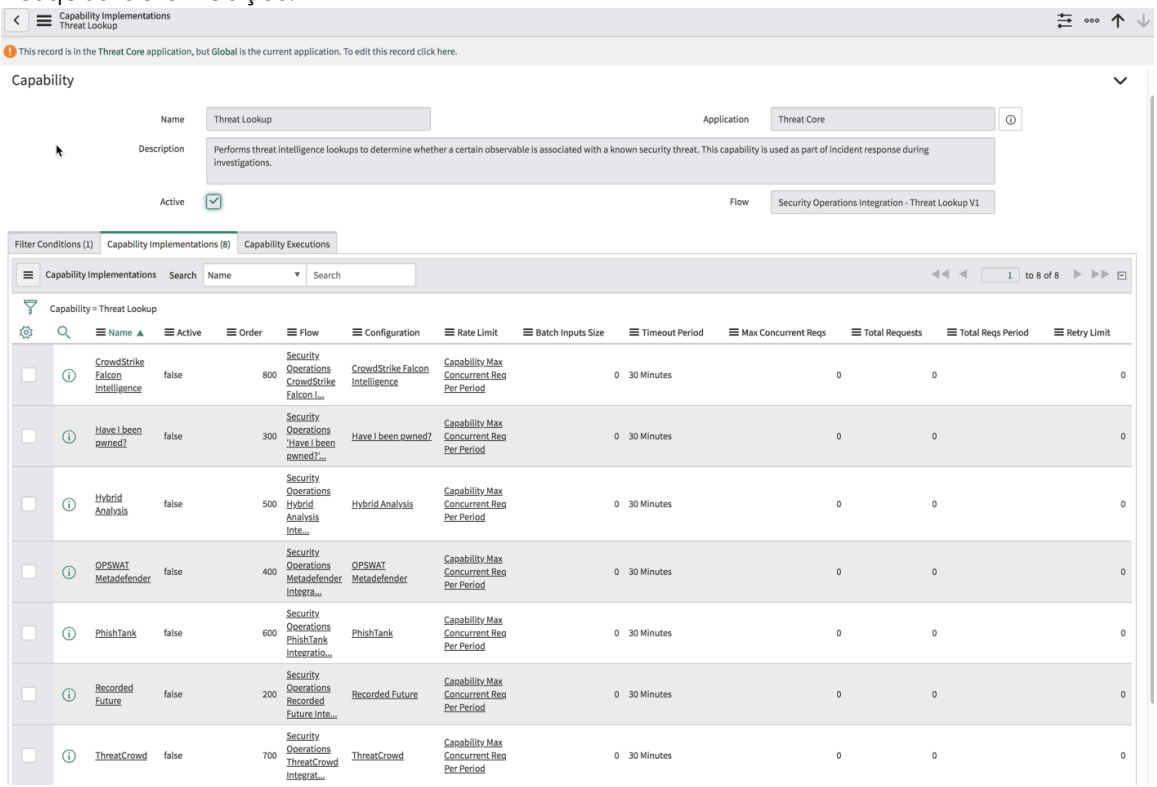
   Nota: As condições de filtro definidas aqui são aplicáveis a todas as integrações ativas definidas na guia **Implementações de capacidade**.

   - **Implementações de capacidade**: clique na guia **Implementações de capacidade**. As implementações (integrações) que foram configuradas para a capacidade são

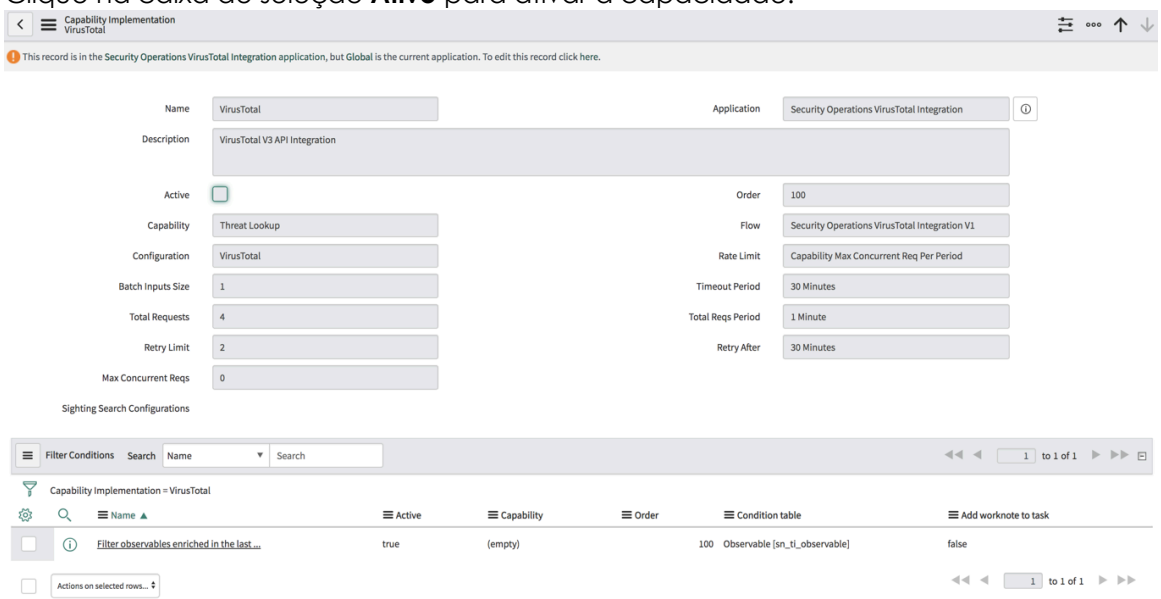
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

exibidas. O exemplo abaixo mostra as integrações configuradas para a capacidade Pesquisa de ameaças:



5. Clique no link Nome para exibir a Implementação da capacidade.
   O Nome, a Aplicação, a Descrição e o Fluxo que a capacidade implementa são exibidos.
6. Clique na caixa de seleção **Ativo** para ativar a capacidade.



Você pode especificar os seguintes detalhes:

Nome do Campo	Descrição
Ativo	Marque esta caixa de seleção para habilitar e desabilitar esta integração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

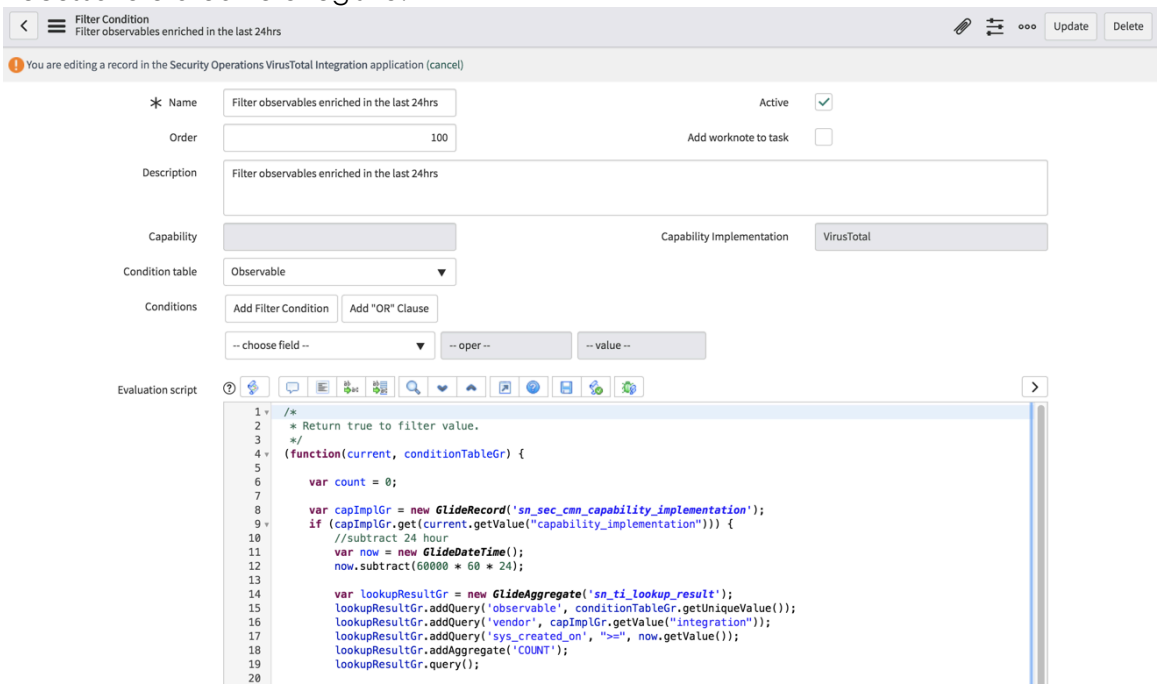
Nome do Campo	Descrição
	Nota: Se você configurar esta integração usando o bloco de integração no **Operações de segurança** > **Integrações** > **Configurações de integrações**página, este sinalizador é definido automaticamente como **Ativo**.
Ordem	Indica a ordem na qual as integrações são executadas.
Capacidade	A capacidade implementada por esta integração.
Fluxo	O subfluxo que implementa a capacidade.
Configuração	A configuração de integração para esta capacidade. **Nota:** Isso é definido inicialmente com a configuração padrão fornecida com o sistema de base. Quando uma integração é configurada usando o bloco de integração na página **Configurações** de integração, esse valor é redefinido automaticamente para a nova configuração criada.
Limite de Taxa	Indica o número de integrações que podem ser executadas em tempo de execução (em paralelo ou por unidade de tempo).
Tamanho das Entradas em Lote	O tamanho da entrada em lote para cada execução. Por exemplo, para uma integração de pesquisa de detecções, convém agrupar os observáveis em lotes de 50 para que as consultas geradas não se tornem muito grandes. 0 indica que não há limite.
Período de tempo limite	A duração máxima antes que o fluxo de implementação da capacidade seja cancelado. 0 indica que não há período de tempo limite.
Total de solicitações	O número total de solicitações de execução de implementação. Este campo, em conjunto com o campo Período total de solicitações, pode ser usado para limitar o número de solicitações ao serviço. Por exemplo, você pode limitar o número a 4 solicitações por minuto.
Período de solicitações total	O número total de solicitações de execução permitidas por período.
Limite de novas tentativas	O número de novas tentativas permitidas para uma solicitação de execução com falha. Este limite será aplicável se o sinalizador **Repetir** estiver definido em sua integração para tentar novamente uma solicitação de execução quando uma condição for atendida. Por exemplo, uma solicitação de nova tentativa é feita quando você excede o limite de licença para esse serviço por um período de tempo ou o serviço está inativo.
Tente novamente após	O período após o qual é feita uma tentativa de tentar novamente uma solicitação de execução com falha.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
Máximo de Solicitações Simultâneas	O número máximo de solicitações de execução de implementação simultâneas. 0 indica que não há limite.
Configurações de Pesquisa de detecções	As consultas de pesquisa de detecções padrão que podem ser executadas.

Clique no link Nome na seção Condições do filtro para configurar as condições definidas para a implementação. Adicione ou exclua condições de filtro, modifique o script se necessário e atualize o registro.



Como usar o novo Capability Framework com uma integração instalada

Esta seção descreve como usar a nova estrutura para uma integração existente.

Use as etapas abaixo para habilitar uma integração já instalada e configurada (consulte a lista de integrações compatíveis em Integrações e componentes compatíveis) para usar a nova estrutura de capacidade.

Nota: A Estrutura de capacidade de integração 2.0 disponível com o Security Incident Response 10.0.2 oferece suporte a implementações para as capacidades **Pesquisa de ameaças** e **Aprimorar observável**. As implementações de outras capacidades serão disponibilizadas em uma versão futura.

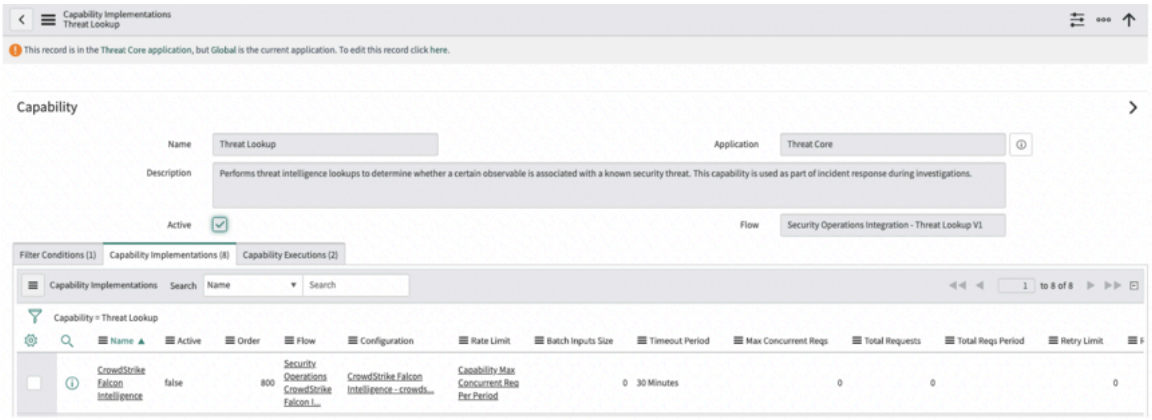
Antes de começar

- Função necessária: sn_si.admin
- Security Incident Response 10.0.2

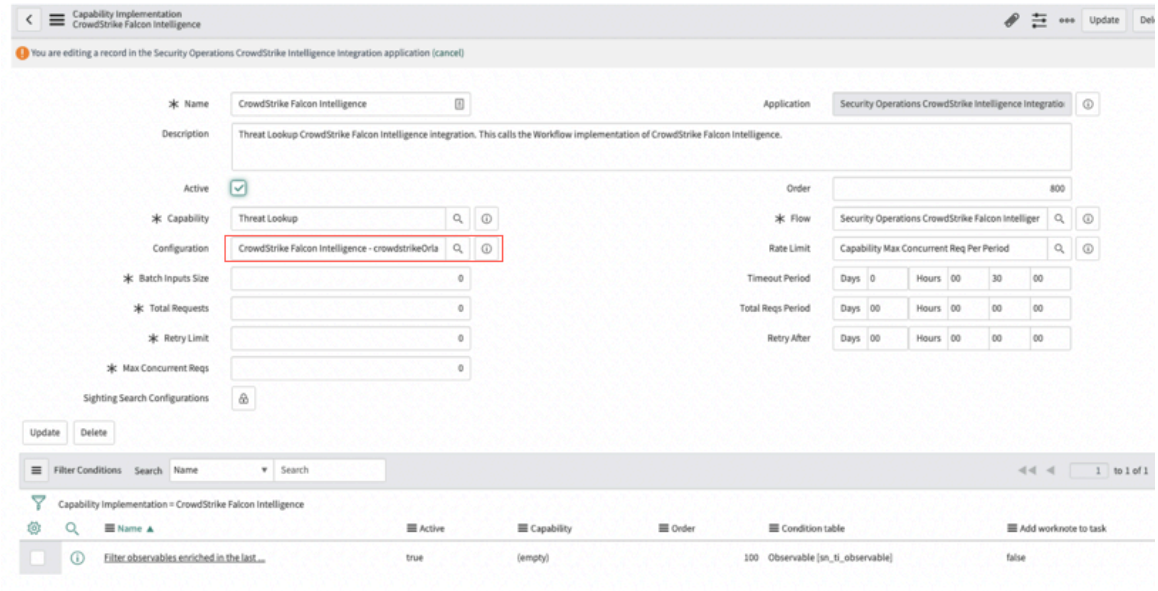
1. Navegar até **Operações de segurança** > **Integrações** > **Capacidades**.
2. Clique na capacidade **Pesquisa de ameaças**.
3. Clique na guia Implementação de capacidades.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



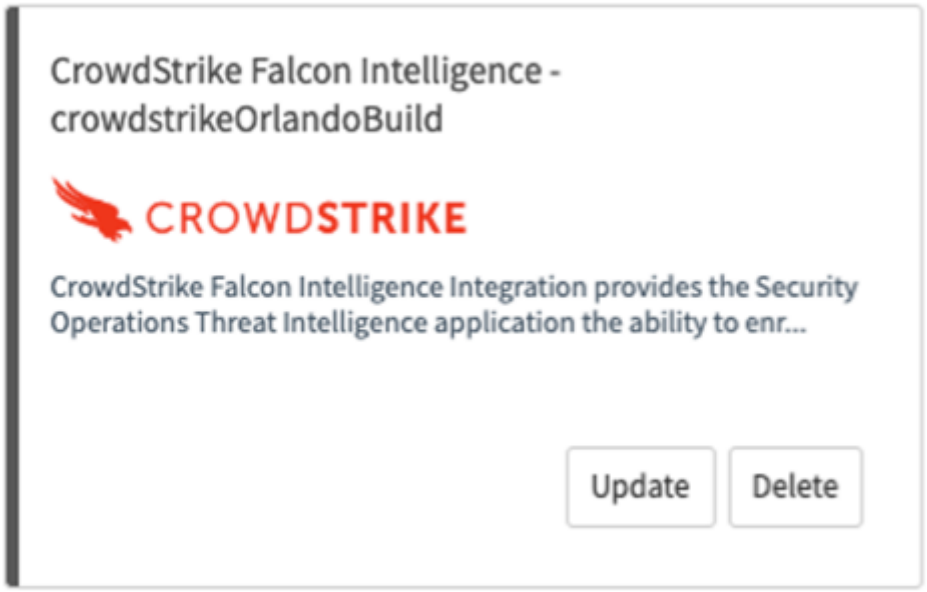
4. 4. Exiba o registro de implementação de capacidade da integração de interesse (exemplo: Crowdstrike Falcon Intelligence). A coluna **Ativa** deve ter o valor **Falso**.
5. Clique no link **Nome** para exibir o registro de implementação.



6. Marque a caixa de seleção **Ativo**.
7. Certifique-se de que o registro de implementação esteja apontando para o registro de configuração correto (o nome do bloco da integração em **Configurações de Integração** > **Mostrar configurações (sim)**).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. A implementação está habilitada para uso com a nova estrutura.

Nota: Todas as integrações compatíveis quando instaladas com o Security Incident Response 10.0.2 serão habilitadas automaticamente na nova estrutura de capacidade de integração.

Como usar o novo Framework de capacidade com um fluxo

Use as etapas abaixo para criar um fluxo e chamar o subfluxo fornecido pela nova estrutura de capacidade.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer, action_designer
- Instale uma das integrações compatíveis (consulte Integrações e componentes compatíveis)

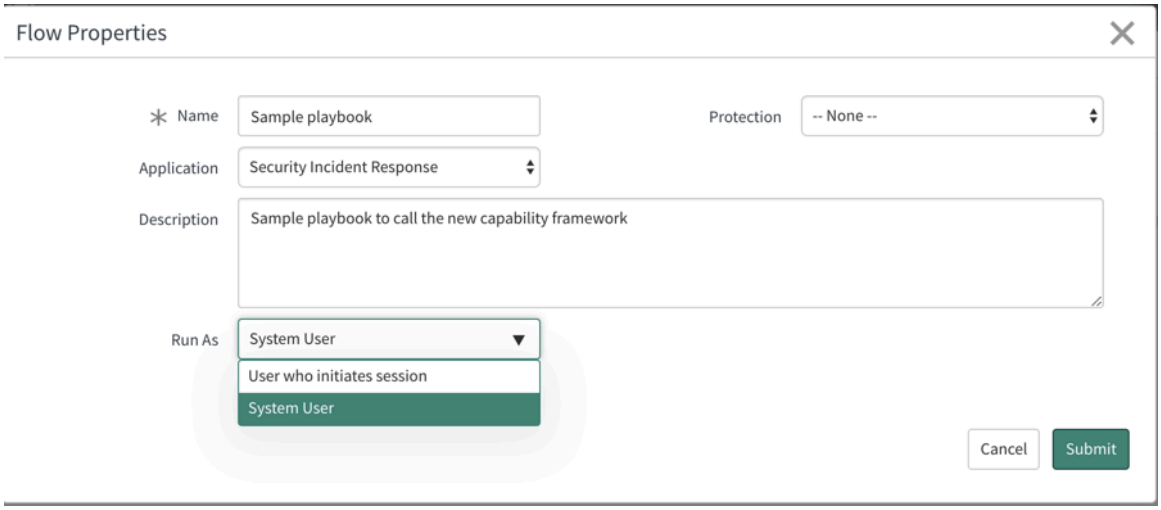
As etapas abaixo descrevem como criar um fluxo de amostra e chamar um dos subfluxos fornecidos com a nova estrutura de capacidade.

Procedimento

1. Navegar até **Todos** > **Flow Designer** > **Designer**.
2. Clique em **Novo** para criar um novo fluxo e forneça as informações necessárias para as propriedades.

Tradução automática

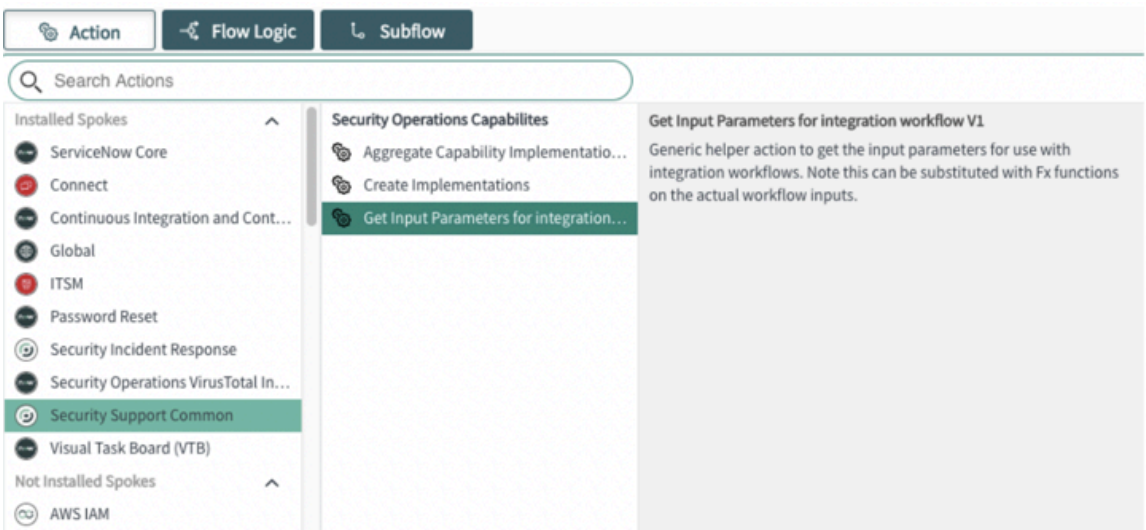
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Selecione **Usuário do sistema** na lista de seleção Executar como, conforme mostrado na imagem acima.

3. Selecione uma condição de gatilho para o fluxo (um gatilho comum é a criação de um registro de incidente de segurança para uma determinada categoria de incidente).

4. Na etapa 1 do fluxo, selecione uma ação para obter entradas do incidente de segurança (por exemplo, observáveis).
Você pode selecionar uma ação das ações fornecidas com o sistema de base com o Spoke comum de suporte de segurança.



5. Na etapa 2, selecione um subfluxo (por exemplo, Pesquisa de ameaças).

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Configure o subfluxo selecionado conforme mostrado abaixo:

7. Salve e publique o fluxo.

Solução de problemas de fluxos de capacidade de integração

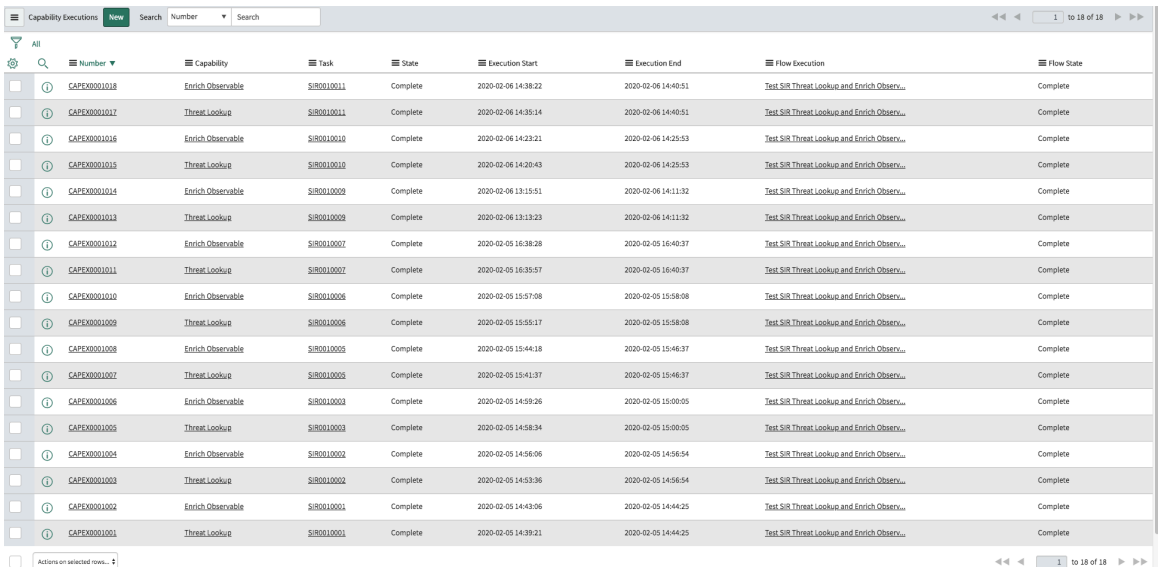
A opção Execuções de capacidade fornece informações detalhadas sobre cada capacidade que foi executada.

Nota: As execuções concluídas são arquivadas após 30 dias.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Operações de segurança** > **Integrações** > **Execuções de capacidade.**.



2. Clique no link Execuções de capacidade para exibir detalhes adicionais.

Anotações de trabalho do registro de incidente de segurança

Quando observáveis são adicionados a um incidente de segurança e a condição do gatilho para o fluxo é atendida, os subfluxos Pesquisa de ameaças e Aprimorar observável são iniciados e as seguintes anotações de trabalho são adicionadas ao incidente de segurança:

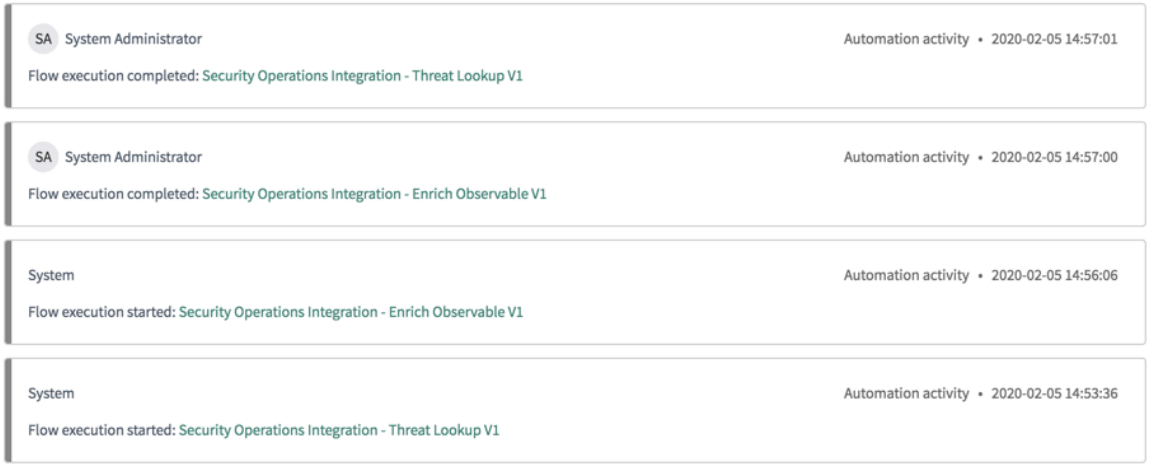
- Execução de fluxo iniciada: Integração de Operações de segurança - Enriquecer observável V1
- Execução de fluxo concluída: Integração de Operações de segurança - Enriquecer observável V1
- Execução de fluxo iniciada: Integração de Operações de segurança – Pesquisa de ameaças V1
- Execução de fluxo concluída: Integração de Operações de segurança – Pesquisa de ameaças V1

Para exibir essas anotações de trabalho, faça login como um usuário com as *funções sn_si.admin* ou *sn_si.analyst* e *flow_designer* e *action_designer*.

Navegue até a página de registro do incidente de segurança e clique nessas anotações de trabalho para exibir os detalhes da execução do fluxo.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



REST APIs para integração de terceiros com Operações de segurança

O sistema base Operações de segurança inclui uma série de REST APIs com script que permitem que clientes e parceiros se integrem facilmente a uma implantação Operações de segurança existente. As APIs permitem coletar dados de fora do seu sistema (por exemplo, um script Python é usado para receber dados do VirusTotal) e enviá-los de volta para sua instância.

Scripts escritos em praticamente qualquer linguagem (Python, por exemplo) podem ser usados com as APIs para executar processos específicos do cliente. Os scripts devem ser escritos em uma linguagem capaz de fazer uma pós-chamada HTTP externa. Por exemplo, se você tiver uma aplicação Java, deverá usar uma biblioteca, como o pacote `java.net.HttpUrlConnection`, para construir uma chamada HTTP e passar uma cadeia de caracteres JSON como corpo da mensagem.

A API é usada exclusivamente para adicionar dados que foram coletados fora do nosso sistema. Por exemplo, se você inseriu o script python do VT e recebeu dados do VT, poderá enviar esses dados de volta para a instância do SN.

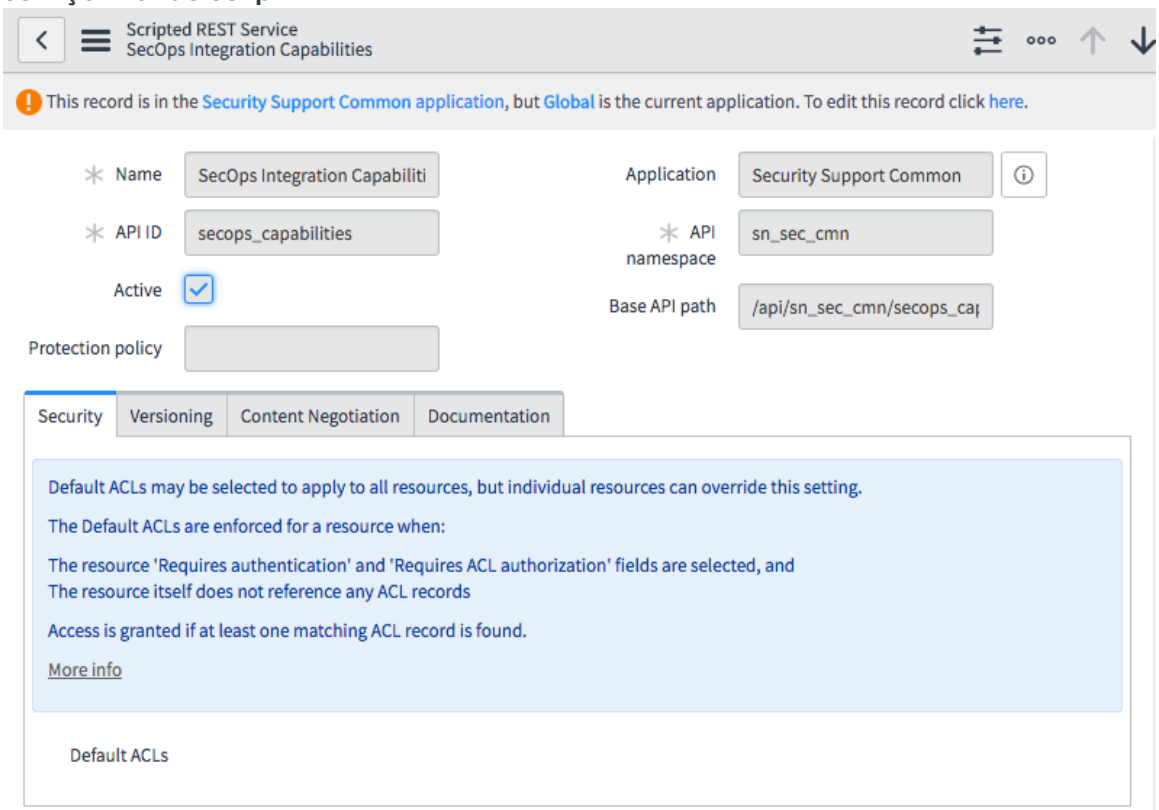
Autenticação

Todas as operações nas definições de API usam a autenticação de plataforma fornecida pelo Recurso de operação deScripted REST APIs . Para acessar, navegue até **Serviços web do sistema** > **Serviços web com script** > **Scripted REST APIs** e localize a API **de capacidades de integração de SecOps**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Serviço REST de Script



O usuário e o domínio do usuário estão prontamente disponíveis no contexto da API. Os registros podem ser vinculados a um usuário, um caminho de auditoria a ser estabelecido e a separação de domínio realizada. Além disso, como você foi autenticado como um usuário específico, pode usar Usando GlideRecordSecure para impedir o acesso não autorizado aos dados.

Autorização

Para proteger o processo de criação de registros de usuários fora da aplicação Operações de segurança, você deve ter a função sn_sec_cmn.api_write. Somente usuários com esta função podem acessar as APIs.

Parâmetros de solicitação de configuração

Os seguintes parâmetros de solicitação estão disponíveis.

Nome	Padrão	Descrição
ignore_mandatory_fields	falso	Se definido como verdadeiro, o registro persistirá mesmo se os campos obrigatórios não forem preenchidos.
include_wrap	falso	Se definido como verdadeiro, a resposta incluirá o wrapper padrão fornecido pela instância para Scripted REST APIs.
resposta_simples	falso	Se definido como verdadeiro, a resposta incluirá somente se a operação foi bem-sucedida.

Respostas de erro

As seguintes respostas de erro podem ocorrer.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem de erro	Quando isso ocorre?	Solução
Acesso insuficiente	O usuário não tem a função sn_sec_cmn.api_write.	Adicione a função ao usuário.
Corpo de publicação inválido	O corpo da solicitação está vazio ou é um objeto vazio.	Em conformidade com a definição da API.
Nenhum campo fornecido	Os campos de dados fornecidos para persistir estão vazios.	Em conformidade com a definição da API.
Campos obrigatórios ausentes: x, y,z	Os campos obrigatórios estão ausentes.	Em conformidade com a definição da tabela de destino ou defina **ignore_mandatory_fields** como verdadeiro.
Não é possível manter o registro	Não é possível manter o registro analisado.	Falha ao inserir GlideRecord(). É necessária uma análise mais aprofundada.
Erro desconhecido	Ocorre se nenhum caminho de erro conhecido tiver sido seguido.	É necessária uma análise mais aprofundada.

Caso de uso de aprimoramento de IC

Usando seus scripts de terceiros, você pode gravar na tabela Aprimoramento de item de configuração [sn_sec_cmn_ci_enrichment_result] para aprimoramento de IC. Os registros de aprimoramento são baseados em capacidades existentes que fornecem informações detalhadas sobre um registro de uma fonte de terceiros.

Solicitação de amostra e respostas para o caso de uso de aprimoramento de IC são mostradas aqui.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar-solicitação para aprimoramento de IC


```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


Criar resposta para enriquecimento de IC


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


Caso de uso de aprimoramento de observável

Usando seus scripts de terceiros, você pode gravar na tabela Resultado de aprimoramento de observável `[sn_ti_observable_enrichment_result]` para aprimoramento de observável. Os registros de aprimoramento são baseados em capacidades existentes que fornecem informações detalhadas sobre um registro de uma fonte de terceiros.

A amostra de solicitação e respostas para o caso de uso de aprimoramento do observável é mostrada aqui.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar-solicitação para enriquecimento de observável

```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```

Criar resposta para enriquecimento de observável

```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```

Nota: Além de aprimorar os registros existentes, você também pode usar Operações de segurança mapeamento de dados de aprimoramento para adicionar novos registros às tabelas, passando em um **richment_mapping_id** para um mapeamento de aprimoramento existente e uma cadeia de caracteres **bruta_data** correspondente que pode ser analisada pelo processo de mapeamento.

Caso de uso de pesquisa de ameaças

Usando seus scripts de terceiros, você pode gravar na tabela Resultado da pesquisa de ameaças [sn_ti_lookup_result] para obter os resultados da pesquisa de ameaças. Os

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

registros de pesquisa são baseados em capacidades existentes que fornecem informações detalhadas sobre um registro de uma fonte de terceiros.

A amostra de solicitação e respostas para o caso de uso de pesquisa de ameaças é mostrada aqui.

Criar-solicitação para pesquisas de ameaças


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar resposta para pesquisas de ameaças


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Capacidades de integração

A estrutura Capacidades de integração fornece uma arquitetura consistente para oferecer suporte à interoperabilidade com integrações de terceiros. Essa interface e modelo de dados abstratos isolam as integrações de mudanças na aplicação principal e garantem uma experiência consistente para tipos semelhantes de integrações.

Cada capacidade de integração persiste na tabela Capacidade de integração `[sn_sec_cmn_integration_capability]`. Os fluxos de trabalho da capacidade de integração não podem ser executados sozinhos e exigem o início de um fluxo de trabalho de implementação. Qualquer plug-in que fornece uma implementação da capacidade adiciona sua implementação à tabela secundária: Implementação da capacidade de integração `[sn_sec_cmn_integration_capability_implementation]`.

A implementação especifica o fluxo de trabalho a ser executado, a integração relacionada (ID do plug-in) e a capacidade que ele implementa. Esses fluxos de trabalho podem ser executados em paralelo usando o inicializador de fluxo de trabalho paralelo; no entanto, a execução sequencial é o padrão no sistema de base. Se necessário, você pode alterar a ordem de execução.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Integração de Operações de segurança - Capacidade de solicitação de bloqueio

A capacidade Bloquear Ação bloqueia observáveis associados a um incidente de segurança em um firewall, proxy da web ou outro ponto de controle, usando fluxos de trabalho de implementação. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A capacidade Solicitação de bloqueio tem um fluxo de trabalho, Integração de Operações de segurança - Fluxo de trabalho de solicitação de bloqueio, que executa a solicitação para bloquear. Este fluxo de trabalho aceita uma lista de observáveis, encontra capacidades de implementação e executa a solicitação com base no fluxo de trabalho configurado.

A capacidade também usa outras implementações:

- Integração de Operações de segurança Palo Alto Networks Fluxo de trabalho do inicializador de firewall
- Operações de segurança Palo Alto Networks - Fluxo de trabalho Verificar e bloquear valor

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Executar bloqueio de solicitação

Bloqueia a comunicação com observáveis associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

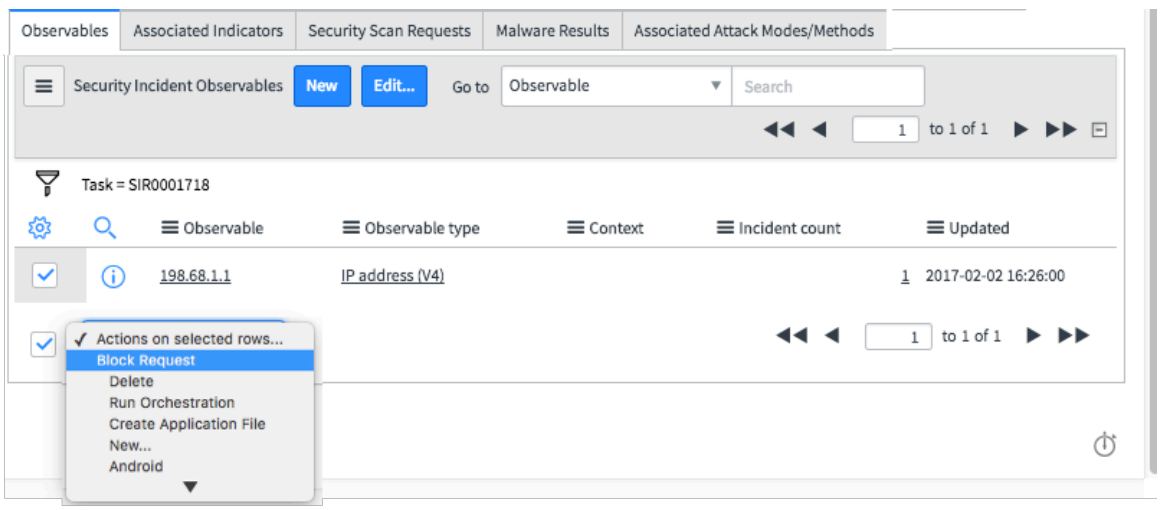
Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

O fluxo de trabalho **Integração de Operações de segurança - Solicitação de bloqueio**pode ser acionado a partir de um formulário de observável ou da lista relacionada **de observáveis** de incidente de segurança em um incidente de segurança.

Este exemplo mostra uma solicitação de bloqueio de um incidente de segurança.

Procedimento

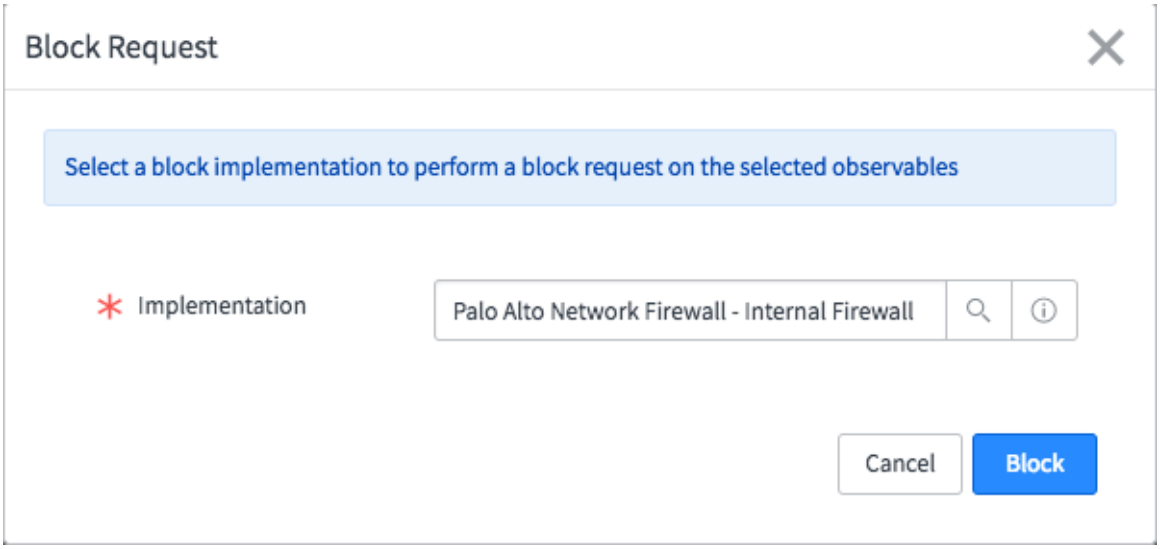
1. Navegue até um incidente de segurança.
2. Selecione observáveis na guia **Lista relacionada**.
3. Clique em **Bloquear solicitação** no menu suspenso **Ações em linhas selecionadas....**



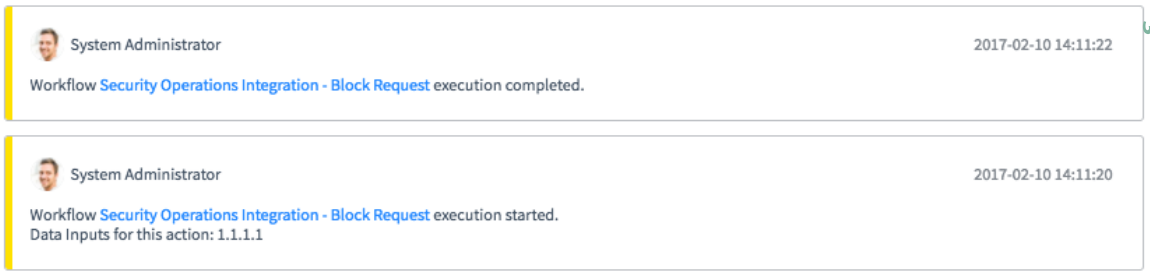
A caixa de diálogo é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Escolha a implementação.
5. Clique **em Bloquear**.
   A auditoria de execução do fluxo de trabalho é exibida na seção de anotações de trabalho.



Integração de Operações de segurança - Fluxo de trabalho de solicitação de bloqueio

O fluxo de trabalho Integração de Operações de segurança - Solicitação de bloqueio é um fluxo de trabalho de alto nível independente de integrações. Ele bloqueia observáveis associados a um incidente de segurança. Use-o para atender a uma integração como Palo Alto Networks - Firewall.

Antes de Iniciar

Função necessária: sn_si.analyst

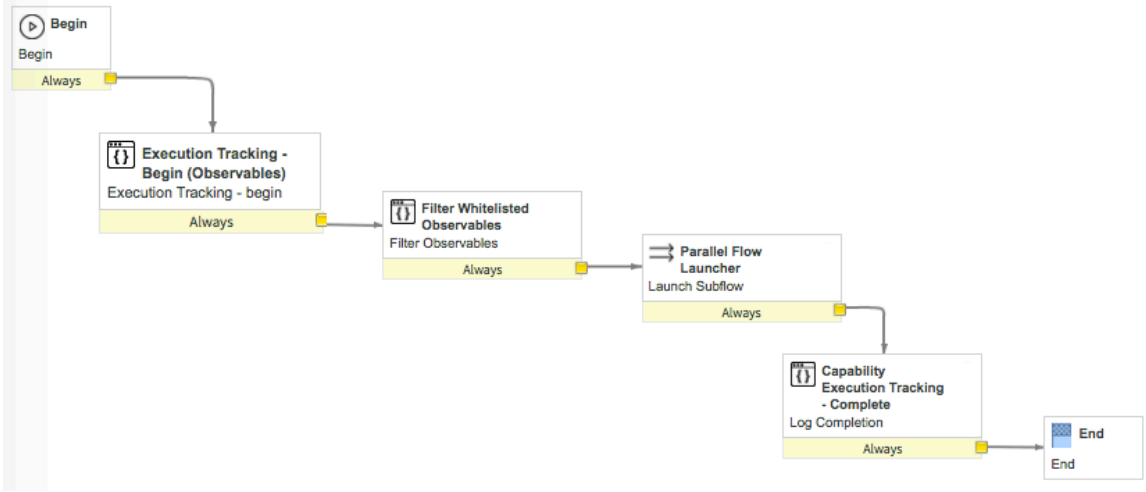
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Integração de Operações de segurança - Solicitação de bloqueio**pode ser acionado em um formulário de observável ou na lista relacionada **de observáveis** de incidente de segurança em um incidente de segurança. Em uma lista, ele está no menu suspenso de ação. Em um formulário, é um link relacionado. O bloqueio de uma solicitação está disponível somente quando você tem uma implementação instalada para a capacidade de solicitação de bloqueio.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bloquear Solicitação



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Integração de Operações de segurança - Capacidade de pesquisa e exclusão de e-mail

A capacidade Pesquisar e excluir e-mail retorna o número de e-mails de ameaça de uma pesquisa de servidor de e-mail e, opcionalmente, retorna detalhes de cada e-mail encontrado. Depois que a pesquisa de e-mail for concluída, você poderá excluir os e-mails.

A capacidade Pesquisa e Exclusão de E-mail tem um fluxo de trabalho que executa os processos de pesquisa e exclusão de e-mail.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto. Além disso, se nenhuma das implementações da capacidade de **pesquisa e exclusão de e-mail** estiver ativa, o link relacionado à **pesquisa** de e-mail em um incidente de segurança não será exibido.

Integração de Operações de segurança - Fluxo de trabalho de pesquisa e exclusão de e-mail

O fluxo de trabalho Integração de Operações de segurança - Pesquisar e excluir e-mail retorna o número de e-mails de ameaça de uma pesquisa de servidor de e-mail e, opcionalmente, retorna detalhes de cada e-mail encontrado. Depois que a pesquisa de e-mail for concluída, você poderá excluir os e-mails.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

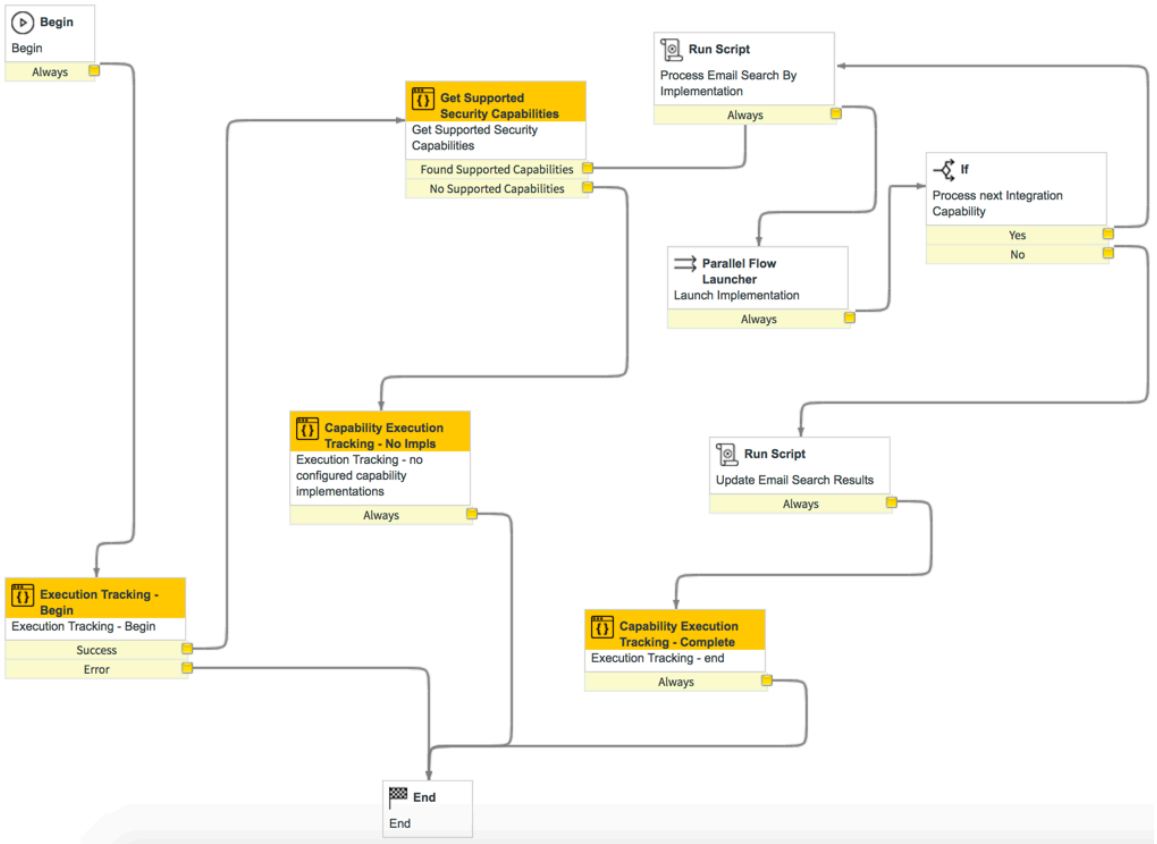
A consulta de pesquisa pode levar algum tempo para ser concluída. Depois que a contagem é recebida, a aprovação é necessária para excluir e-mails de um servidor de e-mail.

Este fluxo de trabalho é acionado pelos botões **Excluir do(s) servidor(es)** de e **-mail e Pesquisar no(s)** servidor(es) de e-mail no formulário **Pesquisa** de e-mail em um incidente de segurança. Para obter mais informações, consulte Pesquisar e excluir e-mails de phishing.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa e Exclusão de E-mails



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades do processo de fluxo de trabalho incluem:

Atividade Início do acompanhamento de execução (pesquisa de e-mail)

A atividade de execução da capacidade Acompanhamento de execução - Iniciar (pesquisa de e-mail) cria um registro de acompanhamento de execução e marca o estado do registro como Iniciado. Esta atividade é usada por todos os fluxos de trabalho de capacidade e implementação para acompanhar seu estado.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O registro de acompanhamento de execução foi criado.
Falha	Não foi possível criar o registro de acompanhamento de execução.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
Id da implementação	Identificador do sistema da implementação da capacidade de integração que está sendo executada.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch.
emailsearchId	O sysid do registro de pesquisa de e-mail na tabela Pesquisa de e-mail [sn_sec_cmn_email_search].

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capabilityExecutionId	Identificador do sistema do registro de acompanhamento de execução.

- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações

Integração de Operações de segurança - Capacidade de IC aprimorada

A capacidade Aprimorar IC permite aprimorar dados para itens de configuração associados a um incidente de segurança.

A capacidade **Aprimorar IC** tem um fluxo de trabalho, Integração de Operações de segurança - Fluxo de trabalho de aprimoramento de IC. Quando o fluxo de trabalho de capacidade é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar o enriquecimento nos ICs selecionados ou pode executar o enriquecimento usando todas as implementações.

Nota: Esses dados aprimorados não são o tipo de dados que você deseja armazenar no seu CMDB, pois são dados forenses específicos para uma determinada investigação - por exemplo, executar um memdump de um IC. Em vez disso, os dados são armazenados na tabela Aprimoramento de item de configuração [sn_sec_cmn_ci_enrichment_result].

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de Operações de segurança - Fluxo de trabalho de aprimoramento de IC

O fluxo de trabalho Integração de Operações de segurança - Aprimoramento de IC permite aprimorar dados em itens de configuração (IC) associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

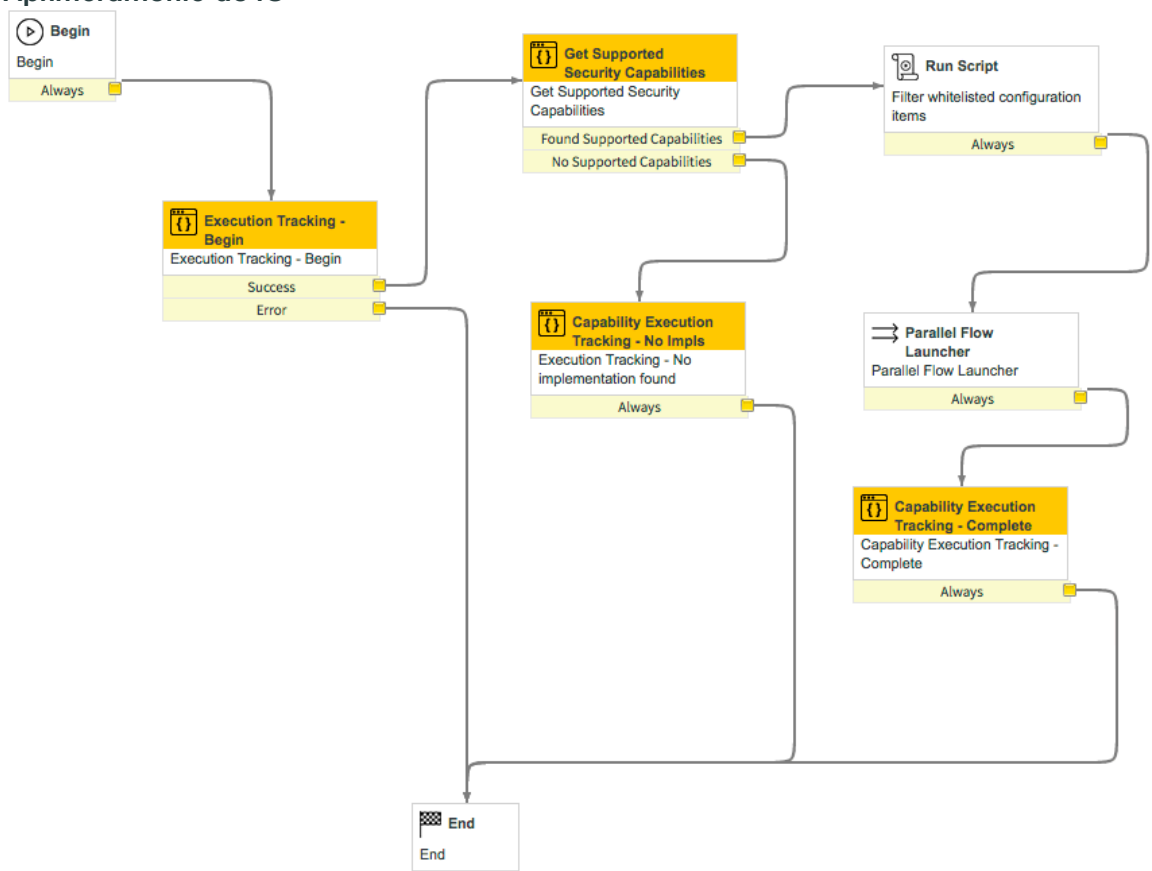
Este fluxo de trabalho é acionado a partir de Security Incident Response de duas maneiras.

- selecionando um ou mais ICs na guia **Itens de configuração** (no link relacionado **Itens afetados**) e selecionando **Executar aprimoramento de IC** na lista de seleção **Ações nas linhas selecionadas**.
- abrindo um registro de IC e clicando no link relacionado **Executar aprimoramento de IC**.

Qualquer um dos métodos permite que você especifique quais implementações serão usadas para aprimorar os ICs selecionados. Os fluxos de trabalho de implementação associados são executados para realizar o aprimoramento.

Nota: O sistema base não inclui um fluxo de trabalho de implementação para esta capacidade. Para aprimorar ICs, você deve criar seu próprio fluxo de trabalho de implementação.

Aprimoramento de IC



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades do processo de fluxo de trabalho incluem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Acompanhamento de execução - Iniciar atividade
- Integração de Operações de segurança - Fluxo de trabalho de aprimoramento de IC
- Acompanhamento de execução de capacidade - atividade sem implementações
- Atividade Obter capacidades de segurança compatíveis

Integração de Operações de segurança - Capacidade de aprimorar observável

A capacidade Aprimorar observável permite aprimorar observáveis com informações adicionais de várias fontes usando fluxos de trabalho de implementação. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.

A capacidade Aprimorar observável tem um fluxo de trabalho, Integração de Operações de segurança - fluxo de trabalho Enriquecer observável. Quando o fluxo de trabalho de capacidade é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar o enriquecimento nos observáveis selecionados ou pode executar o enriquecimento usando todas as implementações que correspondem aos tipos de observável compatíveis.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Integração de Operações de segurança - fluxo de trabalho Enriquecer observável

O subfluxo Integração de Operações de segurança - Aprimorar observável permite aprimorar observáveis com informações adicionais de várias fontes usando o Flow Designer de implementação.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho pode ser acionado a partir de Security Incident Response ou Inteligência contra ameaças de duas maneiras.

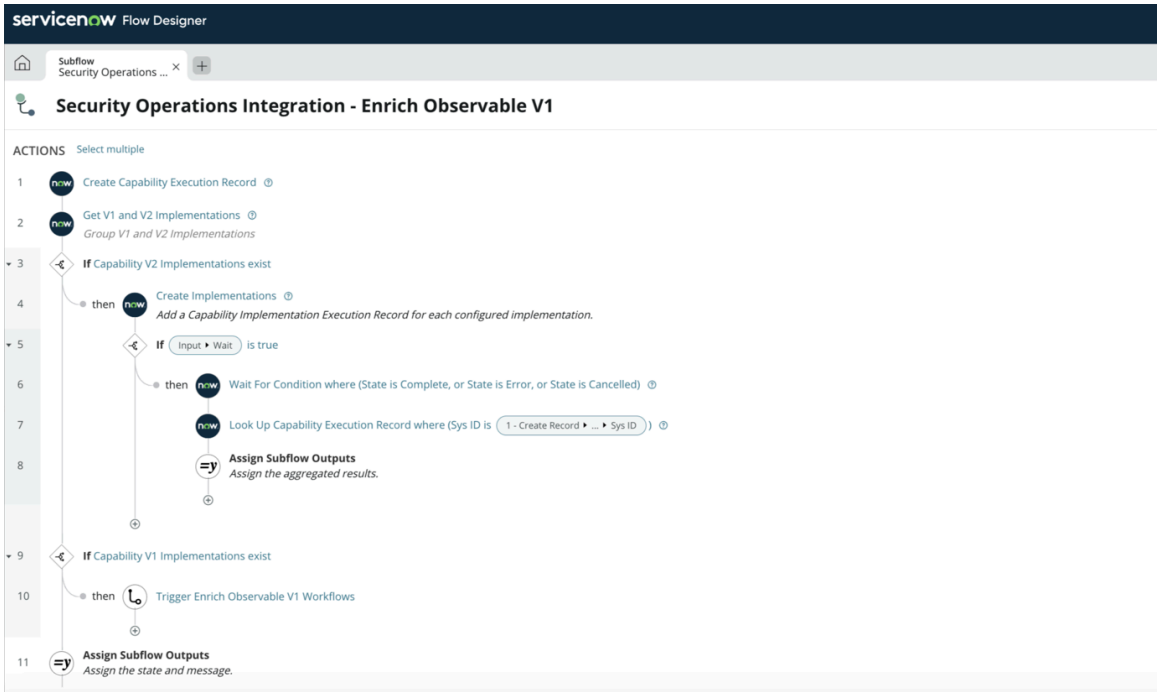
- selecionando um ou mais observáveis na lista Observáveis e selecionando **Executar aprimoramento** de observável na lista de seleção **Ações nas linhas selecionadas**.
- abrindo um registro de observável e clicando no link relacionado **Executar aprimoramento de observável**.

Qualquer um dos métodos permite que você especifique quais implementações serão usadas para aprimorar os observáveis selecionados. Os fluxos de trabalho de implementação associados são executados para realizar o aprimoramento.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprimorar Observável



As atividades específicas para este fluxo são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução de capacidade - atividade sem implementações
- Atividade Obter capacidades de segurança compatíveisAcompanhamento de execução de capacidade - atividade sem implementações

Capacidade de Integração de Operações de segurança - Obter estatísticas de rede

A capacidade Obter estatísticas de rede recupera uma lista de conexões de rede ativas de um host ou endpoint. Ele pode ser usado para enriquecimento de incidentes durante as investigações. Esta capacidade é acionada automaticamente quando um item de configuração é adicionado a um incidente de segurança.

A capacidade **Obter estatísticas de rede** tem um fluxo de trabalho, Integrações de operações de segurança - Fluxo de trabalho Obter estatísticas de rede que aceita um ou mais ICs e tarefas. O fluxo de trabalho itera sobre cada implementação e cada IC e invoca novamente o fluxo de trabalho de implementação.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Integrações de operações de segurança - Fluxo de trabalho Obter estatísticas de rede

O fluxo de trabalho Integrações de operações de segurança - Obter estatísticas de rede recupera uma lista de conexões de rede ativas de um host ou endpoint.

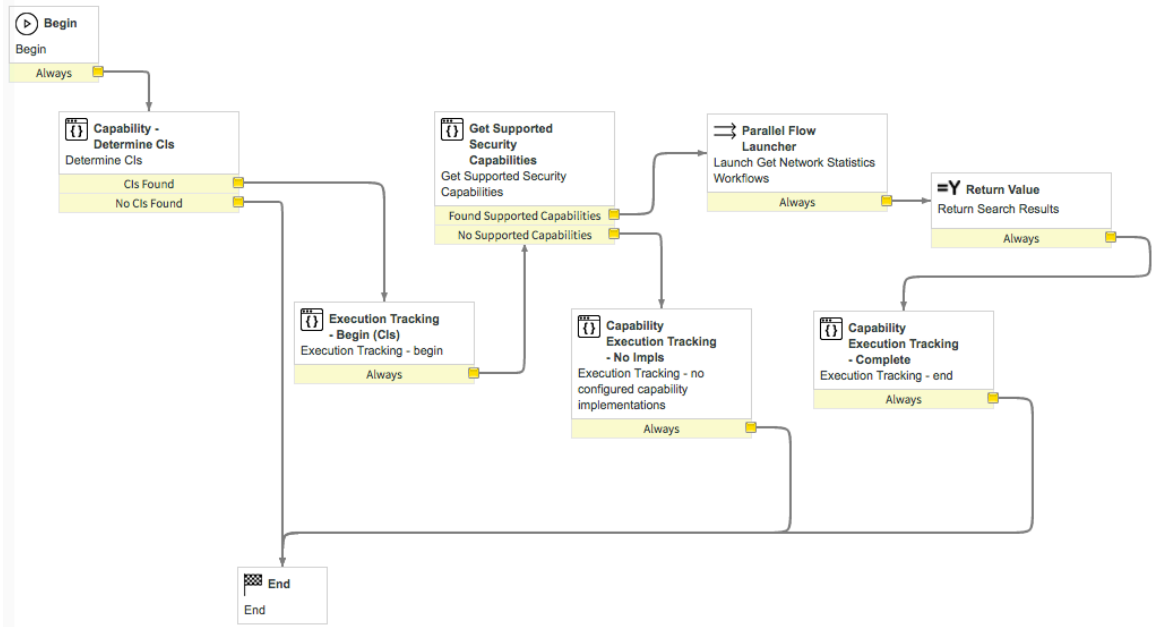
Antes de Iniciar
Função necessária: sn_si.analyst

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é executado automaticamente quando um item de configuração é adicionado a um incidente de segurança.

Obter estatísticas de rede



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades de fluxo de trabalho incluem:

- Atividade Capacidade - Determinar ICs
-

.

Acompanhamento de execução - Atividade Iniciar (ICs)

A atividade de fluxo de trabalho **Acompanhamento de execução - Início (ICs)** inicia o processo de auditoria para um fluxo de trabalho de integração Operações de segurança que opera em itens de configuração (ICs).

A atividade **Acompanhamento de execução - Início (ICs)** pode ser usada com qualquer fluxo de trabalho de IC para começar a registrar o andamento do fluxo de trabalho em uma auditoria.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria foi criado.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
isImpl	Sinalizador que especifica se a auditoria é feita para um fluxo de trabalho de capacidade de integração ou um fluxo de trabalho de implementação de capacidade de integração. Os valores possíveis são: • falso - indica auditoria em um fluxo de trabalho abstrato da capacidade de integração, como Pesquisa de detecções. (padrão.) • verdadeiro - denota auditoria em um fluxo de trabalho de implementação da capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.

listaci	Um ou mais itens de configuração (IC) para executar a ação desejada no seguinte formato:
	`["sysId", "sysId"]`
	ou
	`"sysId"`
	Usado como uma entrada de fluxo de trabalho.

workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capabilityExecutionId	Identificador do sistema do registro de auditoria.

As atividades do processo de fluxo de trabalho incluem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações

Fluxo de trabalho do Security Incident Response - Obter estatísticas de rede

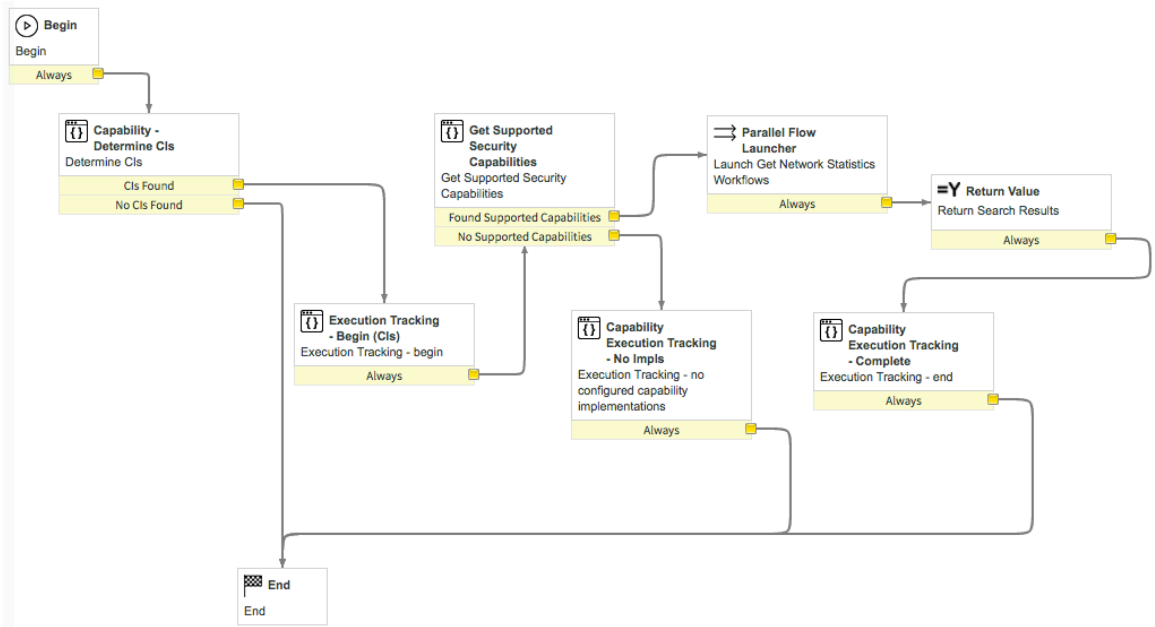
O **Resposta a incidentes de segurança** > **Obter estatísticas de rede** O fluxo de trabalho recupera as estatísticas de rede de um recurso baseado no Windows afetado quando adicionado a um incidente de segurança no estado **Análise**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Para novos incidentes de segurança que contêm itens de configuração, o fluxo de trabalho é executado automaticamente quando o estado muda para **Análise**.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

Obter estatísticas de rede



As atividades do processo de fluxo de trabalho incluem:

Atividade Obter FQDN do item de configuração

Determinar script de shell por sistema operacional

Se a instrução for executada pelo PowerShell

Acompanhamento de execução - Iniciar atividade

Obter estatísticas de rede por meio da atividade netstat

Acompanhamento da execução da capacidade - Atividade com falha

Atividade Criar registros de dados de aprimoramento

Acompanhamento da execução da capacidade - Atividade com falha - Retorna o ID de aprimoramento.

Acompanhamento da execução da capacidade - Concluir atividade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração (computador, servidor ou semelhante).
4. Clique em **Atualizar**.
   Orquestração do Security Incident Response fornece informações de estatísticas de rede no **Links relacionados** > **Aprimoramentos de incidentes de segurança** guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

   As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Capacidade de Obter processos em execução da Integração de Operações de segurança

A capacidade Obter processos em execução recupera uma lista de processos em execução em um item de configuração (IC) de um host ou endpoint. Essa capacidade é usada para aprimoramento de incidentes durante as investigações.

A capacidade Obter processos em execução tem dois fluxos de trabalho de implementação :

- Integração do Carbon Black das Operações de segurança - Obter fluxo de trabalho dos processos em execução
- Integração de comandos do sistema de operações de segurança - Obter fluxo de trabalho de processos em execução

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Operações de segurança - Obter fluxo de trabalho de processos em execução

O fluxo de trabalho Operações de segurança - Obter processos em execução é um fluxo de trabalho de alto nível independente de integrações. Ele recupera uma lista de processos em execução em um item de configuração (IC) de um host. Use-o para atender a uma integração, como Carbon Black, ou para um incidente de segurança baseado no Windows.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

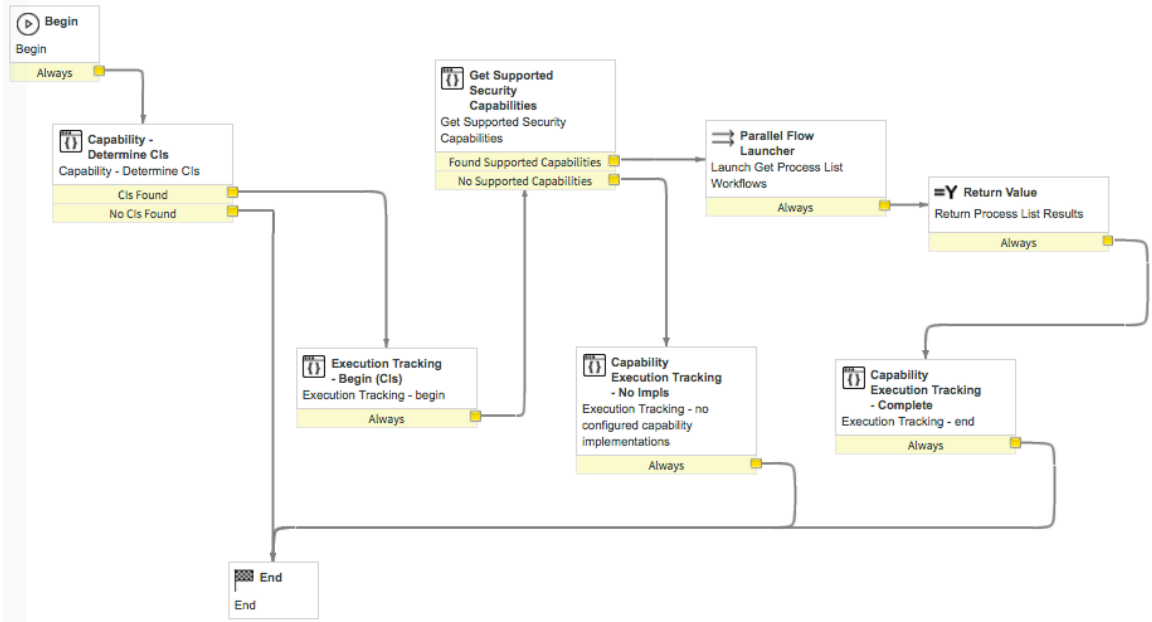
- Atividade Capacidade - Determinar ICs
- Acompanhamento de execução - Atividade Iniciar (ICs)
- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Inicializador de fluxo paralelo - retorna os resultados da pesquisa em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividade

Obter processos em execução



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Integração do Carbon Black das Operações de segurança - Obter fluxo de trabalho dos processos em execução

A integração do Carbon Black das Operações de segurança - Obter processos em execução é a implementação da integração do Carbon Black iniciada pelo fluxo de trabalho Integração das operações de segurança - Obter processo em execução.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

As atividades do processo de fluxo de trabalho incluem:

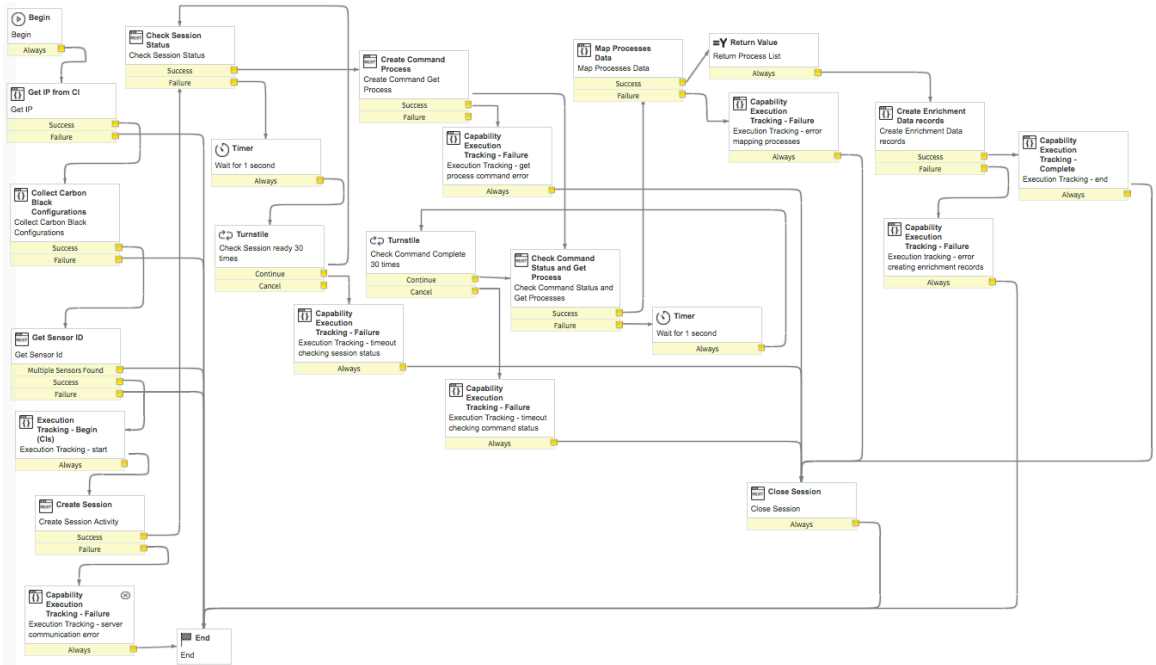
- Obter IP da atividade de IC
- Atividade Coletar configurações de Carbon Black
- Atividade Obter ID do sensor
- Acompanhamento de execução - Iniciar atividade
- Criar Sessão
- Acompanhamento da execução da capacidade - Atividade com falha
- Atividade Verificar status da sessão
- Atividade de fluxo de trabalho Temporizador - Aguarda 1 segundo
- Atividade de fluxo de trabalho da catraca - Verificar se a sessão está pronta 30 vezes
- Atividade Criar processo de comando
- Atividade Verificar status do comando e obter processo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atividade Mapear dados de processos e lista de processos de retorno
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento da execução da capacidade - Concluir atividade
- Atividade Fechar sessão

Obter processos em execução do Carbon Black



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Coletar configurações de Carbon Black

A atividade de fluxo de trabalho Coletar configurações de carbono preto reúne informações de configuração a serem usadas no fluxo de trabalho.

A atividade Coletar configurações do Carbon Black reúne informações de configuração do Carbon Black para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Não há variáveis de entrada para esta atividade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.
api_token	Chave de API de integração de terceiros.

Verificar status do MID Server

Determina se o MID Server identificado no campo **Host do MID Server** da configuração da integração está instalado e em execução. Se o campo estiver definido como **Qualquer**, a atividade verificará se o MID Server está instalado e em execução.

A atividade Verificar status do MID Server pode ser usada com qualquer fluxo de trabalho para verificar a presença de um MID Server em execução no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Status da sessão retornado.
Falha	Erro de status da sessão. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityExecutionId	O ID da capacidade que está sendo executada.
workflowName	O nome do fluxo de trabalho que está sendo executado.
mid_server_host	O MID Server identificado na configuração da integração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
mid_server_live	Identifica se o MID Server identificado no campo **Host do MID Server** da configuração da integração está instalado e em execução. Se o campo

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
	estiver definido como **Qualquer**, a atividade verificará se o MID Server está instalado e em execução.

Atividade Obter ID do sensor

A atividade de fluxo de trabalho Obter ID do sensor reúne identificadores de sensor a serem usados no fluxo de trabalho.

A atividade Obter ID do sensor pode ser usada com qualquer fluxo de trabalho para coletar informações do sensor a serem usadas no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensores encontrados.
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ci_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detalhe	Descrição do sensor Carbon Black no formato JSON.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Criar sessão

A atividade de fluxo de trabalho Criar sessão estabelece uma sessão de Carbon Black para usar no fluxo de trabalho.

A atividade Criar sessão pode ser usada com qualquer fluxo de trabalho para criar uma sessão de Carbon Black dentro do fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sessão criada.
Falha	Sessão não criada. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Atividade Verificar status da sessão

Determina o status de uma sessão de Carbon Black no fluxo de trabalho.

A atividade Verificar status da sessão pode ser usada com qualquer fluxo de trabalho para verificar o status da sessão do Carbon Black no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Status da sessão retornado.
Falha	Erro de status da sessão. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Informações sobre processos em execução do Carbon Black.

Atividade Criar processo de comando

A atividade de fluxo de trabalho Criar processo de comando cria um processo de comando Carbon Black para usar no fluxo de trabalho.

A atividade Criar processo de comando pode ser usada com qualquer fluxo de trabalho para criar um processo de comando Carbon Black no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Processo de comando criado.
Falha	Processo de comando não criado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
command_id	Identificador do comando.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Atividade Verificar status do comando e obter processo

Verifica o status do comando Carbon Black e recupera processos a serem usados no fluxo de trabalho.

A atividade Verificar status do comando e obter processo pode ser usada com qualquer fluxo de trabalho para verificar o status de um comando do Carbon Black e obter processos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Status do comando retornado e processos criados.
Falha	Status do comando ou erro de processo. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
command_id	Identificador do comando.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Atividade Mapear dados de processos

A atividade de fluxo de trabalho Mapear dados de processos mapeia dados de processo de Carbon Black no fluxo de trabalho.

A atividade Mapear dados de processos pode ser usada com qualquer fluxo de trabalho para mapear processos de Carbon Black.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Processos mapeados
Falha	Processos não mapeados. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
IC_afetado	Item de configuração afetado.
Id_implementação	Identificador de implementação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Dados de retorno formatados em processos em execução usados pelo fluxo de trabalho abstrato.
processos	Lista de processos em uma matriz.

Acompanhamento da execução da capacidade - Concluir atividade

A atividade de fluxo de trabalho Acompanhamento da execução da capacidade - Concluir atualiza o registro de auditoria quando o fluxo de trabalho é concluído.

A atividade Acompanhamento da execução da capacidade - Concluir pode ser usada com qualquer fluxo de trabalho para registrar a conclusão do fluxo de trabalho.

Nota: A matriz **Valor de retorno** da atividade principal do **inicializador paralelo** contém uma matriz de resultados de todos os fluxos de trabalho de integração executados e solicita a conclusão bem-sucedida do acompanhamento de execução.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é atualizado para **Concluído**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityExecutionId	Identificador do sistema para o registro de auditoria. Este campo foi a saída de qualquer uma das atividades de auditoria Iniciar.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
mensagem	Mensagem de conclusão.

Variáveis de saída

Não há variáveis de saída.

Atividade Fechar sessão

Encerra uma sessão de Carbon Black no fluxo de trabalho.

A atividade Fechar sessão pode ser usada com qualquer fluxo de trabalho para fechar uma sessão de Carbon Black.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sessão encerrada.
Falha	Sessão não encerrada. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Integração de comandos do sistema de operações de segurança - Obter fluxo de trabalho de processos em execução

O fluxo de trabalho Integração de comandos do sistema de operações de segurança - Obter processos em execução recupera os processos em execução de um item de configuração quando adicionado ou atualizado para um incidente de segurança baseado em Windows ou Unix no estado **Análise**.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Para novos incidentes de segurança, o fluxo de trabalho é executado automaticamente quando você envia o incidente com um item de configuração selecionado, quando o estado muda automaticamente para **Análise**. Se permanecer no estado **Rascunho**, não será executado.

Tradução automática

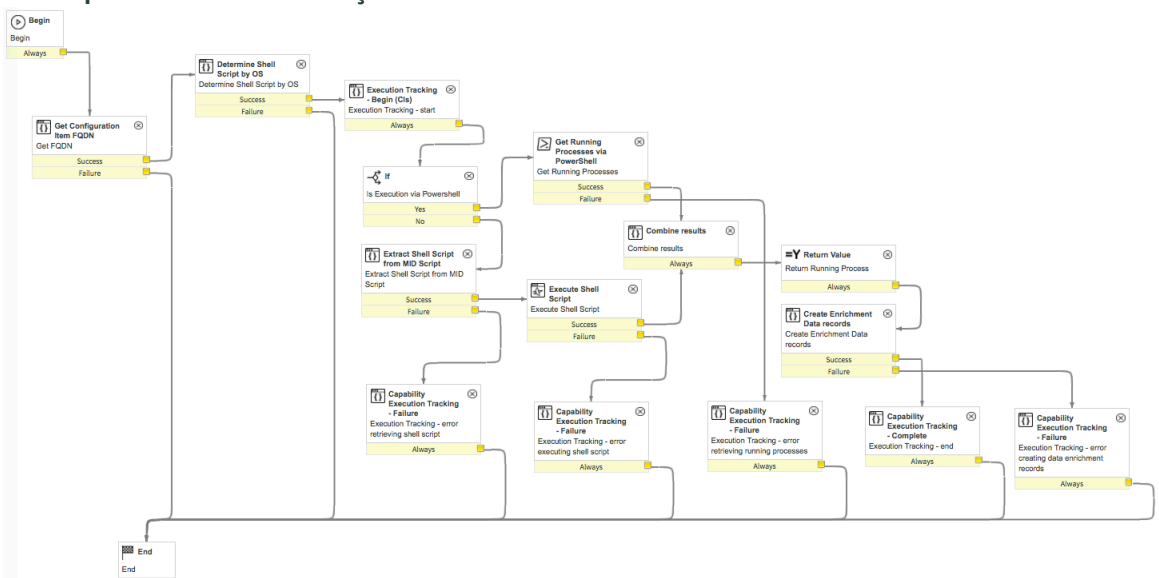
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

As atividades do processo de fluxo de trabalho incluem:

- Atividade Obter FQDN do item de configuração
- Determinar script de shell por atividade do SO
- Acompanhamento de execução - Iniciar atividade
- Obter processos em execução via PowerShell
- Atividade Executar script de shell
- Acompanhamento da execução da capacidade - Atividade com falha
- Atividade Extrair Shell Script da atividade MID Script
- Combinar resultados e retornar valores em uma matriz
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento da execução da capacidade - Concluir atividade

Obter processos em execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração (computador, servidor ou semelhante).
4. Clique em **Atualizar**.
   Orquestração do Security Incident Response fornece informações do processo em execução no **Link relacionado** > **Aprimoramentos de incidentes de segurança**guia. Para obter mais informações, consulte Operações de segurança mapeamento de dados de aprimoramento.

   As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade combinar resultados

A atividade de fluxo de trabalho Combinar resultados mescla os resultados de integrações de terceiros para uso no fluxo de trabalho.

A atividade Combinar resultados pode ser usada com qualquer fluxo de trabalho para executar um script de shell do MID Server no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Resultados combinados.
Falha	Falha na combinação. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
entradaA	Conjunto de resultados A
entradaB	Conjunto de resultados B
Id_implementação	Identificador de implementação.
IC_afetado	Item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	Conjunto de resultados A ou conjunto de resultados B com base em qual é preenchido.

Atividade Executar script de shell

A atividade de fluxo de trabalho Executar script de shell executa um script de shell do MID Server no fluxo de trabalho.

A atividade Executar script de shell pode ser usada com qualquer fluxo de trabalho para executar um script de shell do MID Server no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Script de shell encontrado
Falha	Nenhum script de shell encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
meta	IP ou nome de domínio totalmente qualificado (FQDN) do IC de destino.
scriptValue	Script, como um valor de cadeia de caracteres, executado em um sistema Unix.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Saída bruta. Dados de processos em execução.

Atividade Extrair Shell Script da atividade MID Script

A atividade de fluxo de trabalho Extrair script de shell do script MID extrai um script de shell do MID server para usar com no fluxo de trabalho.

A atividade Extrair Script de Shell de MID Script pode ser usada com qualquer fluxo de trabalho para extrair um script de shell do MID server para incluir no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Script de shell encontrado
Falha	Nenhum script de shell encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
sysId	Identificador do sistema

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
scriptValue	Script, como um valor de cadeia de caracteres, executado em um sistema Unix.

Obter processos em execução por meio da atividade PowerShell

A atividade de fluxo de trabalho Obter ID do sensor reúne processos em execução que usam o PowerShell para usar no fluxo de trabalho.

A atividade de fluxo de trabalho Obter processos em execução via PowerShell pode ser usada com qualquer fluxo de trabalho para recuperar processos a serem incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Processos encontrados
Falha	Nenhum processo encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
meta	IP ou nome de domínio totalmente qualificado (FQDN) do IC de destino.
processamentoScript	Script ECC executado em um sistema baseado no Windows.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resposta	Saída bruta. Dados de processos em execução.

Integração de Operações de segurança - Capacidade de isolamento de host

A capacidade **Isolar host** restringe as conexões do sistema a outros dispositivos. O isolamento de host é executado em um item de configuração (IC).

A capacidade **Isolar host** tem um fluxo de trabalho, Operações de segurança - Isolar fluxo de trabalho de host que aceita um ou mais ICs e, opcionalmente, uma implementação. Você pode especificar uma implementação a ser usada para isolar o host ou para o fluxo de trabalho tentar isolar o host usando todas as implementações.

Nota: Embora não esteja integrado a uma capacidade, um fluxo de trabalho, Integração do Carbon Black das Operações de segurança - Remover fluxo de trabalho de isolamento de host está disponível para orquestração para restaurar a comunicação com um host isolado.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Executar host isolado

Isolar host restringe as conexões do sistema a outros dispositivos.

Antes de Iniciar

Função necessária: sn_si.analyst

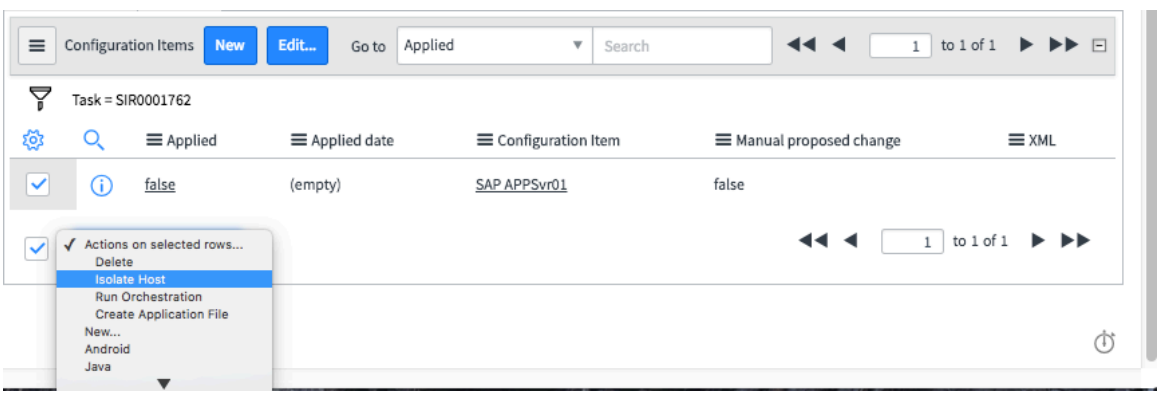
Por Que e Quando Desempenhar Esta Tarefa

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

O fluxo de trabalho **Integração de Operações de segurança - Isolar host ou endpoint**pode ser acionado na lista relacionada em um incidente de segurança.

Procedimento

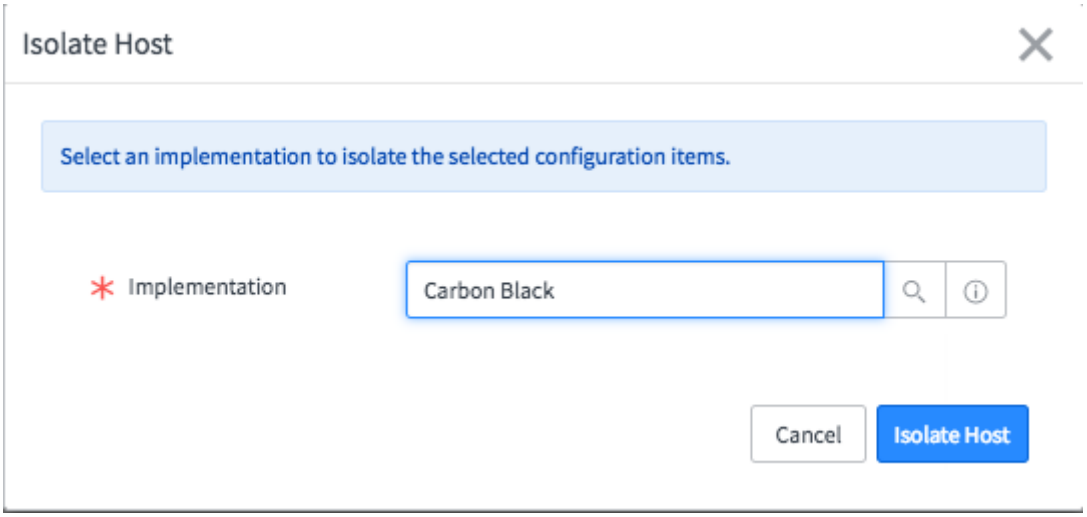
1. Navegue até um incidente de segurança.
2. Selecione **Itens de configuração** na guia **Lista relacionada**.
3. Clique em **Isolar host** no menu suspenso **Ações nas linhas selecionadas....**



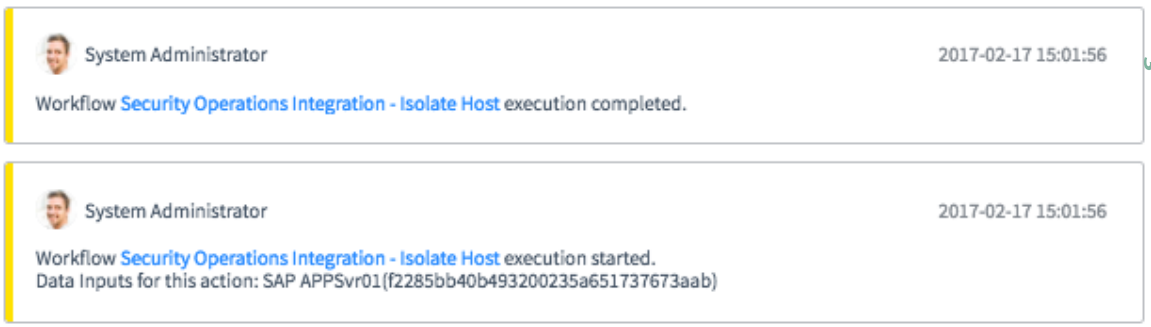
A caixa de diálogo é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Escolha a implementação.
5. Clique **em Isolar host**.
   A auditoria de execução do fluxo de trabalho é exibida na seção de anotações de trabalho.



Operações de segurança - Isolar fluxo de trabalho de host

O fluxo de trabalho **Operações de segurança - Isolar host** é um fluxo de trabalho de alto nível independente de integrações. Ele usa as consultas configuradas para pesquisar um conjunto de itens de configuração. Use-o para atender a uma integração, como Carbon Black.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado na guia **Itens de configuração** em uma lista relacionada a incidentes de segurança.

As atividades do processo de fluxo de trabalho incluem:

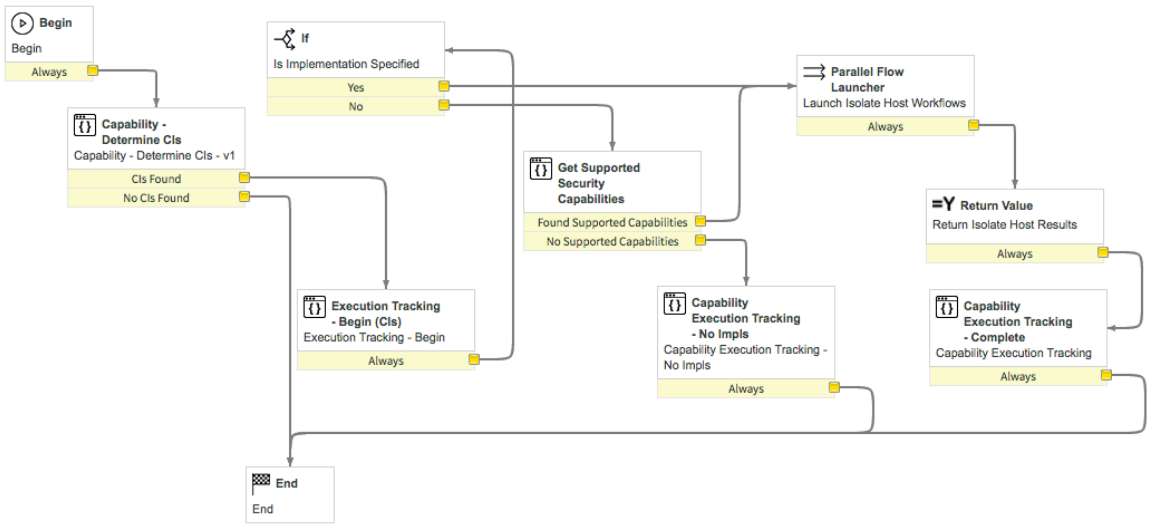
- Atividade Capacidade - Determinar ICs
- Acompanhamento de execução - Atividade Iniciar (ICs)
- Atividade Obter capacidades de segurança compatíveis
- Inicializador de fluxo paralelo - inicie o fluxo de trabalho apropriado. Armazene os resultados em uma matriz.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Acompanhamento de execução de capacidade - atividade sem implementações
- Acompanhamento da execução da capacidade - Atividade com falha

Isolar host



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Integração do Carbon Black das Operações de segurança - Fluxo de trabalho Isolar host

A integração do Carbon Black das Operações de segurança - Isolar host é a implementação da integração do Carbon Black iniciada pelo fluxo de trabalho Integração das Operações de segurança - Isolar host.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Atividade Iniciar (ICs)
- Obter IP de IC
- Coletar configurações de Carbon Black
- Acompanhamento da execução da capacidade - Atividade com falha
- Obter Identificador de Sensor
- Atividade Definir isolamento de rede habilitado
- Atualizar sensor : retorna o resultado de Isolar host.
- Acompanhamento da execução da capacidade - Concluir atividade

As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Obter ID do sensor

A atividade de fluxo de trabalho Obter ID do sensor reúne identificadores de sensor a serem usados no fluxo de trabalho.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade Obter ID do sensor pode ser usada com qualquer fluxo de trabalho para coletar informações do sensor a serem usadas no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensores encontrados.
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ci_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detalhe	Descrição do sensor Carbon Black no formato JSON.

Atividade Definir isolamento de rede habilitado

A atividade de fluxo de trabalho Definir isolamento de rede habilitado habilita o isolamento de rede.

A atividade Definir isolamento de rede habilitado pode ser usada com qualquer fluxo de trabalho para habilitar o isolamento de rede.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Isolamento de rede habilitado.
Falha	O isolamento de rede não pode ser habilitado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
sensor_detalhe	Descrição do sensor Carbon Black no formato JSON.
desativar	Determina se o host está isolado ou remove o isolamento do host. Verdadeiro = desabilitar isolamento Falso = o isolamento permanece habilitado

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
sensor_detalhe	Descrição do sensor Carbon Black no formato JSON.

Atualizar atividade do sensor

A atividade de fluxo de trabalho Atualizar sensor atualiza o sensor para isolar hosts ou endpoints.

A atividade Atualizar sensor pode ser usada com qualquer fluxo de trabalho para isolar hosts ou endpoints.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sensor atualizado.
Falha	Não é possível atualizar o sensor. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com o Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
sensor_detalhe	Descrição do sensor Carbon Black no formato JSON.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.

Integração do Carbon Black das Operações de segurança - Remover fluxo de trabalho de isolamento de host

O fluxo de trabalho **Integração com Carbon Black das Operações de segurança - Remover isolamento de host** desbloqueia a comunicação com um host ou endpoint especificado em um sistema Carbon Black.

Antes de Iniciar
Função necessária: sn_si.analyst

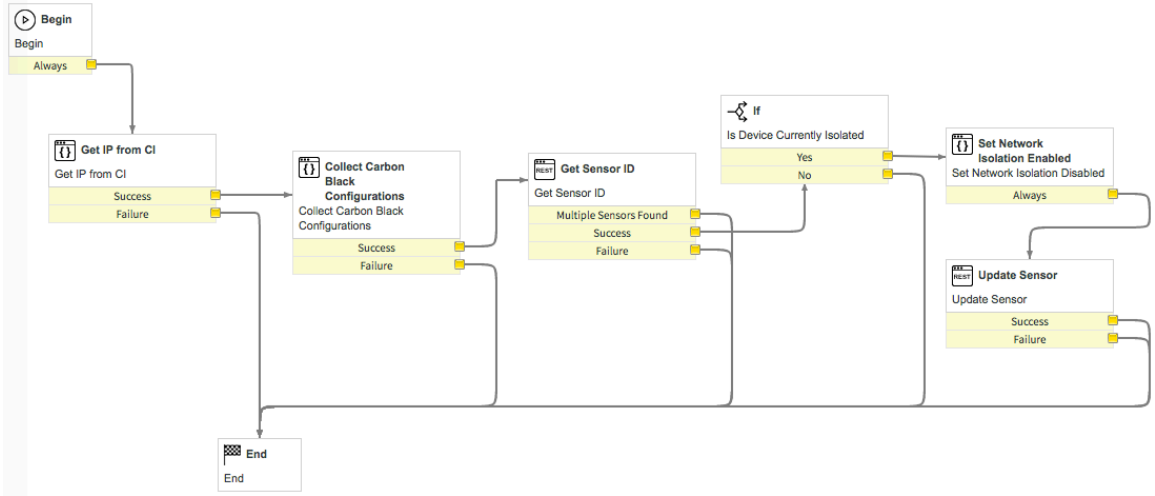
Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho não faz parte de uma capacidade e precisa de uma orquestração personalizada para ser executado.
As atividades do processo de fluxo de trabalho incluem:

- Obter IP da atividade de IC
- Em caso de sucesso- Atividade Coletar configurações de Carbon Black
- Atividade Obter ID do sensorObter Identificador de Sensor
- If- O dispositivo oferece suporte ao isolamento- e o dispositivo não está isolado-Atividade Definir isolamento de rede habilitado para desabilitado.
- Atualizar atividade do sensor- retorna o resultado de Isolar host.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração com Carbon Black - Remover isolamento de host



Integração de Operações de segurança - Capacidade de publicar na lista de observação

A capacidade Publicar na lista de observação adiciona observáveis e indicadores associados a um incidente de segurança a uma lista de observação de terceiros que monitora eventos de segurança e gera alertas. Essa capacidade é usada como parte da resposta do incidente durante as investigações.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Integração de Operações de segurança - Fluxo de trabalho Publicar na lista de observação

O fluxo de trabalho **Integrações de Operações de segurança - Publicar na lista de** observação é um fluxo de trabalho de alto nível independente de integrações. Ele adiciona observáveis a listas de observação de terceiros que oferecem suporte à capacidade. Use-o para atender a uma integração.

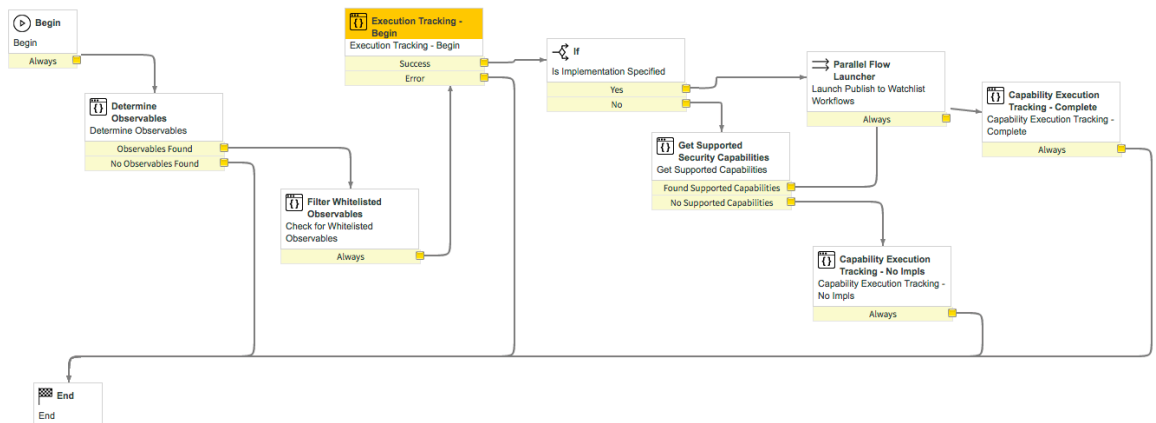
Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho está visível e é executado somente quando uma integração está disponível. É acionado na guia **Observáveis** ou **Indicadores associados** em um incidente de segurança.

Publicar na Watchlist



Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades do processo de fluxo de trabalho incluem:

- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações
- Atividade Filtrar observáveis na lista de permissões

Integração de Operações de segurança - Capacidade de pesquisa de detecções

A capacidade **Pesquisa** de detecções aceita um conjunto de observáveis, encontra integrações que oferecem suporte a uma pesquisa de detecções e executa essas pesquisas.

A capacidade Pesquisa de detecções tem um fluxo de trabalho, Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções, que executa a pesquisa de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra capacidades de implementação, cria as consultas com base nas configurações de pesquisa de detecções e executa as pesquisas com base no fluxo de trabalho configurado. Quando a pesquisa é concluída, uma anotação é adicionada às Anotações de trabalho do incidente, incluindo se alguma detecção foi encontrada e, em caso afirmativo, quantas.

Para exibir as Configurações de pesquisa de detecções, navegue até **Operações de segurança** > **Integrações** > **Configurações da Pesquisa de detecções**.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Criar registros de configuração de pesquisa de detecções

Crie vários registros de configuração de pesquisa de detecções e use-os ao consultar vários armazenamentos de log ou variar os parâmetros de pesquisa.

Antes de Iniciar

Função necessária: sn_si.admin

- O complemento CIM deve ser instalado na instância do Splunk.
- Pesquisas salvas e consultas no local são compatíveis somente com a integração do Splunk.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode criar registros de configuração de pesquisa de detecções para invocar pesquisas salvas no armazenamento de log do Splunk Enterprise.

Nota: As consultas de configuração de pesquisa dependem dos dados de log do Splunk para serem compatíveis com o Splunk Common Information Model (CIM).

Com as configurações de pesquisa salvas, você pode:

- Crie pesquisas personalizadas que combinem vários registros de eventos.
- Pesquisas eficazes e com design eficiente.
- Use entradas com parâmetros na pesquisa salva do Splunk.

O sistema de base inclui as configurações de exemplo, conforme mostrado nesta imagem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de pesquisa salvas

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

A pesquisa salva e as consultas de configuração no local são consultas de exemplo e podem ser substituídas por parâmetros apropriados para o seu ambiente. Crie configurações adicionais de pesquisa salva conforme necessário. Quando você define uma configuração de pesquisa salva, o nome e os parâmetros na consulta de pesquisa devem corresponder à configuração salva definida em sua instância do Splunk. Se o nome e os parâmetros não forem os mesmos, talvez você não veja resultados precisos ao executar uma pesquisa de detecções.

Nota: Em sua instância do Splunk, navegue até a página Pesquisas, relatórios e alertas e localize sua consulta de pesquisa salva. Clique no link **Permissões** para navegar até a página Permissões. Selecione o botão de opção **Todos os aplicativos** e habilite a opção **Permissão de leitura** para **Todos**. Isso mudará o valor da coluna Compartilhamento de Privado para App para sua consulta de pesquisa salva. Se não estiver definido, a consulta de pesquisa salva poderá não retornar resultados.

Para verificar se a configuração de pesquisa salva corresponde à configuração definida na sua instância do Splunk:

1. Navegar até **Configurações** > **Pesquisas, relatórios e alertas**.
2. Mude o **contexto da aplicação** para **Todos**.

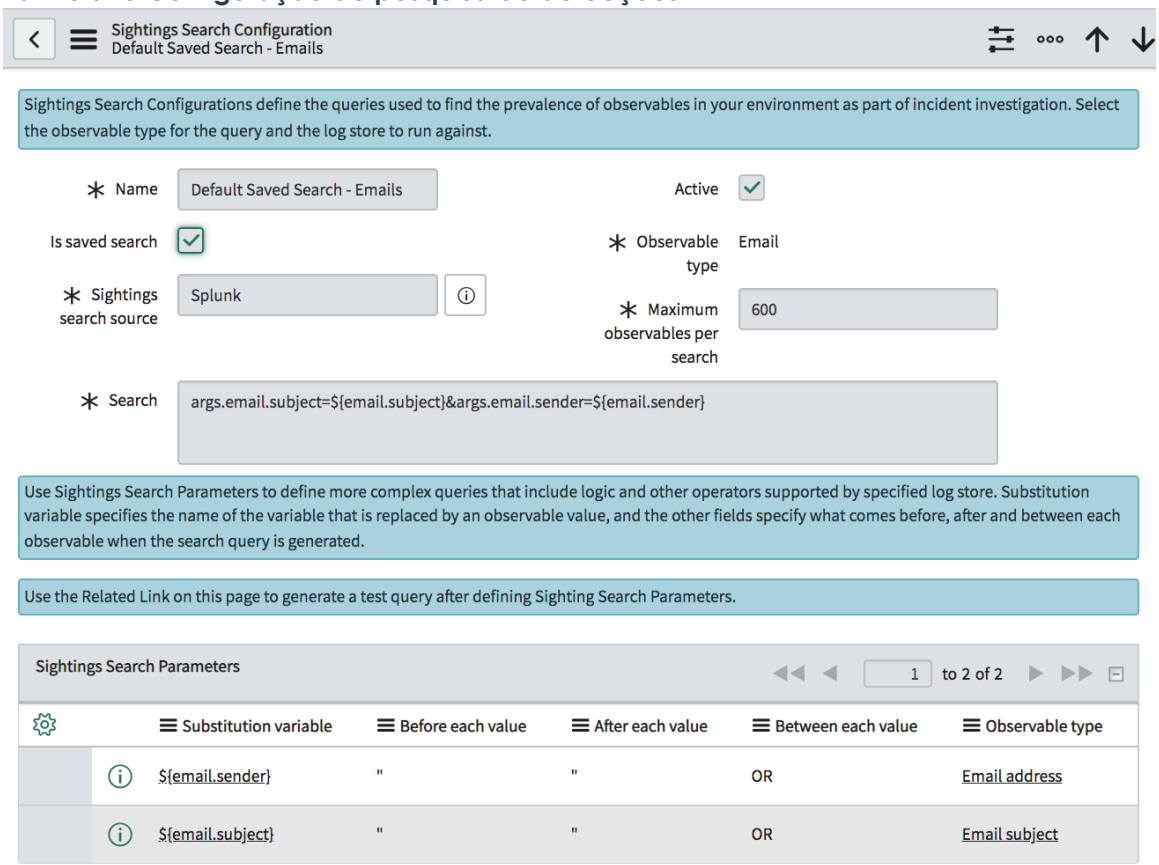
   Uma lista de relatórios de pesquisa é exibida.
3. Confirme se a consulta de pesquisa salva está presente na lista.

Por exemplo, o formulário Configuração de pesquisa de detecções contém o endereço de e-mail e o remetente do e-mail como parâmetros de pesquisa:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Configuração de pesquisa de detecções



Na instância do Splunk, defina a pesquisa salva com o mesmo nome, Pesquisa salva padrão - e-mails e os mesmos parâmetros de pesquisa para o endereço de e-mail e o assunto do e-mail. Se o nome e os parâmetros de pesquisa não forem os mesmos, a pesquisa de detecções não gerará resultados precisos.

Procedimento

1. Navegar até **Operações de segurança** > **Integrações** > **Configuração da Pesquisa de detecções** e crie um novo registro (consulte a tabela para obter as descrições dos campos).

Formulário Configuração de pesquisa de detecções

Campo	Descrição
Nome	Nome da configuração.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem da pesquisa de detecções	A origem da pesquisa de detecções. Selecione o armazenamento de log do Splunk como a origem.
Ativo	Opção para o status de pesquisa salva. Somente configurações de pesquisa ativa podem ser usadas para executar uma pesquisa de detecções.
Tipo de observável	O tipo de observável pode ser qualquer tipo de observável, como IP, valor de hash, URL, nome de domínio e assim por diante.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Máximo de observáveis por pesquisa	Número máximo de observáveis a serem retornados da pesquisa.
Pesquisar	A cadeia de caracteres de pesquisa padrão é `$(observable)`, mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com o armazenamento de log do Splunk.

2. Clique em **Enviar**.

Resultados
Você criou um registro de configuração de pesquisa de detecções.

O que Fazer Depois
Depois de definir a consulta de pesquisa, clique em **Gerar consulta de teste de pesquisa de detecções**e especifique uma lista de valores observáveis para gerar uma consulta de teste com base nesta configuração de pesquisa salva.

Executar uma pesquisa de detecções

Determine a predominância de uma ameaça ao longo do tempo ou teste os esforços de correção ou erradicação. Você pode selecionar observáveis individuais ou múltiplos e o intervalo de datas para sua pesquisa de um incidente de segurança. Os resultados são incluídos na lista relacionada **de observáveis de incidentes de segurança**.

Antes de Iniciar
Função necessária: sn_si.analyst

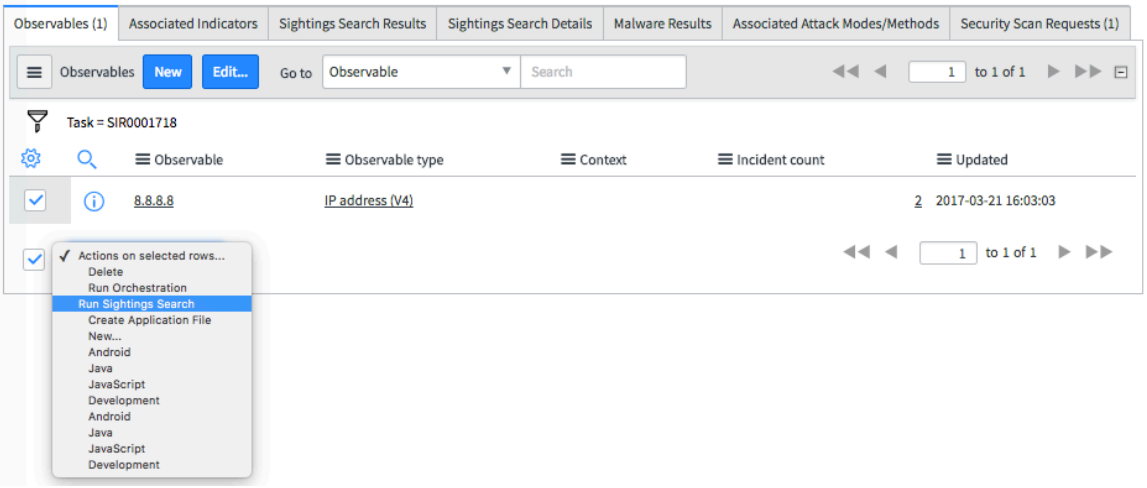
Por Que e Quando Desempenhar Esta Tarefa
A capacidade Pesquisa de detecções tem um fluxo de trabalho, Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções, que executa a pesquisa de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra capacidades de implementação, cria as consultas com base nas configurações de pesquisa de detecções e executa as pesquisas com base no fluxo de trabalho configurado.

Nota: Uma implementação ativa deve ser configurada. A Pesquisa de detecções é compatível com Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger e enriquecimento de incidentes do QRadar. Se não houver implementações disponíveis, as ações de capacidade, como **Executar pesquisa de detecções**, não serão exibidas nos menus do produto.

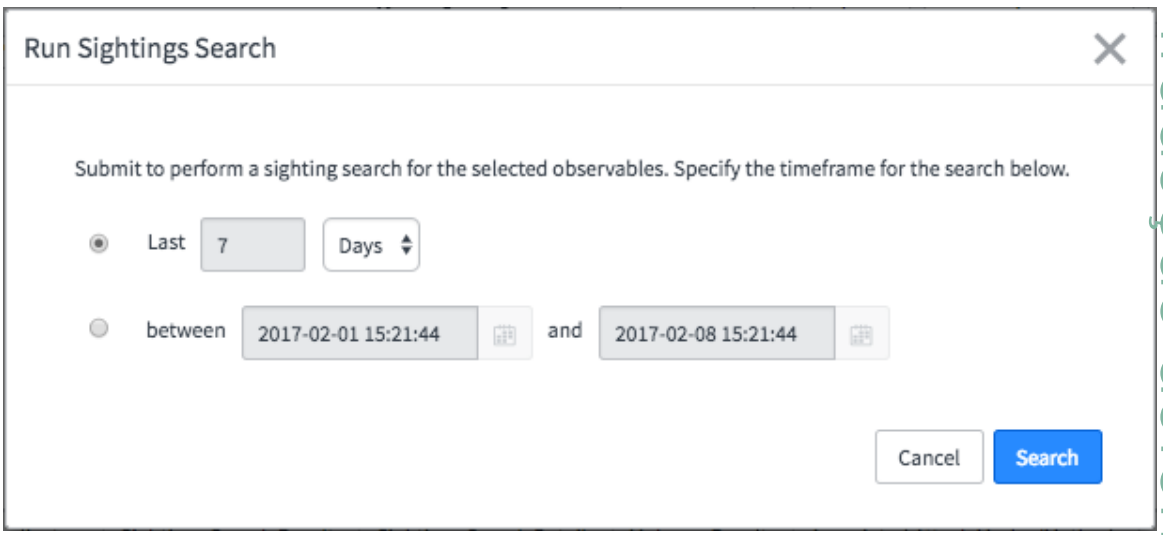
Procedimento
1. Navegue até um incidente de segurança.
2. Clique no link relacionado **Mostrar IoC**.
3. Selecione **Observáveis** na guia Lista relacionada.
4. Selecione os observáveis nos quais você deseja executar uma pesquisa de detecções.
5. Clique em **Executar pesquisa de detecções** no menu suspenso **Ações nas linhas selecionadas...**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo Executar pesquisa de detecções é aberta.



Nota: Os valores inseridos na caixa de diálogo substituem os valores de configuração de capacidade para esta execução.

6. Escolha o número de dias ou um intervalo de datas para pesquisar dados.

Opção	Descrição
Último	O número de horas ou dias anteriores à criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.
entre	Intervalo de datas a serem pesquisadas. As datas padrão são: A data e a hora em que o incidente foi aberto. A data e a hora sete dias antes da abertura do incidente.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: **Último** é o número de horas ou dias anteriores à criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.

7. Clique em **Pesquisar**.
   Um registro de pesquisa de detecções é criado. Os dados agregados e de detecções associados são exibidos no incidente de segurança nas guias **Resultados** da pesquisa de **detecções e Detalhes da pesquisa** de detecções.

Nota: Os dados dos resultados da pesquisa de detecções podem ser compartilhados com Trusted Security Circle, com exceção dos dados brutos no caso de implementações configuradas para incluir dados brutos.

Resultados da pesquisa de detecções

Resultado	Descrição
Número	O identificador da pesquisa de detecções.
Contagem de observáveis	Número de observáveis pesquisados por consulta.
Detecções internas	Contagem de detecções internas.
Vistas externas	Contagem de detecções externas. (Recebido de compartilhamento de ameaças.)
Itens de configuração correspondidos	Contagem de itens de configuração que corresponderam a um registro existente no seu cmdb para cada observável encontrado em seu ambiente.
Intervalo de datas de início	Hora de começar a procurar detecções.
Intervalo de datas de término	Hora de parar de procurar detecções.
Atualizado	Data e hora da última modificação.

Observação: se a implementação usada para a pesquisa de detecções estiver configurada para incluir dados brutos e pelo menos uma detecção for encontrada, um anexo contendo amostras de dados brutos aparecerá na parte superior do incidente de segurança.

Detalhes da pesquisa de detecções

Detalhe	Descrição
Pesquisa de detecção	O identificador da pesquisa de detecções.
Observável	Observável pesquisado por consulta.
Tipo de observável	Tipo de observável pesquisado por consulta.
Detecções internas	Contagem agregada de detecções internas.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhe	Descrição
Vistas externas	Contagem agregada de detecções externas. (Recebido de compartilhamento de ameaças.)
Atualizado	Data e hora da última modificação.

Integração de Operações de segurança - Fluxo de trabalho de pesquisa de detecções

O fluxo de trabalho**Integração de operações de segurança - Pesquisa de** detecções é um fluxo de trabalho de alto nível independente de integrações. Ele usa as consultas configuradas para pesquisar um conjunto de observáveis com base nas integrações configuradas que oferecem suporte à capacidade. Use-o para atender a uma integração como Splunk ou Elasticsearch.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Se um incidente de segurança tiver um observável anexado a ele, este fluxo de trabalho será acionado quando você clicar em **Executar pesquisa de detecções** no menu suspenso **Ações em linhas selecionadas...** na guia **Observáveis de incidentes de segurança**.

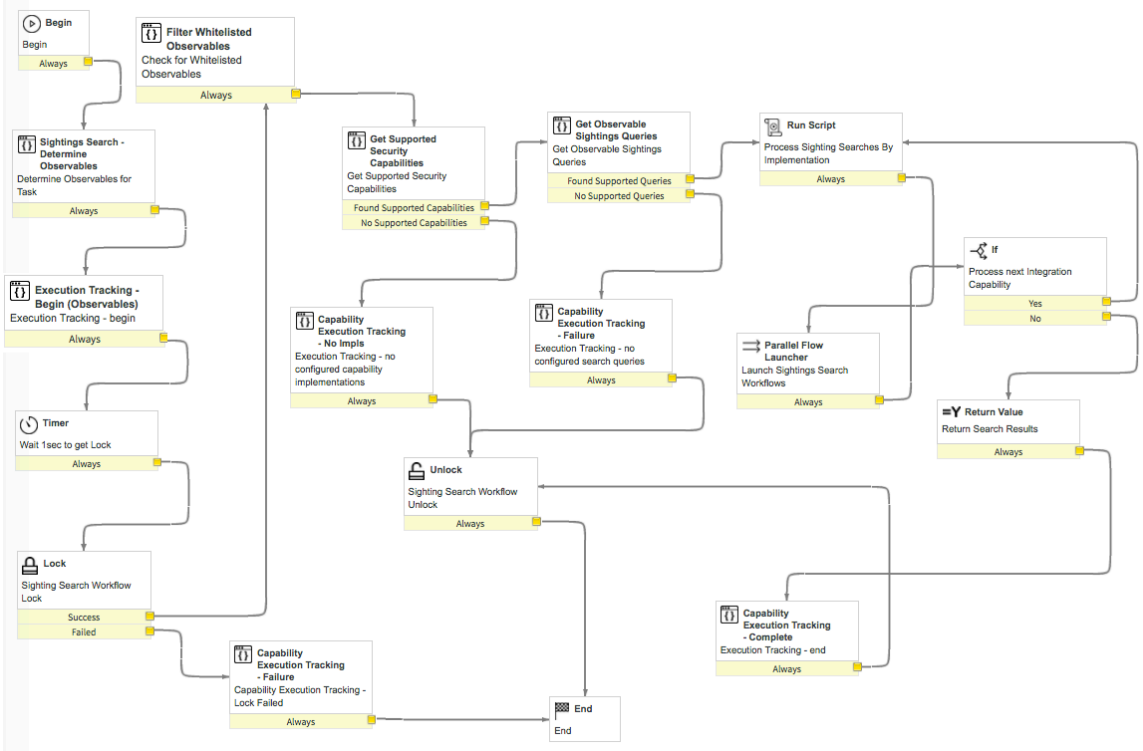
As atividades do processo de fluxo de trabalho incluem:

- Atividade Determinar observáveis
- Acompanhamento de execução - Iniciar atividade
- Atividade de fluxo de trabalho Temporizador - Aguarda um segundo para obter um bloqueio.
- Bloquear atividade de fluxo de trabalho
- Filtrar observáveis da lista de permissões
- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações
- Desbloquear fluxo de trabalho atividade
- Atividade Obter consultas de detecções de observável
- Acompanhamento da execução da capacidade - Atividade com falha
- Executar script fluxo de trabalho atividade
- Inicializador de Fluxo paralelo
- Atividade de fluxo de trabalho If Atividade de fluxo de trabalho If - Iterar até que todos os fluxos de trabalho apropriados tenham sido executados e armazenar os resultados em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de detecções



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Pesquisa de detecções - Determinar observáveis

A atividade de fluxo de trabalho **Pesquisa de detecções - Determinar observáveis** determina quais observáveis serão incluídos no fluxo de trabalho.

A atividade **Pesquisa de detecções - Determinar observáveis** pode ser usada com qualquer fluxo de trabalho para determinar quais observáveis serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis encontrados
Falha	Nenhum observável encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para observáveis).
observáveis	Endereços IP, hash, URLs, nomes de domínio.
workflow_current_sys_id	Identificador do sistema do registro atual. (Usado somente se `task_sys_id`, entradas de observável não estiverem disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis	Observáveis filtrados

Atividade de detecções de observável persistente

A atividade de fluxo de trabalho **Detecções de observáveis persistentes** recupera observáveis da integração de terceiros.

A atividade de vistas de **observáveis persistentes** pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
detecçõesResposta	
taskId	Identificador da tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resposta	

Atividade Obter consultas de detecções de observável

A atividade de fluxo de trabalho **Obter consultas de vistas de observáveis** recupera consultas da configuração de integração.

A atividade **Obter consultas de vistas de observáveis** pode ser usada com qualquer fluxo de trabalho para obter consultas a serem enviadas para a implementação especificada usando o inicializador de **fluxo paralelo**.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consultas encontradas.
Falha	Ocorreu um erro ao tentar obter consultas. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis filtrados.
Capacidades	Lista de capacidades compatíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
consultas	Cadeia de caracteres de pesquisa.
queryCount	Número de consultas a serem executadas.

Operações de segurança - Fluxo de trabalho de pesquisa de detecções do Arcsight Logger

O fluxo de trabalho**Operações de segurança - Pesquisa de detecções do ArcSight Logger** é a implementação da integração Splunk iniciada pelo **fluxo de trabalho Integração de operações de segurança - Pesquisa de detecções**.

Antes de Iniciar

Função necessária: sn_si_analyst

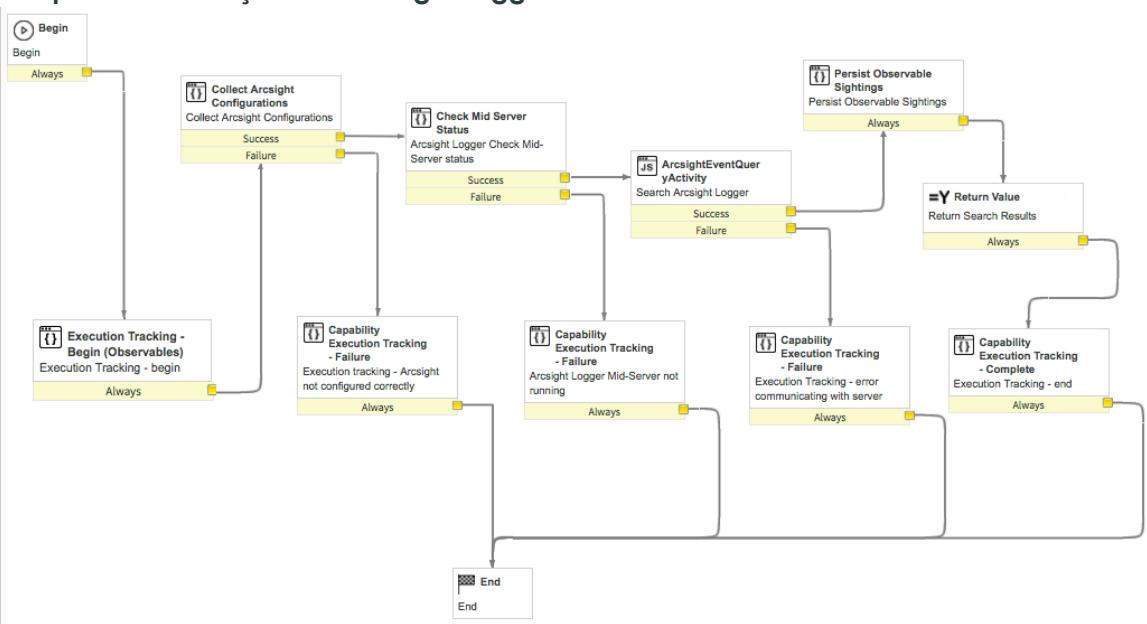
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do ArcSight
- Acompanhamento da execução da capacidade - Atividade com falha
- Atividade de consulta de evento do ArcSight
- Verifica se o MID Server está em execução ou não.
- Atividade de consulta de evento do ArcSight
- Atividade de detecções de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividade

Pesquisa de detecções do Arcsight Logger



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Coletar configurações do ArcSight

A atividade de fluxo de trabalho **Coletar configurações do ArcSight** reúne informações de configuração a serem usadas no fluxo de trabalho.

A atividade **Coletar configurações do ArcSight** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do HPE Security ArcSight Logger.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Trusted Security Circle ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Link para uma interface de pesquisa do ArcSight Logger, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
arcsight_username	Nome de usuário do HPE Security ArcSight Logger
arcsight_password	Senha do HPE Security ArcSight Logger
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.
todos_pares	Determina se todos os outros agentes conectados à rede devem ser pesquisados.

Atividade de consulta de evento do ArcSight

A atividade de fluxo de trabalho **Consulta de eventos** do ArcSight pesquisa indicadores mal-intencionados nos logs de eventos do ArcSight.

A atividade **de consulta de evento do ArcSight** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do HPE Security ArcSight Logger.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema HPE Security ArcSight Logger.
senha	Senha para o sistema HPE Security ArcSight Logger.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL base da API de integração de terceiros.
link_base_URL	Link para uma interface de pesquisa do ArcSight Logger, quando disponível.
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
todos_pares	Determina se todos os outros agentes conectados à rede devem ser pesquisados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Operações de segurança - Fluxo de trabalho de pesquisa de detecções do Elasticsearch

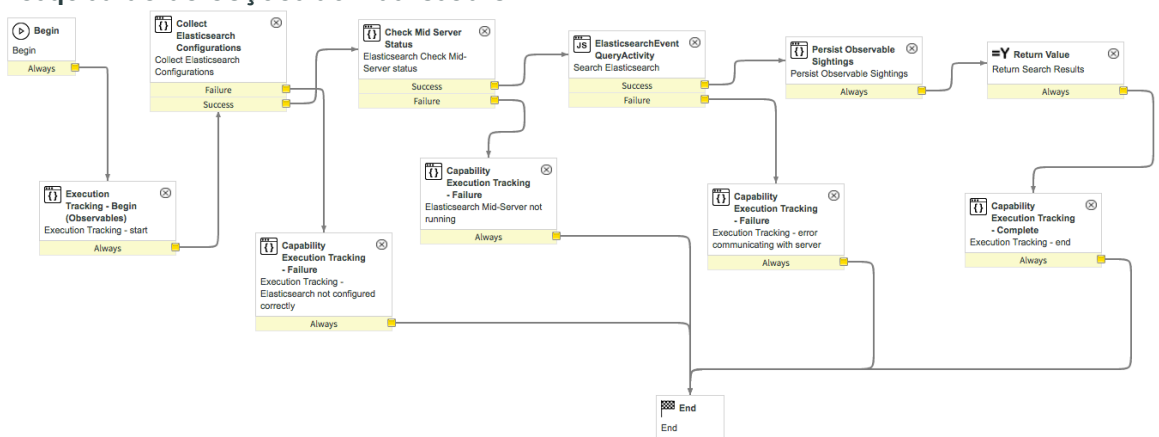
O fluxo de trabalho**Operações de segurança - Pesquisa** de detecções do Elasticsearch é a implementação do Elasticsearch iniciada pelo fluxo de trabalho **Integração de operações de segurança - Pesquisa de** detecções.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do Elasticsearch
- Verifica se o MID Server está em execução ou não.
- Acompanhamento da execução da capacidade - Atividade com falha
- Atividade Elasticsearch Event QueryActivity
- Atividade de detecções de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividadeAcompanhamento de execução de capacidade - atividade sem implementações

Pesquisa de detecções do Elasticsearch



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Coletar configurações do Elasticsearch

A atividade de fluxo de trabalho **Coletar configurações do Elasticsearch** reúne informações de configuração a serem usadas no fluxo de trabalho.

A atividade **Coletar configurações do Elasticsearch** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do Elasticsearch.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	[Opcional] Link para uma instância do Kibana, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
	• verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
elastic_username	Nome de usuário do Elasticsearch
elastic_password	Senha do Elasticsearch
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Atividade Elasticsearch Event QueryActivity

A atividade de fluxo de trabalho **Consulta de evento** do Elasticsearch pesquisa indicadores mal-intencionados nos logs de eventos do Elasticsearch.

A atividade **Elasticsearch Event QueryActivity** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do Elasticsearch.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema Elasticsearch.
senha	Senha do sistema Elasticsearch.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL base da API de integração de terceiros.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
link_base_URL	[Opcional] Link para uma instância do Kibana, quando disponível.
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Operações de segurança - Fluxo de trabalho Pesquisa de detecções do McAfee ESM

O fluxo de trabalho**Security Operations - McAfee ESM Sightings Search** é a implementação da integração Splunk iniciada pelo **fluxo de trabalho Security Operations Integration - Sightings Search**.

Antes de Iniciar
Função necessária: sn_si_analyst

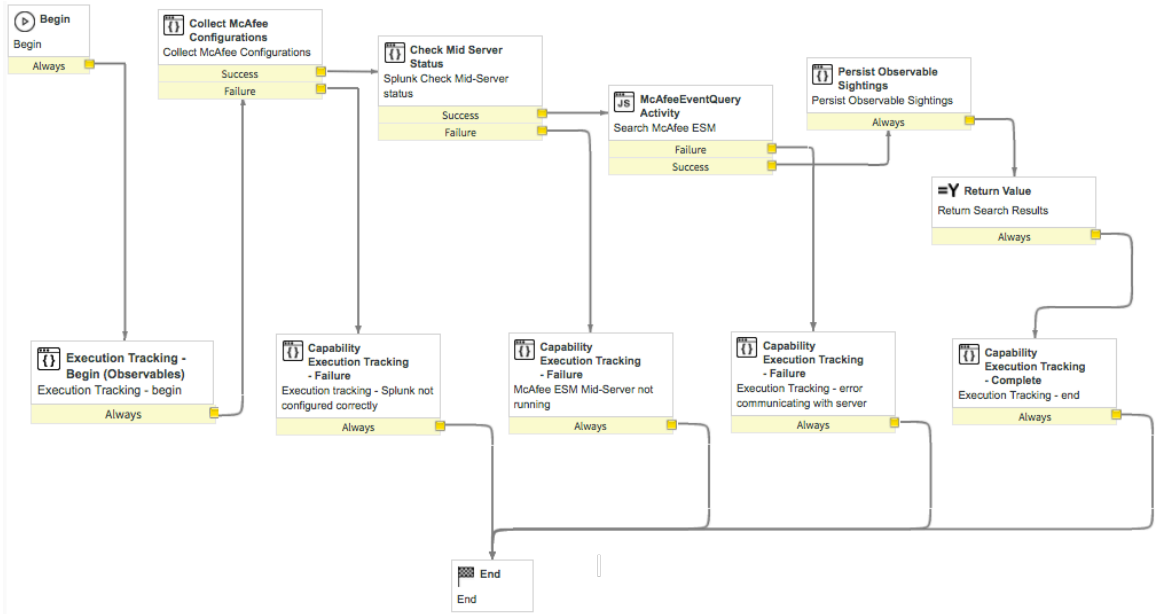
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações da McAfee
- Acompanhamento da execução da capacidade - Atividade com falha
- Atividade de consulta de evento do McAfee ESM
- Verifica se o MID Server está em execução.
- Atividade de detecções de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de detecções do McAfee ESM



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Coletar configurações da McAfee

A atividade de fluxo de trabalho **Coletar configurações da McAfee** reúne informações de configuração a serem usadas no fluxo de trabalho.

A atividade **Coletar configurações da McAfee** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do McAfee ESM.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Link para uma interface da web do McAfee, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
elastic_username	Nome de usuário da McAfee
elastic_password	Senha da McAfee
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Atividade de consulta de evento do McAfee ESM

A atividade de fluxo de trabalho **Consulta de eventos** do McAfee ESM pesquisa indicadores maliciosos nos logs de eventos do McAfee ESM.

A atividade **Consulta de eventos do McAfee ESM** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do HPE Security ArcSight Logger.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema McAfee ESM.
senha	Senha do sistema McAfee ESM.
observáveis	Sintaxe de pesquisa. `$(observable)` é o padrão.
base_url	URL base da API de integração de terceiros.
link_base_URL	Link para uma interface da web do McAfee, quando disponível.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Operações de segurança - Fluxo de trabalho de pesquisa de detecções do QRadar

O fluxo de trabalho**Operações de segurança - Pesquisa de detecções do QRadar** é a implementação da integração do IBM QRadar iniciada pelo **fluxo de trabalho Integração de operações de segurança - Pesquisa**de detecções.

Antes de Iniciar
Função necessária: sn_si_analyst

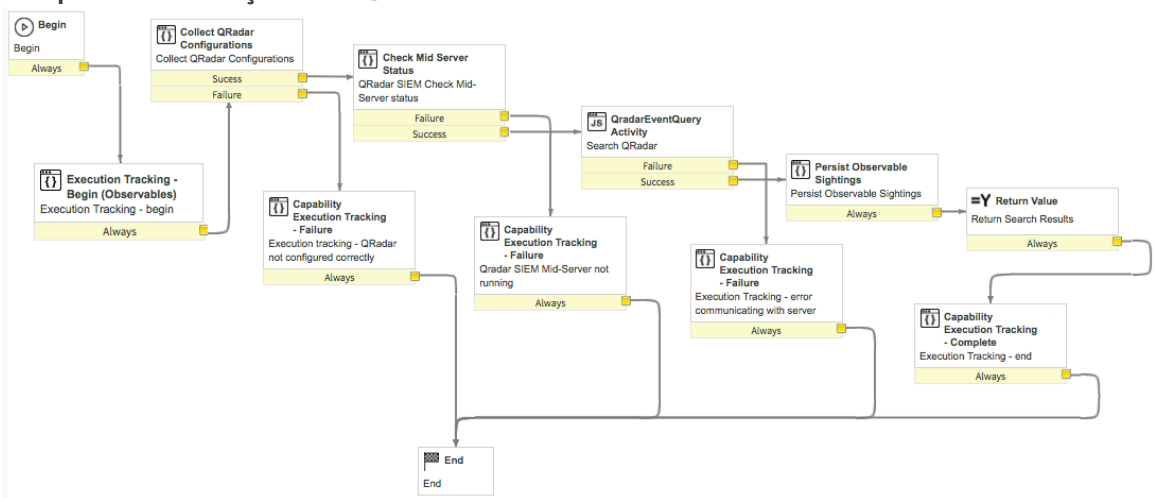
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do QRadar
- Acompanhamento da execução da capacidade - Atividade com falha
- Verifica se o MID Server está em execução.
- Atividade QRadar Event QueryActivity
- Atividade de detecções de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividade

Pesquisa de detecções do QRadar



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Coletar configurações do QRadar

A atividade de fluxo de trabalho **Coletar configurações do QRadar** reúne informações de configuração a serem usadas no fluxo de trabalho.

A atividade **Coletar configurações do QRadar** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do IBM QRadar.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Link para uma instância IBM QRadar, quando disponível.
use_default_workflows	Determina se o fluxo de trabalho que foi instalado com o plug-in deve ser usado ou não. Os valores possíveis são verdadeiro e falso..
elastic_username	Nome de usuário do QRadar
elastic_password	Senha do QRadar
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Atividade QRadar Event QueryActivity

A atividade de fluxo de trabalho **Consulta de eventos** do QRadar pesquisa indicadores mal-intencionados nos logs de eventos do QRadar.

A atividade **QRadar Event QueryActivity** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do Elasticsearch.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema QRadar.
senha	Senha para o sistema QRadar.
observáveis	A lista de observáveis de Círculos de segurança confiável ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL base da API de integração de terceiros.
link_base_URL	Link para uma instância IBM QRadar, quando disponível.
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Integração de Operações de segurança - Fluxo de trabalho de Pesquisa de detecções de Splunk

O fluxo de trabalho**Operações de segurança - Splunk Sightings Search** é a implementação da integração do Splunk iniciada pelo **fluxo de trabalho Integração de operações de segurança - Pesquisa de detecções**.

Antes de Iniciar
Função necessária: sn_si_analyst

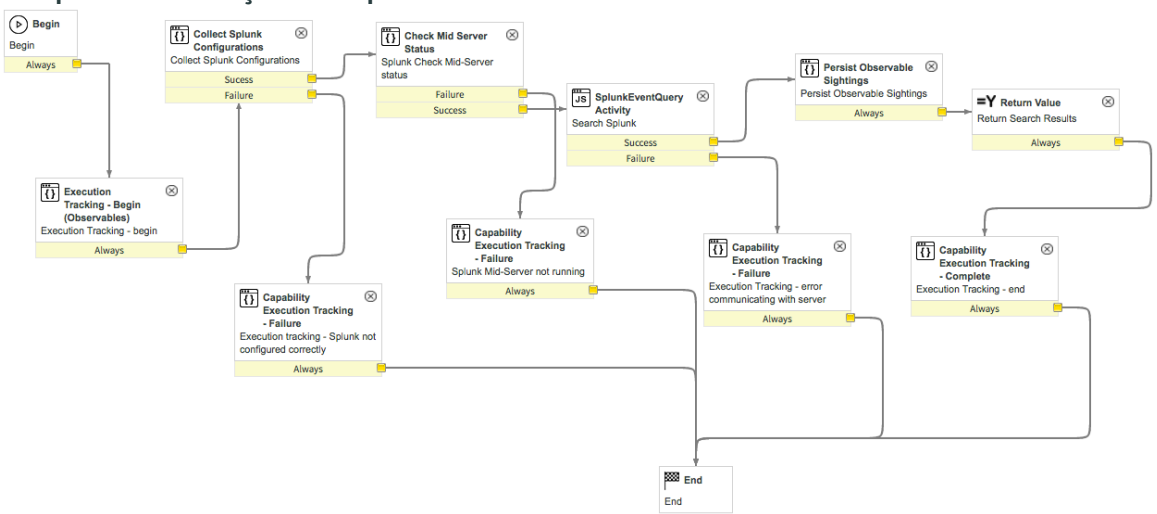
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do Splunk
- Acompanhamento da execução da capacidade - Atividade com falha
- Verifica se o MID Server está em execução ou não.
- Atividade Splunk Event Query
- Atividade de detecções de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento da execução da capacidade - Concluir atividade

Pesquisa de detecções do Splunk



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

Atividade Coletar configurações do Splunk

A atividade de fluxo de trabalho **Coletar configurações do Splunk** reúne informações de configuração a serem usadas no fluxo de trabalho.

A atividade **Coletar configuração do Splunk** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do Splunk.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Trusted Security Circle ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Links para a interface da web Splunk, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
elastic_username	Nome de usuário do Splunk.
elastic_password	Senha do Splunk.
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Atividade Splunk Event Query

A atividade de fluxo de trabalho **Consulta de eventos** do Splunk pesquisa indicadores mal-intencionados nos logs de eventos do Splunk.

A atividade **Splunk Event QueryActivity** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do Splunk.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Splunk
Falha	Ocorreu um erro ao tentar verificar a consulta do Splunk. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema Splunk.
senha	Senha do sistema Splunk.
observáveis	A lista de observáveis de Trusted Security Circle ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL do endpoint de integração do Splunk.
link_base_URL	Link para a interface da web Splunk, quando disponível.
origem	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Círculos de segurança confiável ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
dias_para_pesquisa	Dias para pesquisar a partir do dia atual. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Exibir resultados da pesquisa de detecções

Você pode revisar os resultados da pesquisa de detecções em busca de indicadores maliciosos internos e externos.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

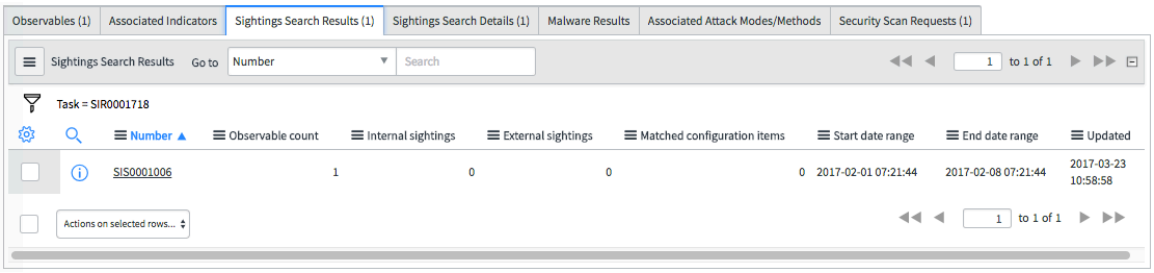
.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione a guia **Resultados** da pesquisa de detecções no grupo **Mostrar lista relacionada de IoC** para exibir a lista de pesquisas de detecções.



Nota: Esses dados podem ser compartilhados com Trusted Security Circle.

Resultados da pesquisa de detecções

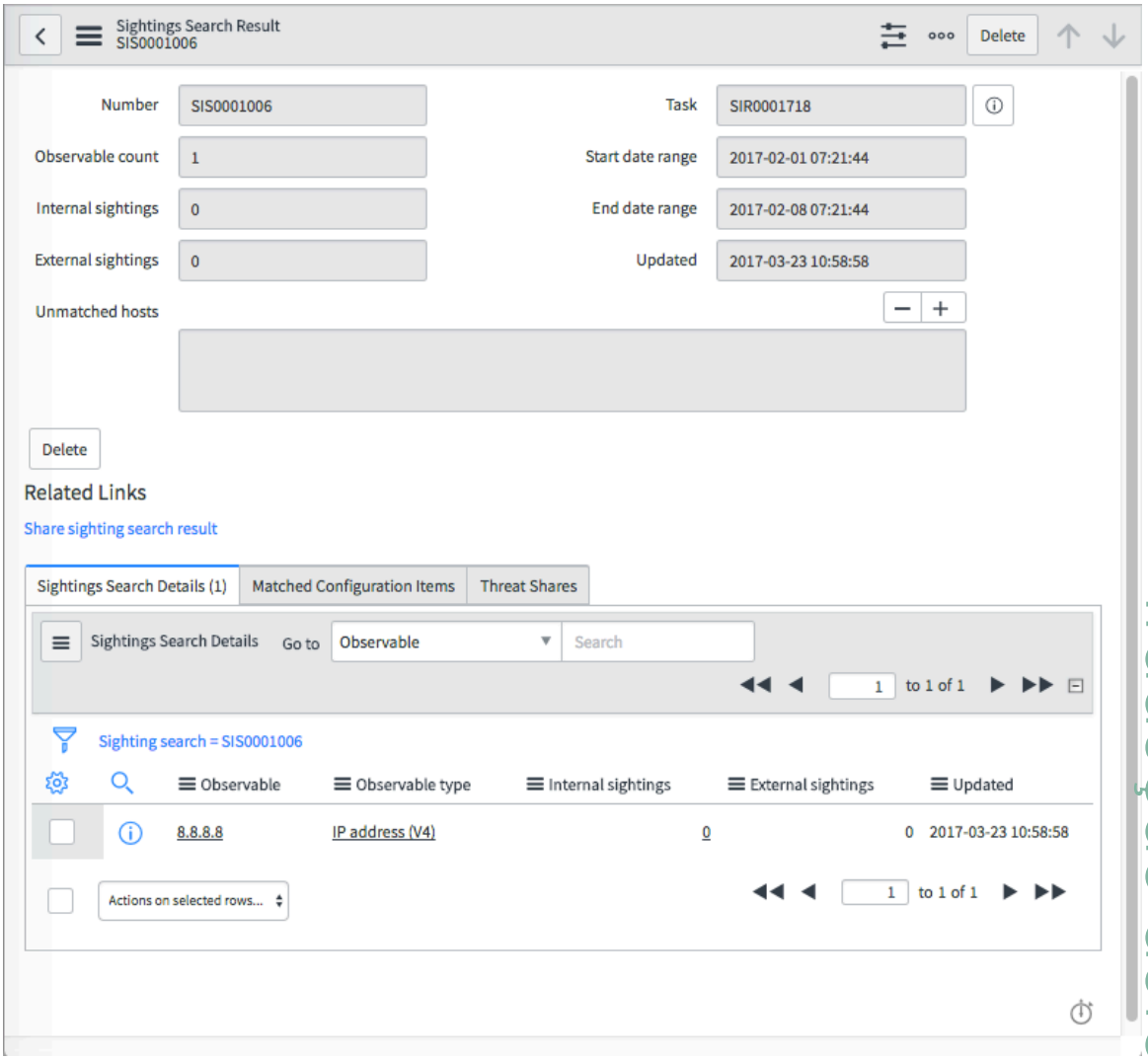
Resultado	Descrição
Número	Identificador da Pesquisa de detecções.
Contagem de observáveis	Número de observáveis pesquisados.
Vistas Internas	Contagem agregada de detecções internas.
Vistas Externas	Contagem agregada de detecções externas. (Recebido de compartilhamento de ameaças.)
Itens de configuração correspondidos	Contagem agregada de itens de configuração que correspondem a um registro existente no seu `cmdb`.
Intervalo de datas de início	Hora de começar a procurar detecções.
Intervalo de datas de término	Hora de parar de procurar detecções.
Atualizado	Data e hora da última modificação.

Para exibir os detalhes de uma única pesquisa:

3. Clique em uma Pesquisa de detecções na lista **Resultados** da pesquisa de detecções.
O formulário Resultado da pesquisa de detecções é exibido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Formulário Resultados da pesquisa de detecções

Detalhe	Descrição
Número	Identificador da Pesquisa de detecções internas.
Contagem de observáveis	Contagem de observáveis pesquisados por esta consulta.
Detecções internas	Contagem de detecções internas para esta pesquisa.
Vistas externas	Contagem de detecções externas para esta pesquisa. (Recebido de Trusted Security Circle.)
Hosts incompatíveis	Lista de possíveis itens de configuração para esta pesquisa que não corresponderam a nenhum registro no seu `cmdb`.
Tarefa	Identificador de tarefa de incidente de segurança.
Intervalo de datas de início	Hora de início da pesquisa de detecções.
Intervalo de datas de término	Hora em que a pesquisa de detecções parou.
Atualizado	Data e hora da última modificação.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhe	Descrição
Detalhes de Pesquisa de detecções	Tipo, número de detecções e data de modificação.
Itens de configuração correspondentes	Contagem de itens de configuração que corresponderam a um registro existente no seu `cmdb`. Lista o IC e a Detecção.
Compartilhamentos de ameaças	Lista de ameaças compartilhadas com Trusted Security Circle.

Compartilhar resultados da pesquisa de detecções

Você pode compartilhar detalhes ou resultados de detecções locais que estão associados a uma pesquisa específica com seu Círculo de Segurança Confiável.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O compartilhamento pode ser automatizado usando as seguintes **propriedades**do Security Incident Response.

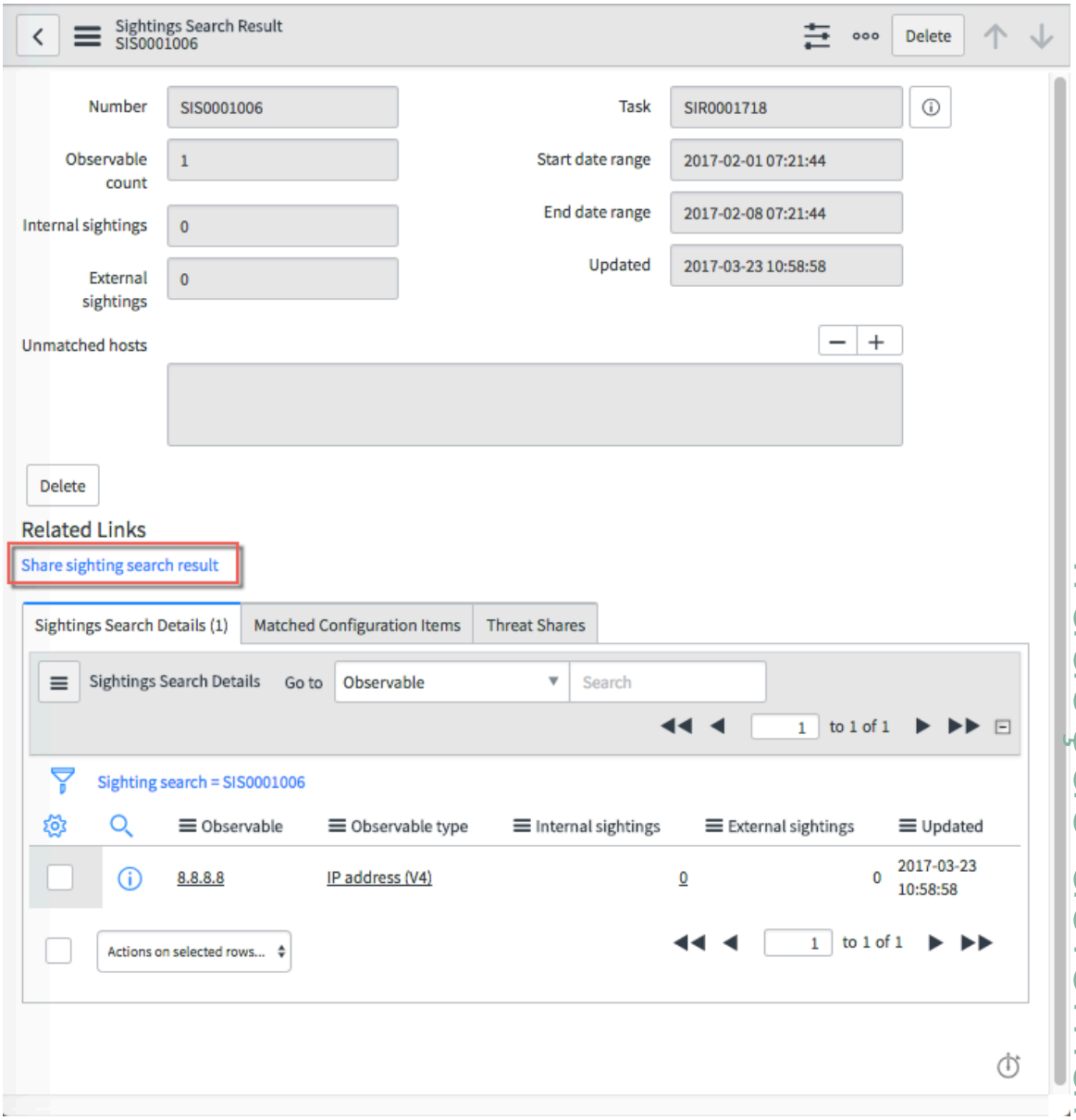
- Compartilhar automaticamente os resultados de uma pesquisa de detecções com o círculo de confiança padrão da ServiceNow
- Incluir observáveis sem detecções locais ao compartilhar automaticamente os resultados da pesquisa de detecções
- Responder com detecções locais sempre que um compartilhamento de ameaça for recebido de um círculo confiável

Procedimento

1. Navegue até um incidente de segurança.
2. Clique na lista relacionada **Mostrar IoC** e selecione a guia **Resultados** da pesquisa de detecções para exibir a lista de pesquisas de detecções.
3. Clique em um resultado de pesquisa de detecções.

Tradução automática

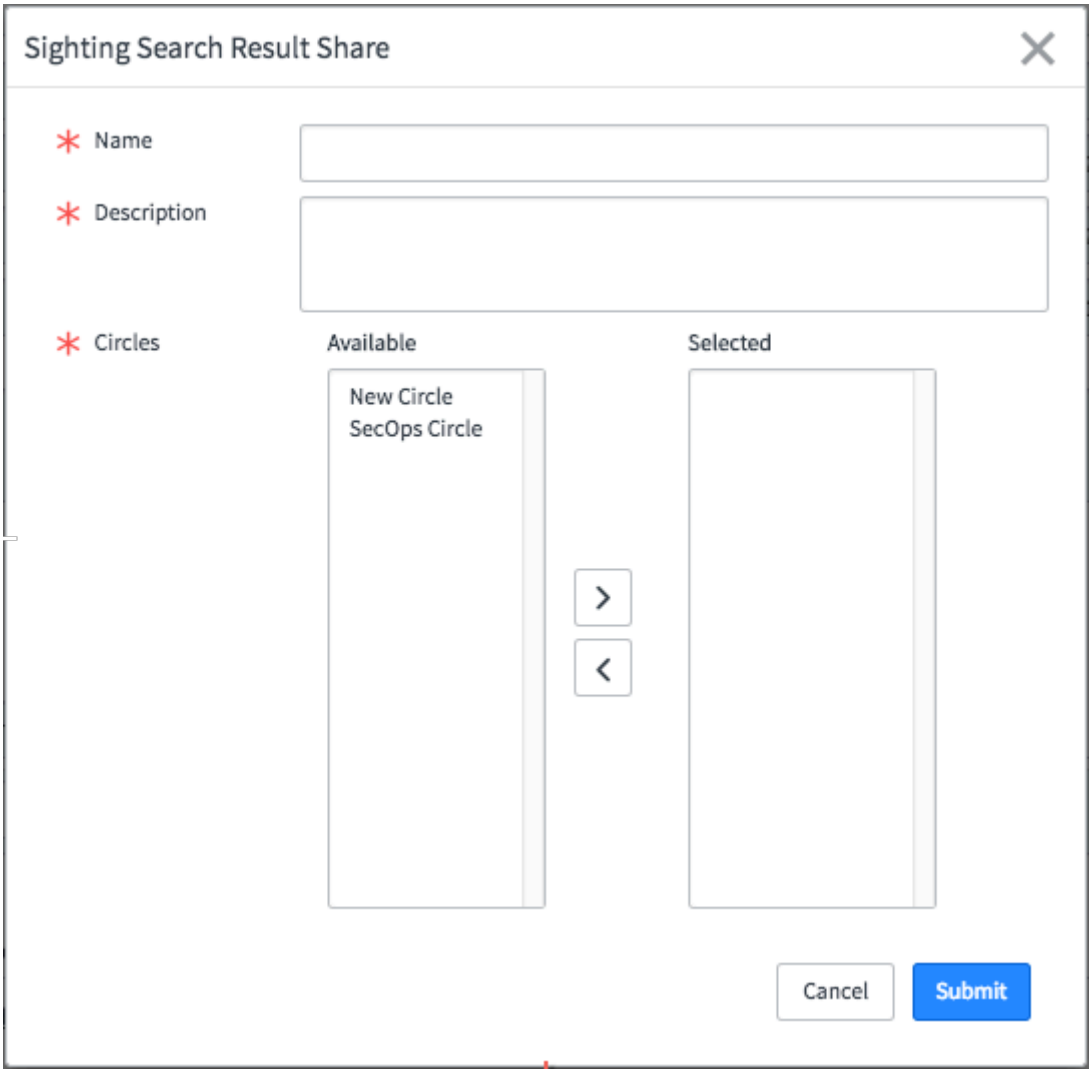
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário **Resultado**da pesquisa de detecções, clique no link relacionado **Compartilhar resultado da pesquisa de detecções**.
   A caixa de diálogo Compartilhamento do resultado da pesquisa de detecções é exibida.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Insira um **Nome** para este registro de compartilhamento de observável.
6. Insira uma **Descrição**dos observáveis a serem compartilhados.
7. Escolha **Círculos** com os quais os observáveis serão compartilhados.
8. Clique em **Enviar**.
   Os observáveis são compartilhados com o Círculo confiável especificado.

Compartilhar observáveis de um incidente de segurança

Os observáveis podem ser compartilhados de um incidente de segurança em Security Incident Response com membros do seu círculo de confiança.

Antes de Iniciar

Função necessária: sn_si.analyst

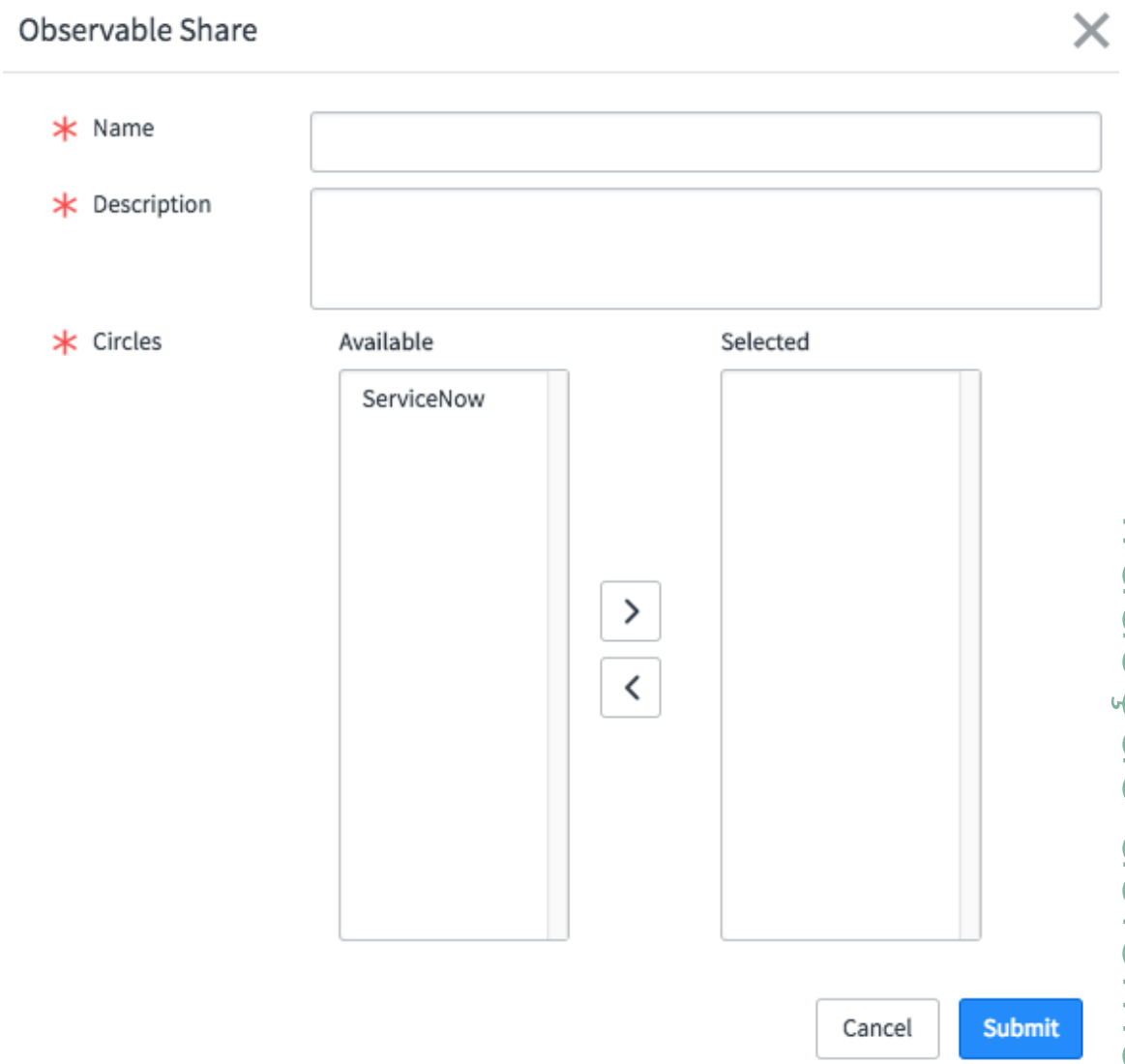
Procedimento

1. Navegue até um incidente de segurança.
2. Selecione a guia **Observáveis** no grupo **Mostrar lista relacionada de IoC**.
3. Clique em um observável.
4. No formulário **Observável**, clique no link relacionado **Compartilhar observável**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A caixa de diálogo Compartilhamento do observável é exibida.



5. Insira um **Nome** para este registro de compartilhamento de ameaças.
6. Insira uma **Descrição**dos observáveis selecionados.
7. Escolha **Círculos** com os quais os observáveis serão compartilhados.
8. Clique em **Enviar**.
   Os observáveis são compartilhados com o Círculo confiável especificado.
9. Você pode exibir os registros de compartilhamento de ameaças clicando na guia **Compartilhamentos** de ameaças.
10. Se algum dos observáveis compartilhados contiver detecções, as detecções também serão compartilhadas e poderão ser exibidas clicando na guia **Detecções**.

Exibir detalhes da pesquisa de detecções

Revise os detalhes agregados de todas as pesquisas de detecções.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione a guia **Detalhes da pesquisa** de detecções no grupo **Mostrar lista relacionada de IoC** para exibir a lista de pesquisas de detecções.

Nota: Esses dados podem ser compartilhados com Trusted Security Circle.

Detalhes de Pesquisa de detecções

Detalhe	Descrição
Observável	Lista de todos os observáveis pesquisados por consulta.
Tipo de observável	
Detecções internas	Contagem de detecções internas para todas as pesquisas.
Vistas externas	Contagem de detecções externas para todas as pesquisas. (Recebido de compartilhamento de ameaças.)
Pesquisa de detecção	Identificador da Pesquisa de detecções.
Atualizado	Data e hora da última modificação.

Integração de Operações de segurança - Capacidade de pesquisa de ameaças

A capacidade Pesquisas de **ameaças** executa pesquisas de inteligência contra ameaças para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

A capacidade Pesquisas de **ameaças** tem um fluxo de trabalho, Integração de Operações de segurança - Fluxo de trabalho de pesquisa de ameaças. Quando o fluxo de trabalho de capacidade é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar uma pesquisa nos observáveis selecionados ou pode executar a pesquisa usando todas as implementações.

Nota: Se não houver implementações disponíveis, as ações de capacidade não serão exibidas nos menus do produto.

Integração de Operações de segurança - Fluxo de trabalho de pesquisa de ameaças

O fluxo de trabalho da capacidade **Integração de Operações de segurança - Pesquisa de ameaças** acessa as implementações de pesquisa de ameaças disponíveis e executa os fluxos de trabalho de implementação associados a cada uma para realizar pesquisas de ameaças de observáveis selecionados.

Antes de Iniciar

Função necessária: sn_ti.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho pode ser acionado dessas maneiras.

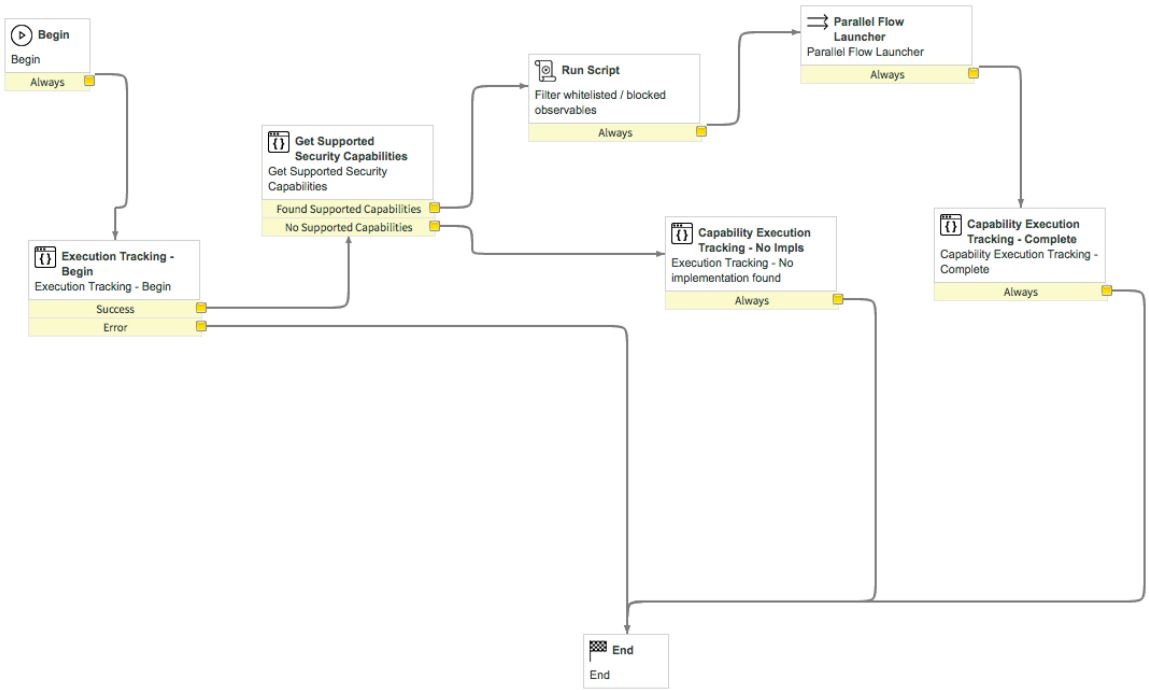
Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- selecionando um ou mais observáveis na lista Observáveis e selecionando **Executar pesquisa de ameaças** na lista de seleção **Ações nas linhas selecionadas**.
- abrindo um registro de observável e clicando no link relacionado **Executar pesquisa de ameaças**.
- Na lista relacionada de observáveis em um incidente de segurança.

Cada método permite que você especifique quais implementações de pesquisa serão usadas para verificar os observáveis selecionados. Os fluxos de trabalho de implementação associados são executados para realizar as pesquisas.

Pesquisa de ameaças



As atividades específicas deste fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração.

As atividades do processo de fluxo de trabalho incluem:

- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações

Alterar a ordem de execução do fluxo de trabalho

As implementações da capacidade de integração especificam o fluxo de trabalho a ser executado. No sistema de base, os fluxos de trabalho são executados sequencialmente, na ordem especificada na implementação. Você pode mudar a ordem conforme necessário.

Antes de Iniciar

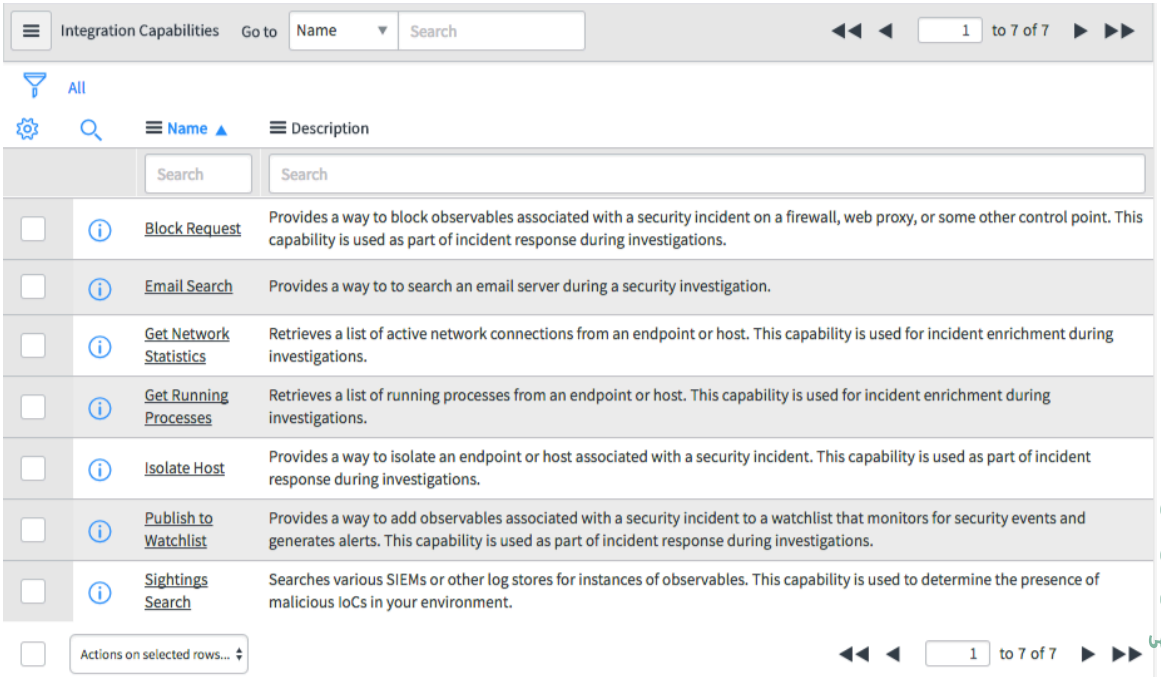
Função necessária: sn_sec_cmn.write

Tradução automática

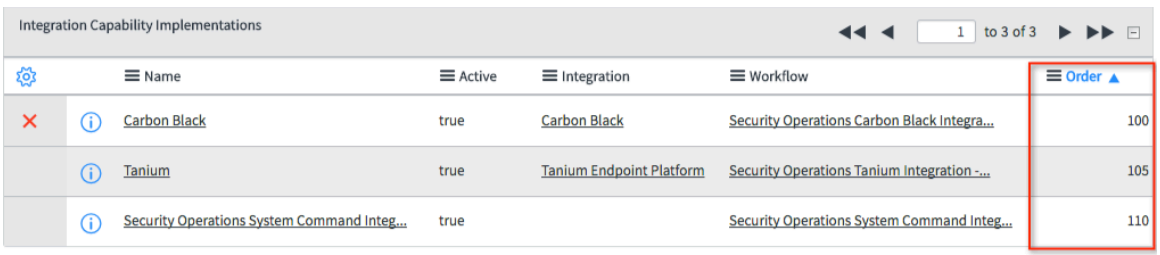
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

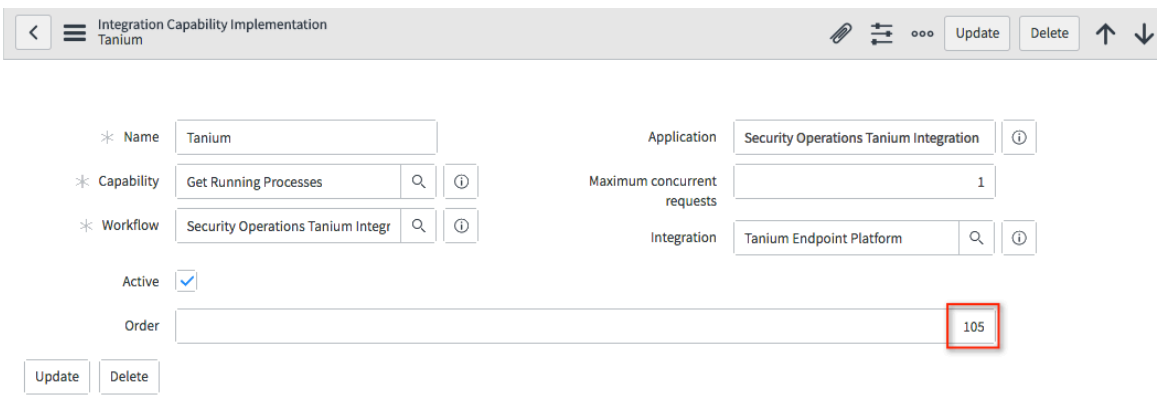
1. Navegar até **Todos** > **Operações de segurança** > **Integrações** > **Capacidades de integração**.



2. Selecione a capacidade de integração para a qual você deseja mudar a ordem de execução.



3. Selecione a implementação que você deseja modificar.



4. Altere a **Ordem** para um número maior ou menor.
   Números menores têm uma prioridade de execução mais alta.
5. Clique em **Enviar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxos de trabalho de integração de Operações de segurança comuns e atividades de orquestração

Muitos dos fluxos de trabalho associados a integrações de terceiros incluem as mesmas atividades. Por exemplo, atividades para iniciar e concluir o processamento.

Acompanhamento de execução - Iniciar atividade

A atividade de fluxo de trabalho Acompanhamento de execução - Iniciar inicia o processo de auditoria para um fluxo de trabalho de integração Operações de segurança que opera em observáveis.

A atividade Acompanhamento de execução - Iniciar pode ser usada com qualquer fluxo de trabalho para começar a registrar o andamento do fluxo de trabalho em uma auditoria.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria foi criado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
isImpl	Sinalizador que especifica se a auditoria é feita para um fluxo de trabalho de capacidade de integração ou um fluxo de trabalho de implementação de capacidade de integração. Os valores possíveis são: • falso - indica auditoria em um fluxo de trabalho abstrato da capacidade de integração, como Pesquisa de detecções. (padrão.) • verdadeiro - denota auditoria em um fluxo de trabalho de implementação da capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
observávelLista	Um ou mais SysIDs observáveis para executar a ação desejada. Usado como uma entrada de fluxo de trabalho.
workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch e VirusTotal.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capabilityExecutionId	Identificador do sistema do registro de auditoria.

- Atividade Obter capacidades de segurança compatíveis
- Acompanhamento de execução de capacidade - atividade sem implementações

Acompanhamento da execução da capacidade - Concluir atividade

A atividade de fluxo de trabalho Acompanhamento da execução da capacidade - Concluir atualiza o registro de auditoria quando o fluxo de trabalho é concluído.

A atividade Acompanhamento da execução da capacidade - Concluir pode ser usada com qualquer fluxo de trabalho para registrar a conclusão do fluxo de trabalho.

Nota: A matriz **Valor de retorno** da atividade principal do **inicializador paralelo** contém uma matriz de resultados de todos os fluxos de trabalho de integração executados e solicita a conclusão bem-sucedida do acompanhamento de execução.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é atualizado para **Concluído**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityExecutionId	Identificador do sistema para o registro de auditoria. Este campo foi a saída de qualquer uma das atividades de auditoria Iniciar.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
mensagem	Mensagem de conclusão.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Não há variáveis de saída.

Acompanhamento da execução da capacidade - Atividade com falha

A atividade de fluxo de trabalho Acompanhamento da execução da capacidade - Falha registra uma falha no registro de auditoria.

A atividade Acompanhamento da execução da capacidade - Falha pode ser usada com qualquer fluxo de trabalho para registrar uma condição de falha.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria está definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityExecutionId	Identificador do sistema para o registro de auditoria. Esta é a saída de qualquer uma das atividades de auditoria Iniciar.
errorMessage	Mensagem indicando o motivo da falha.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Atividade Capacidade - Determinar ICs

A atividade de fluxo de trabalho Capacidade - Determinar ICs determina quais itens de configuração (ICs) serão incluídos no fluxo de trabalho.

A atividade Capacidade - Determinar ICs pode ser usada com qualquer fluxo de trabalho para determinar quais ICs serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Itens de configuração encontrados.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Nenhum IC encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).
cis_afetados	Itens de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
cis_afetados	ICs filtrados
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).

Atividade Criar registros de dados de aprimoramento

A atividade de fluxo de trabalho **Criar registros de dados de** aprimoramento cria ou atualiza registros de aprimoramento para usar no fluxo de trabalho.

A atividade **Criar registros de dados de aprimoramento** pode ser usada com qualquer fluxo de trabalho para atualizar registros de aprimoramento no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Registro de aprimoramento atualizado.
Falha	Registro de aprimoramento não atualizado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_id	Identificador da tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
conteúdo	Conteúdo bruto (dados de processos em execução).
richment_mapping_id	Identificador de mapeamento de aprimoramento.
ci_id	Identificador do item de configuração.
valor_referência	Não usado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	GlideRecords criados usando o script richmentUtils.

Atividade Obter FQDN do item de configuração

O **Orquestração comum de segurança** > **Obter FQDN do item de configuração** A atividade de fluxo de trabalho recupera o nome de domínio totalmente qualificado (FQDN) de um item de configuração. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter FQDN do item de configuração pode ser usada com qualquer fluxo de trabalho para recuperar o nome de domínio totalmente qualificado (FQDN) de um item de configuração.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
cmdb_ci.id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
fqdn [cadeia de caracteres]	O nome do domínio totalmente qualificado (FQDN) do item de configuração.

Anotações adicionais

O campo fqdn no item de configuração deve ser preenchido.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Determinar observáveis

A atividade de fluxo de trabalho **Determinar observáveis** determina qual observável incluir no fluxo de trabalho

A atividade **Determinar observáveis** pode ser usada com qualquer fluxo de trabalho para determinar quais observáveis serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis encontrados
Falha	Nenhum observável encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para observáveis).
observáveis	Endereços IP, hash, URLs, nomes de domínio.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis	Observáveis filtrados

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à capacidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais capacidades são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte à capacidade encontrada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte à capacidade. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Capacidadescompatíveis	Lista de integrações que oferecem suporte à capacidade.
capacidadeContagem	Número de integrações que oferecem suporte à capacidade.

Acompanhamento de execução de capacidade - atividade sem implementações

A atividade de fluxo de trabalho Acompanhamento da execução da capacidade - Sem implementações cria um registro de erro quando nenhuma implementação da capacidade de integração é encontrada.

A atividade Acompanhamento de execução de capacidade - Sem implementações pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução está definido como **Erro** e uma mensagem indicando o erro é registrada.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento da execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Criar atividade de pesquisa de conformidade

A atividade Criar pesquisa de conformidade cria uma pesquisa de conformidade para e-mails nos servidores designados do Exchange usando as consultas de pesquisa definidas e retorna o nome da pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
search_query	Consulta de pesquisa obrigatória usada para localizar e-mails no Exchange Server em todas as caixas de correio.
Local de troca	Campo de local obrigatório usado para pesquisar em locais definidos. Os valores são: • Todos • Nome da caixa de correio específica
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Nome da pesquisa de conformidade criada.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de Saída

Variável	Descrição
Falha na criação da pesquisa	Quando a criação da pesquisa falha devido a uma exceção no servidor do Exchange.
Pesquisa criada com sucesso	Quando a criação da pesquisa é bem-sucedida.
Falha na criação da pesquisa devido a um erro de análise	Quando a criação da pesquisa falha devido a um problema de análise.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Obter IP da atividade de IC

Esta atividade de fluxo de trabalho determina o endereço IPV4 associado a um item de configuração (IC).

A atividade **Obter IP do IC** pode ser usada com qualquer fluxo de trabalho para recuperar o endereço IPv4 de um IC.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
ci_sys_id [cadeia de caracteres]	Identificador do sistema do item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr [cadeia de caracteres]	Endereço IPv4. Se o endereço IP não puder ser determinado, este valor estará vazio.

Condições de Saída

Os resultados possíveis para esta atividade são:

Condições

Condição	Descrição
Êxito	Um endereço IPv4 foi retornado.
Falha	Não foi possível determinar um endereço IPv4.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter estatísticas de rede por meio da atividade netstat

A atividade de fluxo de trabalho Orquestração comum de segurança - Obter estatísticas de rede via netstat recupera as estatísticas de rede de um recurso afetado em um sistema baseado no Windows. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter estatísticas de rede via netstat pode ser usada com qualquer fluxo de trabalho para recuperar estatísticas de rede de um sistema baseado no Windows. A máquina é consultada com o comando **netstat**, incluindo os parâmetros **-a** e **-o**. Para aprimorar os dados de saída, o comando **get-process** também é invocado.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	As estatísticas de rede foram recuperadas no formato JSON.
Falha	Ocorreu um erro ao tentar recuperar estatísticas de rede. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome do domínio totalmente qualificado (FQDN) ou endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução na máquina de destino. Os dados JSON incluem: PID Identificador de processo _porta local Porta local para a transação de rede estado Status da conexão TCP. **Nota:** Este campo é nulo para conexões UDP. endereço_local

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
	Nome de domínio totalmente qualificado (FQDN) local ou endereço IP remote_address Nome de domínio totalmente qualificado (FQDN) ou endereço IP remoto protocolo TCP ou UDP remote_port Porta remota da transação de rede caminho O caminho do arquivo do executável do processo hash O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Restrições

O MID Server deve oferecer suporte ao PowerShell.

O hash SHA-256 requer o PowerShell V4.

Obter processos em execução por meio da atividade WMI

A atividade de fluxo de trabalho**Obter processos em execução** recupera os processos em execução de um item de configuração em um sistema baseado no Windows. Esta atividade pode acelerar o processo de investigação e correção.

A atividade **Obter processos em execução via WMI** pode ser usada com qualquer fluxo de trabalho para recuperar processos em execução em um sistema baseado no Windows.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome do domínio totalmente qualificado (FQDN) ou endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução no sistema de destino. Os dados JSON incluem: PID O identificador do processo nome O nome do processo Além disso, se disponível: Responsável O nome do responsável pelo processo proprietário_sid O identificador do sistema do proprietário do processo proprietário_domínio O domínio do proprietário do processo caminho O caminho do arquivo do executável do processo hash O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Restrições

O MID Server deve oferecer suporte ao **PowerShell**.

O hash SHA-256 requer o PowerShell V4.

Atividade Verificar status de pesquisa de conformidade

A atividade Verificar status de pesquisa de conformidade verifica o status da pesquisa de conformidade criada no servidor do Exchange e, se o status for concluído, retorna as informações sobre a pesquisa de e-mail encontrada para a pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório em que o Exchange Server está localizado.
pesquisarNome	Nome obrigatório da pesquisa de conformidade criada no servidor do Exchange.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da pesquisa de conformidade e o número de e-mails encontrados no servidor do Exchange para a pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Pesquisa em andamento	Quando o status da pesquisa de conformidade está em andamento.
Pesquisa concluída - Nenhum e-mail de ameaça encontrado	Quando o status da pesquisa de conformidade é concluído, nenhum e-mail é encontrado como parte da pesquisa de conformidade.
Pesquisa concluída - E-mails de ameaças encontrados	Quando o status da pesquisa de conformidade é concluído, os e-mails são encontrados como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no servidor do Exchange.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Atividade Atualizar anotações de trabalho da tarefa

A atividade de fluxo de trabalho **Orquestração comum de segurança - Atualizar anotações de trabalho da tarefa** atualiza a seção **Atividade** (anotações de trabalho) de um registro de tarefa. Isso é útil para registrar informações.

A atividade **Atualizar** anotações de trabalho da tarefa pode ser usada com qualquer fluxo de trabalho para atualizar as anotações de trabalho de qualquer registro de tarefa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
task_id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa.
conteúdo [string]	Os dados gravados nas anotações de trabalho de uma tarefa.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Acumular informações de pesquisa na atividade de incidente de segurança

A atividade **Acumular informações de pesquisa para incidente de segurança** pode ser usada com qualquer fluxo de trabalho para coletar informações de uma pesquisa de ameaças e gerar um resumo do conteúdo, bem como o ID do incidente de segurança de origem nas anotações de trabalho da tarefa.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Resumo do relatório de pesquisa acumulado até o incidente de segurança.
Falha	A tarefa de origem e o relatório resumido de pesquisa estão vazios.

Variáveis de entrada

Variável	Descrição
scanID[cadeia de caracteres]	Identificador de pesquisa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
sild[cadeia de caracteres]	Identificador de incidente de segurança.
resposta [cadeia de caracteres]	Resumo dos resultados da pesquisa, incluindo: valor de IoC, resultado, motivo da falha, referência de pesquisa e assim por diante.

Atualizar incidente de segurança com fluxo de trabalho de resultados de pesquisa

O fluxo de trabalho Atualizar **incidente de segurança com resultados de pesquisa** atualiza os incidentes de segurança existentes com resultados de pesquisa.

Antes de Iniciar

Função necessária: sn_si.basic

Tradução automática

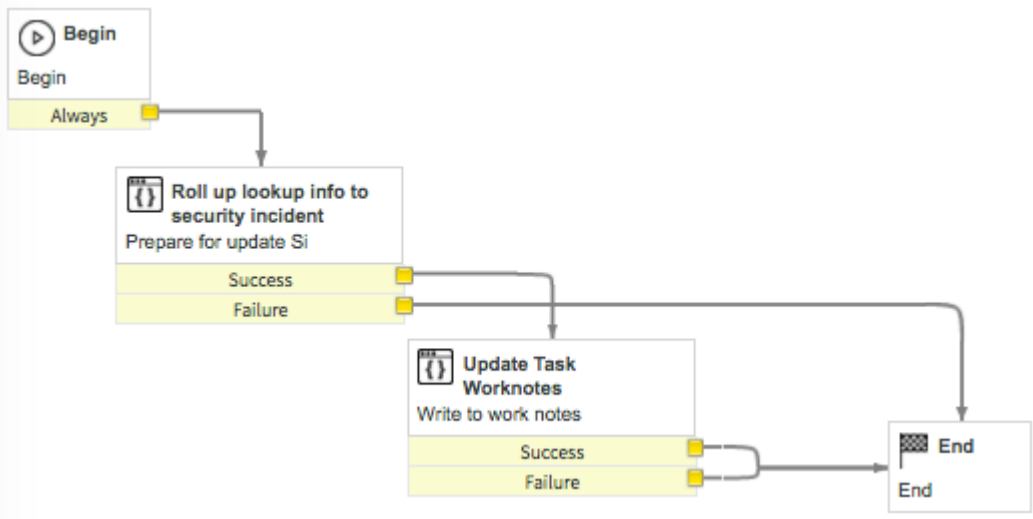
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado por uma regra de negócio na tabela de pesquisa que monitora quando o campo **Resultado** muda para Falha.

As atividades do processo de fluxo de trabalho incluem:

Acumular informações de pesquisa na atividade de incidente de segurança

Atividade Atualizar anotações de trabalho da tarefa



Atividade Filtrar observáveis na lista de permissões

A atividade de fluxo de trabalho Observáveis da lista de permissões filtrados remove observáveis que podem ser ignorados da lista de observáveis. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Filtrar observáveis na lista de permissões pode ser usada com qualquer fluxo de trabalho para filtrar observáveis antes de executar qualquer ação.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Lista de filtros criada.
Falha	Ocorreu um erro ao tentar filtrar os observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis disponíveis.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
filtradosObserváveis	Observáveis filtrados.

Escrever conteúdo para registrar como atividade de anexo

Esta atividade grava o conteúdo passado de uma entrada e cria um anexo designado em um determinado registro.

A atividade **Gravar conteúdo para registrar como anexo** pode ser usada com qualquer fluxo de trabalho para gravar conteúdo e anexá-lo a um registro.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
nome da tabela [cadeia de caracteres]	O nome da tabela para o registro. Este campo de entrada é obrigatório.
sysid [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa. Este campo de entrada é obrigatório.
carga	O conteúdo de texto simples a ser gravado como um anexo. Este campo de entrada é obrigatório.
nome do arquivo	O nome do arquivo de anexo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Obter IP da atividade de IC

A atividade de fluxo de trabalho Obter IP do IC coleta o endereço IP dos itens de configuração (ICs) a serem usados no fluxo de trabalho.

A atividade Obter IP do IC pode ser usada com qualquer fluxo de trabalho para coletar endereços IP de item de configuração (IC) a serem usados no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Endereços IP encontrados.
Falha	Nenhum endereço IP encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ci_sys_id	Identificador do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr	Endereços IP.

Operações de segurança gatilhos de fluxo de trabalho

Operações de segurança Os gatilhos de fluxo de trabalho contêm uma condição em uma tabela. Todos os fluxos de trabalho anexados ao registro do gatilho de fluxo de trabalho são executados quando a condição é atendida.

Criar Operações de segurança gatilhos de fluxo de trabalho

Crie um gatilho de fluxo de trabalho que contenha uma condição em uma tabela.

Antes de Iniciar

Operações de segurança contém vários gatilhos de fluxo de trabalho no sistema de base:

- Mudanças de item de configuração em um incidente de segurança ativo

  Usa a integração para aprimorar os dados relacionados ao IC conforme os itens de configuração mudam.

- Verificar novamente o grupo vulnerável

  Verifica novamente um grupo vulnerável, usando Verificar fluxo de trabalho de vulnerabilidade, quando você **Fecha/Ignora** o grupo.

- Verificar novamente o item vulnerável

  Verifica novamente um item vulnerável, usando o Verificar fluxo de trabalho de item de vulnerabilidade quando você **Fecha/Ignora** o item.

Funções necessárias:

- Para ler: sn_sec_cmn.read
- Para criar ou atualizar: sn_sec_cmn.write
- Para excluir: sn_sec_cmn.admin

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Operações de segurança** > **Utilitários** > **Gatilhos de Fluxo de Trabalho**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme o apropriado.

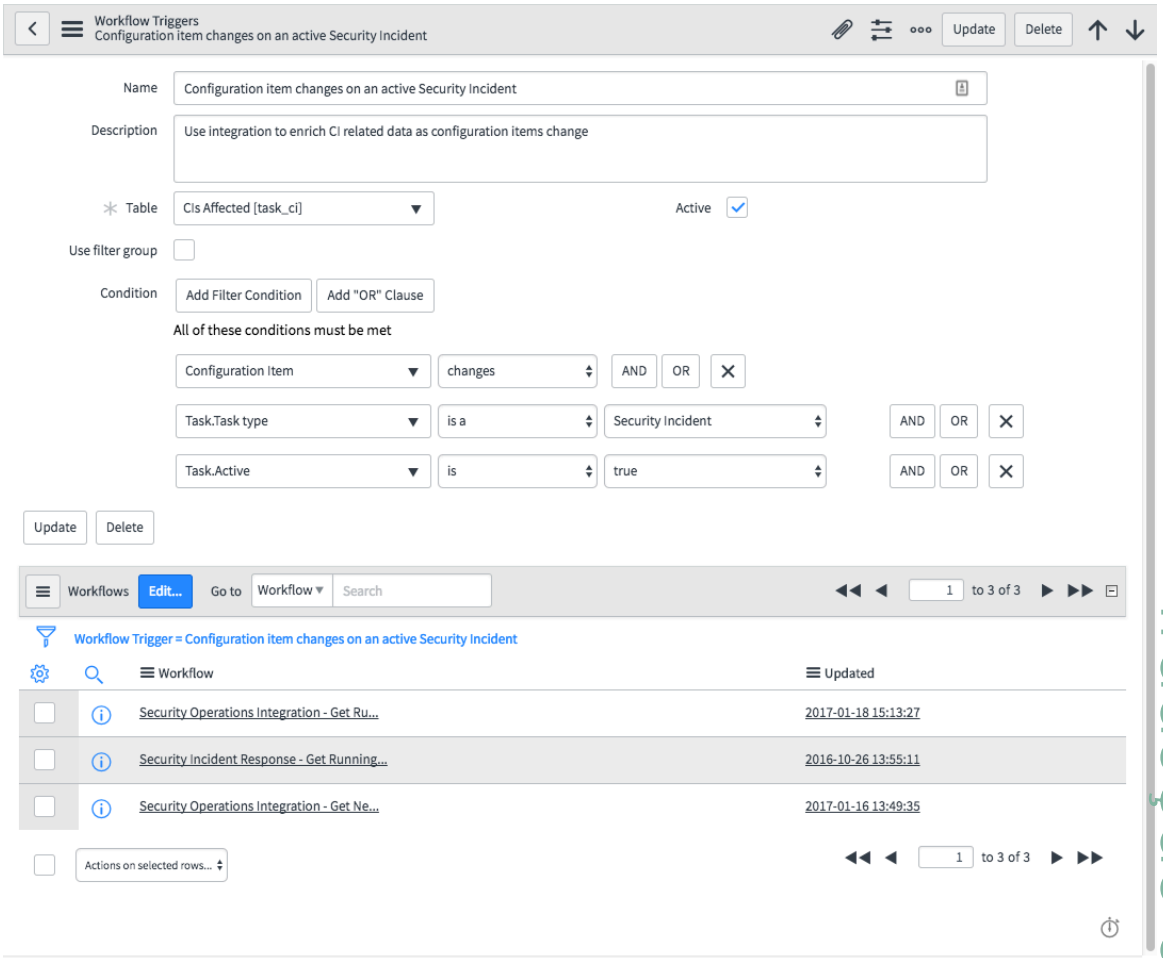
Gatilhos de Fluxo de Trabalho

Campo	Descrição
Nome	O nome do gatilho de fluxo de trabalho.
Descrição	Insira uma descrição para o gatilho de fluxo de trabalho.
Tabela	A tabela que contém o gatilho de fluxo de trabalho. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, este campo será padronizado para a tabela associada ao grupo de filtros selecionado.
Condição	Use o Construtor de condições para definir os critérios do gatilho de fluxo de trabalho. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, os campos **Condição** não serão exibidos.
Ativo	Marque esta caixa de seleção para ativar o gatilho de fluxo de trabalho.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou criar um novo grupo de filtros para definir os critérios de gatilho de fluxo de trabalho.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir gatilhos de fluxo de trabalho. Este campo aparecerá somente se a caixa de seleção **Usar grupos de filtros** estiver marcada.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar**.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia **Fluxos** de trabalho é exibida. Ele contém fluxos de trabalho que são executados quando todas as condições de filtro ou condições de grupo de filtros são atendidas.

5. Para adicionar fluxos de trabalho, execute estas etapas.
   a. Na guia **Fluxos** de trabalho, clique em **Editar**.
   b. Use o construtor de condições, se necessário, para localizar os fluxos de trabalho que deseja selecionar ou use o slushbucket para selecionar fluxos de trabalho e movê-los para a Lista de fluxos de trabalho.
   c. Clique em **Salvar**.
   Os fluxos de trabalho selecionados são adicionados.
6. Clique em **Atualizar**.

Orquestração do Security Operations

Os usuários podem interagir e recuperar dados de sistemas e ambientes baseados no Windows ou UNIX usando pacotes de atividades e fluxos de trabalho em Orquestração de Operações de segurança.

Orquestração de Operações de segurança economiza tempo eliminando processos manuais e obtendo informações contextuais para corrigir incidentes. Os produtos Operações de segurança têm pacotes de atividades e fluxos de trabalho padrão que estão incluídos e ativados em cada um dos plug-ins.

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para criar e acessar atividades de orquestração adicionais que não estão disponíveis com a oferta padrão de produtos Operações de segurança, adquira uma licença de orquestração completa.

- Orquestração do Security Incident Response fluxos de trabalho:
  - Fluxo de trabalho do Security Incident Response - Obter estatísticas de rede
  - Integração de comandos do sistema de operações de segurança - Obter fluxo de trabalho de processos em execução
  - Criar solicitação de pesquisa para fluxo de trabalho de mudanças de IoC
  - Integração de Operações de segurança - Fluxo de trabalho de pesquisa e exclusão de e-mail
- Orquestração de inteligência contra ameaças fluxos de trabalho:
  - Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC
  - Atualizar incidente de segurança com fluxo de trabalho de resultados de pesquisa
- Orquestração de resposta a vulnerabilidades fluxos de trabalho:
  - Verificar fluxo de trabalho de vulnerabilidade
  - Verificar fluxo de trabalho de item de vulnerabilidade

Tradução automática

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.